TORSION GROUPS OF ELLIPTIC CURVES OVER $\mathbb{Q}(\mu_{p^\infty})$

TOMISLAV GUŽVIĆ AND BORNA VUKOREPA

ABSTRACT. Let $E/\mathbb{Q}$ be an elliptic curve and $p \in \{5, 7, 11\}$ be a prime. We determine the possibilities for $E(\mathbb{Q}(\zeta_p))_{\text{tors}}$. Additionally, we determine all the possibilities for $E(\mathbb{Q}(\zeta_{16}))_{\text{tors}}$ and $E(\mathbb{Q}(\zeta_{27}))_{\text{tors}}$. Using these results we are able to determine the possibilities for $E(\mathbb{Q}(\mu_{p^\infty}))_{\text{tors}}$.

1. INTRODUCTION

Let $K$ be a number field such that $[K : \mathbb{Q}] = d$ and let $E/K$ be an elliptic curve. A celebrated theorem of Mordell and Weil shows that $E(K)$ is a finitely generated abelian group. Therefore this group can be decomposed as $E(K) = E(K)_{\text{tors}} \oplus \mathbb{Z}^r$, $r \geq 0$. It is known that $E(K)_{\text{tors}}$ is of the form $C_m \oplus C_n$ for two positive integers $m, n$ such that $m$ divides $n$, where $C_m$ and $C_n$ denote cyclic groups of order $m$ and $n$, respectively.

One of the goals in the theory of elliptic curves is the classification of torsion groups of elliptic curves defined over various fields.

Let $d$ be a positive integer. Define $\Phi(d)$ to be the set of possible isomorphism classes of groups $E(K)_{\text{tors}}$, where $K$ runs through all number fields $K$ of degree $d$ and $E$ runs through all elliptic curves over $K$. In [28], Merel proved that $\Phi(d)$ is finite for all positive integers $d$. The set $\Phi(1)$ can be seen in Theorem 1.1 and was determined by Mazur [26].

Theorem 1.1 (Mazur, [26]). Let $E/\mathbb{Q}$ be an elliptic curve. Then

$$E(\mathbb{Q})_{\text{tors}} \cong \begin{cases} C_m, & m = 1, \ldots, 10, 12, \\ C_2 \oplus C_{2m}, & m = 1, \ldots, 4. \end{cases}$$

The set $\Phi(2)$ has been determined by Kenku, Momose and Kamienny [23], [17]. Derickx, Etropolski, Hoeij, Morrow and Zureick-Brown have determined $\Phi(3)$ in [8].

Define $\Phi^{\text{CM}}(d)$ to be the set of possible isomorphism classes of groups $E(K)_{\text{tors}}$, where $K$ runs through all number fields $K$ of degree $d$ and $E$ runs through all elliptic curves with complex multiplication (CM). The set $\Phi^{\text{CM}}(1)$ has been determined by Olson in [33] and $\Phi^{\text{CM}}(d)$ for $d = 2, 3$ by Zimmer and his collaborators in [9], [29] and [34]. The sets $\Phi^{\text{CM}}(d)$, for $4 \leq d \leq 13$ have been determined by Kenku, et al.
determined by Clark, Corn, Rice and Stankewicz in [7]. Bourdon, Pollack and Stankewicz have determined torsion groups of CM elliptic curves over odd degree number fields in [3].

Define $\Phi_Q(d) \subseteq \Phi(d)$ to be the set of possible isomorphism classes of groups $E(K)_{\text{tors}}$, where $K$ runs through all number fields $K$ of degree $d$ and $E$ runs through all elliptic curves defined over $\mathbb{Q}$. For $d = 2, 3$, the sets $\Phi_Q(d)$ have been determined by Najman [32].

**Theorem 1.2.** Let $E/\mathbb{Q}$ be an elliptic curve and $K/\mathbb{Q}$ a quadratic extension. Then $E(K)_{\text{tors}}$ is isomorphic to the one of the following groups:

- $C_m$, $m = 1, 2, \ldots, 9, 10, 12, 15, 16$
- $C_2 \oplus C_{2m}$, $m = 1, 2, 3, 4, 5, 6$
- $C_3 \oplus C_{3m}$, $m = 1, 2$
- $C_4 \oplus C_4$

$C_{15}$ is the only group which appears in only finitely many cases, and only over the extensions $\mathbb{Q}(\sqrt{5})$ and $\mathbb{Q}(\sqrt{-15})$.

**Theorem 1.3.** Let $E/\mathbb{Q}$ be an elliptic curve and $K/\mathbb{Q}$ a cubic extension. Then $E(K)_{\text{tors}}$ is isomorphic to the one of the following groups:

- $C_m$, $m = 1, 2, \ldots, 10, 12, 13, 14, 18, 21$
- $C_2 \oplus C_{2m}$, $m = 1, 2, 3, 4, 7$

$C_{21}$ is the only group which appears in only finitely many cases, and only over the extension $\mathbb{Q}(\zeta_9)^+$. 

The set $\Phi_Q(4)$ has been determined by Chou [5] and González-Jiménez and Najman [12]. The set $\Phi_Q(5)$ has been determined by González-Jiménez in [10]. González-Jiménez and Najman have also proved that $\Phi_Q(p) = \Phi(1)$ for primes $p \geq 7$ in [12]. For an odd prime $\ell$ and a positive integer $d$, Propp [35] has determined when there exists a degree $d$ number field $K$ and an elliptic curve $E/K$ with $j(E) \in \mathbb{Q} \setminus \{0, 1728\}$ such that $E(K)_{\text{tors}}$ contains a point of order $\ell$.

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

For a prime number $p$, we define a set $\mu_{p^\infty}$ as the set of all complex numbers $\omega$ 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 $p^{\text{th}}$ primitive roots of unity.

In [13], the authors considered the following problem: assume that $E/\mathbb{Q}$ is an elliptic curve, $p$ a prime number and $K = \mathbb{Q}(\mu_p^\infty)$. They show that the torsion subgroup of $E$ grows only over small subfields of $K$. More precisely, they showed the following:
Theorem 1.4. Let $E/\mathbb{Q}$ be an elliptic curve, then for a prime number $p \geq 5$ it holds that

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

Furthermore,

$$E(\mathbb{Q}(\mu_{3^n}))_{\text{tors}} = E(\mathbb{Q}(\mu_{3^3}))_{\text{tors}} \quad \text{and} \quad E(\mathbb{Q}(\mu_{2^n}))_{\text{tors}} = E(\mathbb{Q}(\mu_{2^3}))_{\text{tors}}.$$ 

Remark. This result is “the best possible”. For $E = 27a4$ we have that

$$E(\mathbb{Q}(\mu_{3^2}))_{\text{tors}} = C_9 \subsetneq C_{27} = E(\mathbb{Q}(\mu_{3^3}))_{\text{tors}}$$

and for $E = 32a4$ it holds that

$$E(\mathbb{Q}(\mu_{2^3}))_{\text{tors}} = C_2 \oplus C_4 \subsetneq C_2 \oplus C_8 = E(\mathbb{Q}(\mu_{2^4}))_{\text{tors}}.$$ 

It becomes natural to ask how can the torsion group of $E/\mathbb{Q}$ grow when we consider the base change $E/\mathbb{Q}(\zeta_p)$. This becomes much harder then it seems as $p$ grows because our methods sometimes rely on pure computation.

Our results are the following theorems.

Theorem 1.5. Let $E/\mathbb{Q}$ be an elliptic curve. Then $E(\mathbb{Q}(\zeta_{16}))_{\text{tors}}$ is one of the following groups (apart from those in Mazur’s theorem):

$$C_4 \oplus C_4 \quad (15a1), \quad C_2 \oplus C_{10} \quad (2112bd2).$$

Theorem 1.6. Let $E/\mathbb{Q}$ be an elliptic curve. Then $E(\mathbb{Q}(\zeta_{27}))_{\text{tors}}$ can be only one of the next two groups (apart from those in Mazur’s theorem):

$$C_3 \oplus C_3, \quad C_3 \oplus C_6, \quad C_3 \oplus C_9, \quad C_{21}, \quad C_{27}.$$ 

Additionally, in Lemma 5.1 we give a description of the set of possible group structures $E(\mathbb{Q}(\zeta_p))_{\text{tors}}$ can be isomorphic to for $p = 5, 7$ and 11, where $E/\mathbb{Q}$ is an elliptic curve.

We discuss further attempts to classify $E(\mathbb{Q}(\zeta_p))_{\text{tors}}$, for arbitrary prime number $p$.

Magma [2] code used in this paper can be found here.

2. Notation and auxiliary results

Let $E/F$ be an elliptic curve defined over a number field $F$. There exists an $F$-rational cyclic isogeny $\phi : E \to E'$ of degree $n$ if and only if $\langle P \rangle$, where $P \in E(\bar{F})$ is a point of order $n$, is a $\Gal(\bar{F}/F)$-invariant group; in this case we say that $E$ has an $F$-rational $n$-isogeny. When $F = \mathbb{Q}$, the possible degrees of $n$-isogenies of elliptic curves over $\mathbb{Q}$ are known by the following theorem.
Theorem 2.1 (Mazur [27], Kenku [19], [21], [20], [22]). Let $E/\mathbb{Q}$ be an elliptic curve with a rational $n$-isogeny. Then

$$n \in \{1, \ldots, 19, 21, 25, 27, 37, 43, 67, 163\}.$$  

There are infinitely many elliptic curves (up to $\mathbb{Q}$-isomorphism) with a rational $n$-isogeny over $\mathbb{Q}$ for

$$n \in \{1, \ldots, 10, 12, 13, 16, 18, 25\}$$

and only finitely many for all the other $n$. If $E$ does not have complex multiplication, then $n \leq 18$ with $n \neq 14$ or $n \in \{21, 25, 37\}$.

Galois representations. Let $E/\mathbb{Q}$ be an elliptic curve and let $n$ a positive integer. The field $\mathbb{Q}(E[n])$ is the number field obtained by adjoining to $\mathbb{Q}$ all the $x$ and $y$-coordinates of the points of $E[n]$. The absolute Galois group $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on $E[n]$ by its action on the coordinates of the points, inducing a mod $n$ Galois representation attached to $E$:

$$\rho_{E,n} : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \text{Aut}(E[n]).$$

After we fix a basis for the $n$-torsion, we can identify $\text{Aut}(E[n])$ with $\text{GL}_2(\mathbb{Z}/n\mathbb{Z})$. This means that we can consider $\rho_{E,n}(\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$ as a subgroup of $\text{GL}_2(\mathbb{Z}/n\mathbb{Z})$, uniquely determined up to conjugacy. We shall denote $\rho_{E,n}(\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$ by $G_E(n)$. Moreover, since $\mathbb{Q}(E[n])$ is a Galois extension of $\mathbb{Q}$ and $\ker \rho_{E,n} = \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(E[n])))$, by the first isomorphism theorem we have $G_E(n) \cong \text{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$.

We would like to know what are the possibilities for $G_E(n)$ as a subgroup of $\text{GL}(C_n)$. For some values of $n$, this can be seen in Tables 1 and 2. For most values of $n$ we do not have a list of possibilities of $G_E(n)$, but we have a result that helps us see if for a given matrix subgroup $M$ of $\text{GL}(C_n)$ there exists an elliptic curve $E/\mathbb{Q}$ such that $\rho_{E,n}(\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})) = M$ (up to conjugation). The following lemma is well-known and it will be useful in cases where we analyze torsion group of elliptic curve $E/\mathbb{Q}$ over a maximal real subfield of $\mathbb{Q}(\zeta_p)$.

Lemma 2.2. Let $E/\mathbb{Q}$ be an elliptic curve and $L/K$ a quadratic extension of number fields with $L = K(\sqrt{d})$. Let $E(K)_{(2')}$ be the group of $K$-rational points of $E$ of odd order. Then we have:

$$E(K(\sqrt{d}))_{(2')} \cong E(K)_{(2')} \oplus E^d(K)_{(2')}.$$  

Since all cyclotomic extensions are Galois over $\mathbb{Q}$, the following result imposes restrictions on the possibilities for torsion subgroup of $E/\mathbb{Q}$ over a cyclotomic fields.

Lemma 2.3. Let $E/\mathbb{Q}$ be an elliptic curve, $m, n \in \mathbb{N}$ and $K$ a finite Galois extension of $\mathbb{Q}$. Let $E(K)[mn] \cong C_m \oplus C_{mn}$ and $P \in E(K)$ point of order $mn$. Then we have:

$$[\mathbb{Q}(mP) : \mathbb{Q}] \mid M(\phi(n), [K : \mathbb{Q}]),$$
where \( M(\cdot, \cdot) \) is the greatest common divisor and \( \phi \) is the Euler function.

**Proof.** Let \( P \) be a point of order \( mn \) with coordinates in \( K \). Then we can take \( Q \in E[mn] \) such that \( \{P, Q\} \) is a basis for \( E[mn] \). Consider the Galois representation modulo \( n \) with respect to \( E \):

\[
\rho : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \text{GL}_2(\mathbb{Z}/n\mathbb{Z}).
\]

Let \( \sigma \in \text{Gal}(K/\mathbb{Q}) \). Then we have \( P^\sigma = \alpha P + \beta Q \) for some \( \alpha, \beta \in C_{mn} \) because the action of \( \sigma \) on \( P \) preserves the order of a point.

Now we have \( P^\sigma - \alpha P = \beta Q \), so \( \beta Q \in E(K) \). From that follows \( m\beta \equiv 0 \pmod{mn} \). Multiplying by \( m \) gives us \( (mP)^\sigma = \alpha(mP) \) so \( (mP)^\sigma \in \langle mP \rangle \) for all \( \sigma \in \text{Gal}(K/\mathbb{Q}) \). Because of preserving the order, \( \alpha \) has to be in \( (\mathbb{Z}/n\mathbb{Z})^\times \).

Since by considering the restriction map we get \( \text{Gal}(K/\mathbb{Q}) \cong \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})/\text{Gal}(\overline{\mathbb{Q}}/K) \), we have \( (mP)^\sigma \in \langle mP \rangle \) for all \( \sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \). Therefore, for all \( \sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \):

\[
\rho(\sigma) = \begin{pmatrix} \phi(\sigma) & \tau(\sigma) \\ 0 & \psi(\sigma) \end{pmatrix},
\]

where \( \phi, \psi, \tau : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to C_n \), and \( \phi, \psi \) are homomorphisms with image in \( (C_n)^\times \). We know that \( (mP)^\sigma = g(mP) \iff \phi(\sigma) = g \), for all \( \sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \). Therefore, we have:

\[
|\text{Im}(\phi)| = |\{(mP)^\sigma : \sigma \in \text{Gal}(K/\mathbb{Q})\}| = |\text{Orb}(mP)|.
\]

It is clear that \( \text{Stab}(mP) = \text{Gal}(K/\mathbb{Q}(mP)) \), so by orbit and stabilizer theorem we have:

\[
|\text{Im}(\phi)| = \frac{|\text{Gal}(K/\mathbb{Q})|}{|\text{Gal}(K/\mathbb{Q}(mP))|} = [\mathbb{Q}(mP) : \mathbb{Q}].
\]

On the other hand, we have \( \text{Im}(\phi) \leq (\mathbb{Z}/n\mathbb{Z})^\times \), so we have:

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

\( [\mathbb{Q}(mP) : \mathbb{Q}] \mid [K : \mathbb{Q}] \) is obvious and the proof is complete.  \( \square \)

One of the crucial results that we will need is the main result from [6]:
Theorem 2.4. Let $E / \mathbb{Q}$ be a rational elliptic curve. Then $E(\mathbb{Q}^{ab})_{\text{tors}}$ is isomorphic to one of the following groups:

$$C_m, \quad m = 1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 25, 27, 37, 43, 67, 163$$

$$C_2 \oplus C_{2m}, \quad m = 1, 2, \ldots, 8, 9$$

$$C_3 \oplus C_{3m}, \quad m = 1, 3$$

$$C_4 \oplus C_{4m}, \quad m = 1, 2, 3, 4$$

$$C_5 \oplus C_5,$$

$$C_6 \oplus C_6,$$

$$C_8 \oplus C_8.$$

This means that all of our candidate torsion subgroups are the subgroups of the groups in the above list. Our approach will mainly consist of eliminating a certain set of possibilities from the list above in order to classify torsion groups of elliptic curves over a specific cyclotomic field.

3. TORSION GROWTH OVER $\mathbb{Q}(\zeta_{16})$

Assume that $E / \mathbb{Q}$ is an elliptic curve and that $C_m \oplus C_{mn} \subseteq E(\mathbb{Q}(\zeta_{16}))_{\text{tors}}$. By the properties of the Weil pairing, we have $\mathbb{Q}(\zeta_m) \subseteq \mathbb{Q}(\zeta_{16})$. It follows that $m \in \{1, 2, 4, 8\}$. We first eliminate a certain amount of cyclic groups listed in Theorem 2.4.

Lemma 3.1. Let $E / \mathbb{Q}$ be an elliptic curve. Then $E(\mathbb{Q}(\zeta_{16}))_{\text{tors}}$ is not isomorphic to $C_n$ if

$$n \in \{11, 14, 17, 18, 19, 21, 25, 27, 37, 43, 67, 163\}.$$

Proof. Lemma 2.3 gives us that if $P_n$ is a point of order $n \not\in \{17, 21, 25, 37\}$, we have $[\mathbb{Q}(P_n) : \mathbb{Q}] | 2$, which is impossible by Theorem 1.2. By the same lemma we get that if $P_n$ is a point of order $n \in \{21, 25, 37\}$, then we have $[\mathbb{Q}(P_n) : \mathbb{Q}] | 4$, which is impossible by [5, Theorem 1.4].

It remains to consider the case $n = 17$. By [12, Theorem 5.8] we conclude that the point $P_{17}$ of order 17 cannot be defined over some strictly smaller subfield of $\mathbb{Q}(\zeta_{16})$. That means that all $\sigma \in \text{Gal}(\mathbb{Q}(\zeta_{16}) / \mathbb{Q})$ act differently on $P_{17}$. Since $\text{Gal}(\mathbb{Q}(\zeta_{16}))$ has four elements $\sigma$ such that $\sigma^2 = id$, we have that $P_{17}^2 = k^2 P_{17} = P_{17}$ for four different $\sigma$. That means that we have $k^2 \equiv 1 \pmod{17}$ for four different $k$, a contradiction. □

After eliminating plenty of cyclic groups, we discuss the cases when $E$ obtains full 2-torsion over $\mathbb{Q}(\zeta_{16})$. This is done by the following lemmas:

Lemma 3.2. Let $E / \mathbb{Q}$ be an elliptic curve. Then $E(\mathbb{Q}(\zeta_{16}))_{\text{tors}}$ is not isomorphic to $C_2 \oplus C_{14}$ or $C_2 \oplus C_{18}$.
Proof. We will prove the result for $C_2 \oplus C_{14}$ and the proof for the case $C_2 \oplus C_{18}$ is identical.

Let $P_{14} \in E(\mathbb{Q}(\zeta_{16}))$ be the point of order 14. From Lemma 2.3 we get that $[\mathbb{Q}(2P_{14}) : \mathbb{Q}] = 2$. It is also well-known that $[\mathbb{Q}(E[2]) : \mathbb{Q}] \in \{1, 2, 3, 6\}$. Since $E[2]$ is defined over $\mathbb{Q}(\zeta_{16})$, we have $[\mathbb{Q}(E[2]) : \mathbb{Q}] \in \{1, 2\}$.

Let $Q_2$ be a point of order 2 different from $7P_{14}$. We now have $[\mathbb{Q}(2P_{14}, 7P_{14}, Q_2) : \mathbb{Q}] = 4$. Since $2P_{14}, 7P_{14}$ and $Q_2$ generate our torsion subgroup $C_2 \oplus C_{14}$, we now know that this torsion subgroup appears over some strictly smaller subfield of $\mathbb{Q}(\zeta_{16})$.

Now we get a contradiction by using Theorem 1.2 and [5, Theorem 1.4].

Lemma 3.3. Let $E/\mathbb{Q}$ be an elliptic curve. Then $E(\mathbb{Q}(\zeta_{16}))_{\text{tors}}$ is not isomorphic to $C_{15}$, $C_2 \oplus C_{12}$, $C_4 \oplus C_{12}$, $C_4 \oplus C_8$, $C_4 \oplus C_{16}$ or $C_8 \oplus C_8$.

Proof. Both $X_1(15)$ and $X_1(2, 12)$ are elliptic curves. A computation in Magma shows that $X_1(15)(\mathbb{Q}(\zeta_{16}))$ and $X_1(15)(\mathbb{Q})$ have the same Mordell-Weil group structure. Therefore, since $C_{15} \not\subseteq \Phi(1)$, it also cannot appear over $\mathbb{Q}(\zeta_{16})$.

The curves $X_1(2, 12)(\mathbb{Q}(\zeta_{16}))$ and $X_1(2, 12)(\mathbb{Q}(i))$ have the same Mordell-Weil group structure. It was proven in [31, Lemma 7] that $C_2 \oplus C_{12}$ does not appear as a torsion subgroup over $\mathbb{Q}(i)$. Therefore, it also cannot appear over $\mathbb{Q}(\zeta_{16})$. This also covers the case $C_4 \oplus C_{12}$.

We consider the modular curves $X_1(4, 8)(\mathbb{Q}(\zeta_{16}))$ and $X_1(4, 8)(\mathbb{Q}(\zeta_8))$ which are actually elliptic curves. A computation in Magma shows that $X_1(4, 8)(\mathbb{Q}(\zeta_{16}))$ has rank 0 and the same torsion as $X_1(4, 8)(\mathbb{Q}(\zeta_8))$, which contains only cusps, see [4, Case 6.11]. This also covers the cases $C_8 \oplus C_8$ and $C_4 \oplus C_{16}$.

The following lemma is a bit more complicated than the previous ones. The idea is to consider the corresponding modular curve $X_1(16)$ and its Jacobian $J_1(16)$ over some cyclotomic fields in order to determine that the Jacobian has rank 0. After that, we determine torsion of $J_1(\mathbb{Q}(\zeta_{16}))$ and consequently the number of points on $X_1(16)(\mathbb{Q}(\zeta_{16}))$, all of which turn out to be cusps.

Lemma 3.4. Let $E/\mathbb{Q}$ be an elliptic curve. Then $E(\mathbb{Q}(\zeta_{16}))_{\text{tors}}$ is not isomorphic to $C_{16}$, $C_2 \oplus C_{16}$ or $C_{13}$.

Proof. We consider the modular curve $X_1(16)(\mathbb{Q}(\zeta_{16}))$ and its Jacobian $J_1(16)(\mathbb{Q}(\zeta_{16}))$. We will demonstrate the use of standard methods for determining points on $X_1(16)(\mathbb{Q}(\zeta_{16}))$.

A computation in Magma shows that $r(J_1(16)(\mathbb{Q}(\zeta_{16}))) = 0$. Since

$$r(J_1(16)(\mathbb{Q}(\zeta_8))(\sqrt{\zeta_8})) = r(J_1(16)(\mathbb{Q}(\zeta_8))) + r(J_1^{\phi(16)}(\mathbb{Q}(\zeta_8))),$$

the computation of the rank becomes shorter and we obtain that the rank of our Jacobian is 0.

Now we determine $J_1(16)(\mathbb{Q}(\zeta_{16}))_{\text{tors}}$. Rational prime $p = 17$ splits completely in $\mathbb{Q}(\zeta_{16})$ so by
reducing modulo some \( p \) that lies above \( p \) we get an injection

\[
\text{red}_p : J_1(16)(\mathbb{Q}(\zeta_{16}))_{\text{tors}} \to J_1(16)(\mathbb{F}_{17}).
\]

This map is injective due to the result of Katz [18].

A computation in Magma shows that \( |J_1(16)(\mathbb{F}_{17})| = 400 \). It follows that \( |J_1(16)(\mathbb{Q}(\zeta_{16}))| \leq 400 \). By using the generators of the 2-torsion subgroup of \( J_1(16)(\mathbb{Q}(\zeta_{16})) \) and some elements of \( J_1(16)(\mathbb{Q}(\zeta_{16})) \) that we get from some known points on \( X_1(16)(\mathbb{Q}(\zeta_{16})) \), we are able to generate a group with 400 elements. Therefore, we know exactly how \( J_1(16)(\mathbb{Q}(\zeta_{16})) \) looks like.

Now we are able to determine all points on \( X_1(16)(\mathbb{Q}(\zeta_{16})) \) by considering the Mumford representations of the elements of \( J_1(16)(\mathbb{Q}(\zeta_{16})) \). We easily get that \( |X_1(16)(\mathbb{Q}(\zeta_{16}))| = 14 \) with all points being cusps. Therefore, we can conclude that there are no elliptic curves \( E/\mathbb{Q}(\zeta_{16}) \) (and consequently \( E/\mathbb{Q} \)) with a point of order 16 over \( \mathbb{Q}(\zeta_{16}) \).

It remains to show that \( E(\mathbb{Q}(\zeta_{16}))_{\text{tors}} \) can’t be \( C_{13} \). We consider the modular curve \( X_1(13)(\mathbb{Q}(\zeta_{16})) \) and its Jacobian \( J_1(13)(\mathbb{Q}(\zeta_{16})) \).

A computation in Magma shows that \( r(J_1(13)(\mathbb{Q}(\zeta_{16}))) = 0 \). As in the previous lemma, we obtain:

\[
r(J_1(13)(\mathbb{Q}(\zeta_{16}))) = r(J_1(16)(\mathbb{Q}(\zeta_{8}))) + r(J_1^{\text{tors}}(16)(\mathbb{Q}(\zeta_{8}))) = 0.
\]

The next step is to determine \( J_1(13)(\mathbb{Q}(\zeta_{16}))_{\text{tors}} \). We determine the two-torsion subgroup, which turns out to be trivial. Using the result of Katz [18], we get an injection:

\[
\text{red}_p : J_1(13)(\mathbb{Q}(\zeta_{16}))_{\text{tors}} \to J_1(13)(\mathbb{F}_{17}).
\]

We also get that rational prime \( q = 41 \) has inertia degree 2 in \( \mathbb{Q}(\zeta_{16}) \) so we have another injection:

\[
\text{red}_q : J_1(13)(\mathbb{Q}(\zeta_{16}))_{\text{tors}} \to J_1(13)(\mathbb{F}_{41^2}).
\]

We notice that \( \gcd(\#J_1(13)(\mathbb{F}_{17}), \#J_1(13)(\mathbb{F}_{41^2})) = 76 \), so \( \#J_1(13)(\mathbb{Q}(\zeta_{16})) \mid 76 \).

Since the two torsion subgroup is trivial, we get that \( \#J_1(13)(\mathbb{Q}(\zeta_{16})) \mid 19 \). We can find a point of order 19 on our Jacobian. By checking the Mumford representations of those divisors, we find that all of the points on the Jacobian come from cusps on \( X_1(13)(\mathbb{Q}(\zeta_{16})) \) (and actually \( X_1(13)(\mathbb{Q}) \)). Therefore, we can conclude that there are no elliptic curves \( E/\mathbb{Q}(\zeta_{16}) \) (and consequently \( E/\mathbb{Q} \)) such that \( E(\mathbb{Q}(\zeta_{16}))_{\text{tors}} \cong C_{13} \).

\[\square\]

4. Torsion Growth over \( \mathbb{Q}(\zeta_{27}) \)

In this section we prove Theorem 1.6 using a series of lemmas. First we eliminate some possibilities for a cyclic group to appear as the subgroup of \( E(\mathbb{Q}(\zeta_{27})) \). Assume that \( E/\mathbb{Q} \) is an elliptic curve and that \( C_m \oplus C_{mn} \subseteq E(\mathbb{Q}(\zeta_{27}))_{\text{tors}} \). By the properties of the Weil pairing and taking the Theorem 2.4 into account, we have \( \mathbb{Q}(\zeta_m) \subseteq \mathbb{Q}(\zeta_{27}) \). It follows that \( m \in \{1, 2, 3, 6\} \).
Lemma 4.1. Let $E / \mathbb{Q}$ be an elliptic curve. Then $E(\mathbb{Q}(\zeta_{27}))_{\text{tors}}$ is not isomorphic to $C_n$ if $n \in \{11, 13, 14, 15, 16, 17, 19, 25, 37, 43, 67, 163\}$.

Proof. $[C_{11}, C_{25}]:$ If $n \in \{11, 25\}$ is a point of order $n$, then then by Lemma 2.3 we have $[\mathbb{Q}(P_n) : \mathbb{Q}] \geq 2$, which is impossible by Theorem 1.2.

$[C_{13}]:$ Let $P_{13} \in E(\mathbb{Q}(\zeta_{27}))$ be the point of order 13. By Lemma 2.3 we have $[\mathbb{Q}(P_{13}) : \mathbb{Q}] | 6$. Therefore, this torsion subgroup is defined over $\mathbb{Q}(\zeta_9)$. Theorem 1.2 tells us that this torsion subgroup cannot be defined over any number field. Therefore, it is defined over a sextic field. Assume it is defined over a sextic field. Then we can use Lemma 2.2 to get:

$$C_{13} \cong E(\mathbb{Q}(\zeta_9))(2) \cong E(\mathbb{Q}(\zeta_9^+))(2) \oplus E^{-3}(\mathbb{Q}(\zeta_9^+))(2').$$

This means that either $E$ or $E^{-3}$ has torsion subgroup $\mathbb{Z}/13\mathbb{Z}$ defined over $\mathbb{Q}(\zeta_9)^+$. Now we will be finished if we prove that torsion subgroup $\mathbb{Z}/13\mathbb{Z}$ cannot appear over $\mathbb{Q}(\zeta_9)^+$. To do this, we consider $X_1(13)(\mathbb{Q}(\zeta_9)^+)$.

As before, we use Magma to determine that $J_1(13)(\mathbb{Q}(\zeta_9)^+) \cong J_1(13)(\mathbb{Q})$ and that all points on the Jacobian come from cusps, which completes the proof.

$[C_{14}]:$ Let $P_{14} \in E(\mathbb{Q}(\zeta_{27}))$ be a point of order 14. By Lemma 2.3 it follows that $[\mathbb{Q}(2P_{14}) : \mathbb{Q}]$ divides 6, so $\mathbb{Q}(2P_{14})$ is contained in $\mathbb{Q}(\zeta_9)$. The point $7P_{14}$ of order 2 satisfies $[\mathbb{Q}(7P_{14}) : \mathbb{Q}] \in \{1, 2, 3\}$, which means that it is also contained in $\mathbb{Q}(\zeta_9)$. It follows that $P_{14} \in E(\mathbb{Q}(\zeta_9))$. Consider the modular curve $X_1(14)$. It is an elliptic curve with LMFDB label 14.a5. On the LMFDB page of the mentioned curve we can see that its torsion subgroup does not grow in any number field contained in $\mathbb{Q}(\zeta_9)$. It remains to show that $r(E(\mathbb{Q})) = r(E(\mathbb{Q}(\zeta_9))) = 0$, which turns out to be true by a computation in Magma [2]. Therefore $X_1(14)(\mathbb{Q}) = X_1(14)(\mathbb{Q}(\zeta_9))$ and there does not exist an elliptic curve over $\mathbb{Q}$ with a point of order 14 over $\mathbb{Q}(\zeta_9)$ and consequently over $\mathbb{Q}(\zeta_{27})$.

$[C_{15}]:$ Let $P_{15} \in E(\mathbb{Q}(\zeta_{27}))$ be a point of order 15. Then $3P_{15}$ is a point of order 5 and $[\mathbb{Q}(3P_{15}) : \mathbb{Q}]$ is a divisor of $[\mathbb{Q}(\zeta_{27}) : \mathbb{Q}] = 18$. By Table 1 we see that $[\mathbb{Q}(3P_{15}) : \mathbb{Q}] \in \{1, 2\}$. The same way as in the Lemma 4.3, $C_2 \oplus C_{12}$ case, we see that the point $5P_{15}$ of order 3 is also defined over at most a quadratic extension contained in $\mathbb{Q}(\zeta_{27})$. Since there is only one quadratic extension contained in $\mathbb{Q}(\zeta_{27})$, namely $\mathbb{Q}(\zeta_3)$, we have $P_{15} \in E(\mathbb{Q}(\zeta_3))$, which contradicts the Theorem 1.2.

$[C_{16}]:$ Let $P_{16} \in E(\mathbb{Q}(\zeta_{27}))$ be a point of order 16. Then the point $8P_{16}$ has order 2 and we have $[\mathbb{Q}(8P_{16}) : \mathbb{Q}] \in \{1, 2, 3\}$. By [12, Proposition 4.8.] we have $[\mathbb{Q}(P_{16}) : \mathbb{Q}] = 2^a \cdot 3^b$, where $a \geq 0$ is an integer and $b \in \{0, 1\}$. Since the field $\mathbb{Q}(P_{16})$ is contained in $\mathbb{Q}(\zeta_{27})$, it follows that $2^a \cdot 3^b$ divides $[\mathbb{Q}(\zeta_{27}) : \mathbb{Q}] = 18$. We conclude that $[\mathbb{Q}(P_{16}) : \mathbb{Q}] \in \{1, 2, 3, 6\}$. Assume that $[\mathbb{Q}(8P_{16}) : \mathbb{Q}] = 3$. This means that $\mathbb{Q}(8P_{16})$ is cyclic, so the entire 2-torsion is contained in this field and $P_{16}$ is defined over a number field of degree 3 or 6, but such a field is contained in $\mathbb{Q}(\zeta_9)$. Therefore we have $C_2 \oplus C_{16} \subseteq E(\mathbb{Q}(\zeta_9))$, but this is impossible by [14, Theorem 1.1]. It remains to consider the case when $[\mathbb{Q}(8P_{16}) : \mathbb{Q}] \in \{1, 2\}$. It follows that $[\mathbb{Q}(P_{16}) : \mathbb{Q}] \in \{1, 2\}$ again by [12, Proposition 4.8.].
Since $\mathbb{Q}(P_{16})$ is at most quadratic extension of $\mathbb{Q}$ contained in $\mathbb{Q}(\zeta_{27})$, it follows that $\mathbb{Q}(P_{16}) \subseteq \mathbb{Q}(\zeta_{3})$. By [30, Theorem 1] this turns out to be impossible.

Assume that $n \in \{17, 37\}$ and that $P_n \in E(\mathbb{Q}(\zeta_{27}))$ is a point of order $n$. By [12, Theorem 5.8] it follows that $[\mathbb{Q}(P_n) : \mathbb{Q}]$ is divisible by 4, but since $\mathbb{Q}(P_n) \subseteq \mathbb{Q}(\zeta_{27})$, this is impossible.

Let us consider the case when $n = 19$. If $P_{19} \in E(\mathbb{Q}(\zeta_{27}))$ is a point of order 19, then $E$ has a rational 19-isogeny. By [25], we have $j(E) = -2^{15} \cdot 3^3$. The 19th division polynomial $f_{E,19}$ must have a root over $\mathbb{Q}(\zeta_{27})$. Using Magma, we check that this is not the case and therefore we arrive at the contradiction.

Assume that $n \in \{43, 67, 163\}$ and $P_n \in E(\mathbb{Q}(\zeta_{27}))[n]$. By [25, Theorem 2.1] it follows that $[\mathbb{Q}(P_n) : \mathbb{Q}] \geq \frac{n}{2} > [\mathbb{Q}(\zeta_{27}) : \mathbb{Q}] = 18$, a contradiction. □

**Lemma 4.2.** Let $E/\mathbb{Q}$ be an elliptic curve. Then $E(\mathbb{Q}(\zeta_{27}))_{\text{tors}}$ is not isomorphic to $C_{18}$ or $C_2 \oplus C_{18}$.

**Proof.** If $E(\mathbb{Q}(\zeta_{27}))_{\text{tors}} \cong C_{18}$, then Lemma 2.3 directly gives us that this torsion subgroup is defined over a number field of degree 6 which can only be $\mathbb{Q}(\zeta_6)$.

If $E(\mathbb{Q}(\zeta_{27}))_{\text{tors}} \cong C_2 \oplus C_{18}$, then Lemma 2.3 gives us that if $P_{18} \in E(\mathbb{Q}(\zeta_{27}))_{\text{tors}}$ is a point of order 18, then $2P_{18}$ is defined over $\mathbb{Q}(\zeta_9)$. We know that $[\mathbb{Q}(E[2]) : \mathbb{Q}] \in \{1, 2, 3, 6\}$, but all unique subextensions of $\mathbb{Q}(\zeta_{27})$ of those degrees are contained in $\mathbb{Q}(\zeta_9)$, so again our torsion subgroup is defined over $\mathbb{Q}(\zeta_9)$. Now from Lemma 2.2 we get that

$$C_9 \cong E(\mathbb{Q}(\zeta_9))_{(2)} \cong E(\mathbb{Q}(\zeta_9^+))_{(2)} \oplus E^{-3}(\mathbb{Q}(\zeta_9^+))_{(2')}$$

Therefore, one of $E(\mathbb{Q}(\zeta_9^+))$ and $E^{-3}(\mathbb{Q}(\zeta_9^+))$ has a point of order 9. Let $P_2 \in E(\mathbb{Q}(\zeta_9))_{\text{tors}}$ be a point of order 2. If $[\mathbb{Q}(P_2) : \mathbb{Q}] \in \{1, 3\}$, then $P_2$ is on both $E(\mathbb{Q}(\zeta_9^+))$ and $E^{-3}(\mathbb{Q}(\zeta_9^+))$. If $[\mathbb{Q}(P_2) : \mathbb{Q}] = 2$, then there is another point $Q_2$ of order 2 on $E$ defined over $\mathbb{Q}$. In any case, both $E(\mathbb{Q}(\zeta_9^+))$ and $E^{-3}(\mathbb{Q}(\zeta_9^+))$ have a point of order 2. Finally, one of them has a point of order 18. However, it was proved in [24, Lemma 3.4.7] that all the points on $X_1(18)(\mathbb{Q}(\zeta_9^+))$ are cusps, which completes the proof. □

**Lemma 4.3.** Let $E/\mathbb{Q}$ be an elliptic curve. Assume that $C_2 \oplus C_{2n} \cong E(\mathbb{Q}(\zeta_{27}))_{\text{tors}}$. Then $n \in \{1, 2, 3, 4\}$. Additionally, $C_6 \oplus C_6 \not\subseteq E(\mathbb{Q}(\zeta_{27}))$.

**Proof.** From Theorem 2.4 it follows that $n \leq 9$. We have shown that $E(\mathbb{Q}(\zeta_{27}))$ cannot contain a point of order 18 in Lemma 4.2.

Let $P_5 \in E(\mathbb{Q}(\zeta_{27}))$ be the point of order 5. It follows that $E$ has a rational 5-isogeny and $[\mathbb{Q}(P_5) : \mathbb{Q}] \in \{1, 2\}$. If $G_E(2) \subseteq 2B$, then by Table 1 we see that $[\mathbb{Q}(E[2]) : \mathbb{Q}] \in \{1, 2\}$. Thus we have found two at most quadratic fields contained in $\mathbb{Q}(\zeta_{27})$. Since $\mathbb{Q}(\zeta_{27})$ has an unique quadratic subextension $F = \mathbb{Q}(\sqrt{-3})$, it follows that $F = \mathbb{Q}(E[2]) = \mathbb{Q}(P_5)$. We conclude that $C_2 \oplus C_{10} \subseteq E(F)_{\text{tors}}$, which is impossible by [30, Theorem 1].
Assume that $G_E(2) = 2Cn$. By Theorem [38, Theorem 1.1] it follows that $j(E) = t^2 + 1728$, for some $t \in \mathbb{Q}$. Since $E$ has a rational 5-isogeny, by [38, Theorem 1.3] we have $j(E) = \frac{25(s^2 + 10s + 5)^3}{s^3}$, for some $s \in \mathbb{Q} \setminus \{0\}$. It remains to find rational points on the induced curve. By [16, Page 61] we see that such rational points do not exist.

Let $P_3 \in E(\mathbb{Q}(\zeta_{27}))$ be the point of order 3. The extension $\mathbb{Q}(P_3)$ is cyclic over $\mathbb{Q}$ since it is a subfield of $\mathbb{Q}(\zeta_{27})$. By Table 1 we see that $G_E(3)$ must be contained in the Borel subgroup of $\text{GL}_2(\mathbb{Z}/3\mathbb{Z})$. Applying Theorem [25, Theorem 9.3] it follows that $[\mathbb{Q}(P_3) : \mathbb{Q}] \in \{1, 2\}$, so we have $\mathbb{Q}(P_3) \subseteq \mathbb{Q}(\zeta_3)$. Assume that $G_E(2) \subseteq 2B$. By [12, Proposition 4.6] it follows that $C_2 \oplus C_4 \subseteq E(\mathbb{Q}(\zeta_3))$. We conclude that $C_2 \oplus C_{12} \subseteq E(\mathbb{Q}(\zeta_3))$, which is impossible by [30, Theorem 1].

Consider the case when $G_E(2) = 2Cn$. By [12, Proposition 4.8] it follows that the point $P_4$ of order 4 is defined over cubic or sextic subfield contained in $\mathbb{Q}(\zeta_{27})$. A computation in Magma [2] shows that if a point of order 4 is defined over cubic or sextic number field, then $G_E(2) = \text{GL}_2(\mathbb{Z}/2\mathbb{Z})$, a contradiction.

By [11, Corollary 3.5] it follows that this is impossible.,

Since $\mathbb{Q}(E[6])$ is contained in $\mathbb{Q}(\zeta_{27})$, we have that $|G_E(6)|$ divides $[\mathbb{Q}(\zeta_{27}) : \mathbb{Q}] = 18$. Additionally, the group $G_E(6)$ is cyclic. If $|G_E(6)| < 6$, then it follows that $E$ obtains a full 6-torsion over a number field of degree 1, 2 or 3, but this is impossible by Theorem 1.2 and Theorem 1.3. Assume that $|G_E(6)| \in \{6, 9\}$. A search in Magma [2] shows that there exists only one cyclic group $G$ with such property, namely:

$$G := \langle \begin{bmatrix} 2 & 3 \\ 3 & 1 \end{bmatrix} \rangle.$$ 

Reducing $G$ modulo 2 and modulo 3 we see that $G_E(2) = 2Cn$ and $G_E(3) = 3Cs.1.1$. By [38, Theorem 1.1] we have that $j(E) = t^2 + 1728$, for some $t \in \mathbb{Q}$. Similarly from Theorem [38, Theorem 1.2] we have that $j(E) = f(s)^3$, for some rational function $f(s)$ and $s \in \mathbb{Q}$. A computation in Magma [2] shows that the only affine point on the elliptic curve

$$t^2 + 1728 = x^3$$

is $(t, x) = (0, 12)$. A direct computation shows that the equation $12 = f(s)$ does not have a rational solution in $\mathbb{Q}$. Therefore $E$ cannot have $C_6 \oplus C_6$ torsion over $\mathbb{Q}(\zeta_{27})$.

\[\square\]

5. TORSION GROWTH OVER $\mathbb{Q}(\zeta_5)$, $\mathbb{Q}(\zeta_7)$ AND $\mathbb{Q}(\zeta_{11})$

We note that if $p$ is a prime number and $E/\mathbb{Q}$ an elliptic curve such that $E(\mathbb{Q}(\zeta_p))_{\text{tors}}$ contains a subgroup isomorphic to $C_n \oplus C_m$, then by the properties of Weil pairing we have $\mathbb{Q}(\zeta_n) \subseteq \mathbb{Q}(\zeta_p)$ which forces $n \leq 2$. 


Lemma 5.1. Let $E / \mathbb{Q}$ be an elliptic curve and let $p \in \{5, 7, 11\}$ be a prime number. Apart from the groups in Mazur’s theorem, the group $E(\mathbb{Q}(\zeta_p))_{\text{tors}}$ can only be isomorphic to one of the following groups:

- If $p = 5,$
  \[ C_5 \oplus C_3 (550k^2), \ C_{15} (50a2) \text{ and } C_{16} (15a7). \]
- If $p = 7,$
  \[ C_{13} (147c2), \ C_{14} (49a1), \ C_{18} (14a4), \ C_2 \oplus C_{14} (49a4), \ C_2 \oplus C_{18} (14a5). \]
- If $p = 11,$
  \[ C_{11} (121b2), \ C_{25} (11a3), \ C_2 \oplus C_{10} (10230bg2). \]

Proof. Assume that $p = 5.$ By [4, Theorem 5] we conclude that the only possibilities are the ones listed in this Lemma and $C_{17}.$ It is easy to rule out $C_{17}$ by using [12, Theorem 5.8].

Consider the case when $p = 11.$ If $E / \mathbb{Q}$ is an elliptic curve and if $C_n \oplus C_{mn} \in E(\mathbb{Q}(\zeta_{11})),$ then by the properties of the Weil pairing we have $\mathbb{Q}(\zeta_n) \subseteq \mathbb{Q}(\zeta_{11}),$ which forces $n \in \{1, 2, 11\}.$ Applying the Theorem 2.4 we eliminate the possibility $n = 11.$ By [16, Lemma 6.0.8], it remains to show that the groups $C_{15}, C_{16}$ and $C_2 \oplus C_{12}$ do not occur. We note that the set $\Phi_{\mathbb{Q}}(2)$ is described by Theorem 1.2 and the description of the set $\Phi_{\mathbb{Q}}(5)$ can be found in [10, Theorem 1].

- $C_{15}$: Assume that $P_{15} \in E(\mathbb{Q}(\zeta_{11}))$ is a point of order 15. Obviously we have
  \[ E(\mathbb{Q}(\zeta_{11}))[15] \cong C_{15}. \]
  By Lemma 2.3 it follows that $[\mathbb{Q}(P_{15}) : \mathbb{Q}] \in \{1, 2\},$ but this contradicts the Theorem 1.2.

- $C_{16}$: If $P_{16} \in E(\mathbb{Q}(\zeta_{11}))$ is a point of order 16, then $8P_{16}$ has order 2 and is defined over at most quadratic extension contained in $\mathbb{Q}(\zeta_{11}),$ which is $\mathbb{Q}(\sqrt{-11}).$ By [12, Proposition 4.8] it follows that $[\mathbb{Q}(P_{16}) : \mathbb{Q}] \in \{1, 2\}.$ A computation in Magma [2] shows that $X_1(16)(\mathbb{Q}(\sqrt{-11}))$ contains only cusps.

- $C_2 \oplus C_{12}$: As in the previous case, we show that $C_2 \oplus C_{12} \subseteq E(\mathbb{Q}(\sqrt{-11})).$ The modular curve $X_1(2, 12)(\mathbb{Q}(\sqrt{-11}))$ has rank 0 and same torsion as over $\mathbb{Q},$ which means that there does not exist an elliptic curve with $C_2 \oplus C_{12}$ torsion over $\mathbb{Q}(\sqrt{-11}).$

It remains to consider $p = 7.$ Assume that $n \in \{11, 15, 16, 17, 21, 25, 19, 37, 43, 67, 163, 27\}$ and that $E(\mathbb{Q}(\zeta_i)) \cong C_n.$

- $n \in \{11, 15, 17, 25\}$: Lemma 2.3 gives us that if $P_n$ is a point of order $n,$ we have $[\mathbb{Q}(P_n) : \mathbb{Q}] | 2.$ Now Theorem 1.2 gives us the contradiction.

- $n \in \{19, 37, 43, 67, 163\}$: From [12, Theorem 5.8], we get that the point of order $n$ cannot be defined over the field $\mathbb{Q}(\zeta_7)$ (a degree 6 extension).

- $n = 27$: This follows from [14, Theorem 1.1].
• $n = 16$: Lemma 2.3 gives us that if $P_{16} \in E(\mathbb{Q}(\zeta_7))$ is a point of order 16, we have $[\mathbb{Q}(P_{16}) : \mathbb{Q}] = 2$. That means that $P_{16} \in E(\mathbb{Q}(\sqrt{-7}))$. We can use the similar methods as before in Magma to consider $X_1(16)(\mathbb{Q}(\sqrt{-7}))$ and prove that $E$ cannot have a point of order 16 defined over $\mathbb{Q}(\sqrt{-7})$.

• $n = 21$: For $C_{21}$, we conclude from [5, Lemma 2.7] that $E$ has a $\mathbb{Q}$-rational 21-isogeny. There are 4 elliptic curves (up to $\mathbb{Q}$-isomorphism) with a rational 21-isogeny (see [1, p.78-80]). Therefore, we can use the division polynomial method since the elliptic curves with the same $j$-invariant have identical division polynomials, up to scalar. We will consider the seventh division polynomials. We can use Magma [2] to factor those polynomials in the field $\mathbb{Q}(\zeta_7)$ and see that they have no zeroes there. Hence, this case is impossible.

It remains to eliminate only three non-cyclic groups. For $C_2 \oplus C_{16}$, we can use Lemma 2.3 to show that if $P_{16} \in E(\mathbb{Q}(\zeta_7))$ is of order 16, then $[\mathbb{Q}(2P_{16}) : \mathbb{Q}] = 2$. By [12, Proposition 4.6], we can conclude that $[\mathbb{Q}(P_{16}) : \mathbb{Q}] \in \{1, 2\}$. Hence, we have a point of order 16 defined over $\mathbb{Q}(\sqrt{-7})$. However, we already proved that this can’t happen when we considered $C_{16}$. For $C_2 \oplus C_{10}$ and $C_2 \oplus C_{12}$, we consider modular curves $X_1(2, 10)(\mathbb{Q}(\zeta_7))$ and $X_1(2, 12)(\mathbb{Q}(\zeta_7))$ and use Magma to show that they don’t have non-cuspidal points, which completes the proof. □

Remark. Ideally, one would like to give a useful description of possible isomorphism classes of $E/\mathbb{Q}(\zeta_p)$, where $E/\mathbb{Q}$ is an elliptic curve and $p$ is a prime number. One can start with the following question that seems to be out of reach for the authors at the time of writing this paper.

Let $n \in \{13, 16, 18, 25\}$. Under what conditions on the prime number $p$ does there exist an elliptic curve $E/\mathbb{Q}$ with a point $P_n \in E(\mathbb{Q}(\zeta_p))$ of order $n$?
5.1. **Appendix: Images of Mod $p$ Galois representations associated to elliptic curves over $\mathbb{Q}$.**

For each possible known subgroup $G_E(p) \subseteq \text{GL}_2(\mathbb{F}_p)$ where $E/\mathbb{Q}$ is a non-CM elliptic curve and $p$ is a prime, Tables 1 and 2 list in the first and second column the corresponding labels in Sutherland and Zywina notations, and the following data:

- $d_v = |G_E(p) : G_E(p)_v| = |G_E(p) . v|$ for $v \in \mathbb{F}_p^2$, $v \neq (0,0)$; equivalently, the degrees of the extensions $\mathbb{Q}(P)$ over $\mathbb{Q}$ for points $P \in E(\overline{\mathbb{Q}})$ of order $p$.
- $d = |G_E(p)|$; equivalently, the degree $\mathbb{Q}(E[p])$ over $\mathbb{Q}$.

Note that Tables 1 and 2 are partially extracted from Table 3 of [36]. The difference is that [36, Table 3] only lists the minimum of $d_v$, which is denoted by $d_1$ therein.

| Sutherland | Zywina | $d_v$ | $d$ |
|------------|--------|------|----|
| 2Cs        | $G_1$  | 1    | 1  |
| 2B         | $G_2$  | 1,2  | 2  |
| 2Cn        | $G_3$  | 3    | 3  |
| 3Cs.1.1    | $H_{1,1}$ | 1,2 | 2  |
| 3Cs        | $G_1$  | 2,4  | 4  |
| 3B.1.1     | $H_{3,1}$ | 1,6 | 6  |
| 3B.1.2     | $H_{3,2}$ | 2,3 | 6  |
| 3Ns        | $G_2$  | 4    | 8  |
| 3B         | $G_3$  | 2,6  | 12 |
| 3Nn        | $G_4$  | 8    | 16 |
| 5Cs.1.1    | $H_{1,1}$ | 1,4 | 4  |
| 5Cs.1.3    | $H_{1,2}$ | 2,4 | 4  |
| 5Ns.2.1    | $G_3$  | 8,16 | 16 |
| 5Cs        | $G_2$  | 4,4  | 16 |
| 5B.1.1     | $H_{5,1}$ | 4,5 | 20 |
| 5B.1.2     | $H_{5,2}$ | 2,20| 20 |
| 5B.1.3     | $H_{5,2}$ | 4,10| 20 |
| 5Ns        | $G_4$  | 8,16 | 32 |
| 5B.4.1     | $G_6$  | 2,20 | 40 |
| 5B.4.2     | $G_5$  | 4,40 | 40 |
| 5Nn        | $G_7$  | 24   | 48 |
| 5B         | $G_8$  | 4,80 | 80 |
| 5S4        | $G_9$  | 24   | 96 |

**Acknowledgments.** The authors gratefully acknowledge support from the QuantiXLie Center of Excellence, a project co-financed by the Croatian Government and European Union through the European Regional Development Fund - the Competitiveness and Cohesion Operational Programme (Grant KK.01.1.1.01.0004) and by the Croatian Science Foundation under the project no. IP-2018-01-1313.

**References**

[1] B. J. Birch and W. Kuyk (editors): *Modular functions of one variable IV*, volume 476. Springer Berlin, Heidelberg, 1975. ↑ 13.

[2] W. Bosma, J. Cannon, and C. Playoust: *The Magma Algebra System I: The User Language*. J. Symbolic Comput., 24(3-4):235–265, 1997. ISSN 0747-7171. [http://dx.doi.org/10.1006/jsco.1996.0125](http://dx.doi.org/10.1006/jsco.1996.0125), Computational algebra and number theory (London, 1993). ↑ 3, 9, 11, 12, 13.
| Sutherland | Zywina | $d_v$ | $d$ |
|-----------|--------|-------|-----|
| 7Ns.2.1   | $H_{1,1}$ | 6, 9, 18 | 18 |
| 7Ns.3.1   | $G_1$    | 12, 18  | 36 |
| 7B.1.1    | $H_{3,1}$ | 1, 42   | 42 |
| 7B.1.3    | $H_{4,1}$ | 6, 7    | 42 |
| 7B.1.2    | $H_{5,2}$ | 3, 42   | 42 |
| 7B.1.5    | $H_{5,1}$ | 6, 21   | 42 |
| 7B.1.6    | $H_{3,2}$ | 2, 21   | 42 |
| 7B.1.4    | $H_{4,2}$ | 3, 14   | 42 |
| 7Ns       | $G_2$    | 12, 36  | 72 |
| 7B.6.1    | $G_3$    | 2, 42   | 84 |
| 7B.6.3    | $G_4$    | 6, 14   | 84 |
| 7B.6.2    | $G_5$    | 6, 42   | 84 |

Table 1. Possible images $G_E(p) \neq \text{GL}_2(\mathbb{F}_p)$, for $p \leq 11$, for non-CM elliptic curves $E/\mathbb{Q}$.

| Sutherland | Zywina | $d_v$ | $d$ |
|-----------|--------|-------|-----|
| 13S4      | $G_7$  | 72, 96 | 288 |
| 13B.3.1   | $H_{5,1}$ | 3, 156 | 468 |
| 13B.3.2   | $H_{4,1}$ | 12, 39 | 468 |
| 13B.3.4   | $H_{5,2}$ | 6, 156 | 468 |
| 13B.3.7   | $H_{4,2}$ | 12, 78 | 468 |
| 13B.5.1   | $G_2$  | 4, 156 | 624 |
| 13B.5.2   | $G_1$  | 12, 52 | 624 |
| 13B.5.4   | $G_3$  | 12, 156| 624 |
| 13B.4.1   | $G_5$  | 6, 156 | 936 |
| 13B.4.2   | $G_4$  | 12, 78 | 936 |
| 13B        | $G_6$  | 12, 156| 1872 |
| 17B.4.2   | $G_1$  | 8, 272 | 1088 |
| 17B.4.6   | $G_2$  | 16, 136| 1088 |
| 37B.8.1   | $G_1$  | 12, 1332| 15984 |
| 37B.8.2   | $G_2$  | 36, 444| 15984 |

Table 2. Known images $G_E(p) \neq \text{GL}_2(\mathbb{F}_p)$, for $p = 13, 17$ or 37, for non-CM elliptic curves $E/\mathbb{Q}$.

[3] A. Bourdon and P. Pollack: Torsion subgroups of CM elliptic curves over odd degree number fields. Int. Math. Res. Not. IMRN, 16:4923–4961, 2017. https://doi.org/10.1093/imrn/rnw163. ↑ 2.

[4] P. Bruin and F. Najman: A criterion to rule out torsion groups for elliptic curves over number fields. Res. Number Theory, 2(3), 2016. https://doi.org/10.1007/s40993-015-0031-5. ↑ 7, 12.

[5] M. Chou: Torsion of rational elliptic curves over quartic Galois number fields. J. Number Theory, 160:603–628, 2016. https://doi.org/10.1016/j.jnt.2015.09.013. ↑ 2, 6, 7, 13.

[6] M. Chou: Torsion of rational elliptic curves over the maximal abelian extension of $\mathbb{Q}$. Pacific J. Math., 302(2):481–509, 2019. https://doi.org/10.2140/pjm.2019.302.481. ↑ 5.

[7] P. L. Clark, P. Corn, A. Rice, and J. Stankiewicz: Computation on elliptic curves with complex multiplication. LMS J. Comput. Math., 17:509–539, 2014. https://doi.org/10.1112/S1461157014000072. ↑ 2.
[8] M. Derickx, A. Etropolski, M. V. Hoeij, J. S. Morrow, and D. Zureick-Brown: Sporadic cubic torsion. Algebra Number Theory, 15 (7):1837–1864, 2021. https://doi.org/10.2140/ant.2021.15.1837. ↑ 1.

[9] G. Fung, H. Ströher, H. Williams, and H. Zimmer: Torsion groups of elliptic curves with integral j-invariant over pure cubic fields. J. Number Theory, 36:12–45, 1990. https://doi.org/10.1016/0022-314X(90)90003-A. ↑ 1.

[10] E. González-Jiménez: Complete classification of the torsion structures of rational elliptic curves over quintic number fields. J. Algebra, 478:484–505, 2017. https://doi.org/10.1016/j.jalgebra.2017.01.012. ↑ 2, 12.

[11] E. González-Jiménez and Á. Lozano-Robledo: On the minimal degree of definition of p-primary torsion subgroups of elliptic curves. Math. Res. Lett., 24:1067–1096, 2017. https://dx.doi.org/10.4310/MRL.2017.v24.n4.a7. ↑ 2, 11.

[12] E. González-Jiménez and F. Najman: Growth of torsion groups of elliptic curves upon base change. Math. Comp., 89:1457–1485, 2020. https://doi.org/10.1090/mcom/3478. ↑ 11.

[13] T. Gužvić and I. Krijan: Torsion groups of elliptic curves over some infinite abelian extensions of Q. Submitted. ↑ 2.

[14] T. Gužvić: Torsion growth of rational elliptic curves in sextic number fields. Journal of Number Theory, 220:330–345, 2021. https://doi.org/10.1016/j.jnt.2020.09.010. ↑ 9, 12.

[15] T. Gužvić: Torsion of elliptic curves with rational j-invariant over number fields of prime degree. Proc. Amer. Math. Soc., 149:3261–3275, 2021. https://doi.org/10.1090/proc/15500.

[16] T. Gužvić: Torsion of elliptic curves with rational j-invariant over number fields. Phd thesis, 2021. ↑ 11, 12.

[17] S. Kamienny: Torsion points on elliptic curves and q-coefficients of modular forms. Invent. Math., 109:221–229, 1992. https://doi.org/10.1007/BF01232025. ↑ 1.

[18] N.M. Katz: Galois properties of torsion points on abelian varieties. Invent. Math., 62:481–502, 1981. https://doi.org/10.1007/BF01394256. ↑ 8.

[19] M. A. Kenku: The modular curve X₀(39) and rational isogeny. Math. Proc. Cambridge Philos. Soc., 85:21–23, 1979. https://doi.org/10.1017/S0305004100005544. ↑ 4.

[20] M. A. Kenku: The modular curve X₀(169) and rational isogeny. J. London Math. Soc., s2-22:239–244, 1980. https://doi.org/10.1112/jlms/s2-22.2.239. Corrigendum: https://doi.org/10.1112/jlms/s2-23.3.428-s. ↑ 4.

[21] M. A. Kenku: The modular curves X₀(65) and X₀(91) and rational isogeny. Math. Proc. Cambridge Philos. Soc., 87:15–20, 1980. https://doi.org/10.1017/S0305004100056462. ↑ 4.

[22] M. A. Kenku: The modular curve X₀(125), X₁(25) and X₁(49). J. London Math. Soc., s2-23:415–427, 1981. https://doi.org/10.1112/jlms/s2-23.3.415. ↑ 4.

[23] M. A. Kenku and F. Momose: Torsion points on elliptic curves defined over quadratic fields. Nagoya Math. J., 109:125–149, 1988. https://doi.org/10.1017/S0027763000002816. ↑ 1.

[24] I. Krijan: Torsion groups of elliptic curves over infinite abelian extensions of Q. https://web.math.pmf.unizg.hr/~ikrijan/pdfs/disertacija.pdf, Phd thesis, 2020. ↑ 10.

[25] Á. Lozano-Robledo: On the field of definition of p-torsion points on elliptic curves over the rationals. Math. Ann., 357:279–305, 2013. https://doi.org/10.1007/s00208-013-0906-5. ↑ 10, 11.

[26] B. Mazur: Modular curves and the Eisenstein ideal. Inst. Hautes Etudes Sci. Publ. Math., 47:33–186, 1978. https://doi.org/10.1007/BF02684339. ↑ 1.
[27] B. Mazur: *Rational isogenies of prime degree*. Invent. Math., 44:129–162, 1978. https://doi.org/10.1007/BF01390348. ↑ 4.

[28] L. Merel: *Bornes pour la torsion des courbes elliptiques sur les corps de nombres*. Invent. Math., 124:437–449, 1996. https://doi.org/10.1007/s002220050059. ↑ 1.

[29] H. Müller, H. Ströher, and H. Zimmer: *Torsion groups of elliptic curves with integral j-invariant over quadratic fields*. J. Reine Angew. Math., 397:100–161, 1989. https://doi.org/10.1515/crll.1989.397.100. ↑ 1.

[30] F. Najman: *Complete classification of torsion of elliptic curves over quadratic cyclotomic fields*. J. Number Theory, 130:1964–1968, 2010. https://doi.org/10.1016/j.jnt.2009.12.008. ↑ 10, 11.

[31] F. Najman: *Torsion of elliptic curves over cyclotomic quadratic fields*. Math. J. Okayama Univ., 53:75–82, 2011. https://web.math.pmf.unizg.hr/~fnajman/tors_kon.pdf. ↑ 7.

[32] F. Najman: *Torsion of rational elliptic curves over cubic fields and sporadic points on $X_1(n)$*. Math. Res. Lett., 23(1):245–272, 2016. https://dx.doi.org/10.4310/MRL.2016.v23.n1.a12. ↑ 2.

[33] L. D. Olson: *Points of finite order on elliptic curves with complex multiplication*. Manuscripta Math., 14:195–205, 1974. https://doi.org/10.1007/BF01171442. ↑ 1.

[34] A. Pethő, T. Weis, and H. Zimmer: *Torsion groups of elliptic curves with integral j-invariant over general cubic number fields*. Internat. J. Algebra Comput., 7:353–413, 1997. https://doi.org/10.1142/S0218196797000174. ↑ 1.

[35] O. Propp: *Cartan images and ℓ-torsion points of elliptic curves with rational j-invariant*. Res. Number Theory, 4, 2018. https://doi.org/10.1007/s40993-018-0097-y. ↑ 2.

[36] A. V. Sutherland: *Computing images of Galois representations attached to elliptic curves*. Forum Math. Sigma, 4:41–79, 2016. https://doi.org/10.1017/fms.2015.33. ↑ 14.

[37] The LMFDB Collaboration: *The L-functions and modular forms database*, 2019. http://www.lmfdb.org.[Online; accessed 30 October 2019].

[38] D. Zywina: *On the possible images of the mod ℓ representations associated to elliptic curves over $\mathbb{Q}$*. https://arxiv.org/pdf/1508.07660.pdf, Accepted for publication in Proceedings of the AMS. ↑ 11.