TORSION GROUPS OF ELLIPTIC CURVES OVER SOME INFINITE ABELIAN EXTENSIONS OF $\mathbb{Q}$

TOMISLAV GUŽVIĆ AND IVAN KRIJAN

ABSTRACT. We determine, for an elliptic curve $E/\mathbb{Q}$, all the possible torsion groups $E(\mathcal{K})_{\text{tors}}$, where $\mathcal{K}$ is the compositum of all $\mathbb{Z}_p$-extensions of $\mathbb{Q}$. Furthermore, we prove that for an elliptic curve $E/\mathbb{Q}$ it holds that $E(\mathbb{Q}(\mu_{p^\infty}))_{\text{tors}} = E(\mathbb{Q}(\mu_p))_{\text{tors}}$, for all primes $p \geq 5$ and $E(\mathbb{Q}(\mu_{3^\infty}))_{\text{tors}} = E(\mathbb{Q}(\mu_{3^3}))_{\text{tors}}$, $E(\mathbb{Q}(\mu_{2^\infty}))_{\text{tors}} = E(\mathbb{Q}(\mu_{2^4}))_{\text{tors}}$.

1. INTRODUCTION

For a prime number p, denote by $\mathbb{Q}_{\infty,p}$ the unique $\mathbb{Z}_p$-extension of $\mathbb{Q}$, and for a positive integer n, denote by $\mathbb{Q}_{n,p}$ the nth layer of $\mathbb{Q}_{\infty,p}$, i.e. the unique subfield of $\mathbb{Q}_{\infty,p}$ such that $\text{Gal}\,(\mathbb{Q}_{n,p}/\mathbb{Q}) \simeq \mathbb{Z}/p^n\mathbb{Z}$. Recall that the $\mathbb{Z}_p$-extension of $\mathbb{Q}$ is the unique Galois extension $\mathbb{Q}_{\infty,p}$ of $\mathbb{Q}$ such that

$$\text{Gal}\,(\mathbb{Q}_{\infty,p}/\mathbb{Q}) \simeq \mathbb{Z}_p,$$

where $\mathbb{Z}_p$ is the additive group of the p-adic integers and is constructed as follows. Let

$$G = \text{Gal}\,(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q}) = \varprojlim_n \text{Gal}\,(\mathbb{Q}(\zeta_{p^{n+1}})/\mathbb{Q}) \overset{\sim}{\to} \varprojlim_n (\mathbb{Z}/p^{n+1}\mathbb{Z})^\times = \mathbb{Z}_p^\times.$$

Here we know that $G = \Delta \times \Gamma$, where $\Gamma \simeq \mathbb{Z}_p$ and $\Delta \simeq \mathbb{Z}/(p-1)\mathbb{Z}$ for $p \geq 3$ and $\Delta \simeq \mathbb{Z}/2\mathbb{Z}$ (generated by complex conjugation) for $p = 2$, so we define

$$\mathbb{Q}_{\infty,p} := \mathbb{Q}(\zeta_{p^\infty})^\Delta.$$

We also see that every layer is uniquely determined by

$$\mathbb{Q}_{n,p} = \mathbb{Q}(\zeta_{p^{n+1}})^\Delta,$$

so for $p \geq 3$ it is the unique subfield of $\mathbb{Q}(\zeta_{p^{n+1}})$ of degree p^n over $\mathbb{Q}$. More details and proofs of these facts about $\mathbb{Z}_p$-extensions and Iwasawa theory can be found in [20, Chapter 13].

Iwasawa theory for elliptic curves (see [8]) studies elliptic curves in $\mathbb{Z}_p$-extensions, in particular the growth of the rank and n-Selmer groups in the layers of the $\mathbb{Z}_p$-extensions.

In the paper [3] we can find completely solved problem of determining how the torsion of an elliptic curve defined over $\mathbb{Q}$ grows in the $\mathbb{Z}_p$-extensions of $\mathbb{Q}$. In this paper we go a step further.

Let $\mathcal{K}_{\geq 5}$ be the compositum of all $\mathbb{Z}_p$-extensions of $\mathbb{Q}$, for $p \geq 5$, i.e.

$$\mathcal{K}_{\geq 5} = \prod_{p \geq 5 \text{ prime}} \mathbb{Q}_{\infty,p}$$

and let $\mathcal{K}$ be the compositum of all $\mathbb{Z}_p$-extensions of $\mathbb{Q}$, i.e.

$$\mathcal{K} = \prod_{p \text{ prime}} \mathbb{Q}_{\infty,p}.$$

Our results are the following.

Theorem 1.1. *Let $E/\mathbb{Q}$ be an elliptic curve, then*

$$E(\mathcal{K}_{\geq 5})_{tors} = E(\mathbb{Q})_{tors}.$$

Theorem 1.2. *Let $E/\mathbb{Q}$ be an elliptic curve, then $E(\mathcal{K})_{tors}$ is exactly one of the following groups:*

$$\mathbb{Z}/n\mathbb{Z}, \quad 1 \leq n \leq 10 \text{ or } n \in \{12, 13, 21, 27\},$$
$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, \quad 1 \leq n \leq 4.$$

For each group G from the list above there exists an $E/\mathbb{Q}$ such that $E(\mathcal{K})_{tors} \simeq G$.

Remark. By Mazur's theorem [15] we see that

$$\{E(\mathcal{K})_{\text{tors}} : E/\mathbb{Q} \text{ elliptic curve}\} = \{E(\mathbb{Q})_{\text{tors}} : E/\mathbb{Q} \text{ elliptic curve}\} \cup \{\mathbb{Z}/13\mathbb{Z}, \mathbb{Z}/21\mathbb{Z}, \mathbb{Z}/27\mathbb{Z}\}.$$

However, there are many elliptic curves $E/\mathbb{Q}$ for which torsion grows from $\mathbb{Q}$ to $\mathcal{K}$. In [3] one can find many examples of torsion growth $\mathbb{Q} \to \mathbb{Q}_{\infty,2}$ and $\mathbb{Q} \to \mathbb{Q}_{\infty,3}$. Same examples apply here. At the and of the proof of the Theorem 1.2 (more precisely, in the Lemma 4.10) we show that there are some elliptic curves $E/\mathbb{Q}$ such that $E(\mathcal{K})_{\text{tors}} \simeq \mathbb{Z}/13\mathbb{Z}$.

Furthermore, let μ_n be the set of all complex numbers ω such that $\omega^n = 1$. Note that for a prime number p we have that $\mathbb{Q}(\mu_p) = \mathbb{Q}(\zeta_p)$, where ζ_p is, as usual, p^{th} primitive root of unity.

For a prime number p, we define a set μ_{p^∞} as the set of all complex numbers ω for which there exists non-negative integer k such that $\omega^{p^k} = 1$. Note that $\mathbb{Q}(\mu_{p^\infty})$ is the set $\mathbb{Q}$ extended with all $p^{n^{\text{th}}}$ primitive roots of unity.

Theorem 1.3. *Let $E/\mathbb{Q}$ be an elliptic curve, then for a prime number $p \geq 5$ it holds that*

$$E(\mathbb{Q}(\mu_{p^\infty}))_{tors} = E(\mathbb{Q}(\mu_p))_{tors}.$$

Furthermore,

$$E(\mathbb{Q}(\mu_{3^\infty}))_{tors} = E(\mathbb{Q}(\mu_{3^3}))_{tors} \qquad and \qquad E(\mathbb{Q}(\mu_{2^\infty}))_{tors} = E(\mathbb{Q}(\mu_{2^4}))_{tors}.$$

Remark. This situation is "the best possible". For $E = 27a4$ (Cremona reference from [19]) we have that

$$E(\mathbb{Q}(\mu_{3^2}))_{\text{tors}} = \mathbb{Z}/9\mathbb{Z} \subsetneq \mathbb{Z}/27\mathbb{Z} = E(\mathbb{Q}(\mu_{3^3}))_{\text{tors}}$$

and for $E = 32a4$ it holds that

$$E(\mathbb{Q}(\mu_{2^3}))_{\text{tors}} = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \subsetneq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z} = E(\mathbb{Q}(\mu_{2^4}))_{\text{tors}}.$$

2. NOTATION AND AUXILIARY RESULTS

In this paper we deal with elliptic curves defined over $\mathbb{Q}$, so unless noted otherwise, all elliptic curves will be assumed to be defined over $\mathbb{Q}$.

We will use standard notation regarding Galois representations attached to elliptic curves throughout the paper following [18]. More details can be found in [3, §2].

To make this paper as self-contained as reasonably possible, we now list the most important known results that we will use.

Firstly, we state main results from [3]:

Theorem 2.1. *Let $p \geq 5$ be a prime number, and $E/\mathbb{Q}$ an elliptic curve. Then*

$$E(\mathbb{Q}_{\infty,p})_{tors} = E(\mathbb{Q})_{tors}.$$

Theorem 2.2. *Let $E/\mathbb{Q}$ be an elliptic curve. $E(\mathbb{Q}_{\infty,2})_{tors}$ is exactly one of the following groups:*

$$\mathbb{Z}/N\mathbb{Z}, \quad 1 \leq N \leq 10, \text{ or } N = 12,$$
$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N\mathbb{Z}, \quad 1 \leq N \leq 4,$$

Theorem 2.3. *Let $E/\mathbb{Q}$ be an elliptic curve. $E(\mathbb{Q}_{\infty,3})_{tors}$ is exactly one of the following groups:*

$$\mathbb{Z}/N\mathbb{Z}, \quad 1 \leq N \leq 10, \text{ or } N = 12, 21 \text{ or } 27,$$
$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N\mathbb{Z}, \quad 1 \leq N \leq 4.$$

and for each group G from the list above there exists an $E/\mathbb{Q}$ such that $E(\mathbb{Q}_{\infty,3})_{tors} \simeq G$.

Furthermore, we state known results that we will be using through this paper. Most of these results are stated in [3], but we will state them here also (although without the proofs), for the sake of completeness.

Proposition 2.4. [18, Ch. III, Cor. 8.1.1] *Let E/L be an elliptic curve with $L \subseteq \overline{\mathbb{Q}}$. For each integer $n \geq 1$, if $E[n] \subseteq E(L)$ then the nth cyclotomic field $\mathbb{Q}(\zeta_n)$ is a subfield of L.*

An immediate consequence of this proposition is

Corollary 2.5. *Let p and q be odd prime numbers. Then*

$$E(\mathbb{Q}_{\infty,p})[q] \simeq \{O\} \quad or \quad \mathbb{Z}/q\mathbb{Z}.$$

Remark. We have that $E[q^n] \nsubseteq E(\mathbb{Q}_{\infty,p})$, for each positive integer n.

Lemma 2.6. [4, Lemma 4.6] *Let E be an elliptic curve over a number field K, let F be a Galois extension of $\mathbb{Q}$, let p be a prime, and let k be the largest integer for which $E[p^k] \subseteq E(F)$. If $E(F)_{tors}$ contains a subgroup isomorphic to $\mathbb{Z}/p^k\mathbb{Z} \oplus \mathbb{Z}/p^j\mathbb{Z}$ with $j \geq k$, then E admits a K-rational p^{j-k}-isogeny.*

Theorem 2.7. [15, 10, 12, 11, 13] *Let $E/\mathbb{Q}$ be an elliptic curve with a rational n-isogeny. Then*

$$n \leq 19 \text{ or } n \in \{21, 25, 27, 37, 43, 67, 163\}.$$

Corollary 2.8. *Let p be an odd prime number, $E/\mathbb{Q}$ elliptic curve and $P \in E(\mathbb{Q}_{\infty,p})_{tors}$ a point of order q^n for some prime q and positive integer n, then*

$$q^n \in \{2, 3, 4, 5, 7, 8, 9, 11, 13, 16, 17, 19, 25, 27, 32, 37, 43, 67, 163\}.$$

Theorem 2.9. [7, Theorem 5.7] *Let $E/\mathbb{Q}$ be an elliptic curve, p a prime and P a point of order p on E. Then all of the cases in the table below occur for $p \leq 13$ or $p = 37$, and they are the only ones possible.*

p	$[\mathbb{Q}(P) : \mathbb{Q}]$
2	$1, 2, 3$
3	$1, 2, 3, 4, 6, 8$
5	$1, 2, 4, 5, 8, 10, 16, 20, 24$
7	$1, 2, 3, 6, 7, 9, 12, 14, 18, 21, 24, 36, 42, 48$
11	$5, 10, 20, 40, 55, 80, 100, 110, 120$
13	$3, 4, 6, 12, 24, 39, 48, 52, 72, 78, 96, 144, 156, 168$
37	$12, 36, 72, 444, 1296, 1332, 1368$

For all other p, for $[\mathbb{Q}(P) : \mathbb{Q}]$ the following cases do occur:

(1) $p^2 - 1$,   *for all p,*

(2) $8,\ 16,\ 32,\ 136,\ 256,\ 272,\ 288,$ *for $p = 17$,*

(3) $\dfrac{p-1}{2},\ p-1,\ \dfrac{p(p-1)}{2},\ p(p-1),$ *if $p \in \{19, 43, 67, 163\}$,*

(4) $2(p-1),\ (p-1)^2,$ *if $p \equiv 1 \pmod{3}$ or $\left(\frac{-D}{p}\right) = 1$,*
                                       for some $D \in \{1, 2, 7, 11, 19, 43, 67, 163\}$,

(5) $\dfrac{(p-1)^2}{3},\ \dfrac{2(p-1)^2}{3},$ *if $p \equiv 4, 7 \pmod{9}$,*

(6) $\dfrac{p^2-1}{3},\ \dfrac{2(p^2-1)}{3},$ *if $p \equiv 2, 5 \pmod{9}$,*

Apart from the cases above that have been proven to appear, the only other options that might be possible are:

$$\frac{p^2-1}{3},\ \frac{2(p^2-1)}{3}, \quad \text{for } p \equiv 8 \pmod{9}.$$

Theorem 2.10. [7, Theorem 7.2.] *Let p be the smallest prime divisor of a positive integer d and let $K/\mathbb{Q}$ be a number field of degree d.*

- *If $p \geq 11$, then $E(K)_{tors} = E(\mathbb{Q})_{tors}$.*
- *If $p = 7$, then $E(K)[q^\infty] = E(\mathbb{Q})[q^\infty]$, for all primes $q \neq 7$.*
- *If $p = 5$, then $E(K)[q^\infty] = E(\mathbb{Q})[q^\infty]$, for all primes $q \neq 5, 7, 11$.*
- *If $p = 3$, then $E(K)[q^\infty] = E(\mathbb{Q})[q^\infty]$, for all primes $q \neq 2, 3, 5, 7, 11, 13, 19, 43, 67, 163$.*

We now prove a lemma that we will find useful.

Lemma 2.11. *Let p and q be prime numbers such that $q - 1 \nmid p$ and $p \nmid q - 1$. Let $K/\mathbb{Q}$ be a cyclic extension of degree p, and $P \in E$ a point of degree q. If $P \in E(K)$, then $P \in E(\mathbb{Q})$.*

The following lemma will tell us how far up the tower we have to go to find a point of order n, if such a point exists.

Lemma 2.12. *Let $E/\mathbb{Q}$ be an elliptic curve and $P \in E$ a point of order n such that $\mathbb{Q}(P)/\mathbb{Q}$ is Galois and let $E(\mathbb{Q}(P))[n] \simeq \mathbb{Z}/n\mathbb{Z}$. Then $\mathrm{Gal}(\mathbb{Q}(P)/\mathbb{Q})$ is isomorphic to a subgroup of $(\mathbb{Z}/n\mathbb{Z})^{\times}$.*

We immediately obtain the following corollary.

Corollary 2.13. *Let $P \in E$ be a point of order n such that $\mathbb{Q}(P) \subseteq \mathbb{Q}_{\infty,p}$. Then $\mathbb{Q}(P) \subseteq \mathbb{Q}_{m,p}$, where $m = v_p(\phi(n))$.*

Proposition 2.14. *Let E/F be an elliptic curve over a number field F, n a positive integer, $P \in E$ be a point of order p^{n+1} such that $E(F(pP))$ has no points of order p^{n+1} and such that $F(P)/F(pP)$ is Galois. Then $[F(P) : F(pP)]$ divides p^2.*

Remark. Proposition 2.14 is a version of [7, Proposition 4.6.] with stronger assumptions.

3. Proof of Theorem 1.1

We know that $\mathrm{Gal}\,(\mathcal{K}_{\geq 5}/\mathbb{Q}) \simeq \prod_{p \geq 5 \text{ prime}} \mathbb{Z}_p$. Therefore, we see that the following holds:

Let $\mathbb{F}$ be a number field contained in $\mathcal{K}_{\geq 5}$ and let $[\mathbb{F} : \mathbb{Q}] = d$. If p is the smallest prime divisor of d, then $p \geq 5$. Any point in $E(\mathcal{K}_{\geq 5})_{\mathrm{tors}}$ is defined over some finite extension $\mathbb{F}$ of $\mathbb{Q}$, where $\mathbb{Q} \subseteq \mathbb{F} \subseteq \mathcal{K}_{\geq 5}$. Using the Theorem 2.9 we can see that

$$E(\mathcal{K}_{\geq 5})[q^{\infty}] = E(\mathbb{Q})[q^{\infty}],$$

for all prime numbers q different from 5, 7 and 11. Therefore, it remains to show that

$$E(\mathcal{K}_{\geq 5})[5^{\infty}] = E(\mathbb{Q})[5^{\infty}], \quad E(\mathcal{K}_{\geq 5})[7^{\infty}] = E(\mathbb{Q})[7^{\infty}] \quad \text{and} \quad E(\mathcal{K}_{\geq 5})[11^{\infty}] = E(\mathbb{Q})[11^{\infty}],$$

which is proven by the following three Lemmas.

Before stating and proving these Lemmas, let us mention that the Corollary 2.8 holds for the field $\mathcal{K}_{\geq 5}$. It is enough to notice that $\mathcal{K}_{\geq 5}$ is an cyclic extension of $\mathbb{Q}$ and therefore so are all subfields of $\mathcal{K}_{\geq 5}$. Furthermore, the only roots of unity contained in $\mathcal{K}_{\geq 5}$ are ± 1, so we have all the necessary ingredients for proving Corollary 2.8 in the case when the field is $\mathcal{K}_{\geq 5}$.

Lemma 3.1. *Let $E/\mathbb{Q}$ be an elliptic curve. Then*

$$E(\mathcal{K}_{\geq 5})[5^{\infty}] = E(\mathbb{Q})[5^{\infty}].$$

Proof. Keeping in mind the above observation, we can see that the proof is analogous to the proof of [3, Lemma 3.6.]. $\qquad\square$

Lemma 3.2. *Let $E/\mathbb{Q}$ be an elliptic curve. Then*

$$E(\mathcal{K}_{\geq 5})[7^{\infty}] = E(\mathbb{Q})[7^{\infty}].$$

Proof. By the Corollary 2.8 we have that there are no points of order 49 in $E(\mathcal{K}_{\geq 5})$. It remains to show that $E(\mathcal{K}_{\geq 5})[7] = E(\mathbb{Q})[7]$. Theorem 2.9 implies that the only possibility is $P \in E(\mathbb{Q}_{1,7})$, where $P \in E(\mathcal{K}_{\geq 5})$ is a point of order 7. As we did in the proof of [3, Theorem 3.1], we conclude that $P \in E(\mathbb{Q})$. $\qquad\square$

Before proving that $E(\mathcal{K}_{\geq 5})[11^\infty] = E(\mathbb{Q})[11^\infty]$, we shall state and prove one technical consequence of Lemma 2.12 that we shall find useful also in the proof of Theorem 1.2..

Corollary 3.3. *Let $E/\mathbb{Q}$ be an elliptic curve and let $P \in E$ be a point of order n. If E has a rational n-isogeny with kernel $\langle P \rangle$, then $[\mathbb{Q}(P) : \mathbb{Q}] \mid \phi(n)$.*

Proof. This follows directly from Lemma 2.12, since the group $(\mathbb{Z}/n\mathbb{Z})^\times$ has exactly $\phi(n)$ elements.   □

Lemma 3.4. *Let $E/\mathbb{Q}$ be an elliptic curve. Then*

$$E(\mathcal{K}_{\geq 5})[11^\infty] = \{0\}.$$

Proof. By the Corollary 2.8 we see that $E(\mathcal{K}_{\geq 5})$ does not contain a point of order 121. Therefore, it remains to show that $E(\mathcal{K}_{\geq 5})[11] = \{0\}$. Assume that $P \in E(\mathcal{K}_{\geq 5})$, where P is a point of order 11. Combining the Theorem 2.9 with the fact that $\mathbb{Q} \subseteq \mathbb{Q}(P) \subseteq \mathcal{K}_{\geq 5}$, we see that $[\mathbb{Q}(P) : \mathbb{Q}] \in \{5, 55\}$. Using Corollary 3.3 we see that $[\mathbb{Q}(P) : \mathbb{Q}] = 5$. But this implies that $\mathbb{Q}(P) = \mathbb{Q}_{1,5}$. The rest of the proof is the same as the proof of [3, Lemma 3.2.].   □

4. Proof of Theorem 1.2

Proving this theorem will require a little more work. Namely, the approach used in the Theorem 1.1 will not help us in this case, since finite subextension $\mathbb{Q} \subseteq \mathbb{F} \subseteq \mathcal{K}$ can be of arbitrary degree over $\mathbb{Q}$. First we shall mention the main result from the paper [2, Theorem 1.2.], whose author is Michael Chou.

Theorem 4.1. *Let $E/\mathbb{Q}$ be an elliptic curve and let $\mathbb{Q}^{ab}$ be a maximal Abelian extension of $\mathbb{Q}$. The group $E(\mathbb{Q}^{ab})_{tors}$ is isomorphic to one of the following groups:*

$$
\begin{aligned}
\mathbb{Z}/N_1\mathbb{Z}, \quad & N_1 = 1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 25, 27, 37, 43, 67, 163, \\
\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N_2\mathbb{Z}, \quad & N_2 = 1, 2, 3, 4, 5, 6, 7, 8, 9, \\
\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3N_3\mathbb{Z}, \quad & N_3 = 1, 3, \\
\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4N_4\mathbb{Z}, \quad & N_4 = 1, 2, 3, 4, \\
\mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}, \quad & \\
\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}, \quad & \\
\mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}. \quad &
\end{aligned}
$$

For every group G in the list above, there exists an elliptic curve $E/\mathbb{Q}$ such that $E(\mathbb{Q}^{ab})_{tors} \simeq G$.

Notice that $E(\mathcal{K})$ does not contain a full $\mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$ torsion for any $n > 2$. We also know that $\mathcal{K} \subseteq \mathbb{Q}^{ab}$. Combining these two facts and the Theorem 4.1, we conclude that the group $E(\mathcal{K})_{tors}$ is isomorphic to one of the following groups:

$$
\begin{aligned}
\mathbb{Z}/n\mathbb{Z}, \quad & 1 \leq n \leq 19 \text{ or } n \in \{21, 25, 27, 37, 43, 67, 163\}, \\
\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, \quad & 1 \leq n \leq 9.
\end{aligned}
$$

Now we see that in order to prove the Theorem 1.2, we have to show that $E(\mathcal{K})_{tors}$ does not contain points of order

$$11, \ 14, \ 15, \ 16, \ 17, \ 18, \ 19, \ 25, \ 37, \ 43, \ 67, \ 163,$$

and that if $E(\mathcal{K})_{\text{tors}}$ contains a point of order 10 or 12, then $E(\mathcal{K})_{\text{tors}} \simeq \mathbb{Z}/10\mathbb{Z}$ or $E(\mathcal{K})_{\text{tors}} \simeq \mathbb{Z}/12\mathbb{Z}$, respectively. We shall prove this with a series of Lemmas. Finally, using the Lemma 4.10 we show that there exist elliptic curves $E/\mathbb{Q}$ that contain a point of order 13 defned over $\mathcal{K}$.

Lemma 4.2. *Let $E/\mathbb{Q}$ be an elliptic curve and let $p \in \{11, 19, 37, 43, 67, 163\}$. Then*

$$E(\mathcal{K})[p] = \{0\}.$$

Proof. Assume that $P \in E(\mathcal{K})$ is a point of order p. Using Lemma 2.6 we know that E has a rational p-isogeny with kernel $\langle P \rangle$. Corollary 3.3 implies that

$$[\mathbb{Q}(P) : \mathbb{Q}] \mid \phi(p) = p - 1.$$

It is known that such elliptic curve has CM. By the [14, Table 3] we can see all the possibilities for j-invariants of E. For the convenience of the reader, we list them in the table below. It

p	j-invariant	Cremona label
11	$-11 \cdot 131^3$	121a1
	-2^{15}	121b1
	-11^2	121c1
19	$-2^{15} \cdot 3^3$	361a1
37	$-7 \cdot 11^3$	1225h1
	$-7 \cdot 137^3 \cdot 2083^3$	1225h2
43	$-2^{18} \cdot 3^3 \cdot 5^3$	1849a1
67	$-2^{15} \cdot 3^3 \cdot 5^3 \cdot 11^3$	4489a1
163	$-2^{18} \cdot 3^3 \cdot 5^3 \cdot 23^3 \cdot 29^3$	26569a1

TABLE 1. Elliptic curves with j-invariant j with minimal conductor [19]

is known that the division polynomials of elliptic curves with same j-invariant differ by a multiplicative constant. Therefore, the pth division polynomial of E is the same (up to multiplication by a constant) as the pth division polynomial of some elliptic curve from the Table 1.

Using `magma` [1] we can easily calculate the pth division polynomial of elliptic curves given in the Table 1. Since $[\mathbb{Q}(P) : \mathbb{Q}] \leq p - 1$, we are searching for the irreducible factors of these polynomials that are of degree $\leq p - 1$ and we can easily see that they do not have zeroes over $\mathcal{K}$. Namely, each zero of an irreducible (over $\mathbb{Q}$) polynomial of degree d is defined over some degree d number field. The degree d number field contained in $\mathcal{K}$ is unique and we can easily find it using `magma` [1]. It remains to check that the polynomial does not have zeroes defined over that field which completes the proof in all cases except when $p = 163$. Namely, in all other cases, `magma` [1] computes what we need in a matter of seconds. The case when $p = 163$ requires slightly different approach. As we can see in the Table 2, the only irreducible factor (call it φ) of the 163rd division polynomial whose degree is less then or equal to 163 has a degree 81. If we assume that $E(\mathcal{K})$ contains a point of order 163, then

we know that it's x-coordinate must be defined over a field of degree 81, which is $\mathbb{Q}_{4,3}$. But $\mathbb{Q}_{4,3}/\mathbb{Q}$ is Galois extension and we know that over $\mathbb{Q}_{1,3} = \mathbb{Q}(\zeta_9)^+$, φ splits into a product of three irreducible factors, each having a degree 27. Computation in `magma` [1] shows that this is not the case. Namely, the polynomial φ remains irreducible over $\mathbb{Q}(\zeta_9)^+$, which leads to a contradiction. $\qquad\square$

p	Elliptic curve	$\deg\psi_p$	irreducible factors of degree $\leq p-1$
11	121a1	60	one of degree 5
	121b1	60	one of degree 5
	121c1	60	one of degree 5
19	361a1	180	one of degree 9
37	1225h1	684	three of degree 6
	1225h2	684	one of degree 18
43	1849a1	924	one of degree 21
67	4489a1	2244	one of degree 33
163	26569a1	13284	one of degree 81

TABLE 2. Possible degrees of irreducible factors of degree $\leq p-1$

Proposition 4.3. [7, Proposition 4.6.] *Let F be a number field and E/F be an elliptic curve. Let p be a prime number, $n \in \mathbb{N}$ and $P \in E(\overline{\mathbb{F}})$ a point of order p^{n+1}. Then $[\mathbb{F}(P) : \mathbb{F}(pP)]$ divides p^2 or $(p-1)p$.*

Lemma 4.4. *Let $E/\mathbb{Q}$ be an elliptic curve. Then $E(\mathcal{K})$ does not contain a point of order 16.*

Proof. Assume that $P \in E(\mathcal{K})$ is a point of order 16. Lemma 2.6 implies that E has a rational 2-isogeny. We also know that $E(\mathcal{K})_{\mathrm{tors}}$ is isomorphic to a subgroup of $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z}$ by the Theorem 4.1. By the [17, Theorem 4] we see that

$$[\mathbb{Q}(E[2]) : \mathbb{Q}] = |G_{E,\mathbb{Q}}(2)| \leq |B(2)| = 2.$$

The point $8P$ is of order 2 so we have $[\mathbb{Q}(8P) : \mathbb{Q}] \in \{1, 2\}$. By Proposition 4.3 we have

$$[\mathbb{Q}(P) : \mathbb{Q}] = \underbrace{[\mathbb{Q}(P) : \mathbb{Q}(2P)]}_{\in\{1,2,4\}}\underbrace{[\mathbb{Q}(2P) : \mathbb{Q}(4P)]}_{\in\{1,2,4\}}\underbrace{[\mathbb{Q}(4P) : \mathbb{Q}(8P)]}_{\in\{1,2,4\}}\underbrace{[\mathbb{Q}(8P) : \mathbb{Q}]}_{\in\{1,2\}}.$$

Therefore, $[\mathbb{Q}(P) : \mathbb{Q}]$ is a power of 2 which means that P is defined over $\mathbb{Q}_{\infty,2}$, which contradicts the Theorem 2.2. $\qquad\square$

Lemma 4.5. *Let $E/\mathbb{Q}$ be an elliptic curve and let $n \in \{15, 17\}$. Then $E(\mathcal{K})$ does not contain a point of order n.*

Proof. Assume that $P \in E(\mathcal{K})$ is a point of order n. It follows that E has a rational n-isogeny by the Lemma 2.6. By the Corollary 3.3 we see that

$$[\mathbb{Q}(P) : \mathbb{Q}] \mid \phi(n).$$

On the other hand, we know that $\phi(15) = 8$ and $\phi(17) = 16$, which means that P is defined over $\mathbb{Q}_{\infty,2}$, which contradicts the Theorem 2.2. $\qquad\square$

Lemma 4.6. *Let $E/\mathbb{Q}$ be an elliptic curve and let $n \in \{14, 18\}$. Then $E(\mathcal{K})$ does not contain a point of order n.*

Proof. Notice that $n = 2k$, where $k \in \{7, 9\}$. Assume that $E(\mathcal{K})$ contains a point P of order n. Then $E(\mathcal{K})$ has a point P_k of order k. By the Lemma 2.6 and the Corollary 3.3 we see that

$$[\mathbb{Q}(P_k) : \mathbb{Q}] \mid \phi(k) = 6.$$

This means that P_k is defined over a number field of degree at most 6, so it's defined over the compositum $\mathbb{Q}_{1,2}\mathbb{Q}_{1,3}$. From the [16, Corollary 4] we get that

$$E(\mathbb{Q}_{1,2}\mathbb{Q}_{1,3})[k] \simeq E(\mathbb{Q}_{1,3})[k] \oplus E^{(2)}(\mathbb{Q}_{1,3})[k],$$

where $E^{(2)}$ is the quadratic twist of E by 2. We know that $E^{(2)}$ is defined over $\mathbb{Q}$ and that having a 2-torsion is a twist invariant property. Since kP is of order 2, we know that E and $E^{(2)}$ have at least one point of order 2 defined over $\mathbb{Q}_{1,3}$. This means that there exists an elliptic curve defined over $\mathbb{Q}$ that has a point of order k and a point of order 2 defined over $\mathbb{Q}_{1,3}$, so it has a point of order $n = 2k$ defined over $\mathbb{Q}_{1,3}$, which contradicts the Theorem 2.3. $\qquad\square$

Lemma 4.7. *Let $E/\mathbb{Q}$ be an elliptic curve. Then $E(\mathcal{K})$ does not contain a point of order 25.*

Proof. Assume that $P \in E(\mathcal{K})$ is a point of order 25. Using the Lemma 2.6 we see that E has a rational 25-isogeny, which means that $\mathrm{Gal}\,(\mathbb{Q}(E[25])/\mathbb{Q})$ acts on $\langle P \rangle$, so for each $\sigma \in \mathrm{Gal}\,(\mathbb{Q}(E[25])/\mathbb{Q})$ there exists some $a \in (\mathbb{Z}/25\mathbb{Z})^{\times}$ such that $P^{\sigma} = aP$. By the Corollary 3.3 we see that $[\mathbb{Q}(P) : \mathbb{Q}] \mid \phi(25) = 20$. Furthermore, the point $5P$ is of order 5 and by the same reasoning we conclude that $[\mathbb{Q}(5P) : \mathbb{Q}] \mid \phi(5) = 4$. Therefore, we have

$$\mathbb{Q}(P) \subseteq \mathbb{Q}_{2,2}\mathbb{Q}_{1,5} \qquad \text{and} \qquad \mathbb{Q}(5P) \subseteq \mathbb{Q}_{2,2}.$$

Each $\sigma \in \mathrm{Gal}\,(\mathbb{Q}(E[25])/\mathbb{Q}_{2,2})$ fixes the point $5P$, so we conclude that $G_{\mathbb{Q}_{2,2}}(25)$ is (up to conjugacy) of the form

$$\left\{ \begin{pmatrix} a & * \\ 0 & * \end{pmatrix} : a \in 1 + 5\mathbb{Z}/25\mathbb{Z} \right\}.$$

We also know that $[\mathbb{Q}(\zeta_{25}) : \mathbb{Q}_{1,5}] = 4$, which means that $|\mathrm{Gal}\,(\mathbb{Q}(\zeta_{25})/\mathbb{Q}_{1,5})| = 4$. By the [3, Lemma 3.4.] we have that $\det G_{\mathbb{Q}_{2,2}\mathbb{Q}_{1,5}}(25)$ is isomorphic to an unique order 4 subgroup of $(\mathbb{Z}/25\mathbb{Z})^{\times}$, which is $\langle 7 \rangle = \{7, -1, -7, 1\}$. Let us recall that $\mathrm{Gal}\,(\overline{\mathbb{Q}}/\mathbb{Q}_{2,2}\mathbb{Q}_{1,5})$ fixes the point P, so

$$G_{\mathbb{Q}_{2,2}\mathbb{Q}_{1,5}}(25) \leq \left\{ \begin{pmatrix} 1 & * \\ 0 & b \end{pmatrix} : b \in \{7, -1, -7, 1\} \right\}.$$

Notice that $\mathrm{Gal}\,(\mathbb{Q}(E[25])/\mathbb{Q}_{2,2})$ does not fix the point P, by the Theorem 2.2 and that

$$[G_{\mathbb{Q}_{2,2}}(25) : G_{\mathbb{Q}_{2,2}\mathbb{Q}_{1,5}}(25)] = [\mathbb{Q}_{2,2}\mathbb{Q}_{1,5} : \mathbb{Q}_{2,2}] = 5.$$

Therefore we have that

$$G_{\mathbb{Q}_{2,2}}(25) \leq \left\{ \begin{pmatrix} a & * \\ 0 & b \end{pmatrix} : a \in 1 + 5\mathbb{Z}/25\mathbb{Z}, \ b \in \{7, -1, -7, 1\} \right\}.$$

We have that $[G_{\mathbb{Q}}(25) : G_{\mathbb{Q}_{2,2}}(25)] = [\mathbb{Q}_{2,2} : \mathbb{Q}] = 4$ and

$$[(\mathbb{Z}/25\mathbb{Z})^{\times} : 1 + 5\mathbb{Z}/25\mathbb{Z}] = 4 \qquad \text{i} \qquad [(\mathbb{Z}/25\mathbb{Z})^{\times} : \langle 7 \rangle] = 5.$$

Finally we conclude that

$$G_{\mathbb{Q}}(25) \leq \left\{ \begin{pmatrix} a & * \\ 0 & b \end{pmatrix} : a \in (\mathbb{Z}/25\mathbb{Z})^{\times}, \ b \in \{7, -1, -7, 1\} \right\}.$$

We compute

$$25 \mid 150 \mid [\mathrm{GL}_2(\mathbb{Z}/25\mathbb{Z}) : G_{\mathbb{Q}}(25)] \mid [\mathrm{Aut}_{\mathbb{Z}_5}(T_5(E)) : \mathrm{Img}(\overline{\rho}_{5,E})],$$

which contradicts the Theorem [9, Theorem 2]. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad \square$

Lemma 4.8. *Let $E/\mathbb{Q}$ be an elliptic curve such that $E(\mathcal{K})$ contains a point of order 10. Then*

$$E(\mathcal{K})_{tors} \simeq \mathbb{Z}/10\mathbb{Z}.$$

Proof. The only other possibility for $E(\mathcal{K})_{\mathrm{tors}}$ is the group $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$, so we shall eliminate that possibility. For the sake of contradiction, assume that $E(\mathcal{K})_{\mathrm{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$.

The entire 2-torsion of E is defined over $\mathcal{K}$ which is Galois over $\mathbb{Q}$ so we conclude that $G_{\mathbb{Q}}(2)$ is conjugate to one of the following groups:

$$G_1 = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}, \quad G_2 = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\}, \quad G_3 = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \right\}.$$

In the case when $G_{\mathbb{Q}}(2) = G_1$ or $G_{\mathbb{Q}}(2) \cong G_2$ (up to conjugacy), we can immediately conclude that the entire 2-torsion subgroup of E is defined over at most quadratic extension of $\mathbb{Q}$, so it's defined over $\mathbb{Q}_{1,2}$. Furthermore, using the Lemma 2.6 and the Corollary 3.3 we see that the point of order 5 is defined over $\mathbb{Q}$, $\mathbb{Q}_{1,2}$ or and $\mathbb{Q}_{2,2}$. We conclude that $E(\mathbb{Q}_{\infty,2})_{\mathrm{tors}}$ contains $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$, which contradicts the Theorem 2.2. It remains to consider the case when $G_{\mathbb{Q}}(2) = G_3$. Using the [7, Theorem 3.6.] we conclude that E does not have CM. Moreover, using the [21, Theorem 1.1.] we see that there exists a rational number u such that

$$j(E) = u^2 + 1728.$$

The Lemma 2.6 implies that E has a rational 5-isogeny, which means that $G_{\mathbb{Q}}(5)$ is conjugate subgroup of

$$\left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : a, c \in \mathbb{F}_5^{\times}, b \in \mathbb{F}_5 \right\}.$$

Using the [21, Theorem 1.4.] we see that there exists a rational number $v \neq 0$ such that

$$j(E) = \frac{5^2(v^2 + 10v + 5)^3}{v^5}.$$

Therefore, we get the modular curve

$$C \ : \ 25(v^2 + 10v + 5)^3 - u^2 v^5 - 1728 v^5 = 0.$$

Computation in `magma` [1] shows that C is birrationally equivalent to an elliptic curve with Cremona label 20a3. That curve has only two rational points and both of those points do not correspond to affine points on C. □

Lemma 4.9. *Let $E/\mathbb{Q}$ be an elliptic curve such that $E(\mathcal{K})$ contains a point of order* 12. *Then*

$$E(\mathcal{K})_{tors} \simeq \mathbb{Z}/12\mathbb{Z}.$$

Proof. The only other possibility for $E(\mathcal{K})_{\text{tors}}$ is $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$. Assume that $E(\mathcal{K})_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$. The Lemma 2.6 implies that E has a rational 2-isogeny, which means that $G_{\mathbb{Q}}(2) = G_1$ or $G_{\mathbb{Q}}(2) \sim G_2$ (up to conjugacy), where G_1 and G_2 are the same as in the proof of Lemma 4.8. Therefore we conclude that the entire 2-torsion subgroup of E is defined over $\mathbb{Q}_{\infty,2}$. By the Lemma 2.6 we have that E has a rational 3-isogeny, which means that the point of order 3 is defined over at most quadratic extension of $\mathbb{Q}$, so it's defined over $\mathbb{Q}_{\infty,2}$. From the Proposition 4.3 we have that the point of order 4 is also defined over $\mathbb{Q}_{\infty,2}$. Finally, we have that $E(\mathbb{Q}_{\infty,2})_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$, which contradicts the Theorem 2.2. □

Lemma 4.10. *There exists elliptic curves $E/\mathbb{Q}$ such that*

$$E(\mathbb{Q})_{tors} = \{0\} \qquad and \qquad E(\mathcal{K})_{tors} \simeq \mathbb{Z}/13\mathbb{Z}.$$

Proof. Assume that $P \in E(\mathcal{K})$ is a point of order 13. We know that $P \notin E(\mathbb{Q})$ and we know that by the Lemma 2.6, E has a rational 13-isogeny. Assume that $E(\mathcal{K})$ contains a point Q of order q, for some prime number $q \neq 13$. It would then follow that E has a rational $13q$-isogeny, which is impossible by the Corollary 2.8. Same reasoning shows that E can't have a point of order 13^2. Therefore, it remains to find an example of elliptic curve $E/\mathbb{Q}$ that has a point of order 13 defined over $\mathcal{K}$. Searching the LMFDB [19] database using `magma` [1] we find two elliptic curves defined over $\mathbb{Q}$ with such property:

$$20736c1 \ : \qquad y^2 = x^3 + 6x + 8,$$
$$20736d1 \ : \qquad y^2 = x^3 + 24x + 64. \qquad \square$$

5. Proof of Theorem 1.3

In order to prove this theorem, we will use a few well known results and some technical facts that we will now mention. The proof itself follows from the series of Lemmas.

First, let us recall the Mazur's famous isogeny theorem (Theorem 2.7). Let $E/\mathbb{Q}$ be an elliptic curve with a rational n-isogeny. Then n has to be one of the values from the table below. We shall also need the values $\phi(n)$.

Numbers n that are contained in a ☐ are the ones that will require special care. Soon it will be obvious why is that the case.

We will also need the following theorem:
[6, Theorem 1.1]:

n	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\phi(n)$	1	2	2	2^2	2	$2\cdot3$	2^2	$2\cdot3$	2^2	$2\cdot5$	2^2	$2^2\cdot3$	$2\cdot3$	2^3	2^3

n	17	18	19	21	25	27	37	43	67	163
$\phi(n)$	2^4	$2\cdot3$	$2\cdot3^2$	$2^2\cdot3$	$2^2\cdot5$	$2\cdot3^2$	$2^2\cdot3^2$	$2\cdot3\cdot7$	$2\cdot3\cdot11$	$2\cdot3^4$

TABLE 3. Possible rational n-isogenies together with values $\phi(n)$.

Theorem 5.1. *Let $E/\mathbb{Q}$ be an elliptic curve and let $n \geq 2$ be a natural number.*

If $\mathbb{Q}(E[n]) = \mathbb{Q}(\mu_n)$, then $n \in \{2,3,4,5\}$. Furthermore, if the extension $\mathbb{Q}(E[n])/\mathbb{Q}$ is Abelian, then $n \in \{2,3,4,5,6,8\}$ and the group $G = \mathrm{Gal}\,(\mathbb{Q}(E[n])/\mathbb{Q})$ is isomorphic to one of the following groups:

n	2	3	4	5	6	8
G	$\{0\}$ $\mathbb{Z}/2\mathbb{Z}$ $\mathbb{Z}/3\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z}$ $(\mathbb{Z}/2\mathbb{Z})^2$	$\mathbb{Z}/2\mathbb{Z}$ $(\mathbb{Z}/2\mathbb{Z})^2$ $(\mathbb{Z}/2\mathbb{Z})^3$ $(\mathbb{Z}/2\mathbb{Z})^4$	$\mathbb{Z}/4\mathbb{Z}$ $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ $(\mathbb{Z}/4\mathbb{Z})^2$	$(\mathbb{Z}/2\mathbb{Z})^2$ $(\mathbb{Z}/2\mathbb{Z})^3$	$(\mathbb{Z}/2\mathbb{Z})^4$ $(\mathbb{Z}/2\mathbb{Z})^5$ $(\mathbb{Z}/2\mathbb{Z})^6$

The following Corollary makes things easier.

Corollary 5.2. *Let $E/\mathbb{Q}$ be an elliptic curve. Let $p \geq 3$ be a prime number and let $n \geq 2$ be a natural number. If $\mathbb{Q}(E[n]) \subseteq \mathbb{Q}(\mu_{p^\infty})$, then $n \in \{2,3,4,5\}$ and*

$$\mathbb{Q}(E[n]) \subseteq \mathbb{Q}(\mu_{3^3}), \;\; for\; p = 3 \quad and \quad \mathbb{Q}(E[n]) \subseteq \mathbb{Q}(\mu_p), \;\; for\; p \geq 5.$$

Proof. We know that $\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}$ is cyclic, which means that $\mathbb{Q}(E[n])/\mathbb{Q}$ is also cyclic. From the Theorem 5.1, we see that the only possibilities for n are $n \in \{2,3,4,5\}$ and that $[\mathbb{Q}(E[n]) : \mathbb{Q}] \in \{1,2,3,4\}$, which concludes the proof. $\square$

Proposition 5.3. *Let $E/\mathbb{Q}$ be an elliptic curve and let $P \in E(\overline{\mathbb{Q}})$ be a point of order 2^{n+1}, for some natural number n. Then*

$$[\mathbb{Q}(P) : \mathbb{Q}(2P)] \mid 4.$$

Corollary 5.4. *Let $E/\mathbb{Q}$ be an elliptic curve and $P \in E(\mathbb{Q}(\mu_{p^\infty}))$ be a point of order 2^n, for some natural number n and $p \geq 3$ a prime number. Then*

$$\mathbb{Q}(P) \subseteq \mathbb{Q}(\mu_{3^3}), \;\; for\; p = 3 \quad and \quad \mathbb{Q}(P) \subseteq \mathbb{Q}(\mu_p), \;\; for\; p \geq 5.$$
$$\mathbb{Q}(P) \subseteq \mathbb{Q}(\mu_{3^3}), \;\; za\; p = 3 \quad and \quad \mathbb{Q}(P) \subseteq \mathbb{Q}(\mu_p), \;\; za\; p \geq 5.$$

Proof. The point $2^{n-1}P$ is of order 2 and we know that $[\mathbb{Q}(2^{n-1}P) : \mathbb{Q}] \in \{1,2,3\}$. Applying the Proposition 5.3 $(n-1)$ times we conclude that $[\mathbb{Q}(P) : \mathbb{Q}(2^{n-1}P)] = 2^a$, for some $a \in \{0,1,2,\ldots,2n-2\}$, from which it follows that $[\mathbb{Q}(P) : \mathbb{Q}] = 2^a 3^b$, for some $a \in \{0,1,2,\ldots,2n-1\}$, $b \in \{0,1\}$ and the claim follows. $\square$

Lemma 5.5. *Let $E/\mathbb{Q}$ be an elliptic curve and let $p \geq 13$ be a prime number. Then we have*

$$E(\mathbb{Q}(\mu_{p^\infty}))_{tors} = E(\mathbb{Q}(\mu_p))_{tors}.$$

Proof. Let q be a prime number different then 2 and p. We know that $\mathbb{Q}(\mu_{p^\infty})$ does not contain ζ_q. By the Proposition 2.4 we conclude that $E(\mathbb{Q}(\mu_{p^\infty}))$ does not contain $E[q]$. Assume that n is a natural number such that $E(\mathbb{Q}(\mu_{p^\infty}))$ contains a point P of order q^n. By the Lemma 2.6 we see that E has a rational q^n-isogeny. The Corollary 3.3 implies that $[\mathbb{Q}(P) : \mathbb{Q}] \mid \phi(q^n)$. By the Table 3 we see that $\mathbb{Q}(P) \subseteq \mathbb{Q}(\mu_p)$. Let us now consider the case $q = 2$. By the Corollary 5.4 we see that the points of order 2^n contained in $E(\mathbb{Q}(\mu_{p^\infty}))_{\text{tors}}$ are defined over $\mathbb{Q}(\mu_p)$. Finally, using the Corollary 5.2 we conclude that $E(\mathbb{Q}(\mu_{p^\infty}))$ does not contain $E[p]$. Therefore, when a point $P \in E(\mathbb{Q}(\mu_{p^\infty}))$ is of order p^n the same argument applies as in the case when the order equals q^n. $\qquad\square$

Lemma 5.6. *Let $E/\mathbb{Q}$ be an elliptic curve. Then*

$$E(\mathbb{Q}(\mu_{11^\infty}))_{tors} = E(\mathbb{Q}(\mu_{11}))_{tors}.$$

Proof. The proof is analogous to the proof of the previous Lemma, except in the case when $P \in E(\mathbb{Q}(\mu_{11^\infty}))$ is of order 67. In this case E has a rational 67-isogeny. This means that $j(E) = -2^{15} \cdot 3^3 \cdot 5^3 \cdot 11^3$. From the proof of the Lemma 4.2 we know that the 67th division polynomial of elliptic curves with this j-invariant has one irreducible factor of degree ≤ 66 and that this factor, call is φ, is of degree 33. This is impossible since $\mathbb{Q}(\mu_{11^\infty})$ does not contain a subfield of degree 33 over $\mathbb{Q}$. $\qquad\square$

Lemma 5.7. *Let $E/\mathbb{Q}$ be an elliptic curve. Then*

$$E(\mathbb{Q}(\mu_{7^\infty}))_{tors} = E(\mathbb{Q}(\mu_7))_{tors}.$$

Proof. Let P be a point of order n in $E(\mathbb{Q}(\mu_{7^\infty}))$. If $n \neq 43$, then the same argument as in the previous lemma applies. Let us consider the case when $n = 43$. Using Table 3 and `magma` [1] we can easily show that such a point does not exist. The proof is basically the same as in the previous Lemma 5.6. $\qquad\square$

Lemma 5.8. *Let $E/\mathbb{Q}$ be an elliptic curve. Then*

$$E(\mathbb{Q}(\mu_{5^\infty}))_{tors} = E(\mathbb{Q}(\mu_5))_{tors}.$$

Proof. If $E(\mathbb{Q}(\mu_{5^\infty}))$ contains a point of order 11, then $E(\mathbb{Q}(\mu_{5^\infty}))_{\text{tors}} = \mathbb{Z}/11\mathbb{Z}$. Therefore, E has a rational 11-isogeny. By Table 2 we see that the 11th division polynomial of elliptic curve $E/\mathbb{Q}$ with a rational 11-isogeny has a unique irreducible factor of degree ≤ 10 and that factor is of degree 5. In the proof of Lemma 4.2 we have shown that such irreducible factor does not have zeroes over the unique subfield $\mathbb{Q}_{1,5}$ of $\mathbb{Q}(\mu_{5^\infty})$ of degree 5 over $\mathbb{Q}$. It remains to consider the case when $E(\mathbb{Q}(\mu_{5^\infty}))$ contains a point of order 25. Assume that $P \in E(\mathbb{Q}(\mu_{5^\infty}))$ is a point of order 25. We can easily see that $E(\mathbb{Q}(\mu_{5^\infty}))_{\text{tors}} \simeq \mathbb{Z}/25\mathbb{Z}$ and so E has a rational 25-isogeny. This means that $\mathbb{Q}(P) \subseteq \mathbb{Q}(\mu_{25})$. Assume that $\mathbb{Q}(P) \not\subseteq \mathbb{Q}(\mu_5)$ (otherwise, we're immediately done). By the analogous argument we conclude that $\mathbb{Q}(5P) \subseteq \mathbb{Q}(\mu_5)$. Since every $\sigma \in \text{Gal}\,(\mathbb{Q}(E[25])/\mathbb{Q}(\mu_5))$ fixes a point $5P$, we conclude that $G_{\mathbb{Q}(\mu_5)}(25)$ is (up to conjugacy) of the form

$$\left\{ \begin{pmatrix} a & * \\ 0 & * \end{pmatrix} : a \in 1 + 5\mathbb{Z}/25\mathbb{Z} \right\}.$$

By the [3, Lemma 3.4.] we have $\det G_{\mathbb{Q}(\mu_{25})}(25) \simeq \{1\}$. Recall that the group $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}(\mu_{25})\right)$ fixes point P and so

$$G_{\mathbb{Q}(\mu_{25})}(25) \leq \left\{ \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \right\}.$$

Notice that $\mathrm{Gal}\left(\mathbb{Q}(E[25])/\mathbb{Q}(\mu_5)\right)$ does not fix the point P and that

$$[G_{\mathbb{Q}(\mu_5)}(25) : G_{\mathbb{Q}(\mu_{25})}(25)] = [\mathbb{Q}(\mu_{25}) : \mathbb{Q}(\mu_5)] = 5.$$

Therefore we have

$$G_{\mathbb{Q}(\mu_5)}(25) \leq \left\{ \begin{pmatrix} a & * \\ 0 & 1 \end{pmatrix} : a \in 1 + 5\mathbb{Z}/25\mathbb{Z} \right\}.$$

We also have $[G_{\mathbb{Q}}(25) : G_{\mathbb{Q}(\mu_5)}(25)] = [\mathbb{Q}(\mu_5) : \mathbb{Q}] = 4$ and

$$[(\mathbb{Z}/25\mathbb{Z})^{\times} : 1 + 5\mathbb{Z}/25\mathbb{Z}] = 4 \qquad \text{i} \qquad [\langle 7 \rangle : \{1\}] = 4.$$

Finally we conclude that

$$G_{\mathbb{Q}}(25) \leq \left\{ \begin{pmatrix} a & * \\ 0 & b \end{pmatrix} : a \in (\mathbb{Z}/25\mathbb{Z})^{\times}, \ b \in \{7, -1, -7, 1\} \right\}$$

and we have

$$25 \mid 150 \mid [\mathrm{GL}_2(\mathbb{Z}/25\mathbb{Z}) : G_{\mathbb{Q}}(25)] \mid [\mathrm{Aut}_{\mathbb{Z}_5}(T_5(E)) : \mathrm{Img}(\overline{\rho}_{5,E})],$$

which contradicts the [9, Theorem 2].   □

Lemma 5.9. *Let $E/\mathbb{Q}$ be an elliptic curve. Then*

$$E(\mathbb{Q}(\mu_{3^\infty}))_{tors} = E(\mathbb{Q}(\mu_{3^3}))_{tors}.$$

Proof. If $q \neq 3$ is a prime number and n is a natural number such that $E(\mathbb{Q}(\mu_{3^\infty}))$ contains a point P of order q^n, then as in the proofs of the previous lemmas we see that $\mathbb{Q}(P) \subseteq \mathbb{Q}(\mu_{3^3})$, except when $q = 163$ and $n = 1$. Assume that $P \in E(\mathbb{Q}(\mu_{3^\infty}))$ is the point of order 163. We know that the only possibility is $E(\mathbb{Q}(\mu_{3^\infty}))_{tors} \simeq \mathbb{Z}/163\mathbb{Z}$, which implies that E has a rational 163-isogeny. Furthermore, we have $\mathbb{Q}(P) \subseteq \mathbb{Q}(\mu_{3^5})$. By Table 2 we see that the 163rd division polynomial of E has only one irreducible factor of degree ≤ 162 and that such factor (call it ψ) has degree 81. This means that the polynomial ψ needs to have zeroes defined over the field $\mathbb{Q}(\mu_{3^5})$. More precisely, it needs to have zeroes defined over a number field of degree 81 that is contained in $\mathbb{Q}(\mu_{3^5})$. Such a field is unique and it is equal to $\mathbb{Q}_{4,3}$. In the proof of the Lemma 4.2 we have shown that this is in fact false. Therefore we have arrived at the contradiction. We conclude that $E(\mathbb{Q}(\mu_{3^\infty}))$ can't contain a point of order 163. It remains to consider the points of order 3^n. We see that $E(\mathbb{Q}(\mu_{3^\infty}))[3^\infty]$ is isomorphic to one of the following groups:

$$\mathbb{Z}/3\mathbb{Z}, \quad \mathbb{Z}/9\mathbb{Z}, \quad \mathbb{Z}/27\mathbb{Z}, \quad \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}, \quad \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z}.$$

If $E(\mathbb{Q}(\mu_{3^\infty}))[3^\infty] \simeq \mathbb{Z}/3^n\mathbb{Z}$, for some $n \in \{1, 2, 3\}$, then we know that E has a rational 3^n-isogeny and the claim of the Lemma follows immediately by the Table 3. The case when $E(\mathbb{Q}(\mu_{3^\infty}))[3^\infty] \simeq \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$ follows from the Corollary 5.2. Let us check the remaining possibility, when $E(\mathbb{Q}(\mu_{3^\infty}))[3^\infty] \simeq \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z}$. Let $\{P, Q\}$ be the basis for $E(\mathbb{Q}(\mu_{3^\infty}))[3^\infty]$.

The point P is of order 3 and the point Q is of order 9. By the Theorem 5.1, we know that $\mathbb{Q}(P) = \mathbb{Q}(3Q) = \mathbb{Q}(\mu_3)$. Proposition [7, Proposition 4.6.] implies that

$$[\mathbb{Q}(Q) : \mathbb{Q}(3Q)] \in \{1, 2, 3, 6, 9\},$$

which shows that $\mathbb{Q}(P, Q) \subseteq \mathbb{Q}(\mu_{3^3})$. $\square$

Before proving that $E(\mathbb{Q}(\mu_{2^\infty}))_{\text{tors}} = E(\mathbb{Q}(\mu_{2^4}))_{\text{tors}}$, we shall state the two techical results we shall need.

Lemma 5.10. *Let $E/\mathbb{Q}$ be an elliptic curve such that $E(\mathbb{Q}(\mu_{2^\infty}))[2^\infty] \simeq \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$. Then*

$$E(\mathbb{Q}(\mu_{2^4}))[2^\infty] \simeq \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}.$$

Proof. Let P and Q be a points in $E(\mathbb{Q}(\mu_{2^\infty}))$ of orders 4 and 8 respectively that generate $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$ torsion subgroup. We need to show that $\mathbb{Q}(P, Q) \subseteq \mathbb{Q}(\zeta_{2^4})$. By the Theorem 5.1 we see that $\mathbb{Q}(P, 2Q) \subseteq \mathbb{Q}(\zeta_{2^3})$. Using the Proposition 5.3 we can see that $\mathbb{Q}(P, Q) \subseteq \mathbb{Q}(\zeta_{2^5})$. In [5] M. Derickx and A. V. Sutherland have computed the models for a certain number of modular curves $X_1(m, mn)$. This list can be found in `http://math.mit.edu/~drew/X1mn.html`. We observe that $X_1(4, 8)$ is actually an elliptic curve 32a2 (data [19]):

$$E' \; : \; y^2 = x^3 - x.$$

We want to show that $r(E'(\mathbb{Q}(\mu_{2^5}))) = r(E(\mathbb{Q}(\mu_{2^4}))) = 0$ and $E'(\mathbb{Q}(\mu_{2^5}))_{\text{tors}} = E(\mathbb{Q}(\mu_{2^4}))_{\text{tors}}$. We shall use the fact that

$$r(E'(\mathbb{Q}(\mu_{2^5}))) = r(E'(\mathbb{Q}_{3,2})) + r(E'^{(-1)}(\mathbb{Q}_{3,2})).$$

This is easily seen to be true because $\mathbb{Q}(\mu_{2^5}) = \mathbb{Q}_{3,2}\mathbb{Q}(i)$. Computation in `magma` [1] shows that this claim holds. $\square$

Lemma 5.11. *Let $E/\mathbb{Q}$ be an elliptic curve with CM. Then E does not contain a point of order 16 defined over $\mathbb{Q}(\mu_{2^\infty})$.*

Proof. Assume that $E(\mathbb{Q}(\mu_{2^\infty}))$ contains a point P of order 16. We see that $E(\mathbb{Q}(\mu_{2^\infty}))_{\text{tors}}$ is isomorphic to one of the groups

$$\mathbb{Z}/16\mathbb{Z}, \quad \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z}, \quad \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z}.$$

In the first scenario, by the Table 3 we see that $\mathbb{Q}(P) \subseteq \mathbb{Q}(\mu_{2^4})$. In the second case ($\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z}$), we know that $\langle 2P \rangle$ is the kernel of a rational 8-isogeny and so $\mathbb{Q}(2P) \subseteq \mathbb{Q}(\mu_{2^3})$. Using the Proposition 5.3 we conclude that $\mathbb{Q}(P) \subseteq \mathbb{Q}(\mu_{2^5})$. Finally, consider the third case. The group $\langle 4P \rangle$ is the kernel of a rational 4-isogeny and so $\mathbb{Q}(4P) \subseteq \mathbb{Q}(\mu_{2^2})$. By the Proposition [7, Proposition 4.6.], it follows that $\mathbb{Q}(P) \subseteq \mathbb{Q}(\mu_{2^6})$. In any of these cases, the point P is defined over $\mathbb{Q}(\mu_{2^6})$. Since E has CM, j-invariant of E is equal to one of the following 13 values:

$$-262537412640768000, \; -147197952000, \; -884736000, \; -12288000, \; -884736,$$

$$-32768, \; -3375, \; 0, \; 1728, \; 8000, \; 54000, \; 287496, \; 16581375.$$

Computation in `magma` [1] shows that the 8th division polynomial of elliptic curves with those j-invariants does not have zeroes over $\mathbb{Q}(\mu_{2^6})$, which completes the proof. $\square$

Lemma 5.12. *Let $E/\mathbb{Q}$ be an elliptic curve such that $E(\mathbb{Q}(\mu_{2^\infty}))[2^\infty] \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z}$. Then*

$$E(\mathbb{Q}(\mu_{2^4}))[2^\infty] \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z}.$$

Proof. Let P and Q be the points in $E(\mathbb{Q}(\mu_{2^\infty}))$ of orders 2 and 16 respectively, that generate the $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z}$ torsion subgroup. We need to show that $\mathbb{Q}(P,Q) \subseteq \mathbb{Q}(\zeta_{2^4})$. We can see that $\langle 2Q \rangle$ is the kernel of the rational 8-isogeny, which means that $2Q$ is defined over a number field of degree at most 4. By the Proposition 5.3, we see that Q is defined over a number field of degree at most 16. Therefore, $\mathbb{Q}(P,Q) \subseteq \mathbb{Q}(\zeta_{2^5})$. Let us show the following claim:
If $[\mathbb{Q}(P,Q) : \mathbb{Q}] \geq 16$, then $\mathbb{Q}(P,Q)$ is not contained in $\mathbb{Q}(\mu_{2^\infty})$. This will imply the claim of our Lemma. We know that $\mathrm{Gal}\,(\mathbb{Q}(\zeta_2)/\mathbb{Q}) \simeq \{0\}$, $\mathrm{Gal}\,(\mathbb{Q}(\zeta_4)/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z}$ and

$$\mathrm{Gal}\,(\mathbb{Q}(\zeta_{2^k})/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2^{k-2}\mathbb{Z},$$

for every positive integer $k > 2$. In the case when $[\mathbb{Q}(P,Q) : \mathbb{Q}] \geq 16$, we have that $\mathrm{Gal}\,(\mathbb{Q}(P,Q)/\mathbb{Q})$ is not of this form and the claim follows. By the previous Lemma 5.11 we know that E does not have CM. In the proof of [7, Lemma 8.15.], E. González-Jiménez and F. Najman have used `magma` [1] code (http://verso.mat.uam.es/~enrique.gonzalez.jimenez/research/tables/growth/growth.html). We shall do the same. Examining each possible 2-adic representation, we find all possibilities for $\mathrm{Gal}\,(\mathbb{Q}(P,Q)/\mathbb{Q})$, under the assumption that $[\mathbb{Q}(P,Q) : \mathbb{Q}] \geq 16$. Let us mention that the key to this approach is the data available at 2primary_Ss.txt which was computed by E. González-Jiménez and Á. Lozano-Robledo. All `magma` [1] codes can be found on http://verso.mat.uam.es/~enrique.gonzalez.jimenez/research/tables/growth/growth.html. Finally, a calculation in `magma` [1] shows that the field $\mathbb{K}$ such that $\mathbb{Q}(P,Q) = \mathbb{K}$ and $[\mathbb{K} : \mathbb{Q}] \geq 16$ satisfies $\mathrm{Gal}\,(\mathbb{K}/\mathbb{Q}) \simeq (\mathbb{Z}/2\mathbb{Z})^2 \oplus \mathbb{Z}/4\mathbb{Z}$. This means that $\mathbb{K}$ is not contained in $\mathbb{Q}(\mu_{2^\infty})$, which completes the proof. $\square$

Lemma 5.13. *Let $E/\mathbb{Q}$ be an elliptic curve such that $E(\mathbb{Q}(\mu_{2^\infty}))[2^\infty] \simeq \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z}$. Then*

$$E(\mathbb{Q}(\mu_{2^4}))[2^\infty] \simeq \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z}.$$

Proof. The proof is similar to the proof of the previous Lemma. If P and Q are the points in $E(\mathbb{Q}(\mu_{2^\infty}))$ of orders 4 and 16 respectively that generate torsion subgroup $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z}$, then $\langle 4Q \rangle$ is the kernel of the rational 4-isogeny and $\mathbb{Q}(4Q)$ is at most quadratic extension of $\mathbb{Q}$. We conclude that the degree of $\mathbb{Q}(P,Q)$ is at most 32. Therefore, $\mathbb{Q}(P,Q) \subseteq \mathbb{Q}(\mu_{2^6})$. A calculation in `magma` [1] shows that if $\mathbb{K} = \mathbb{Q}(P,Q)$ and $[\mathbb{K} : \mathbb{Q}] \geq 16$, then $\mathrm{Gal}\,(\mathbb{K}/\mathbb{Q})$ is isomorphic to one of the groups

$$(\mathbb{Z}/2\mathbb{Z})^4, \quad (\mathbb{Z}/2\mathbb{Z})^2 \oplus \mathbb{Z}/4\mathbb{Z}, \quad (\mathbb{Z}/2\mathbb{Z})^5, \quad (\mathbb{Z}/2\mathbb{Z})^3 \oplus \mathbb{Z}/4\mathbb{Z}.$$

We conclude that $\mathbb{K}$ is not contained in $\mathbb{Q}(\mu_{2^\infty})$, which completes the proof. $\square$

Finally, the following Lemma concludes the proof of Theorem 1.3.

Lemma 5.14. *Let $E/\mathbb{Q}$ be an elliptic curve. Then*

$$E(\mathbb{Q}(\mu_{2^\infty}))_{tors} = E(\mathbb{Q}(\mu_{2^4}))_{tors}.$$

Proof. Let $q > 2$ be a prime number and n a positive integer such that $E(\mathbb{Q}(\mu_{2^\infty}))$ contains a point P of order q^n. As before, we conclude that $\mathbb{Q}(P) \subseteq \mathbb{Q}(\mu_{2^4})$, except when $q = 17$ and $n = 1$. Let $P \in E(\mathbb{Q}(\mu_{2^\infty}))$ be a point of order 17. We know that $E(\mathbb{Q}(\mu_{2^\infty}))_{\text{tors}} \simeq \mathbb{Z}/17\mathbb{Z}$, which means that E has a rational 17-isogeny. Furthermore, we have $\mathbb{Q}(P) \subseteq \mathbb{Q}(\mu_{2^5})$. By [14] and [19], we see that

$$j(E) = \frac{-17^2 \cdot 101^3}{2}, \quad \text{which is true for elliptic curve } 14450\text{p1}$$

$$\text{or}$$

$$j(E) = \frac{-17 \cdot 373^3}{2^{17}}, \quad \text{which is true for elliptic curve } 14450\text{p2}.$$

For each of those two j-invariants we compute and factor the 17th division polynomials associated to the two elliptic curves previously mentioned. More precisely, we're searching for irreducible factors of degree ≤ 16 and we check that no such factors have zeroes defined over $\mathbb{Q}(\mu_{2^5})$. Therefore, $E(\mathbb{Q}(\mu_{2^\infty}))$ can't contain a point of order 17.

It remains to consider the points of order 2^n. We see that $E(\mathbb{Q}(\mu_{2^\infty}))[2^\infty]$ is isomorphic to one of the following groups:

$$\mathbb{Z}/2\mathbb{Z}, \quad \mathbb{Z}/4\mathbb{Z}, \quad \mathbb{Z}/8\mathbb{Z}, \quad \mathbb{Z}/16\mathbb{Z},$$

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}, \quad \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}, \quad \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}, \quad \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z},$$

$$\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}, \quad \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}, \quad \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z},$$

$$\mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}.$$

If $E(\mathbb{Q}(\mu_{2^\infty}))[2^\infty] \simeq \mathbb{Z}/2^n\mathbb{Z}$, for some $n \in \{1, 2, 3, 4\}$, then E has a rational 2^n-isogeny so the claim immediately follows from the Table 3.

We know that $\text{Gal}(\mathbb{Q}(\zeta_2)/\mathbb{Q}) \simeq \{0\}$, $\text{Gal}(\mathbb{Q}(\zeta_4)/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z}$ and

$$\text{Gal}(\mathbb{Q}(\zeta_{2^k})/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2^{k-2}\mathbb{Z},$$

for every positive integer $k > 2$. Using the Theorem 5.1 we conclude that the torsion $\mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$ can not occur. Furthermore, the same Theorem implies that our claim holds in the case when the torsion subgroup is isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$.

Lemma 5.10 implies that if $E(\mathbb{Q}(\mu_{2^\infty}))[2^\infty] \simeq \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$, then that torsion subgroup is actually defined over $\mathbb{Q}(\mu_{2^4})$. When the torsion subgroup equals to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z}$ or $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z}$, the claim follows by the Lemma 5.12 or the Lemma 5.13, respectively.

It remains to check the case when the torsion subgroup is $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$. Assume that the points P and Q generate such torsion subgroup. The group $\langle 2Q \rangle$ is the kernel of a rational k-isogeny and we know that $2Q$ is defined over a number field of degree at most 2. This means that the point Q is defined over a number field of degree at most $2 \cdot 4 = 8$, so it's defined over $\mathbb{Q}(\mu_{2^4})$. This completes the proof of this Lemma and the proof of the Theorem 1.3. $\qquad\square$

Remark. `Magma` [1] code used in this paper can be found on Ivan Krijan's webpage.

References

[1] W. Bosma, J. Cannon, and C. Playoust. The magma algebra system. i. the user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. ↑ 7, 8, 11, 13, 15, 16, 17.

[2] M. Chou. Torsion of rational elliptic curves over the maximal abelian extension of $\mathbb{Q}$. *Pacific J. Math.*, 302(2):481–509, 2019. ↑ 6.

[3] M. Chou, H. B. Daniels, I. Krijan, and F. Najman. Torsion groups of elliptic curves over the $\mathbb{Z}_p$-extensions of $\mathbb{Q}$. Submitted. ↑ 1, 2, 3, 5, 6, 9, 14.

[4] H. B. Daniels, Á. Lozano-Robledo, F. Najman, and A. V. Sutherland. Torsion points on rational elliptic curves over the compositum of all cubic fields. *Math. Comp.*, 87:425–458, 2018. ↑ 3.

[5] M. Derickx and A. V. Sutherland. Torsion subgroups of elliptic curves over quintic and sextic number fields. *Proc. Amer. Math. Soc.*, 145:4233–4245, 2017. ↑ 15.

[6] E. González-Jiménez and Á. Lozano-Robledo. Elliptic curves with abelian division fields. *Math. Z.*, 283:835—-859, 2016. ↑ 11.

[7] E. González-Jiménez and F. Najman. Growth of torsion groups of elliptic curves upon base change. *Math. Comp.*, 89:1457–1485, 2020. ↑ 4, 5, 8, 10, 15, 16.

[8] R. Greenberg. Iwasawa theory for elliptic curves. In C. Viola, editor, *Arithmetic Theory of Elliptic Curves*, volume 1716 of *Lecture Notes in Mathematics*, pages 51–144. Springer, Berlin, Heidelberg, 1999. ↑ 1.

[9] R. Greenberg. The image of galois representations attached to elliptic curves with an isogeny. *Amer. J. Math.*, 134(5):1167–1196, 2012. ↑ 10, 14.

[10] M. A. Kenku. The modular curve $x_0(39)$ and rational isogeny. *Math. Proc. Cambridge Philos. Soc.*, 85:21–23, 1979. ↑ 3.

[11] M. A. Kenku. The modular curve $x_0(169)$ and rational isogeny. *J. London Math. Soc.*, s2-22:239–244, 1980. Corrigendum: https://doi.org/10.1112/jlms/s2-23.3.428-s. ↑ 3.

[12] M. A. Kenku. The modular curves $x_0(65)$ and $x_0(91)$ and rational isogeny. *Math. Proc. Cambridge Philos. Soc.*, 87:15–20, 1980. ↑ 3.

[13] M. A. Kenku. The modular curve $x_0(125)$, $x_1(25)$ and $x_1(49)$. *J. London Math. Soc.*, s2-23:415–427, 1981. ↑ 3.

[14] Á Lozano-Robledo. On the field of definition of p-torsion points on elliptic curves over the rationals. *Math. Ann.*, 357:279–305, 2013. ↑ 7, 17.

[15] B. Mazur. Rational isogenies of prime degree. *Invent. Math.*, 44:129–162, 1978. ↑ 2, 3.

[16] F. Najman. The number of twists with large torsion of an elliptic curve. *Rev. R. Acad. Cienc. Exactas Fís. Nat. Ser. A Mat. RACSAM*, 109:535–547, 2015. ↑ 9.

[17] S. Siksek. Explicit methods for modular curves, 2019. Lecture notes. ↑ 8.

[18] J. H. Silverman. *The Arithmetic of Elliptic Curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag New York, 2 edition, 2009. ↑ 3.

[19] The LMFDB Collaboration. The l-functions and modular forms database, 2019. [Online; accessed 30 October 2019]. ↑ 2, 7, 11, 15, 17.

[20] L. C. Washington. *Introduction to Cyclotomic Fields*, volume 83 of *Graduate Texts in Mathematics*. Springer-Verlag New York, 2 edition, 1997. ↑ 1.

[21] D. Zywina. On the possible images of the mod ℓ representations associated to elliptic curves over $\mathbb{Q}$. Submitted. ↑ 10.

DEPARTMENT OD MATHEMATICS, UNIVERSITY OF ZAGREB, BIJENIČKA CESTA 30, 10000 ZAGREB, CROATIA
  Email address: tguzvic@math.hr
  URL: https://web.math.pmf.unizg.hr/~tguzvic/

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF ZAGREB, BIJENIČKA CESTA 30, 10000 ZAGREB, CROATIA
  Email address: ikrijan@math.hr
  URL: http://web.math.pmf.unizg.hr/~ikrijan/