Torsion of elliptic curves over $\mathbb{Q}_p$ with good reduction in cyclotomic extensions

Yoshiyasu Ozeki*and Manabu Yoshida†

October 15, 2025

Abstract

In this paper, for every prime p and every $0 \leq n \leq \infty$, we classify the structure of the torsion subgroup of the group of $\mathbb{Q}_p(\mu_{p^n})$-rational points of elliptic curves over $\mathbb{Q}_p$ with good reduction, where μ_{p^n} is the set of the p^n-th roots of unity.

Contents

*Faculty of Science, Kanagawa University, 3-27-1 Rokkakubashi, Kanagawa-ku, Yokohama-shi, Kanagawa 221-8686, JAPAN
e-mail: ozeki@kanagawa-u.ac.jp
†Faculty of Science and Engineering, Yamato university, 2-5-1 Katayama-cyo, Suita-shi, Osaka 564-0082, JAPAN
email: yoshida.manabu@yamato-u.ac.jp
Keywords: elliptic curves, p-adic fields, cyclotomic extensions
AMS 2020 Mathematics subject classification: 11G07 (primary), 14G20 (secondary)

1 Introduction

It is well-known as the Mordell-Weil theorem that the group of K-rational points $E(K)$ on an elliptic curve E over a number field K is finitely generated. In particular, the torsion subgroup $E(K)_{\mathrm{tor}}$ of $E(K)$ is finite. In 1996, Merel [Mer96] proved that there exists an upper bound on the size of $E(K)_{\mathrm{tor}}$ which depends only on the degree of K. Thus, for a fixed integer $d > 0$, there exist only finitely many possibilities (up to isomorphism) for the groups $E(K)_{\mathrm{tor}}$ where K ranges over a number field of degree d and E ranges elliptic curves over K. To give a classification of such groups for given d is one of the crucial problems for arithmetic theory of elliptic curves. A landmark theorem concerning this problem is a theorem of Mazur [Maz78], which studies the case $d = 1$ (i.e. $K = \mathbb{Q}$); he showed that if E is an elliptic curve over $\mathbb{Q}$, then its torsion subgroup $E(\mathbb{Q})_{\mathrm{tor}}$ is isomorphic to one of the following 15 groups

$$\mathbb{Z}/n\mathbb{Z} \quad (n = 1, 2, \ldots, 10, 12),$$
$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z} \quad (m = 1, 2, 3, 4).$$

After Mazur's paper, Kammieny [Kam92] and Kenku and Momose [KM88] gave an answer of the classification problem for $d = 2$, and the classification for $d = 3$ was given by Derickx, Etropolski, Morrow, van Hoeij, and Zureick-Brown [DEvH+21].

This paper begins by establishing a p-adic analogue of Mazur's theorem in the case of good reduction. Let us introduce some notation needed for our results. We denote by I the set of pairs (k, m) of positive integers such that $m \mid p - 1$ and $(\sqrt{p} - 1)^2 < km^2 < (\sqrt{p} + 1)^2$. We also denote by I_{ord} the subset of I consisting of elements (k, m) such that $km^2 \not\equiv 1 \bmod p$. Our first main result in this paper is as follows.

Theorem 1.1. *Let E be an elliptic curve over $\mathbb{Q}_p$ with good reduction.*

(1) *Assume $p \geq 3$. Then, $E(\mathbb{Q}_p)_{\mathrm{tor}}$ is isomorphic to one of the following groups.*

$$\begin{cases} \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/mk\mathbb{Z}, & (m, k) \in I, \\ 0. \end{cases}$$

Each of these groups appears as $E(\mathbb{Q}_p)_{\mathrm{tor}}$ for some elliptic curve E over $\mathbb{Q}_p$ with good reduction.

Moreover, if E has good ordinary reduction (resp. good supersigular reduciton), then $E(\mathbb{Q}_p)_{\mathrm{tor}}$ is isomorphic to one of the following groups in (I) (resp. (II)).

$$(I) \begin{cases} \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/mk\mathbb{Z}, & (m, k) \in I_{\mathrm{ord}}, \\ 0. \end{cases}$$

$$(II) \begin{cases} 0, \mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/7\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, & \text{if } p = 3, \\ \mathbb{Z}/(1+p)\mathbb{Z}, & \text{if } p \equiv 1 \bmod 4 \\ \mathbb{Z}/(1+p)\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/\frac{1+p}{2}\mathbb{Z} & \text{if } p \neq 3,\ p \equiv 3 \bmod 4. \end{cases}$$

Each of these groups in (I) (resp. (II)) appears as $E(\mathbb{Q}_p)_{\mathrm{tor}}$ for some elliptic curve E over $\mathbb{Q}_p$ with good ordinary reduction (resp. good supersingular reduction).

(2) *Assume $p = 2$. Then, $E(\mathbb{Q}_2)_{\mathrm{tor}}$ is isomorphic to one of the following groups.*

$$\begin{cases} \mathbb{Z}/m\mathbb{Z}, & m = 1, 2, 3, 4, 5, 8, \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2k\mathbb{Z}, & k = 1, 2. \end{cases}$$

Each of these groups appears as $E(\mathbb{Q}_2)_{\mathrm{tor}}$ for some elliptic curve E over $\mathbb{Q}_2$ with good reduction.

Moreover, if E has good ordinary reduction (resp. good supersigular reduciton), then $E(\mathbb{Q}_2)_{\mathrm{tor}}$ is isomorphic to one of the following groups in $(I)'$ (resp. $(II)'$).

$$(I)' \quad \begin{cases} \mathbb{Z}/m\mathbb{Z}, & m = 2, 4, 8 \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2k\mathbb{Z}, & k = 1, 2 \end{cases}$$
$$(II)' \quad 0, \mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/5\mathbb{Z}.$$

Each of these groups in $(I)'$ (resp. $(II)'$) appears as $E(\mathbb{Q}_2)_{\mathrm{tor}}$ for some elliptic curve E over $\mathbb{Q}_2$ with good ordinary reduction (resp. good supersingular reduction).

Before stating our second result, it should be better to mention some known results on the group structures of elliptic curves over (infinite degree) abelian extensions of $\mathbb{Q}$. Chou [Cho19] determined the possible torsion subgroups of $E(\mathbb{Q}^{\mathrm{ab}})$ for an elliptic curve E over $\mathbb{Q}$ and established the sharp bound $\#E(\mathbb{Q}^{\mathrm{ab}}) \leq 163$. Building on Chou's results, Gužvić and Vukorepa [GV23] classified all possible torsion subgroups of $E(\mathbb{Q}(\mu_{p^\infty}))$ in the case $p = 2, 3, 5, 7$ and 11. where μ_{p^n} is the group of p^n-th roots of unity. We consider a p-adic analogue of these results. Let E be an elliptic curve over $\mathbb{Q}_p$ with good reduction. As an analogue of Chou ' s result, it is natural to study the group structure of $E(\mathbb{Q}_p^{\mathrm{ab}})_{\mathrm{tor}}$, where $\mathbb{Q}_p^{\mathrm{ab}}$ denotes the maximal abelian extensions of $\mathbb{Q}_p$. However, we immediately see that this group is always infinite (indeed, the reduction map induces an isomorphism between the prime-to-p parts of $E(\mathbb{Q}_p^{\mathrm{ab}})_{\mathrm{tor}}$ and that of $\bar{E}(\overline{\mathbb{F}}_p)$, where $\bar{E}$ denotes the reduction of E and $\overline{\mathbb{F}}_p$ is the separable closure of $\mathbb{F}_p$. So we study the torsion subgroup of $E(\mathbb{Q}_p(\mu_{p^\infty}))$, which may be regarded as a p-adic analogue of the work of Gužvić and Vukorepa. The second main theorem below forms the central part of this paper.

Theorem 1.2. *Let E be an elliptic curve over $\mathbb{Q}_p$.*

(1) *If E has good supersingular reduction, then it holds $E(\mathbb{Q}_p(\mu_{p^\infty}))_{\mathrm{tor}} = E(\mathbb{Q}_p)_{\mathrm{tor}}$. (Thus the possible group structures of this group are given in Theorem 1.1.)*

(2) *Assume $p \geq 3$ and assume also that E has good ordinary reduction. Then,*

- *it holds $E(\mathbb{Q}_p(\mu_{p^\infty}))_{\mathrm{tor}} = E(\mathbb{Q}_p(\mu_p))_{\mathrm{tor}}$.*
- *Moreover, $E(\mathbb{Q}_p(\mu_{p^\infty}))_{\mathrm{tor}}$ is isomorphic to one of the following groups in $(I)_\infty$.*

$$(I)_\infty \quad \begin{cases} \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/mk\mathbb{Z}, & (m, k) \in I_{\mathrm{ord}}, \\ \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}, & \\ \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/2p\mathbb{Z} & \text{if } p \leq 5. \end{cases}$$

Each of these groups in $(I)_\infty$ appears as $E(\mathbb{Q}_p(\mu_{p^\infty}))_{\mathrm{tor}}$ for some elliptic curve E over $\mathbb{Q}_p$ with good ordinary reduction.

(3) *Assume $p = 2$ and assume also that E has good ordinary reduction. Then,*

- *it holds $E(\mathbb{Q}_2(\mu_{2^\infty}))_{\mathrm{tor}} = E(\mathbb{Q}_2(\mu_8))_{\mathrm{tor}}$.*

– *Moreover,* $E(\mathbb{Q}_2(\mu_{2^\infty}))_{\mathrm{tor}}$ *is isomorphic to one of the following groups in* $(I)'_\infty$.

$$(I)'_\infty \begin{cases} \mathbb{Z}/m\mathbb{Z}, & m = 4, 8 \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2k\mathbb{Z}, & k = 1, 4 \\ \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}. \end{cases}$$

Each of these groups in $(I)'_\infty$ *appears as* $E(\mathbb{Q}_2(\mu_{2^\infty}))_{\mathrm{tor}}$ *for some elliptic curve* E *over* $\mathbb{Q}_2$ *with good ordinary reduction.*

As a consequence, we obtain explicit upper bounds for $E(\mathbb{Q}_p)_{\mathrm{tor}}$ and $E(\mathbb{Q}_p(\mu_{p^\infty}))_{\mathrm{tor}}$ when E is an elliptic curve over $\mathbb{Q}_p$ with good ordinary reduction (resp. good supersingular reduction) as stated in (I) (resp. (II)) below. All these bounds are sharp:

$$(I)\ \#E(\mathbb{Q}_p)_{\mathrm{tor}} \leq (\sqrt{p}+1)^2, \#E(\mathbb{Q}_p(\mu_{p^\infty}))_{\mathrm{tor}} \leq \begin{cases} p^2 & (p \geq 7), \\ 2p^2 & (p = 3, 5), \\ 16 & (p = 2). \end{cases}$$

$$(II)\ \#E(\mathbb{Q}_p)_{\mathrm{tor}} = \#E(\mathbb{Q}_p(\mu_{p^\infty}))_{\mathrm{tor}} \leq \begin{cases} 1+p & (p \geq 5), \\ 7 & (p = 3), \\ 5 & (p = 2). \end{cases}$$

Note that Theorem 1.1 and Theorem 1.2 above give the classifications of the possible group structures of $E(\mathbb{Q}_p(\mu_{p^n}))_{\mathrm{tor}}$ for all primes p and $0 \leq n \leq \infty$ except the case where $(p, n) = (2, 2)$ and E has good ordinary reduction. The classification result on the exceptional case is as follows.

Theorem 1.3. *Let* E *be an elliptic curve over* $\mathbb{Q}_2$ *with good ordinary reduction. Then,* $E(\mathbb{Q}_2(\mu_4))_{\mathrm{tor}}$ *is isomorphic to one of the following groups in* $(I)'_2$.

$$(I)'_2 \begin{cases} \mathbb{Z}/4\mathbb{Z}, \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2k\mathbb{Z}, & k = 1, 2, 4 \\ \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}. \end{cases}$$

Each of these groups in $(I)'_2$ *appears as* $E(\mathbb{Q}_2(\mu_4))_{\mathrm{tor}}$ *for some elliptic curve* E *over* $\mathbb{Q}_2$ *with good ordinary reduction.*

Therefore, we conclude that, for all primes p and $0 \leq n \leq \infty$, we obtained the complete classifications of the groups those arise as $E(\mathbb{Q}_p(\mu_{p^n}))_{\mathrm{tor}}$ for some elliptic curve E over $\mathbb{Q}_p$ with good reduction.

Corollary 1.4. *Assume* $p \geq 3$. *Let* K_∞ *be the cyclotomic* $\mathbb{Z}_p$*-extension of* $\mathbb{Q}_p$. *Then, we have* $E(K_\infty)_{\mathrm{tor}} = E(\mathbb{Q}_p)_{\mathrm{tor}}$ *for an elliptic curve* E *over* $\mathbb{Q}_p$ *with good reduction.*

Proof. If E has good supersingular reduction, the result is clear by Theorem 1.2 (1). In the case where E has good ordinary reduction, the result follows from Theorem 1.2 (2); $E(K_\infty)_{\mathrm{tor}} = E(K_\infty)_{\mathrm{tor}} \cap E(\mathbb{Q}_p(\mu_{p^\infty}))_{\mathrm{tor}} = E(K_\infty)_{\mathrm{tor}} \cap E(\mathbb{Q}_p(\mu_p))_{\mathrm{tor}} = E(\mathbb{Q}_p)_{\mathrm{tor}}$. □

The organization of the paper is as follows. In Section 2, we give a proof of Theorem 1.1. The arguments differs significantly depending on whether p is odd or $p = 2$. When p is odd, we use theoretical arguments involving the theory of canonical lifts. In case $p = 2$, by using MAGMA [BC06] and Algorithm A.1, we explicitly find elliptic curves

listed in the Cremona database with prescribed torsion subgroups. Section 3 is the main part of this paper. In this seciton, we give proofs of Theorem 1.2 and Theorem 1.3. As in Section 2, the arguments also differ depending on whether p is odd or $p = 2$. For the case where p is odd, the key is Proposition 3.3, which gives a classification of p-parts of the torsion subgroup of $E(\mathbb{Q}_p(\mu_{p^\infty}))$. For the case where $p = 2$, theoretical perspectives such as ramification theory play an even more important role in addition to verification using the Cremona database and computations by MAGMA. In Appendix A, we provide data on certain extensions of $\mathbb{Q}_2$ and some elliptic curves that are required for our proof. The labels of elliptic curves in this paper follow the convention used in the Cremona database. The data available in the LMFDB [LMF25] is also useful for referencing elliptic curves; however, note that the labeling in the LMFDB differs from that of the Cremona label.

Notation : In this paper, p-adic fields are finite extension fields of $\mathbb{Q}_p$. If F is an algebraic extension of $\mathbb{Q}_p$, we denote by G_F the absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}_p/F)$ of F. We also denote by μ_{p^n} the set of p^n-th roots of unity in $\overline{\mathbb{Q}}_p$ and $\mu_{p^\infty} := \cup_{m\geq 0}\mu_{p^m}$.

2 Group structures of $E(\mathbb{Q}_p)_{\mathrm{tor}}$

The aim of this section is to prove Theorem 1.1, which gives the complete list of the groups those arise as the torsion subgroups of the Mordell-Weil groups of elliptic curves over $\mathbb{Q}_p$ with good reduction. Theorem 1.1 is a combination of Theorem 2.2 and Theorem 2.3 below.

In the rest of this paper, we use the following notations.

- For an elliptic curve E over $\mathbb{Q}_p$ with good reduction, we denote by $\hat{E}$ and $\bar{E}$ the formal group over $\mathbb{Z}_p$ associated with E and the reduction of E, respectively. We denote by $T_p(E) := \varprojlim_n E[p^n]$ the p-adic Tate module of E and put $V_p(E) = T_p(E) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. Similarly, we often use notations $T_p(\hat{E}), V_p(\hat{E}), T_p(\bar{E})$ and $V_p(\bar{E})$.
- For a field K, we denote by $\mathcal{E}(K)$ the set of the isomorphism classes of groups which are isomorphic to the torsion subgroup $E(K)_{\mathrm{tor}}$ of $E(K)$ for some elliptic curve E over K.
- For integers $m, k \geq 1$, we set $G_{m,k} := \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/mk\mathbb{Z}$.
- We denote by I the set of pairs (k, m) of positive integers such that $m \mid p-1$ and $(\sqrt{p}-1)^2 < km^2 < (\sqrt{p}+1)^2$.

The set $\mathcal{E}(\mathbb{F}_p)$ was well-studied by Hasse, Deuring,..., Rück and Volock. The following statement is due to [BPS12, Lemma 3.5].

Theorem 2.1. $\mathcal{E}(\mathbb{F}_p) = \{G_{m,k} \mid (m,k) \in I\}$.

We denote by $\mathcal{E}_{\mathrm{good}}(\mathbb{Q}_p)$ (resp. $\mathcal{E}_{\mathrm{ord}}(\mathbb{Q}_p)$, resp. $\mathcal{E}_{\mathrm{ss}}(\mathbb{Q}_p)$) the subset of $\mathcal{E}(\mathbb{Q}_p)$ consisting of isomorphism classes of $E(\mathbb{Q}_p)_{\mathrm{tor}}$ for some elliptic curve E over $\mathbb{Q}_p$ with good reduction (resp. good ordinary reduction, resp. good supersingular reduction). We clearly have

$$\mathcal{E}_{\mathrm{good}}(\mathbb{Q}_p) = \mathcal{E}_{\mathrm{ord}}(\mathbb{Q}_p) \cup \mathcal{E}_{\mathrm{ss}}(\mathbb{Q}_p).$$

Let E be an elliptic curve over $\mathbb{Q}_p$ with good reduction. We have an exact sequence

$$0 \to \hat{E}(\mathbb{Q}_p) \to E(\mathbb{Q}_p) \to \bar{E}(\mathbb{F}_p) \to 0$$

of modules (cf. [Sil09, Section VII.2])[1]. Since the pro-p group $\hat{E}(\mathbb{Q}_p)$ has no torsion points if $p \geq 3$ (cf. [Sil09, Section IV, Proposition 3.2 and Theorem 6.1]) and $\bar{E}(\mathbb{F}_p)[p^\infty] = \bar{E}(\mathbb{F}_p)[p]$ by the Hasse bound, the reduction map induces an isomorphism

$$E(\mathbb{Q}_p)_{p'} \simeq \bar{E}(\mathbb{F}_p)_{p'} \tag{2.1}$$

and an injection

$$E(\mathbb{Q}_p)[p^\infty] \hookrightarrow \bar{E}(\mathbb{F}_p)[p] \quad \text{if } p \geq 3. \tag{2.2}$$

Here, for a module M, we denote by $M[p^n]$ the submodule of M killed by p^n, $M[p^\infty] := \cup_{n>0} M[p^n]$, and also denote by $M_{p'}$ the prime-to-p part of M.

2.1 The case $p \geq 3$

We study $\mathcal{E}_{\mathrm{ord}}(\mathbb{Q}_p)$, $\mathcal{E}_{\mathrm{ss}}(\mathbb{Q}_p)$ and $\mathcal{E}_{\mathrm{good}}(\mathbb{Q}_p)$ for an odd prime p. We use the following notations.

- We denote by $I_{\mathrm{ord}}\,(\subset I)$ the set of pairs (k,m) of positive integers such that $m \mid p-1$, $(\sqrt{p}-1)^2 < km^2 < (\sqrt{p}+1)^2$ and $km^2 \not\equiv 1 \bmod p$.
- We denote by $I_{\mathrm{ss}}\,(\subset I)$ the set of pairs (k,m) of positive integers such that $m \mid p-1$, $(\sqrt{p}-1)^2 < km^2 < (\sqrt{p}+1)^2$ and $km^2 \equiv 1 \bmod p$.

By definition we have $I = I_{\mathrm{ord}} \cup I_{\mathrm{ss}}$. A straight forward calculation shows that the set I_{ss} coincides with $\{(1,1),(1,4),(1,7),(2,1)\}$ (resp. $\{(1,1+p)\}$, resp. $\{(1,1+p),(2,\frac{1+p}{4})\}$) if $p=3$ (resp. $p \equiv 1 \bmod 4$, resp. $p \neq 3$ and $p \equiv 3 \bmod 4$).

Theorem 2.2 (=Theorem 1.1 (1))**.** *Assume $p \geq 3$.*

(1) $\mathcal{E}_{\mathrm{ord}}(\mathbb{Q}_p) = \{G_{m,k} \mid (m,k) \in I_{\mathrm{ord}}\} \cup \{0\}$.

(2) $\mathcal{E}_{\mathrm{ss}}(\mathbb{Q}_p) = \{G_{m,k} \mid (m,k) \in I_{\mathrm{ss}}\}$. *Explicitly, we have*

$$\mathcal{E}_{\mathrm{ss}}(\mathbb{Q}_p) = \begin{cases} \{G_{1,1}, G_{1,4}, G_{1,7}, G_{2,1}\} & if\ p=3 \\ \{G_{1,1+p}\} & if\ p \equiv 1 \bmod 4 \\ \{G_{1,1+p}, G_{2,\frac{1+p}{4}}\} & if\ p \neq 3,\ p \equiv 3 \bmod 4 \end{cases}$$

(3) $\mathcal{E}_{\mathrm{good}}(\mathbb{Q}_p) = \mathcal{E}(\mathbb{F}_p) \cup \{0\} = \{G_{m,k} \mid (m,k) \in I\} \cup \{0\}$.

For the proof of the theorem, it suffices to show (1) and (2).

[1] In this paper, for an algebraic extension K of $\mathbb{Q}_p$ with maximal ideal $\mathbf{m}_K$, we denote by $\hat{E}(K)$ the group $\hat{E}(\mathbf{m}_K) = \mathbf{m}_K$ determined by the formal group $\hat{E}$ (cf. [Sil09, Chapter IV.3]).

2.1.1 The case of ordinary reduction

We show Theorem 2.2 (1). Let E be an elliptic curve over $\mathbb{Q}_p$ with good reduction. Suppose that $\bar{E}$ is ordinary and $\bar{E}(\mathbb{F}_p) = G_{m,k}$. Since $a_p(E) := 1 + p - \#\bar{E}(\mathbb{F}_p)$ is prime to p, we have $km^2 \not\equiv 1 \bmod p$. By (2.1) and (2.2), we see that $E(\mathbb{Q}_p)_{\mathrm{tor}}$ is isomorphic to $G_{m,k}$ or $G_{m,k/p}$ (with $p \mid k$). Hence we obtain

$$\mathcal{E}_{\mathrm{ord}}(\mathbb{Q}_p) \subset \mathcal{E}^1_{\mathrm{ord}}(\mathbb{Q}_p) \cup \mathcal{E}^2_{\mathrm{ord}}(\mathbb{Q}_p) \cup \mathcal{E}^3_{\mathrm{ord}}(\mathbb{Q}_p)$$

where

$$\begin{aligned}
\mathcal{E}^1_{\mathrm{ord}}(\mathbb{Q}_p) &:= \{G_{m,k} \mid (m,k) \in I_{\mathrm{ord}},\ p \nmid k\},\\
\mathcal{E}^2_{\mathrm{ord}}(\mathbb{Q}_p) &:= \{G_{m,k} \mid (m,k) \in I_{\mathrm{ord}},\ p \mid k\},\\
\mathcal{E}^3_{\mathrm{ord}}(\mathbb{Q}_p) &:= \{G_{m,k/p} \mid (m,k) \in I_{\mathrm{ord}},\ p \mid k\}.
\end{aligned}$$

In the following, we show that the inclusion "$\subset$" above is in fact equal. It suffices to show that each $\mathcal{E}^i_{\mathrm{ord}}(\mathbb{Q}_p)$ is a subset of $\mathcal{E}_{\mathrm{ord}}(\mathbb{Q}_p)$.

Let $G_{m,k} \in \mathcal{E}^1_{\mathrm{ord}}(\mathbb{Q}_p)$. By Theorem 2.1, there exists an elliptic curve $\bar{E}$ over $\mathbb{F}_p$ such that $G_{m,k} \simeq \bar{E}(\mathbb{F}_p)$. By considering lifts to $\mathbb{Z}_p$ of the coefficients of the Weierstrass equation of $\bar{E}$, we obtain an elliptic curve E over $\mathbb{Q}_p$ with good ordinary reduction whose reduction is $\bar{E}$. Since $\bar{E}(\mathbb{F}_p)$ has no p-torsion points by $p \nmid k$, it follows from (2.1) and (2.2) that $E(\mathbb{Q}_p)_{\mathrm{tor}} \simeq G_{m,k}$. Thus we have $\mathcal{E}^1_{\mathrm{ord}}(\mathbb{Q}_p) \subset \mathcal{E}_{\mathrm{ord}}(\mathbb{Q}_p)$.

Let $G_{m,k} \in \mathcal{E}^2_{\mathrm{ord}}(\mathbb{Q}_p)$. In this case, we see $(m,k) \in \{(1,p),(1,2p)\}$ if $p \leq 5$ and $(m,k) \in \{(1,p)\}$ if $p > 5$. Write $k = jp$. By Theorem 2.1, there exists an elliptic curve $\bar{E}$ over $\mathbb{F}_p$ such that $\bar{E}(\mathbb{F}_p) \simeq G_{m,k} = G_{1,jp}$. Let $E_0/_{\mathbb{Q}_p}$ be the canonical lift of $\bar{E}$. Since $\mathrm{End}_{\mathbb{Q}_p} E_0 = \mathrm{End}_{\mathbb{F}_p} \bar{E}$ is an order of an imaginary quadratic field, the $G_{\mathbb{Q}_p}$-action on $E_0[p]$ factors an abelian quotient. In addition, we see $\hat{E}[p] \simeq \mathbb{F}_p(1)$ and $\bar{E}[p] \simeq \mathbb{F}_p$ as $\mathbb{G}_{\mathbb{Q}_p}$-modules since $\bar{E}(\mathbb{F}_p)[p]$ is not trivial. Hence we have (non-canonical) isomorphisms $E_0[p] \simeq \hat{E}[p] \oplus \bar{E}[p] \simeq \mathbb{F}_p(1) \oplus \mathbb{F}_p$ of $G_{\mathbb{Q}_p}$-modules. Thus we obtain $E_0(\mathbb{Q}_p)[p] \simeq \bar{E}(\mathbb{F}_p)[p] \simeq G_{1,p}$, which gives $E(\mathbb{Q}_p)[p^\infty] \simeq G_{1,p}$ by (2.2). On the other hand, we also have $E_0(\mathbb{Q}_p)_{p'} \simeq \bar{E}(\mathbb{F}_p)_{p'} \simeq G_{1,j}$ by (2.1). Hence we obtain $E_0(\mathbb{Q}_p)_{\mathrm{tor}} \simeq G_{1,jp}$. Therefore, we obtain $\mathcal{E}^2_{\mathrm{ord}}(\mathbb{Q}_p) \subset \mathcal{E}_{\mathrm{ord}}(\mathbb{Q}_p)$.

Let $G_{m,k/p} \in \mathcal{E}^3_{\mathrm{ord}}(\mathbb{Q}_p)$. In this case, we see $(m,k) \in \{(1,p),(1,2p)\}$ if $p \leq 5$ and $(m,k) \in \{(1,p)\}$ if $p > 5$. Since $G_{1,2} \in \mathcal{E}^1_{\mathrm{ord}}(\mathbb{Q}_p)$ if $p \leq 5$, it suffices to show that $G_{1,1}\,(= 0)$ is an element of $\mathcal{E}_{\mathrm{ord}}(\mathbb{Q}_p)$. By Theorem 2.1, there exists an elliptic curve $\bar{E}$ over $\mathbb{F}_p$ such that $\bar{E}(\mathbb{F}_p) \simeq G_{m,k} = G_{1,p}$. Take any lift $\tilde{E}$ to $W_2 := W(\mathbb{F}_p)/p^2W(\mathbb{F}_p)$ of $\bar{E}$ such that $\dim_{\mathbb{F}_p} \tilde{E}(W_2) \otimes_{\mathbb{Z}} \mathbb{F}_p = 1$ (there exist $p-1$ isomorphism class of such $\tilde{E}$ by [DW08, Lemma 3.1 and Lemma 3.2]). Taking any lift $E/_{\mathbb{Q}_p}$ of $\tilde{E}$, we have $E(\mathbb{Q}_p)[p] = 0$ by [DW08, Lemma 3.1]. Since we have $E(\mathbb{Q}_p)_{p'} \simeq \bar{E}(\mathbb{F}_p)_{p'} = 0$, it holds $E(\mathbb{Q}_p)_{\mathrm{tor}} = 0 = G_{1,1}$. Consequently, we have $\mathcal{E}^3_{\mathrm{ord}}(\mathbb{Q}_p) \subset \mathcal{E}_{\mathrm{ord}}(\mathbb{Q}_p)$. Thus we proved Theorem 2.2 (1).

2.1.2 The case of supersingular reduction

We show Theorem 2.2 (2). Let E be an elliptic curve over $\mathbb{Q}_p$ with good reduction. Suppose that $\bar{E}$ is supersingular. By (2.1) and (2.2), we have $E(\mathbb{Q}_p)_{\mathrm{tor}} \simeq \bar{E}(\mathbb{F}_p)$. Thus we have

$$\mathcal{E}_{\mathrm{ss}}(\mathbb{Q}_p) \subset \{G_{m,k} \mid (m,k) \in I_{\mathrm{ss}}\}. \tag{2.3}$$

Conversely, let $G_{m,k}$ be in the right hand side of the above and let $\bar{E}$ be the elliptic curve over $\mathbb{F}_p$ with $\bar{E}(\mathbb{F}_p) \simeq G_{m,k}$. Note that $\bar{E}$ is supersingular since $a_p(E) = 1+p-\#\bar{E}(\mathbb{F}_p) \equiv 0 \bmod p$. By taking any lift $E/_{\mathbb{Q}_p}$ of $\bar{E}$, we have $E(\mathbb{Q}_p)_{\mathrm{tor}} \simeq \bar{E}(\mathbb{F}_p) \simeq G_{m,k}$ by (2.1) and (2.2) again. Thus the inclusion "$\subset$" in (2.3) is in fact equal. This finises a proof of Theorem 2.2 (2).

2.2 The case $p = 2$

We study $\mathcal{E}_{\mathrm{ord}}(\mathbb{Q}_p)$, $\mathcal{E}_{\mathrm{ss}}(\mathbb{Q}_p)$ and $\mathcal{E}_{\mathrm{good}}(\mathbb{Q}_p)$ for $p = 2$.

Theorem 2.3 (=Theorem 1.1 (2))**.** (1) $\mathcal{E}_{\mathrm{ord}}(\mathbb{Q}_2) = \{G_{1,2}, G_{1,4}, G_{1,8}, G_{2,1}, G_{2,2}\}$.

(2) $\mathcal{E}_{\mathrm{ss}}(\mathbb{Q}_2) = \{G_{1,1}, G_{1,3}, G_{1,5}\}$.

(3) $\mathcal{E}_{\mathrm{good}}(\mathbb{Q}_2) = \{G_{1,1}, G_{1,2}, G_{1,3}, G_{1,4}, G_{1,5}, G_{1,8}, G_{2,1}, G_{2,2}\}$.

For the proof of the theorem, it suffices to show (1) and (2).

2.2.1 The case of ordinary reduction

We show Theorem 2.3 (1). Let E be an elliptic curve over $\mathbb{Q}_2$ with good reduction. Suppose that $\bar{E}$ is ordinary. Then torsion subgroup of $\hat{E}(\mathbb{Q}_2)$ have order at most 2 by [Sil09, Chapter IV, Proposition 3.2 and Theorem 6.1] and those of $\bar{E}(\mathbb{F}_2)$ have order at most 5 by the Hasse bound. Moreover, since $\hat{E}[2]$ and $\bar{E}[2]$ are cyclic of order 2, $G_{\mathbb{Q}_2}$ acts trivially on them. Thus $\hat{E}(\mathbb{Q}_2)_{\mathrm{tor}} \simeq \mathbb{Z}/2\mathbb{Z}$ and $\bar{E}(\mathbb{F}_2)$ is isomorphic to either $\mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}/4\mathbb{Z}$. Since we have an exact sequence $0 \to \hat{E}(\mathbb{Q}_2)_{\mathrm{tor}} \to E(\mathbb{Q}_2)_{\mathrm{tor}} \to \bar{E}(\mathbb{F}_2)$ of modules, the group $E(\mathbb{Q}_2)_{\mathrm{tor}}$ is isomorphic to one of the following groups:

$$G_{1,2}, G_{1,4}, G_{1,8}, G_{2,1}, G_{2,2}.$$

In fact, it follows from MAGMA calculation with Algorithm A.1 that, for each $G_{m,k}$ appearing above, there exists an elliptic curve E over $\mathbb{Q}_2$ with good ordinary reduction such that $E(\mathbb{Q}_2)_{\mathrm{tor}}$ is isomorphic to $G_{m,k}$. For example,

- E =15.a5 satisfies $E(\mathbb{Q}_2)_{\mathrm{tor}} \simeq G_{1,2}$,
- E =15.a7 satisfies $E(\mathbb{Q}_2)_{\mathrm{tor}} \simeq G_{1,4}$,
- E =15.a4 satisfies $E(\mathbb{Q}_2)_{\mathrm{tor}} \simeq G_{1,8}$,
- E =15.a2 satisfies $E(\mathbb{Q}_2)_{\mathrm{tor}} \simeq G_{2,1}$,
- E =15.a1 satisfies $E(\mathbb{Q}_2)_{\mathrm{tor}} \simeq G_{2,2}$.

This finishes a proof of Theorem 2.3 (1).

2.2.2 The case of supersingular reduction

We show Theorem 2.3 (2). Let E be an elliptic curve over $\mathbb{Q}_2$ with good reduction. Suppose that $\bar{E}$ is supersingular. Note that $E(\mathbb{Q}_2)[2] = 0$ since $E[2]$ is irreducible as a $G_{\mathbb{Q}_2}$-module (cf. [Ser72, Section 1.12, Proposition 12]). Hence, it follows from (2.1) that the reduction map induces an isomorphism $E(\mathbb{Q}_2)_{\mathrm{tor}} \simeq \bar{E}(\mathbb{F}_2)$. By the Hasse bound, we have $\#\bar{E}(\mathbb{F}_2) \in \{1, 3, 5\}$. Thus, $E(\mathbb{Q}_2)_{\mathrm{tor}}$ is isomorphic to one of $G_{1,1}$, $G_{1,3}$ and $G_{1,5}$. In fact, it follows from MAGMA calculation with Algorithm A.1 that, for each $G_{m,k}$ appearing above, there exists an elliptic curve E over $\mathbb{Q}_2$ with good supersingular reduction such that $E(\mathbb{Q}_2)_{\mathrm{tor}}$ is isomorphic to $G_{m,k}$. For example,

- $E =$67.a1 satisfies $E(\mathbb{Q}_2)_{\mathrm{tor}} \simeq G_{1,1}$,
- $E =$19.a1 satisfies $E(\mathbb{Q}_2)_{\mathrm{tor}} \simeq G_{1,3}$,
- $E =$11.a1 satisfies $E(\mathbb{Q}_2)_{\mathrm{tor}} \simeq G_{1,5}$.

This finishes a proof of Theorem 2.3 (2).

3 Group structures of $E(\mathbb{Q}_p(\mu_{p^n}))_{\mathrm{tor}}$

The aim of this section is to prove Theorem 1.2 and Theorem 1.3, which gives the classification of the groups appearing as $E(\mathbb{Q}_p(\mu_{p^\infty}))_{\mathrm{tor}}$ for some elliptic curve E over $\mathbb{Q}_p$ with good reduction. We begin with a proof of Theorem 1.2 (1).

Proof of Theorem 1.2 (1). By [Ser72, Section 1.12, Proposition 12], we know that $E[p]$ is irreducible as $G_{\mathbb{Q}_2}$-modules. If we assume that $E(\mathbb{Q}_p(\mu_{p^\infty}))[p]$ is not zero, then it follows from the irreducibility that we have $E(\mathbb{Q}_p(\mu_{p^\infty}))[p] = E[p]$. This shows that $\mathbb{Q}_p(E[p])$ is a subfield of $\mathbb{Q}_p(\mu_{p^\infty})$. Thus the prime-to-$p$ part of the ramification index of $\mathbb{Q}_p(E[p])/\mathbb{Q}_p$ must be a divisor of $p-1$. However, by [Ser72, Section 1.12, Proposition 12] again, the ramification index of $\mathbb{Q}_p(E[p])/\mathbb{Q}_p$ is p^2-1. This is a contradiction. Hence we obtain $E(\mathbb{Q}_p(\mu_{p^\infty}))[p] = 0$. In particular, we have $E(\mathbb{Q}_p(\mu_{p^\infty}))[p^\infty] = E(\mathbb{Q}_p)[p^\infty]\,(= 0)$. On the other hand, it follows from the Néron-Ogg-Shafarevich criterion that the prime-to-p parts of $E(\mathbb{Q}_p(\mu_{p^\infty}))_{\mathrm{tor}}$ and $E(\mathbb{Q}_p)_{\mathrm{tor}}$ coincides with each other. Thus we conclude $E(\mathbb{Q}_p(\mu_{p^\infty}))_{\mathrm{tor}} = E(\mathbb{Q}_p)_{\mathrm{tor}}$ as desired. □

For the arguments below, We use the following lemma.

Lemma 3.1. *Let $E_{/\mathbb{Q}_p}$ be an elliptic curve with good ordinary reduction. Let α be the non-unit root of $T^2 - a_p(E)T + p = 0$ and denote by $\chi_\alpha \colon G_{\mathbb{Q}_p} \to \mathbb{Z}_p^\times$ the Lubin-Tate character[2] associated with α. Then, the $G_{\mathbb{Q}_p}$-action on the p-adic Tate module $V_p(\hat{E})$ of $\hat{E}$ is given by χ_α.*

Proof. Let $\chi \colon G_{\mathbb{Q}_p} \to \mathbb{Z}_p^\times$ be the character obtained by the $G_{\mathbb{Q}_p}$-action on $V_p(\hat{E})$ and $\phi \colon G_{\mathbb{Q}_p} \to \mathbb{Z}_p^\times$ be the character obtained by the $G_{\mathbb{Q}_p}$-action on $V_p(E)$. Put $T^2 - a_p(E)T + p = f_E(T)$. For any crystalline $\mathbb{Q}_p$-representation V of $G_{\mathbb{Q}_p}$, let $D_{\mathrm{cris}}(V) = (B_{\mathrm{cirs}} \otimes_{\mathbb{Q}_p} V)^{G_{\mathbb{Q}_p}}$ be the Fontaine's filtered φ-module[3]. By p-adic Hodge theory, it is known that

[2] For the definition of Lubin-Tate characters, see Appendix A.4 of Chapter III of [Ser98]

[3] For the basic notion of p-adic Hodge theory, it is helpful for the reader to refer [Fon94a] and [Fon94b].

$f_E(T)$ coincides with the characteristic polynomial of the φ-module $D_{\mathrm{cris}}(V_p(E)^\vee)$, that is, $f_E(T) = \det(T - \varphi \mid D_{\mathrm{cris}}(V_p(E)^\vee))$. Here, $\vee$ stands for the dual representation. Moreover, this coincides with the products of the characteristic polynomials of $D_{\mathrm{cris}}(\mathbb{Q}_p(\chi^{-1}))$ and $D_{\mathrm{cris}}(\mathbb{Q}_p(\phi^{-1}))$. Since χ restricted to the inertia $I_{\mathbb{Q}_p}$ coincides with the p-adic cyclotomic character, for any choice of a uniformizer π of $\mathbb{Q}_p$, it follows from [Con11, Proposition B.4] that $\det(T - \varphi \mid D_{\mathrm{cris}}(\mathbb{Q}_p(\chi^{-1}))) = \chi(\pi) \cdot \pi$, which is independent of the choice of π (here, we regard χ as a character of $\mathbb{Q}_p^\times$ via the local reciprosity map). Since $\chi(\pi) \cdot \pi$ has a postive p-adic valuation, we have $\chi(\pi) \cdot \pi = \alpha$ for any π. By choosing α as π, we have $\chi(\alpha) = 1$. Since we have $\chi = \chi_\alpha$ on $I_{\mathbb{Q}_p}$, we find $\chi = \chi_\alpha$. □

3.1 The case $p \geq 3$

We show Theorem 1.2 (2).

Lemma 3.2. *Assume $p \geq 3$. Let E be an elliptic curve over $\mathbb{Q}_p$ with good ordinary reduction and $\hat{E}$ the formal group associated with E. Then, it holds $\#E(\mathbb{Q}_p(\mu_{p^\infty}))[p^\infty] \leq p^2$ and $\#\hat{E}(\mathbb{Q}_p(\mu_{p^\infty}))[p^\infty] \leq p$.*

Proof. Consider an exact sequence

$$0 \to \hat{E}(\mathbb{Q}_p(\mu_{p^\infty}))[p^\infty] \to E(\mathbb{Q}_p(\mu_{p^\infty}))[p^\infty] \to \bar{E}(\mathbb{F}_p)[p^\infty]$$

of $G_{\mathbb{Q}_p}$-modules. By the Hasse bound, the order of $\bar{E}(\mathbb{F}_p)[p^\infty]$ is at most p (note that p is now odd). Thus it suffices to check that any element of $\hat{E}(\mathbb{Q}_p(\mu_{p^\infty}))[p^\infty]$ is killed by p. Denote by α the non-unit root of the equation $T^2 - a_p(E)T + p = 0$. Then, α is a uniformizer of $\mathbb{Q}_p$ and the $G_{\mathbb{Q}_p}$-action on the Tate module $T_p(\hat{E})$ of $\hat{E}$ is given by the Lubin-Tate character $\chi\colon G_{\mathbb{Q}_p} \to \mathbb{Z}_p^\times$ associated with α by Lemma 3.1. Now take any $P \in \hat{E}(\mathbb{Q}_p(\mu_{p^\infty}))[p^\infty]$. Then $(\chi(\sigma) - 1)P = 0$ for every $\sigma \in G_{\mathbb{Q}_p(\mu_{p^\infty})}$. By abuse of notation, we also denote by χ the composite of χ (considered as a character of $G_{\mathbb{Q}_p}^{\mathrm{ab}}$) and the local reciprocity map $\mathbb{Q}_p^\times \to G_{\mathbb{Q}_p}^{\mathrm{ab}}$. Here, $G_{\mathbb{Q}_p}^{\mathrm{ab}}$ is the maximal abelian quotient of $G_{\mathbb{Q}_p}$. If we denote by v_p the p-adic valuation normalized by $v_p(p) = 1$, then we have

$$\mathrm{Min}\{v_p(\chi(\sigma) - 1) \mid \sigma \in G_{\mathbb{Q}_p(\mu_{p^\infty})}\} \leq v_p(\chi(p^{-1}) - 1) = v_p(p\alpha^{-1} - 1) \tag{3.1}$$

by [Oze24, Proposition 2.1]. Note that $\beta := p\alpha^{-1}$ is the unit root of the equation $T^2 - a_p(E)T + p = 0$. Since $0 = \beta^2 - a_p(E)\beta + p = (\beta - 1)(\beta - a_p(E) + 1) + \#\bar{E}(\mathbb{F}_p)$, we have

$$v_p(p\alpha^{-1} - 1) \leq v_p(\#\bar{E}(\mathbb{F}_p)) \leq 1 \tag{3.2}$$

by the Hasse bound. Therefore, we obtain $pP = 0$ for every $P \in \hat{E}(\mathbb{Q}_p(\mu_{p^\infty}))[p^\infty]$ as desired. □

Proposition 3.3. *Assume $p \geq 3$. Let E be an elliptic curve over $\mathbb{Q}_p$ with good ordinary reduction. Then, we have*

$$E(\mathbb{Q}_p(\mu_{p^\infty}))[p^\infty] \simeq \begin{cases} 0 & \text{if } \bar{E}(\mathbb{F}_p)[p] = 0, \\ \mathbb{Z}/p\mathbb{Z} & \text{if } \bar{E}(\mathbb{F}_p)[p] \neq 0 \text{ and } E(\mathbb{Q}_p)[p] = 0, \\ \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} & \text{if } \bar{E}(\mathbb{F}_p)[p] \neq 0 \text{ and } E(\mathbb{Q}_p)[p] \neq 0. \end{cases}$$

Furthermore, if $\bar{E}(\mathbb{F}_p)[p] \neq 0$, then the minimum fields of definition of $E(\mathbb{Q}_p(\mu_{p^\infty}))[p^\infty]$ and $E(\mathbb{Q}_p(\mu_{p^\infty}))_{\mathrm{tor}}$ are $\mathbb{Q}_p(\mu_p)$.

Proof. Let us first consider the case where $\bar{E}(\mathbb{F}_p)[p] = 0$. Let $\chi\colon G_{\mathbb{Q}_p} \to \mathbb{F}_p^\times$ (resp. $\psi\colon G_{\mathbb{Q}_p} \to \mathbb{F}_p^\times$) be the characters obtained by the $G_{\mathbb{Q}_p}$-action on $\hat{E}[p]$ (resp. $\bar{E}[p]$). Since $\bar{E}(\mathbb{F}_p)[p] = 0$, ψ is not trivial. Since ψ is unramified and $\chi\psi$ coincides with mod p cyclotomic character, we see that χ is not trivial on $G_{\mathbb{Q}_p(\mu_{p^\infty})}$. Thus we have $\hat{E}(\mathbb{Q}_p(\mu_{p^\infty}))[p] = 0$. Now the result immediately follows from an exact sequence $0 \to \hat{E}[p] \to E[p] \to \bar{E}[p] \to 0$ of $\mathbb{F}_p[G_{\mathbb{Q}_p}]$-modules.

Next we consider the case where $\bar{E}(\mathbb{F}_p)[p] \neq 0$ and $E(\mathbb{Q}_p)[p] = 0$. Since $G_{\mathbb{Q}_p}$ acts on $\bar{E}[p]$ trivial, we have isomorphisms $\hat{E}[p] \simeq \mathbb{F}_p(1)$ and $\bar{E}[p] \simeq \mathbb{F}_p$ of $G_{\mathbb{Q}_p}$-modules. Thus there exists a natural exact sequence

$$0 \to \mathbb{F}_p(1) \to E[p] \to \mathbb{F}_p \to 0 \tag{3.3}$$

of $\mathbb{F}_p[G_{\mathbb{Q}_p}]$-modules. In particular, $E(\mathbb{Q}_p(\mu_p))[p]$ contains a submodule $\hat{E}(\mathbb{Q}_p(\mu_p))[p]$ of order p. Now we assume that $E(\mathbb{Q}_p(\mu_{p^n}))[p]$ is isomorphic to $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ for some $n > 0$. Then the extension (3.3) splits as $\mathbb{F}_p[G_{\mathbb{Q}_p(\mu_{p^n})}]$-modules. Since the kernel of the restriction map $H^1(\mathbb{Q}_p, \mathbb{F}_p(1)) \to H^1(\mathbb{Q}_p(\mu_{p^n}), \mathbb{F}_p(1))$, which is isomorphic to $H^1(\mathbb{Q}_p(\mu_{p^n})/\mathbb{Q}_p, \mathbb{F}_p(1))$, is trivial, the extension (3.3) splits as $\mathbb{F}_p[G_{\mathbb{Q}_p}]$-modules. Thus we have $E(\mathbb{Q}_p)[p] = \mathbb{Z}/p\mathbb{Z}$ but this contradicts the assumption that $E(\mathbb{Q}_p)[p] = 0$. Hence, we obtain $E(\mathbb{Q}_p(\mu_{p^n}))[p] \simeq \mathbb{Z}/p\mathbb{Z}$ for any $n > 0$. This shows

$$E(\mathbb{Q}_p(\mu_{p^\infty}))[p] = E(\mathbb{Q}_p(\mu_p))[p] = \hat{E}(\mathbb{Q}_p(\mu_p))[p]$$

and these are isomorphic to $\mathbb{F}_p(1)$ as $G_{\mathbb{Q}_p}$-modules. It follows from Lemma 3.2 that $E(\mathbb{Q}_p(\mu_{p^\infty}))[p^\infty]$ is isomorphic to either $\mathbb{Z}/p\mathbb{Z}$ or $\mathbb{Z}/p^2\mathbb{Z}$ as modules. Therefore, for the proof, it suffices to show that $E(\mathbb{Q}_p(\mu_{p^\infty}))[p^\infty]$ is not isomorphic to $\mathbb{Z}/p^2\mathbb{Z}$. Assume that $E(\mathbb{Q}_p(\mu_{p^\infty}))[p^\infty] \simeq \mathbb{Z}/p^2\mathbb{Z}$. Consider the following commutative diagram.

$$\begin{array}{ccccccc}
0 & \longrightarrow & \hat{E}(\mathbb{Q}_p(\mu_{p^\infty}))[p^\infty] & \longrightarrow & E(\mathbb{Q}_p(\mu_{p^\infty}))[p^\infty] & \longrightarrow & \bar{E}(\mathbb{F}_p)[p^\infty] \\
 & & \uparrow & & \uparrow & & \uparrow \\
0 & \longrightarrow & \hat{E}(\mathbb{Q}_p(\mu_p))[p] & \longrightarrow & E(\mathbb{Q}_p(\mu_p))[p] & \longrightarrow & \bar{E}(\mathbb{F}_p)[p].
\end{array}$$

By Lemma 3.2, the left vertical arrow is bijective. By the Hasse bound, the right vertical arrow is bijective. Thus we find that the reduction map $E(\mathbb{Q}_p(\mu_{p^\infty}))[p^\infty] \to \bar{E}(\mathbb{F}_p)[p^\infty]$ is surjective. Applying Lemma 3.4 below with $G = G_{\mathbb{Q}_p}$ and $M = E(\mathbb{Q}_p(\mu_{p^\infty}))[p^\infty]$, we obtain an isomorphism $\hat{E}(\mathbb{Q}_p(\mu_{p^\infty}))[p^\infty] \simeq \bar{E}(\mathbb{F}_p)[p^\infty]$ of $G_{\mathbb{Q}_p}$-modules. This gives

$$\mathbb{F}_p(1) \simeq \hat{E}[p] = \hat{E}(\mathbb{Q}_p(\mu_{p^\infty}))[p^\infty] \simeq \bar{E}(\mathbb{F}_p)[p^\infty] = \bar{E}(\mathbb{F}_p)[p] \simeq \mathbb{F}_p$$

as $G_{\mathbb{Q}_p}$-modules but this is a contradiction. Therefore, we obtain $E(\mathbb{Q}_p(\mu_{p^\infty}))[p^\infty] \simeq \mathbb{Z}/p\mathbb{Z}$ as desired. Moreover, since we also showed that $E(\mathbb{Q}_p(\mu_{p^\infty}))[p^\infty] = \hat{E}(\mathbb{Q}_p(\mu_p))[p] \simeq \mathbb{F}_p(1)$ as $G_{\mathbb{Q}_p}$-modules, we find that the definition field of $E(\mathbb{Q}_p(\mu_{p^\infty}))[p^\infty]$ is $\mathbb{Q}_p(\mu_p)$. Note that the fields of definition of $E(\mathbb{Q}_p(\mu_{p^\infty}))[p^\infty]$ coincides with that of $E(\mathbb{Q}_p(\mu_{p^\infty}))_{\mathrm{tor}}$ since the prime-to-p part of $E(\mathbb{Q}_p(\mu_{p^\infty}))_{\mathrm{tor}}$ is rational over $\mathbb{Q}_p$ by the Néron-Ogg-Shafarevich criterion.

Finally we consider the case where $\bar{E}(\mathbb{F}_p)[p] \neq 0$ and $E(\mathbb{Q}_p)[p] \neq 0$. Since $\hat{E}[p]\,(\simeq \mathbb{F}_p(1))$ and $E(\mathbb{Q}_p)[p]\,(\simeq \mathbb{F}_p)$ are non-isomorphic $G_{\mathbb{Q}_p}$-submodules of $E[p]$, we have isomorphisms

$$E[p] = \hat{E}[p] \oplus E(\mathbb{Q}_p)[p] \simeq \mathbb{F}_p(1) \oplus \mathbb{F}_p$$

of $G_{\mathbb{Q}_p}$-submodules. In particular, we have $E(\mathbb{Q}_p(\mu_{p^\infty}))[p] = E[p]$. Since the order of $E(\mathbb{Q}_p(\mu_{p^\infty}))[p^\infty]$ is at most p^2 by Lemma 3.2, we obtain $E(\mathbb{Q}_p(\mu_{p^\infty}))[p^\infty] = E[p]$. In particular, the definition field of $E(\mathbb{Q}_p(\mu_{p^\infty}))[p^\infty]$ is $\mathbb{Q}_p(\mu_p)$. As we have seen above, it follows from the Néron-Ogg-Shafarevich criterion that the fields of definition of $E(\mathbb{Q}_p(\mu_{p^\infty}))_{\mathrm{tor}}$ is also $\mathbb{Q}_p(\mu_p)$. □

In the proof above, we used the following lemma.

Lemma 3.4. *Let G be a group, p a prime (including the case $p = 2$) and $n > 0$ an integer. Let M be a $\mathbb{Z}/p^{2n}\mathbb{Z}[G]$-module which is free of finite rank over $\mathbb{Z}/p^{2n}\mathbb{Z}$. Then, we have a canonical isomorphism $p^n M \simeq M/p^n M$ of $\mathbb{Z}/p^n\mathbb{Z}[G]$-modules.*

Proof. The result immediately follows by applying the snake lemma to the commutative diagram of G-modules below:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & p^nM & \longrightarrow & M & \longrightarrow & M/p^nM & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle p^n} & & \downarrow{\scriptstyle p^n} & & \downarrow{\scriptstyle p^n} & & \\ 0 & \longrightarrow & p^nM & \longrightarrow & M & \longrightarrow & M/p^nM & \longrightarrow & 0. \end{array}$$

□

Proof of the first part of Theorem 1.2 (2). The Néron-Ogg-Shafarevich criterion shows that the prime-to-p parts of $E(\mathbb{Q}_p(\mu_{p^\infty}))_{\mathrm{tor}}$ and $E(\mathbb{Q}_p(\mu_p))_{\mathrm{tor}}$ coincide with each other. Moreover, we have $E(\mathbb{Q}_p(\mu_{p^\infty}))[p^\infty] = E(\mathbb{Q}_p(\mu_p))[p^\infty]$ by Proposition 3.3. This finishes a proof. □

Let us prove the second part of Theorem 1.2 (2). The statement is equivalent to say that, for an elliptic curve E over $\mathbb{Q}_p$ with good ordinary reduction, then $E(\mathbb{Q}_p(\mu_{p^\infty}))_{\mathrm{tor}}$ is isomorphic to one of the following groups.

(a) $G_{m,k}$, $(m,k) \in I_{\mathrm{ord}}$,

(b) $G_{p,1}$,

(c) $G_{p,2}$ with $p \leq 5$,

and each of these groups appears as $E(\mathbb{Q}_p(\mu_{p^\infty}))_{\mathrm{tor}}$ for some elliptic curve E over $\mathbb{Q}_p$ with good ordinary reduction.

Lemma 3.5. *Let E be an elliptic curve over $\mathbb{Q}_p$ with good ordinary reduction.*

(1) *If $E(\mathbb{Q}_p)[p] = 0$, then $E(\mathbb{Q}_p(\mu_{p^\infty}))_{\mathrm{tor}} \simeq \bar{E}(\mathbb{F}_p)$ as abstract groups.*

(2) *If $E(\mathbb{Q}_p)[p] \neq 0$, then $E(\mathbb{Q}_p(\mu_{p^\infty}))_{\mathrm{tor}} \simeq \bar{E}(\mathbb{F}_p) \times \mathbb{Z}/p\mathbb{Z}$ as abstract groups.*

Proof. Assume that an elliptic curve E over $\mathbb{Q}_p$ has good ordinary reduction. If $E(\mathbb{Q}_p)[p] = 0$ (resp. $E(\mathbb{Q}_p)[p] \neq 0$), we have $E(\mathbb{Q}_p(\mu_{p^\infty}))[p^\infty] \simeq \bar{E}(\mathbb{F}_p)[p^\infty]$ (resp. $E(\mathbb{Q}_p(\mu_{p^\infty}))[p^\infty] \simeq \bar{E}(\mathbb{F}_p)[p^\infty] \times \mathbb{Z}/p\mathbb{Z}$) by Proposition 3.3. Since the reduction map gives an isomorphism between the prime-to-p parts of $E(\mathbb{Q}_p(\mu_{p^\infty}))$ and $\bar{E}(\mathbb{F}_p)$, the result follows. □

Proof of the second part of Theorem 1.2 (2). Suppose that an elliptic curve E over $\mathbb{Q}_p$ has good ordinary reduction. If $E(\mathbb{Q}_p)[p] = 0$, then it follows from Lemma 3.5 (1) that $E(\mathbb{Q}_p(\mu_{p^\infty}))$ is isomorphic to $G_{m,k}$ for some $(m,k) \in I_{\mathrm{ord}}$. If $E(\mathbb{Q}_p)[p] \neq 0$, then it follows from Lemma 3.5 (2) that $E(\mathbb{Q}_p(\mu_{p^\infty}))_{\mathrm{tor}}$ is isomorphic to $G_{m,k} \times \mathbb{Z}/p\mathbb{Z}$ for some $(m,k) \in I_{\mathrm{ord}}$. Note that we moreover have $p \mid k$ since $\bar{E}(\mathbb{F}_p)[p]$ is not zero by (2.2). In this case we see $(m,k) = (1, jp)$ with $j \in \{1,2\}$ (resp. $j = 1$) for $p \leq 5$ (resp. $p > 5$), and then $E(\mathbb{Q}_p(\mu_{p^\infty}))_{\mathrm{tor}}$ is isomorphic to and $G_{m,k} \times \mathbb{Z}/p\mathbb{Z} \simeq G_{p,j}$. Therefore, we showed that $E(\mathbb{Q}_p(\mu_{p^\infty}))_{\mathrm{tor}}$ is isomorphic to one of the groups appearing in (a), (b) or (c).

Conversely, let G be a group appearing in (a), (b) or (c). Suppose $G = G_{m,k}$ as in (a) and suppose in addition $p \nmid k$. By Theorem 2.1, there exists an ordinary elliptic curve $\bar{E}$ over $\mathbb{F}_p$ such that $G \simeq \bar{E}(\mathbb{F}_p)$. Take any lift E of $\bar{E}$ to $\mathbb{Q}_p$. By $p \nmid k$, $\bar{E}(\mathbb{F}_p)[p]$ is trivial, and thus we have $E(\mathbb{Q}_p)[p] = 0$ by (2.2). By Lemma 3.5, we have $E(\mathbb{Q}_p(\mu_{p^\infty}))_{\mathrm{tor}} \simeq G$. Next we suppose one of the following situations.

- $G = G_{m,k}$ as in (a) and suppose in addition $p \mid k$. In this case $G = G_{1,jp}$ for $j \in \{1,2\}$ (resp. $j = 1$) for $p \leq 5$ (resp. $p > 5$).
- $G = G_{p,j}$ ($\simeq G_{1,jp} \times \mathbb{Z}/p\mathbb{Z}$) is as in (b) or (c).

By Theorem 2.1, there exists an ordinary elliptic curve $\bar{E}$ over $\mathbb{F}_p$ such that $G_{1,jp} \simeq \bar{E}(\mathbb{F}_p)$. By Lemma 3.1 and Lemma 3.2 of [DW08], there exist elliptic curves E_1 and E_2 over $\mathbb{Q}_p$ whose reductions are $\bar{E}$ such that $E_1(\mathbb{Q}_p)[p] = 0$ and $E_2(\mathbb{Q}_p)[p] \neq 0$. (Note that the canonical lift of $\bar{E}$ satisfies the desired condition for E_2.) It follows from Lemma 3.5 that $E_1(\mathbb{Q}_p(\mu_{p^\infty})) \simeq G_{1,jp}$ and $E_2(\mathbb{Q}_p(\mu_{p^\infty})) \simeq G_{p,j}$. This finishes a proof. □

3.2 The case $p = 2$

We show Theorem 1.2 (3) and Theorem 1.3. We begin with a proof of the second statement of Theorem 1.2 (3); it suffices to show that, for an elliptic curve E over $\mathbb{Q}_2$ with good ordinary reduction, then $E(\mathbb{Q}_2(\mu_{2^\infty}))_{\mathrm{tor}}$ is isomorphic to one of the following groups.

(a) $G_{1,k}$, $k \in \{4, 8\}$,

(b) $G_{2,k}$, $k \in \{1, 4\}$,

(c) $G_{4,1}$,

and each of these groups appears as $E(\mathbb{Q}_2(\mu_{2^\infty}))_{\mathrm{tor}}$ for some elliptic curve E over $\mathbb{Q}_2$ with good ordinary reduction.

For our proof below, we need Fontaine's results on ramification theory of finite flat commutative group schemes. We give a brief sketch here (with restricting 2-adic cases); see [Ser68] and [Fon85] for more precise information. Let K be a 2-adic field and L/K be a (not necessarily finite) Galois extension. For any non-negative real number $u \geq 0$, let $\mathrm{Gal}(L/K)^{(u)}$ be the u-th upper ramification subgroup of $\mathrm{Gal}(L/K)$ in the sense of [Fon85]. For a finite Galois extension L/K, we define *the maximal upper ramification break* of L/K defined by $u_{L/K} = \sup\{u \in \mathbb{R} \mid \mathrm{Gal}(L/K)^{(u)} \neq 1\}$. It is well-known that

– L/K is unramified if and only if $u_{L/K} = 0$,

– L/K is tamely ramified if and only if $u_{L/K} \leq 1$, and

– L/K is wildly ramified if and only if $u_{L/K} > 1$.

For example, there exist 7 quadratic extensions of $\mathbb{Q}_2$, and their maximal upper ramification breaks are given in the Table A.1. We set $G_K^{(u)} := \mathrm{Gal}(\overline{\mathbb{Q}}_2/K)^{(u)}$. It is shown by Fontaine [Fon85, Section 2, Théorèm 1] that, for any finite flat commutative group scheme $\mathcal{G}$ over K killed by 2^n, the group $G_K^{(u)}$ acts trivial on $\mathcal{G}(\overline{K})$ for $u > e_K(n+1)$. This is equivalent to say that, if we denote by L/K the Galois extension corresponding to the kernel of the G_K-action on $\mathcal{G}(\overline{K})$, then $\mathrm{Gal}(L/K)^{(u)}$ is trivial for $u > e_K(n+1)$, that is, $u_{L/K} \leq e_K(n+1)$. By applying the result for $E[2^n]$, we have $u_{L/\mathbb{Q}_2} \leq n+1$ for $L = \mathbb{Q}_2(E[2^n])$. Since $u_{\mathbb{Q}_2(\mu_{2^n})/\mathbb{Q}_2} = n$ for any integer $n > 1$ (cf. [Ser68, Chap. IV, Sect. 4, Cor.]), we have

$$E(\mathbb{Q}_2(\mu_{2^\infty}))[2^n] = E(\mathbb{Q}_2(\mu_{2^{n+1}}))[2^n] \tag{3.4}$$

Let us return to the proof of the second statement of Theorem 1.2 (3). We need the following lemma.

Lemma 3.6. *For an elliptic curve E over $\mathbb{Q}_2$ with good ordinary reduction, we have $\hat{E}(\mathbb{Q}_2(\mu_{2^\infty}))_{\mathrm{tor}} \simeq \bar{E}(\mathbb{F}_2)$ as abstract groups.*

Proof. First we note that $\bar{E}(\mathbb{F}_2)$ contains the element of order 2 since the Galois group $G_{\mathbb{Q}_2}$ acts on $\bar{E}[2]\,(\simeq \mathbb{Z}/2\mathbb{Z})$ trivial. The Hasse bound shows that $\bar{E}(\mathbb{F}_2)$ is isomorphic to either $\mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}/4\mathbb{Z}$. Thus

$$a_2(E) = \begin{cases} 1 & if\ \bar{E}(\mathbb{F}_2) \simeq \mathbb{Z}/2\mathbb{Z}, \\ -1 & if\ \bar{E}(\mathbb{F}_2) \simeq \mathbb{Z}/4\mathbb{Z}. \end{cases}$$

Denote by α (resp. β) the non-unit root (resp. unit root) of the equation $T^2 - a_2(E)T + 2 = 0$, where $a_2(E) = 1 + 2 - \#\bar{E}(\mathbb{F}_2)$. Then $G_{\mathbb{Q}_2}$ acts on the Tate module $V_2(\hat{E})$ of $\hat{E}$ by the Lubin-Tate character χ associated with the uniformizer α by Lemma 3.1. By abuse of notation we also denote by $\chi\colon \mathbb{Q}_2^\times \to \mathbb{Q}_2^\times$ the composite of χ (considered as a character of $G_{\mathbb{Q}_2}^{\mathrm{ab}}$) and the local reciprocity map $\mathbb{Q}_2^\times \to G_{\mathbb{Q}_2}^{\mathrm{ab}}$. Here, $G_{\mathbb{Q}_2}^{\mathrm{ab}} = \mathrm{Gal}(\mathbb{Q}_2^{\mathrm{ab}}/\mathbb{Q}_2(\mu_{2^\infty}))$ is the maximal abelian quotient of $G_{\mathbb{Q}_2}$. Then $\chi(2) = \chi(\alpha\beta) = \beta^{-1} \equiv -a_2(E) \bmod 4$. Since the subgroup of $\mathbb{Q}_2^\times$ corresponding to $\mathrm{Gal}(\mathbb{Q}_2^{\mathrm{ab}}/\mathbb{Q}_2(\mu_{2^\infty}))$ via the local reciprocity map is the closure of the group generated by 2, we obtain that

$$\begin{cases} \chi \not\equiv 1 \bmod 4 & if\ \bar{E}(\mathbb{F}_2) \simeq \mathbb{Z}/2\mathbb{Z}, \\ \chi \equiv 1 \bmod 4 & if\ \bar{E}(\mathbb{F}_2) \simeq \mathbb{Z}/4\mathbb{Z} \end{cases}$$

on $G_{\mathbb{Q}_2(\mu_{2^\infty})}$. Therefore, we see $\hat{E}(\mathbb{Q}_p(\mu_{2^\infty}))[2^\infty] \simeq \bar{E}(\mathbb{F}_2)$ as abstract groups. Since orders of torsion elements of $\hat{E}$ are power of 2, we finish the proof of the lemma. □

Proof of the second statement of Theorem 1.2 (3). Consider an exact sequence

$$0 \to \hat{E}(\mathbb{Q}_p(\mu_{2^\infty}))_{\mathrm{tor}} \to E(\mathbb{Q}_p(\mu_{2^\infty}))_{\mathrm{tor}} \to \bar{E}(\mathbb{F}_2)$$

of $G_{\mathbb{Q}_2}$-modules. It follows from Lemma 3.6 that $\hat{E}(\mathbb{Q}_p(\mu_{2^\infty}))_{\mathrm{tor}} \simeq \bar{E}(\mathbb{F}_2)$ as abstract groups, and the orders of these groups are 2 or 4 by the Hasse bound. This shows that $E(\mathbb{Q}_2(\mu_{2^\infty}))_{\mathrm{tor}}$ is isomorphic to one of the groups appearing in the following.

(a)' $G_{1,k}$, $k \in \{2, 4, 8, 16\}$,

(b)' $G_{2,k}$, $k \in \{1,2,4\}$,

(c) $G_{4,1}$.

We claim that $E(\mathbb{Q}_2(\mu_{2^\infty}))_{\mathrm{tor}}$ is not isomorphic to $G_{1,16}$. Assume $E(\mathbb{Q}_2(\mu_{2^\infty}))_{\mathrm{tor}} \simeq \mathbb{Z}/16\mathbb{Z}$. If this is the case, putting $M = E(\mathbb{Q}_2(\mu_{2^\infty}))_{\mathrm{tor}}$, we have $4M = \hat{E}(\mathbb{Q}_2(\mu_{2^\infty}))[2^\infty]$ and $M/4M = \bar{E}(\mathbb{F}_2)$. It follows from Lemma 3.4 that we have an isomorphism $\hat{E}(\mathbb{Q}_2(\mu_{2^\infty}))[2^\infty] \simeq \bar{E}(\mathbb{F}_2)$ of $G_{\mathbb{Q}_2}$-modules but this is a contradiction since $G_{\mathbb{Q}_2}$ acts on $\hat{E}(\mathbb{Q}_2(\mu_{2^\infty}))[2^\infty] = \hat{E}(\mathbb{Q}_2(\mu_{2^\infty}))[4]$ $(\simeq \mathbb{Z}/4\mathbb{Z})$ by the 2-adic cyclotomic character modulo 4.

By the claim above, $E(\mathbb{Q}_2(\mu_{2^\infty}))_{\mathrm{tor}}$ is killed by 2^3. By (3.4), we see that $E(\mathbb{Q}_2(\mu_{2^\infty}))_{\mathrm{tor}} = E(\mathbb{Q}_2(\mu_{16}))_{\mathrm{tor}}$. Since we have a descent from $\mathbb{Q}_2(\mu_{2^\infty})$ to a (not so large) finite extension $\mathbb{Q}_2(\mu_{16})$ of $\mathbb{Q}_2$, we can apply a computational approach; by MAGMA calculation with Algorithm A.1, we can check that some of the groups in (a)', (b)' or (c) above appears as $E(\mathbb{Q}_p(\mu_{p^\infty}))_{\mathrm{tor}}$ for some elliptic curve E over $\mathbb{Q}_2$ with good ordinary reduction:

- $E =$33.a3 satisfies $E(\mathbb{Q}_2(\mu_{2^\infty}))_{\mathrm{tor}} \simeq G_{1,4}$.
- $E =$15.a5 satisfies $E(\mathbb{Q}_2(\mu_{2^\infty}))_{\mathrm{tor}} \simeq G_{1,8}$.
- $E =$33.a1 satisfies $E(\mathbb{Q}_2(\mu_{2^\infty}))_{\mathrm{tor}} \simeq G_{2,1}$.
- $E =$15.a2 satisfies $E(\mathbb{Q}_2(\mu_{2^\infty}))_{\mathrm{tor}} \simeq G_{2,4}$.
- $E =$15.a1 satisfies $E(\mathbb{Q}_2(\mu_{2^\infty}))_{\mathrm{tor}} \simeq G_{4,1}$.

For the proof of the theorem, it suffices to show that there is no elliptic curve E over $\mathbb{Q}_2$ with good ordinary reduction such that $E(\mathbb{Q}_p(\mu_{p^\infty}))_{\mathrm{tor}}$ is isomorphic to either $G_{1,2}$ or $G_{2,2}$. In the rest of the proof, we denote by $\chi\colon G_{\mathbb{Q}_2} \to \mathbb{Z}_2^\times$ the crystalline character defined by the $G_{\mathbb{Q}_p}$-action on the p-adic Tate module $T_p(\hat{E})$ of the formal group associated with E. We also denote by $\psi\colon G_{\mathbb{Q}_2} \to \mathbb{Z}_2^\times$ the unramified character defined by the $G_{\mathbb{Q}_p}$-action on the p-adic Tate module $T_p(\bar{E})$ of the reduction $\bar{E}$ of E. The Weil pairing shows that $\chi\psi = \chi_2$ where χ_2 is the 2-adic cyclotomic character. Thus we have $\chi\psi \bmod 2^n = 1$ on $G_{\mathbb{Q}_2(\mu_{2^n})}$ for each $n > 0$.

(I) Non-existence of $G_{1,2}$: If $E(\mathbb{Q}_2(\mu_{2^\infty}))_{\mathrm{tor}} \simeq \mathbb{Z}/2\mathbb{Z}$ for some elliptic curve E over $\mathbb{Q}_2$ with good reduction, it follows from Fontaine's ramification bound (3.4) that $E(\mathbb{Q}_2(\mu_{2^\infty}))_{\mathrm{tor}} = E(\mathbb{Q}_2(\mu_4))_{\mathrm{tor}}$. Hence, it suffices to show that $E(\mathbb{Q}_2(\mu_4))_{\mathrm{tor}} \not\simeq \mathbb{Z}/2\mathbb{Z}$ for any elliptic curve E over $\mathbb{Q}_2$ with good ordinary reduction.

Assume that $E(\mathbb{Q}_2(\mu_4))_{\mathrm{tor}} \simeq \mathbb{Z}/2\mathbb{Z}$ for some elliptic curve E over $\mathbb{Q}_2$ with good ordinary reduction. For a suitable choice of a $\mathbb{Z}/4\mathbb{Z}$-basis of $E[4]$, the $G_{\mathbb{Q}_2}$-action on $E[4]$ is given by

$$\rho_{E[4]} = \begin{pmatrix} \chi \bmod 4 & u \\ 0 & \psi \bmod 4 \end{pmatrix} : G_{\mathbb{Q}_2} \to GL_2(\mathbb{Z}/4\mathbb{Z})$$

for some map $u\colon G_{\mathbb{Q}_2} \to \mathbb{Z}/4\mathbb{Z}$.

We claim that

$$[\mathbb{Q}_2(E[4]) : \mathbb{Q}_2] = 16.$$

Since $\chi \equiv \psi \bmod 4$ on $G_{\mathbb{Q}_2(\mu_4)}$, we may regard $H := \mathrm{Gal}(\mathbb{Q}_2(E[4])/\mathbb{Q}_2(\mu_4))$ as a subgroup of

$$G := \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \mid a \in (\mathbb{Z}/4\mathbb{Z})^\times, b \in \mathbb{Z}/4\mathbb{Z} \right\}$$

via $\rho_{E[4]}$. Since $E(\mathbb{Q}_2(\mu_4)) \not\supset E[2]$, we have $u \bmod 2 \neq 0$ on $G_{\mathbb{Q}_2(\mu_4)}$. Thus H contains at least either $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ or $\begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix}$. If we assume that H is generated by one of these matrices, we find that $E(\mathbb{Q}_2(\mu_4)))$ must contain an element of order 4 but this is a contradiction. Thus we have $H = G$. Now the claim immediately follows.

By considering from the view point of ramification, we show below that

$$[\mathbb{Q}_2(E[4]) : \mathbb{Q}_2] < 16$$

holds (of course this is a contradiction). Since ψ is unramified, $\psi \bmod 4$ is trivial on G_F where F is the unramified quadratic extension field F of $\mathbb{Q}_2$. In particular, we have $\chi \bmod 4 = \chi_2 \bmod 4$ on G_F. Since $E(\mathbb{Q}_2(\mu_4))$ does not contain $E[2]$, we have $u \bmod 2 \neq 0$ on $G_{\mathbb{Q}_2(\mu_4)}$. Thus the field L corresponding to the kernel of $u \bmod 2 \colon G_{\mathbb{Q}_2} \to \mathbb{Z}/2\mathbb{Z}$ is a quadratic extension of $\mathbb{Q}_2$. Note that we have $L = \mathbb{Q}_2(E[2])$ and

$$u(G_L) \subset 2 \cdot \mathbb{Z}/4\mathbb{Z}. \tag{3.5}$$

By [Fon85, Section 2, Théorèm 1], the maximal ramification break $u_{L/\mathbb{Q}_2}$ of $L/\mathbb{Q}_2$ is at most 2. Hence there are three possibilities for L; L is isomorphic to either $L_1 = \mathbb{Q}_2[x]/(x^2 + 2x + 2)$ $(\simeq \mathbb{Q}_2(\mu_4))$, $L_2 = \mathbb{Q}_2[x]/(x^2 + 2x + 6)$ or F (see Table A.1). Since $E(\mathbb{Q}_2(\mu_4))$ does not contain $E[2]$, L is isomorphic to either L_2 or F.

(i) Suppose $L = F$. We have

$$\rho_{E[4]} = \begin{pmatrix} \chi \bmod 4 & u \\ 0 & 1 \end{pmatrix}$$

on G_F. Since the order of $u(G_F)$ is at most 2 by (3.5), we see that $[\mathbb{Q}_2(E[4]) : F] \leq 4$, which shows $[\mathbb{Q}_2(E[4]) : \mathbb{Q}_2] \leq 8 < 16$ as desired.

(ii) Suppose $L = L_2$. In this case, the field $L(\mu_4)$ cotains F by Proposition A.1 (1). Thus we have

$$\rho_{E[4]} = \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix}$$

on $G_{L(\mu_4)}$. Since the order of $u(G_{L(\mu_4)})$ is at most 2 by (3.5), we see that $[\mathbb{Q}_2(E[4]) : L(\mu_4)] \leq 2$, which shows $[\mathbb{Q}_2(E[4]) : \mathbb{Q}_2] \leq 8 < 16$ as desired.

Therefore, we finish the proof of (I).

(II) Non-existence of $G_{2,2}$: If $E(\mathbb{Q}_2(\mu_{2^\infty}))_{\mathrm{tor}} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ for some elliptic curve E over $\mathbb{Q}_2$ with good reduction, it follows from Fontaine's ramification bound (3.4) that $E(\mathbb{Q}_2(\mu_{2^\infty}))_{\mathrm{tor}} = E(\mathbb{Q}_2(\mu_8))_{\mathrm{tor}}$. Hence, it suffices to show that $E(\mathbb{Q}_2(\mu_8))_{\mathrm{tor}} \not\simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ for any elliptic curve E over $\mathbb{Q}_2$ with good ordinary reduction.

Assume that $E(\mathbb{Q}_2(\mu_8))_{\mathrm{tor}} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ for some elliptic curve E over $\mathbb{Q}_2$ with good ordinary reduction. For a suitable choice of a $\mathbb{Z}/8\mathbb{Z}$-basis of $E[8]$, the $G_{\mathbb{Q}_2}$-action on $E[8]$ is given by

$$\rho_{E[8]} = \begin{pmatrix} \chi \bmod 8 & u \\ 0 & \psi \bmod 8 \end{pmatrix} : G_{\mathbb{Q}_2} \to GL_2(\mathbb{Z}/8\mathbb{Z})$$

for some map $u \colon G_{\mathbb{Q}_2} \to \mathbb{Z}/8\mathbb{Z}$. Here we give some remarks on the character $\psi \bmod 8$ and the map u. By Lemma 3.6 and the assumption that $E(\mathbb{Q}_2(\mu_{2^\infty}))$ is of order ≥ 8, we have

$\bar{E}(\mathbb{F}_2) \simeq \mathbb{Z}/4\mathbb{Z}$. Thus any element of $\bar{E}[4]$ is $\mathbb{F}_2$-rational but some element of $\bar{E}[8]$ is not $\mathbb{F}_2$-rational. This gives

$$\psi \bmod 4 = 1 \text{ on } G_{\mathbb{Q}_2} \quad \text{and} \quad \psi \bmod 8 \neq 1 \text{ on } G_{\mathbb{Q}_2(\mu_8)}. \tag{3.6}$$

In particular, $\psi \bmod 8 \colon G_{\mathbb{Q}_2} \to (\mathbb{Z}/8\mathbb{Z})^\times$ has values in $\{1,5\}$ and hence $\psi \bmod 8 \colon G_{\mathbb{Q}_2} \to \{1,5\}\,(\subset (\mathbb{Z}/8\mathbb{Z})^\times)$ is the surjective unramified character. By $E[2] \subset E(\mathbb{Q}_2(\mu_8)))_{\mathrm{tor}}$, we see that $u \bmod 2$ is trivial on $G_{\mathbb{Q}_2(\mu_8)}$, that is, $u(G_{\mathbb{Q}_2(\mu_8)}) \subset 2 \cdot \mathbb{Z}/8\mathbb{Z}$. Note that $\rho_{E[4]} = \begin{pmatrix} \chi_2 \bmod 4 & u \bmod 4 \\ 0 & 1 \end{pmatrix}$ on $G_{\mathbb{Q}_2}$ by (3.6). Since $E(\mathbb{Q}_2(\mu_{2^\infty}))$ does not contain $E[4]$, it holds

$$u \bmod 4 \neq 0 \text{ on } G_{\mathbb{Q}_2(\mu_8)}. \tag{3.7}$$

On the other hand, since $u \bmod 4$ on $G_{\mathbb{Q}_2(E[2])}$ has values in $2 \cdot \mathbb{Z}/4\mathbb{Z}$, it holds $\chi(\sigma)u(\sigma) \equiv u(\sigma) \bmod 4$ for any $\sigma \in G_{\mathbb{Q}_2(E[2])}$. This gives the fact that $u \bmod 4$ on $G_{\mathbb{Q}_2(E[2])}$ is a homomorphism with values in $2 \cdot \mathbb{Z}/4\mathbb{Z}$.

We claim that

$$[\mathbb{Q}_2(E[8]) : \mathbb{Q}_2] = 32.$$

Since $\chi \equiv \psi \bmod 8$ on $G_{\mathbb{Q}_2(\mu_8)}$, it follows from (3.6) and $u(G_{\mathbb{Q}_2(\mu_8)}) \subset 2 \cdot \mathbb{Z}/8\mathbb{Z}$ that we may regard $H := \mathrm{Gal}(\mathbb{Q}_2(E[8])/\mathbb{Q}_2(\mu_8))$ as a subgroup of

$$G := \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \mid a \in \{1,5\} \subset (\mathbb{Z}/8\mathbb{Z})^\times, b \in 2 \cdot \mathbb{Z}/8\mathbb{Z} \right\}$$

via $\rho_{E[8]}$. By (3.7), H contains at least either $\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ or $\begin{pmatrix} 5 & 2 \\ 0 & 5 \end{pmatrix}$. If H is generated by one of these matrices, we find that $E(\mathbb{Q}_2(\mu_8))$ must contain an element of order 8 but this is a contradiction. Thus we have $H = G$. Now the claim immediately follows.

As we have done in the case (I), by considering from the view point of ramification, we show below that

$$[\mathbb{Q}_2(E[8]) : \mathbb{Q}_2] < 32$$

holds (of course this is a contradiction). First we note that $\mathbb{Q}_2(E[2])$ is a subfield of $\mathbb{Q}_2(\mu_8)$ since $E(\mathbb{Q}_2(\mu_8))$ contains $E[2]$. By (3.7) and the fact that $u \bmod 4$ on $G_{\mathbb{Q}_2(E[2])}$ is a homomorphism with values in $2 \cdot \mathbb{Z}/4\mathbb{Z}$, we know that the homomorphism $u \bmod 4 \colon G_{\mathbb{Q}_2(E[2])} \to 2 \cdot \mathbb{Z}/4\mathbb{Z}$ is surjective. We denote by L the quadratic extension of $\mathbb{Q}_2(E[2])$ which corresponds to the kernel of this homomorphism. By definition of L, L is a quadratic extension of $\mathbb{Q}_2(E[2])$ and we have

$$u(G_L) \subset 4 \cdot \mathbb{Z}/8\mathbb{Z}. \tag{3.8}$$

Since L is a subfield of $\mathbb{Q}_2(E[4])$, it follows from Fontaine's ramification bound (3.4) that $u_{L/\mathbb{Q}_2} \leq 3$. Furthermore, L does not contained in $\mathbb{Q}_2(\mu_8)$. In fact, if L is a subfield of $\mathbb{Q}_2(\mu_8)$, then $\rho_{E[4]}$ must be trivial on $G_{\mathbb{Q}_2(\mu_8)}$, which shows $E(\mathbb{Q}_2(\mu_8))$ contains $E[4]$ but this is a contradiction. Since $\mathbb{Q}_2(E[2])$ is now contained in $\mathbb{Q}_2(\mu_8)$ and is of degree at most 2 over $\mathbb{Q}_2$, it follows (3.4) again that $\mathbb{Q}_2(E[2])$ is either $\mathbb{Q}_2$ or $\mathbb{Q}_2(\mu_4)$ (see Table A.1). We make a case distinction depending on which of these two situations occurs.

(II-1) Suppose that $\mathbb{Q}_2(E[2]) = \mathbb{Q}_2$. Since $\rho_{E[4]} = \begin{pmatrix} \chi_2 \bmod 4 & u \bmod 4 \\ 0 & 1 \end{pmatrix}$ on $G_{\mathbb{Q}_2}$ by (3.6), we have $\mathbb{Q}_2(E[4]) = L(\mu_4)$. We recall that L satisfies all the following properties:

(a) L is a quadratic extension of $\mathbb{Q}_2$,

(b) $u_{L/\mathbb{Q}_2} \leq 3$ and

(c) L does not contained in $\mathbb{Q}_2(\mu_8)$.

Note that $u_{L/\mathbb{Q}_2}$ is not equal to one since $L/\mathbb{Q}_2$ is either unramified or wildly ramified.

- Suppose $u_{L/\mathbb{Q}_2} = 0$. If this is the case, we have $L = F$ and $\rho_{E[8]} = \begin{pmatrix} \chi_2 \bmod 8 & u \\ 0 & 1 \end{pmatrix}$ on G_F by (3.6). Thus it follows from (3.8) that we have $[\mathbb{Q}_2(E[8]) : F] \leq 8$, which shows $[\mathbb{Q}_2(E[8]) : \mathbb{Q}_2] \leq 16 < 32$ as desired.

- Suppose $u_{L/\mathbb{Q}_2} = 2$. By (a), (b) and (c) above, we find that L is isomorphic to $L_2 = \mathbb{Q}_2[x]/(x^2 + 2x + 6)$ (see Table A.1). In particular, $L(\mu_4)$ contains F by Proposition A.1 (1). We have $\rho_{E[8]} = \begin{pmatrix} \chi_2 \bmod 8 & u \\ 0 & 1 \end{pmatrix}$ on $G_{L(\mu_4)}$ by (3.6). Thus it follows from (3.8) that we have $[\mathbb{Q}_2(E[8]) : L(\mu_4)] \leq 4$, which shows $[\mathbb{Q}_2(E[8]) : \mathbb{Q}_2] \leq 16 < 32$ as desired.

- Suppose $u_{L/\mathbb{Q}_2} = 3$. There exist only 4 possibility for such L. Explicitly, L is isomorphic to one of the following (see Table A.1).

$$L_3 = \mathbb{Q}_2[x]/(x^2 + 2), \qquad L_4 = \mathbb{Q}_2[x]/(x^2 + 10),$$
$$L_5 = \mathbb{Q}_2[x]/(x^2 + 4x + 2), \qquad L_6 = \mathbb{Q}_2[x]/(x^2 + 4x + 10).$$

  For each of the fields, their composite with $F(\mu_4)$ contains μ_8 by Proposition A.1 (2). This implies that $LF(\mu_4)$ contains μ_8. Hence we have $\rho_{E[8]} = \begin{pmatrix} 1 & u \bmod 8 \\ 0 & 1 \end{pmatrix}$ on $G_{LF(\mu_4)}$ by (3.6). Thus it follows from (3.8) that we have $[\mathbb{Q}_2(E[8]) : LF(\mu_4)] \leq 2$, which shows $[\mathbb{Q}_2(E[8]) : \mathbb{Q}_2] \leq 16 < 32$ as desired.

(II-2) Suppose that $\mathbb{Q}_2(E[2]) = \mathbb{Q}_2(\mu_4)$. Since $\rho_{E[4]} = \begin{pmatrix} 1 & u \bmod 4 \\ 0 & 1 \end{pmatrix}$ on $G_{\mathbb{Q}_2(\mu_4)}$ by (3.6), we have $\mathbb{Q}_2(E[4]) = L$. In particular, L is a Galois extension of $\mathbb{Q}_2$. Here we summarize properties of L.

(a) L is a Galois extension over $\mathbb{Q}_2$ of degree 4 with $L \supset \mathbb{Q}_2(\mu_4)$,

(b) $u_{L/\mathbb{Q}_2} \leq 3$ and

(c) L does not conatined in $\mathbb{Q}_2(\mu_8)$.

We claim that either $L = F(\mu_4)$ or $LF \supset \mathbb{Q}_2(\mu_8)$. If $L/\mathbb{Q}_2(\mu_4)$ is unramified, then we have $L = F(\mu_4)$. Suppose that $L/\mathbb{Q}_2(\mu_4)$ is totally ramified. Then L is a totally ramified Galois extension over $\mathbb{Q}_2$ of degree 4. By $\mathbb{Q}_2(\mu_4) \subset L = \mathbb{Q}_2(E[4])$, Fontiane's ramification bound implies $2 \leq u_{L/\mathbb{Q}_2} \leq 3$. In fact, there does not exist[4] a totally ramified Galois extension over $\mathbb{Q}_2$ of degree 4 with maximal ramification break 2. Thus we have $u_{L/\mathbb{Q}_2} = 3$. There

[4]This is easily checked as in the database of p-adic fields in LMFDB [LMF25].

exist only 4 possibilities of such L; L is isomorphic to one of the followings (see Table A.2).

$$M_1 = \mathbb{Q}_2[x]/(x^4+2x^2+4x+2), \qquad M_2 = \mathbb{Q}_2[x]/(x^4+2x^2+4x+10),$$
$$M_3 = \mathbb{Q}_2[x]/(x^4+4x^3+2x^2+4x+6), \qquad M_4 = \mathbb{Q}_2[x]/(x^4+4x^3+2x^2+4x+14).$$

In each case[5], we know that LF contains μ_8 by Proposition A.1 (3). Thus the claim follows.

- Suppose $L = F(\mu_4)$. We have $\rho_{E[8]} = \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix}$ on $G_{F(\mu_8)}$ by (3.6). Thus it follows from (3.8) that we have $[\mathbb{Q}_2(E[8]) : F(\mu_8)] \leq 2$, which shows $[\mathbb{Q}_2(E[8]) : \mathbb{Q}_2] \leq 16 < 32$ as desired.
- Suppose $LF \supset \mathbb{Q}_2(\mu_8)$. We have $\rho_{E[8]} = \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix}$ on G_{LF} by (3.6). Thus it follows from (3.8) that we have $[\mathbb{Q}_2(E[8]) : LF] \leq 2$, which shows $[\mathbb{Q}_2(E[8]) : \mathbb{Q}_2] \leq 16 < 32$ as desired.

Therefore, we finish the proof of the theorem. □

Remark 3.7. As we have seen in the arguments of (I) and (II) above, it holds that $E(\mathbb{Q}_2(\mu_4))_{\mathrm{tor}} \not\simeq \mathbb{Z}/2\mathbb{Z}$ and $E(\mathbb{Q}_2(\mu_8))_{\mathrm{tor}} \not\simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ for any elliptic curve E over $\mathbb{Q}_2$ with good ordinary reduction.

Next we show the first statement of Theorem 1.2 (3).

Proof of the first statement of Theorem 1.2 (3). By Fontaine's ramification bound (3.4), any element of $E(\mathbb{Q}_2(\mu_{2^\infty}))_{\mathrm{tor}}$ killed by 2^n is rational over $\mathbb{Q}_2(\mu_{n+1})$ for any n. Thus, by the second statement of Theorem 1.2 (3), which has already been proved, it suffices to show $E(\mathbb{Q}_2(\mu_{2^\infty}))[2^\infty] = E(\mathbb{Q}_2(\mu_8))[2^\infty]$ if $E(\mathbb{Q}_2(\mu_{2^\infty}))[2^\infty]$ is isomorphic to either $\mathbb{Z}/8\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/8\mathbb{Z}$. If this is the case, by Lemma 3.6 and the condition $\#E(\mathbb{Q}_2(\mu_{2^\infty}))[2^\infty] > 4$, we have $\bar{E}(\mathbb{F}_2) \simeq \mathbb{Z}/4\mathbb{Z}$. Thus the $G_{\mathbb{Q}_2}$-action on $E[4]$ is given by

$$\rho_{E[4]} = \begin{pmatrix} \chi_2 \bmod 4 & u \\ 0 & 1 \end{pmatrix} : G_{\mathbb{Q}_2} \to GL_2(\mathbb{Z}/4\mathbb{Z}) \tag{3.9}$$

for some map $u\colon G_{\mathbb{Q}_2} \to \mathbb{Z}/4\mathbb{Z}$.

First we consider the case where $E(\mathbb{Q}_2(\mu_{2^\infty}))[2^\infty] \simeq \mathbb{Z}/8\mathbb{Z}$. Since $E(\mathbb{Q}_2(\mu_{2^\infty}))[2^\infty]$ does not contain $E[2]$, it holds $u \bmod 2 \neq 0$ on G_K. In particular, $\rho_{E[4]}(G_{\mathbb{Q}_2(\mu_4)})$ is generated by $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. We assume that $\mathbb{Q}_2(E[4]) \supset \mathbb{Q}_2(\mu_8)$. If this is the case, $\rho_{E[4]}(G_{\mathbb{Q}_2(\mu_8)})$ is generated by $\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ since it is the subgroup of index 2 in $\rho_{E[4]}(G_{\mathbb{Q}_2(\mu_4)})$. Thus we see that $E(\mathbb{Q}_2(\mu_8))$ contains $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$ but this contradicts the assumption $E(\mathbb{Q}_2(\mu_{2^\infty}))[2^\infty] \simeq \mathbb{Z}/8\mathbb{Z}$. Thus we obtain $\mathbb{Q}_2(E[4]) \not\supset \mathbb{Q}_2(\mu_8)$. This is equivalent to say that $\mathbb{Q}_2(E[4]) \cap \mathbb{Q}_2(\mu_{2^\infty}) = \mathbb{Q}_2(\mu_4)$. Now we claim[6]

$$\mathbb{Q}_2(E[8]) \cap \mathbb{Q}_2(\mu_{2^\infty}) = \mathbb{Q}_2(\mu_8).$$

[5] In fact, since L contains μ_4 but does not contain μ_8, we obtain the fact that $L = M_2$.

[6] This claim follows immediately from Proposition 2.11 of [BK01]. Our proof of the claim here follows their arguments.

Consider a homomorphism $\mathrm{Gal}(\mathbb{Q}_2(E[8])/\mathbb{Q}_2) \to GL_2(\mathbb{Z}/8\mathbb{Z})$ coming from the $G_{\mathbb{Q}_2}$-action on $E[8]$. Since the restriction of this map to $\mathrm{Gal}(\mathbb{Q}_2(E[8])/\mathbb{Q}_2(E[4]))$ has values in the kernel of the mod 4 reduction $GL_2(\mathbb{Z}/8\mathbb{Z}) \to GL_2(\mathbb{Z}/4\mathbb{Z})$, it holds that the Galois group of the extension $\mathbb{Q}_2(E[8])$ over $\mathbb{Q}_2(E[4])$ is of exponent 2. Thus the Galois group of the extension $\mathbb{Q}_2(E[8]) \cap \mathbb{Q}_2(\mu_{2^\infty})$ over $\mathbb{Q}_2(E[4]) \cap \mathbb{Q}_2(\mu_{2^\infty})$ is also of exponent 2. Let $n \geq 3$ be an integer such that $\mathbb{Q}_2(E[8]) \cap \mathbb{Q}_2(\mu_{2^\infty}) = \mathbb{Q}_2(\mu_{2^n})$. By the condition $\mathbb{Q}_2(E[4]) \cap \mathbb{Q}_2(\mu_{2^\infty}) = \mathbb{Q}_2(\mu_4)$, the Galois group of the extension $\mathbb{Q}_2(E[8]) \cap \mathbb{Q}_2(\mu_{2^\infty})$ over $\mathbb{Q}_2(E[4]) \cap \mathbb{Q}_2(\mu_{2^\infty}))$ is isomorphic to $\mathbb{Z}/2^{n-2}\mathbb{Z}$. Since this is of exponent 2, we have $n = 3$. Thus the claim is now proved. Since $E(\mathbb{Q}_2(\mu_{2^\infty}))[2^\infty]$ is killed by 8, it follows from the claim that we have

$$E(\mathbb{Q}_2(\mu_{2^\infty}))[2^\infty] = E(\mathbb{Q}_2(E[8]) \cap \mathbb{Q}_2(\mu_{2^\infty}))[2^\infty] = E(\mathbb{Q}_2(\mu_8))[2^\infty]$$

as desired.

Next we consider the case where $E(\mathbb{Q}_2(\mu_{2^\infty}))[2^\infty] \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$. Assume that $E(\mathbb{Q}_2(\mu_{2^\infty}))[2^\infty] \neq E(\mathbb{Q}_2(\mu_8))[2^\infty]$. Since $\mathbb{Q}_2(E[2])$ is a subfield of $\mathbb{Q}_2(\mu_{2^\infty})$, it follows that $\mathbb{Q}_2(E[2])$ is either $\mathbb{Q}_2$ or $\mathbb{Q}_2(\mu_4)$. In particular, we have $\mathbb{Q}_2(E[2]) \subset \mathbb{Q}_2(\mu_8)$. Hence $E(\mathbb{Q}_2(\mu_8))[2^\infty]$ is isomorphic to either $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. By Remark 3.7, we have $E(\mathbb{Q}_2(\mu_8))[2^\infty] \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. However, (3.9) implies that $E(\mathbb{Q}_2(\mu_8))[4]$ must contain some element of order just 4. This is a contradiction. Therefore, we conclude $E(\mathbb{Q}_2(\mu_{2^\infty}))[2^\infty] = E(\mathbb{Q}_2(\mu_8))[2^\infty]$ as desired. □

Remark 3.8. We should note that the field $\mathbb{Q}_p(\mu_p)$ (resp. $\mathbb{Q}_2(\mu_8)$) in the first statement of Theorem 1.2 (2) (resp. Theorem 1.2 (3)) is "the best possible" in the sense that, for each odd prime p (resp. $p = 2$), there exists an elliptic cureve E over $\mathbb{Q}_p$ with good ordinary reduction such that the definition field of $E(\mathbb{Q}_p(\mu_{p^\infty}))_{\mathrm{tor}}$ is $\mathbb{Q}_p(\mu_p)$ (resp. $\mathbb{Q}_2(\mu_8)$). Examples for such situations are as follows.

- Suppose $p \geq 3$ and take an elliptic curve $\bar{E}$ such that $\bar{E}(\mathbb{F}_p) \neq 0$ (such $\bar{E}$ exists for any p). Let $E_{/\mathbb{Q}_p}$ be the canonical lift of $\bar{E}$. Then, $E[p]$ is isomorphic to $\mathbb{F}_p(1) \oplus \mathbb{F}_p$ as a $G_{\mathbb{Q}_p}$-representation (see the argument of Section 2.1.1), where $G_{\mathbb{Q}_p}$ is the absolute Galois group of $\mathbb{Q}_p$. Thus $\mathbb{Q}_p(E[p]) = \mathbb{Q}_p(\mu_p)$. On the other hand, the prime-to-p part of $E(\mathbb{Q}_p(\mu_{p^\infty}))$ coincides with that of $E(\mathbb{Q}_p)$ by the Néron-Ogg -Shafarevich criterion. Thus, the definition field of $E(\mathbb{Q}_p(\mu_{p^\infty}))_{\mathrm{tor}}$ is $\mathbb{Q}_p(\mu_p)$.
- The definition field of $E(\mathbb{Q}_2(\mu_{2^\infty}))_{\mathrm{tor}}$ for $E =$15.a7 is $\mathbb{Q}_2(\mu_8)$.

We end this section by proving Theorem 1.3.

Proof of Theorem 1.3. Since the group $E(\mathbb{Q}_2(\mu_4))_{\mathrm{tor}}$ is a subgroup of $E(\mathbb{Q}_2(\mu_{2^\infty}))_{\mathrm{tor}}$, it is isomorphic to a subgroup of the groups listed in $(I)'_\infty$. Since the kernel of the reduction map $E[2] \to \bar{E}[2]$ is rational over $\mathbb{Q}_2$, we know that $E(\mathbb{Q}_2)_{\mathrm{tor}}$ (and also $E(\mathbb{Q}_2(\mu_4))_{\mathrm{tor}}$) are not zero. Furthermore, by Remark 3.7, we also have $E(\mathbb{Q}_2(\mu_4))_{\mathrm{tor}} \not\simeq \mathbb{Z}/2\mathbb{Z}$. On the other hand, for each group $G_{i,j}$ in $(I)'_2$, MAGMA computations with Algorithm A.1 give examples of E such that $E(\mathbb{Q}_2(\mu_4))_{\mathrm{tor}} \simeq G_{i,j}$ as follows.

- $E =$15.a1 satisfies $E(\mathbb{Q}_2(\mu_4))_{\mathrm{tor}} \simeq G_{1,4}$,
- $E =$33.a2 satisfies $E(\mathbb{Q}_2(\mu_4))_{\mathrm{tor}} \simeq G_{2,1}$,

- E =15.a2 satisfies $E(\mathbb{Q}_2(\mu_4))_{\mathrm{tor}} \simeq G_{2,2}$,
- E =15.a8 satisfies $E(\mathbb{Q}_2(\mu_4))_{\mathrm{tor}} \simeq G_{2,4}$,
- E =15.a5 satisfies $E(\mathbb{Q}_2(\mu_4))_{\mathrm{tor}} \simeq G_{4,1}$.

Therefore, to finish the proof of the theorem, it suffices to show that $E(\mathbb{Q}_2(\mu_4))_{\mathrm{tor}}$ is not isomorphic to $G_{1,8} = \mathbb{Z}/8\mathbb{Z}$. Assume $E(\mathbb{Q}_2(\mu_4))_{\mathrm{tor}} \simeq \mathbb{Z}/8\mathbb{Z}$. By Theorem 1.2 (3), $E(\mathbb{Q}_2(\mu_8))_{\mathrm{tor}}$ is isomorphic to $\mathbb{Z}/8\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$. By assumption, we have $E(\mathbb{Q}_2(\mu_4))_{\mathrm{tor}} \not\supset E[2]$ and thus $\mathbb{Q}_2(E[2])$ is not contained in $\mathbb{Q}_2(\mu_4)$. Since the extension $\mathbb{Q}_2(E[2])/\mathbb{Q}_2$ is of degree at most 2 and $u_{\mathbb{Q}_2(E[2])/\mathbb{Q}_2} \leq 2$, it holds that $\mathbb{Q}_2(E[2])$ is F or L_2 (see Table A.1). In both cases, $\mathbb{Q}_2(E[2])$ is not a subfield of $\mathbb{Q}_2(\mu_8)$. Thus $E(\mathbb{Q}_2(\mu_8))_{\mathrm{tor}}$ does not contain $E[2]$. Therefore, we obtain

$$E(\mathbb{Q}_2(\mu_4))_{\mathrm{tor}} = E(\mathbb{Q}_2(\mu_8))_{\mathrm{tor}} \simeq \mathbb{Z}/8\mathbb{Z}.$$

Let $\chi\colon G_{\mathbb{Q}_2} \to \mathbb{Z}_2^\times$ and $\psi\colon G_{\mathbb{Q}_2} \to \mathbb{Z}_2^\times$ be the crystalline characters obtained by the $G_{\mathbb{Q}_2}$-action on the 2-adic Tate modules $T_2(\hat{E})$ and $T_2(\bar{E})$, respectively. Consider the $G_{\mathbb{Q}_2}$-action on $E[8]$. Identifying $E[8] = \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ by a suitable choice of $\mathbb{Z}/8\mathbb{Z}$-basis of $E[8]$, the $G_{\mathbb{Q}_2}$-action on $E[8]$ is given by a continuous homomorphism $\rho_{E[8]}\colon G_{\mathbb{Q}_2} \to GL_2(\mathbb{Z}/8\mathbb{Z})$ with the matrix form

$$\rho_{E[8]} = \begin{pmatrix} \chi \bmod 8 & u \\ 0 & \psi \bmod 8 \end{pmatrix} \tag{3.10}$$

for some map $u\colon G_{\mathbb{Q}_2} \to \mathbb{Z}/8\mathbb{Z}$. Let us study subgroups $\rho_{E[8]}(G_{\mathbb{Q}_2(\mu_8)})$ and $\rho_{E[8]}(G_{\mathbb{Q}_2(\mu_4)})$ of $GL_2(\mathbb{Z}/8\mathbb{Z})$. Since we have $\bar{E}(\mathbb{F}_2) \simeq \mathbb{Z}/4\mathbb{Z}$ by Lemma 3.6, the image of ψ mod 8 on $G_{\mathbb{Q}_2}$ is $\{1, 5\} \subset (\mathbb{Z}/8\mathbb{Z})^\times$. In particular, ψ mod 8 is an unramified character with kernel G_F. Since $\chi\psi$ mod 8 is trivial on $G_{\mathbb{Q}_2(\mu_8)}$, we see $\chi \equiv \psi$ mod 8 on $G_{\mathbb{Q}_2(\mu_8)}$. We find that $\rho_{E[8]}(G_{\mathbb{Q}_2(\mu_8)})$ is a subgroup of

$$H := \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \mid a = 1, 5 \in \mathbb{Z}/8\mathbb{Z} \text{ and } b \in \mathbb{Z}/8\mathbb{Z} \right\}$$

The order of the group H is 16. We note that u mod 2 is not trivial on $G_{\mathbb{Q}_2(\mu_8)}$ since $E(\mathbb{Q}_2(\mu_8))_{\mathrm{tor}}$ does not contain $E[2]$. Thus there exist $a \in \mathbb{Z}/8\mathbb{Z}$ and an odd $b \in \mathbb{Z}/8\mathbb{Z}$ such that $\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \in \rho_{E[8]}(G_{\mathbb{Q}_2(\mu_8)})$. Since the group generated by such a matrix $\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}$ is either the group H_1 generated by $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ or the group H_2 generated by $\begin{pmatrix} 5 & 1 \\ 0 & 5 \end{pmatrix}$, we find that $\rho_{E[8]}(G_{\mathbb{Q}_2(\mu_8)})$ is either H_1, H_2 or H. By the facts that ψ mod 8 is not trivial on $G_{\mathbb{Q}_2(\mu_8)}$ and $E(\mathbb{Q}_2(\mu_8))_{\mathrm{tor}} \simeq \mathbb{Z}/8\mathbb{Z}$, we obtain that $\rho_{E[8]}(G_{\mathbb{Q}_2(\mu_8)})$ is not equal to H_1 and H, that is,

$$\rho_{E[8]}(G_{\mathbb{Q}_2(\mu_8)}) = H_2 = \langle \begin{pmatrix} 5 & 1 \\ 0 & 5 \end{pmatrix} \rangle \tag{3.11}$$

and $E(\mathbb{Q}_2(\mu_8))[2^\infty] = \langle \begin{pmatrix} 1 \\ 4 \end{pmatrix} \rangle$. Next we consider $\rho_{E[8]}(G_{\mathbb{Q}_2(\mu_4)})$. We find that $\rho_{E[8]}(G_{\mathbb{Q}_2(\mu_4)})$ is a subgroup of

$$G := \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, c = 1, 5 \in \mathbb{Z}/8\mathbb{Z} \text{ and } b \in \mathbb{Z}/8\mathbb{Z} \right\}$$

by (3.10) and the fact that ψ and χ_2 on $G_{\mathbb{Q}_2(\mu_4)}$ have values in $\{1,5\} \subset (\mathbb{Z}/8\mathbb{Z})^\times$. The order of the group G is 32. We see that $\rho_{E[8]}(G_{\mathbb{Q}_2(\mu_8)})$ is a normal subgroup of G, the quotient $G/\rho_{E[8]}(G_{\mathbb{Q}_2(\mu_8)})$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and $G/\rho_{E[8]}(G_{\mathbb{Q}_2(\mu_8)})$ is generated by the classes with respect to $\begin{pmatrix} 5 & 0 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ 0 & 5 \end{pmatrix}$. Since the quotient $\rho_{E[8]}(G_{\mathbb{Q}_2(\mu_4)})/\rho_{E[8]}(G_{\mathbb{Q}_2(\mu_8)})$ is a subgroup of $G/\rho_{E[8]}(G_{\mathbb{Q}_2(\mu_8)})$ of order 2, we find that $\rho_{E[8]}(G_{\mathbb{Q}_2(\mu_4)})$ is one of the following groups;

$$\langle \begin{pmatrix} 5 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 5 & 1 \\ 0 & 5 \end{pmatrix} \rangle, \quad \langle \begin{pmatrix} 1 & 0 \\ 0 & 5 \end{pmatrix}, \begin{pmatrix} 5 & 1 \\ 0 & 5 \end{pmatrix} \rangle, \quad \langle \begin{pmatrix} 5 & 0 \\ 0 & 5 \end{pmatrix}, \begin{pmatrix} 5 & 1 \\ 0 & 5 \end{pmatrix} \rangle.$$

Since we now have $E(\mathbb{Q}_2(\mu_4))[2^\infty] = E(\mathbb{Q}_2(\mu_8))[2^\infty] = \langle \begin{pmatrix} 1 \\ 4 \end{pmatrix} \rangle$, we find

$$\rho_{E[8]}(G_{\mathbb{Q}_2(\mu_4)}) = \langle \begin{pmatrix} 1 & 0 \\ 0 & 5 \end{pmatrix}, \begin{pmatrix} 5 & 1 \\ 0 & 5 \end{pmatrix} \rangle. \tag{3.12}$$

It follows from (3.11) and (3.12) that there exists $\sigma_0 \in G_{\mathbb{Q}_2(\mu_4)} \setminus G_{\mathbb{Q}_2(\mu_8)}$ such that $\rho_{E[8]}(\sigma_0) = \begin{pmatrix} 1 & 0 \\ 0 & 5 \end{pmatrix}$. Since $\psi(\sigma_0) \equiv 5 \bmod 8$, we have

$$\sigma_0 \notin G_F. \tag{3.13}$$

On the other hand, as we have already checked, the field $\mathbb{Q}_2(E[2])$ is either F or L_2 (see Table A.1). In each case, $\mathbb{Q}_2(E[2], \mu_4)$ contains F by Proposition A.1 (1). Since $\rho_{E[8]}(\sigma_0) \bmod 2$ is trivial, we have $\sigma_0 \in G_{\mathbb{Q}_2(E[2])}$, which gives $\sigma_0 \in G_{\mathbb{Q}_2(E[2])} \cap G_{\mathbb{Q}_2(\mu_4)} \subset G_F$. This contradicts (3.13). Therefore, we conclude $E(\mathbb{Q}_2(\mu_4)) \not\simeq \mathbb{Z}/8\mathbb{Z}$ as desired and this finishes the proof. □

A Appendix : Data and algorithm

In this section, we present the data obtained by using the computer algebra system MAGMA [BC06].

A.1 Quadratic and quartic extensions of $\mathbb{Q}_2$

In this subsection, we give the tables of quadratic and certain quartic extensions of $\mathbb{Q}_2$ for using to our proof in subsection 3.2. They can be easily checked by LMFDB database [LMF25]. Tabel A.1 shows the defining polynomials for all the quadratic extensions of $\mathbb{Q}_2$. Tabel A.2 shows the defining polynomials for all the quartic extensions $L/\mathbb{Q}_2$ with $u_{L/\mathbb{Q}_2} = 3$. In these tables, the integer f presents the inertia degree, e the ramification index, $u_{L/\mathbb{Q}_2}$ the maximal upper ramification break and μ_n the roots of unity which are included in L.

L	Polynomial	f	e	$u_{L/\mathbb{Q}_2}$	μ_n
F	x^2+x+1	2	1	0	μ_6
L_1	x^2+2x+2	1	2	2	μ_4
L_2	x^2+2x+6	1	2	2	μ_2
L_3	x^2+2	1	2	3	μ_2
L_4	x^2+10	1	2	3	μ_2
L_5	x^2+4x+2	1	2	3	μ_2
L_6	$x^2+4x+10$	1	2	3	μ_2

Table A.1: The quadratic extensions of $\mathbb{Q}_2$

L	Polynomial	f	e	$u_{L/\mathbb{Q}_2}$	μ_n
M_1	x^4+2x^2+4x+2	1	4	3	μ_8
M_2	$x^4+2x^2+4x+10$	1	4	3	μ_4
M_3	$x^4+4x^3+2x^2+4x+6$	1	4	3	μ_2
M_4	$x^4+4x^3+2x^2+4x+14$	1	4	3	μ_2

Table A.2: The quartic Galois extensions of $\mathbb{Q}_2$ with $u_{L/\mathbb{Q}_2}=3$

We can easily check the equalities of the composite fields by using MAGMA as follows:

Proposition A.1. *In Table A.1 and A.2, we have the equalities:*

(1) $L_1L_2 = F(\mu_4)$.

(2) $L_3F(\mu_4) = L_4F(\mu_4) = L_5F(\mu_4) = L_6F(\mu_4) = F(\mu_8)$.

(3) $FM_1 = FM_2 = FM_3 = FM_4 = F(\mu_8)$.

A.2 Algorithm for computing $\#E(K)[n]$

In this subsection, we give an algorithm for calculating the order $\#E(K)[n]$ for given K, E and n, where K is a finite extension of $\mathbb{Q}_p$, E is an elliptic curve over K and $n>1$ is an integer. In the case where K is an algebraic number filed, we can compute the torsion subgroup $E(K)_{\mathrm{tor}}$ by the intrinsic function `TorsionSubgroup`(E) which is implemented in MAGMA. However, this intrinsic function is not valid for a p-adic field K. In spite of such a function, we use the several functions that they are implemented in MAGMA and valid even for a p-adic field. First, the function `DivisionPolynomial`(E,n) gives a polynomial whose roots are the x-coordinates of the points of $E(K)[n]$ for a p-adic field K, an elliptic curve E and an integer $n>1$. Second, the function `Roots`(f) gives the roots of a given polynomial f over K. Finally, the function `Points`$(E(K),x_0)$ gives the points of E whose x-coordinate equals x_0. By combining these functions, we can compute the order $\#E(K)[n]$ as follows:

Algorithm A.1 Calculate $\#E(K)[n]$

Require: $n > 1$, K, E
Ensure: $t = \#E(K)[n]$
  $t \leftarrow 1$
  $f \leftarrow \texttt{DivisionPolynomial}(E, n)$
  $R \leftarrow \texttt{Roots}(f, K)$
  $r \leftarrow \#R$
  if $r \neq 0$ **then**
    for $x \in R$ **do**
      $t \leftarrow t + \#\texttt{Points}(E(K), x)$
    end for
  end if
  return t

A.3 List of torsion subgroups

In this subsection, we give a list of possible candidates that they actually occur for torsion subgroups of $E(\mathbb{Q}_p)$ and $E(\mathbb{Q}_p(\mu_{p^\infty}))$. In each list, we use Cremona's database of elliptic curves. Hence the label of each elliptic curve is presented as Cremona label, which is different from the one used in LMFDB. We use Algorithm A.1 which can compute $\#E(K)[n]$ for given K, E and $n > 1$. As in the proof of Theorem 1.2, it is enough to compute $E(\mathbb{Q}_p(\mu_p))$ (resp. $E(\mathbb{Q}_2(\mu_{16}))$) instead of computing $E(\mathbb{Q}_p(\mu_{p^\infty}))$ for an odd prime p (resp. for $p = 2$)[7].

$E(\mathbb{Q}_2)$	Label
$G_{1,2}$	15a5
$G_{1,4}$	15a7
$G_{1,8}$	15a4
$G_{2,1}$	15a2
$G_{2,2}$	15a1

$E(\mathbb{Q}_3)$	Label
$G_{1,1}$	26a2
$G_{1,2}$	14a3
$G_{1,3}$	26a1
$G_{1,5}$	11a1
$G_{1,6}$	14a1

$E(\mathbb{Q}_5)$	Label
$G_{1,1}$	11a2
$G_{1,2}$	38b2
$G_{1,3}$	19a1
$G_{1,4}$	39a2
$G_{1,5}$	11a1
$G_{1,7}$	26b1
$G_{1,8}$	17a3
$G_{1,9}$	26a1
$G_{1,10}$	38b1
$G_{2,1}$	39a1
$G_{2,2}$	17a1

$E(\mathbb{Q}_7)$	Label
$G_{1,1}$	26b2
$G_{1,3}$	104a1
$G_{1,4}$	17a1
$G_{1,5}$	38b1
$G_{1,6}$	20a1
$G_{1,7}$	26b1
$G_{1,9}$	19a2
$G_{1,10}$	11a1
$G_{1,11}$	75a1
$G_{1,12}$	30a1
$G_{1,13}$	57a1
$G_{2,1}$	17a2
$G_{2,3}$	30a2
$G_{3,1}$	19a1

Table A.3: Examples of $E(\mathbb{Q}_p)_{\mathrm{tor}}$ with good ordinary reduction

[7] In case $p = 2$, we actually have $E(\mathbb{Q}_2(\mu_{2^\infty}))_{\mathrm{tor}} = E(\mathbb{Q}_2(\mu_8))_{\mathrm{tor}}$, as stated in Theorem 1.2.

$E(\mathbb{Q}_2)$	Label
$G_{1,1}$	67a1
$G_{1,3}$	19a1
$G_{1,5}$	11a1

$E(\mathbb{Q}_3)$	Label
$G_{1,1}$	140b1
$G_{1,4}$	17a1
$G_{2,1}$	17a2
$G_{1,7}$	26b1

$E(\mathbb{Q}_5)$	Label
$G_{1,6}$	14a1

$E(\mathbb{Q}_7)$	Label
$G_{1,8}$	15a4
$G_{2,2}$	15a1

Table A.4: Examples of $E(\mathbb{Q}_p)_{\mathrm{tor}}$ with good supersingular reduction

$E(\mathbb{Q}_2(\mu_{2^\infty}))$	Label
$G_{1,4}$	33a3
$G_{1,8}$	15a5
$G_{2,1}$	33a1
$G_{2,4}$	15a2
$G_{4,1}$	15a1

$E(\mathbb{Q}_3(\mu_{3^\infty}))$	Label
$G_{1,2}$	56b1
$G_{1,3}$	26a2
$G_{1,5}$	11a1
$G_{1,6}$	14a3
$G_{3,1}$	26a1
$G_{3,2}$	14a1

$E(\mathbb{Q}_5(\mu_{5^\infty}))$	Label
$G_{1,2}$	46a1
$G_{1,3}$	19a1
$G_{1,4}$	39a2
$G_{1,5}$	11a2
$G_{1,7}$	26b1
$G_{1,8}$	17a3
$G_{1,9}$	26a1
$G_{1,10}$	38b2
$G_{2,1}$	39a1
$G_{2,2}$	17a1
$G_{5,1}$	11a1
$G_{5,2}$	38b1

$E(\mathbb{Q}_7(\mu_{7^\infty}))$	Label
$G_{1,3}$	104a1
$G_{1,4}$	17a1
$G_{1,5}$	38b1
$G_{1,6}$	20a1
$G_{1,7}$	26b2
$G_{1,9}$	19a2
$G_{1,10}$	11a1
$G_{1,11}$	75a1
$G_{1,12}$	30a1
$G_{1,13}$	57a1
$G_{2,1}$	17a2
$G_{2,3}$	30a2
$G_{3,1}$	19a1
$G_{7,1}$	26b1

Table A.5: Examples of $E(\mathbb{Q}_p(\mu_{p^\infty}))_{\mathrm{tor}}$ with good ordinary reduction

$E(\mathbb{Q}_2(\mu_4))$	Label
$G_{1,4}$	15a5
$G_{2,1}$	33a1
$G_{2,2}$	15a2
$G_{2,4}$	15a4
$G_{4,1}$	15a1

Table A.6: Examples of $E(\mathbb{Q}_2(\mu_4))_{\mathrm{tor}}$ with good ordinary reduction

$E(\mathbb{Q}_2(\mu_{2^\infty}))$	Label	$E(\mathbb{Q}_5(\mu_{5^\infty}))$	Label
$G_{1,1}$	67a1	$G_{1,6}$	14a1
$G_{1,3}$	19a1		
$G_{1,5}$	11a1		
$E(\mathbb{Q}_3(\mu_{3^\infty}))$	Label	$E(\mathbb{Q}_7(\mu_{7^\infty}))$	Label
$G_{1,1}$	140b1	$G_{1,8}$	15a4
$G_{1,4}$	17a1	$G_{2,2}$	15a1
$G_{2,1}$	17a2		
$G_{1,7}$	26b1		

Table A.7: Examples of $E(\mathbb{Q}_p(\mu_{p^\infty}))_{\mathrm{tor}}$ with good supersingular reduction

References

[BC06] Wieb Bosma and John Cannon, editors. *Discovering mathematics with Magma*, volume 19 of *Algorithms and Computation in Mathematics*. Springer-Verlag, Berlin, 2006. Reducing the abstract to the concrete.

[BK01] Armand Brumer and Kenneth Kramer. Non-existence of certain semistable abelian varieties. *Manuscripta Math.*, 106(3):291–304, 2001.

[BPS12] William D. Banks, Francesco Pappalardi, and Igor E. Shparlinski. On group structures realized by elliptic curves over arbitrary finite fields. *Exp. Math.*, 21(1):11–25, 2012.

[Cho19] Michael Chou. Torsion of rational elliptic curves over the maximal abelian extension of $\mathbb{Q}$. *Pacific J. Math.*, 302(2):481–509, 2019.

[Con11] Brian Conrad. Lifting global representations with local properties. *preprint, available at* `http://math.stanford.edu/~conrad/papers/locchar.pdf`, 2011.

[DEvH+21] Maarten Derickx, Anastassia Etropolski, Mark van Hoeij, Jackson S. Morrow, and David Zureick-Brown. Sporadic cubic torsion. *Algebra Number Theory*, 15(7):1837–1864, 2021.

[DW08] Chantal David and Tom Weston. Local torsion on elliptic curves and the deformation theory of Galois representations. *Math. Res. Lett.*, 15(3):599–611, 2008.

[Fon85] Jean-Marc Fontaine. Il n'y a pas de variété abélienne sur $\mathbf{Z}$. *Invent. Math.*, 81(3):515–538, 1985.

[Fon94a] Jean-Marc Fontaine. Le corps des périodes p-adiques. Number 223, pages 59–111. 1994. With an appendix by Pierre Colmez, Périodes p-adiques (Bures-sur-Yvette, 1988).

[Fon94b] Jean-Marc Fontaine. Représentations p-adiques semi-stables. Number 223, pages 113–184. 1994. With an appendix by Pierre Colmez, Périodes p-adiques (Bures-sur-Yvette, 1988).

[GV23] Tomislav Gužvić and Borna Vukorepa. Torsion groups of elliptic curves over $\mathbb{Q}(\mu_{p^\infty})$. *Int. J. Number Theory*, 19(8):1745–1761, 2023.

[Kam92] S. Kamienny. Torsion points on elliptic curves and q-coefficients of modular forms. *Invent. Math.*, 109(2):221–229, 1992.

[KM88] M. A. Kenku and F. Momose. Torsion points on elliptic curves defined over quadratic fields. *Nagoya Math. J.*, 109:125–149, 1988.

[LMF25] The LMFDB Collaboration. The L-functions and modular forms database. `https://www.lmfdb.org`, 2025. [Online; accessed 13 April 2025].

[Maz78] B. Mazur. Rational isogenies of prime degree (with an appendix by D. Goldfeld). *Invent. Math.*, 44(2):129–162, 1978.

[Mer96] Loïc Merel. Bornes pour la torsion des courbes elliptiques sur les corps de nombres. *Invent. Math.*, 124(1-3):437–449, 1996.

[Oze24] Yoshiyasu Ozeki. Explicit bounds on torsion of CM abelian varieties over p-adic fields with values in Lubin-Tate extensions. *Pacific J. Math.*, 330(1):171–197, 2024.

[Ser68] Jean-Pierre Serre. *Corps locaux*, volume No. VIII of *Publications de l'Université de Nancago*. Hermann, Paris, 1968. Deuxième édition.

[Ser72] Jean-Pierre Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.*, 15(4):259–331, 1972.

[Ser98] Jean-Pierre Serre. *Abelian l-adic representations and elliptic curves*, volume 7 of *Research Notes in Mathematics*. A K Peters, Ltd., Wellesley, MA, 1998. With the collaboration of Willem Kuyk and John Labute, Revised reprint of the 1968 original.

[Sil09] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.