TORSION GROUPS OF MORDELL CURVES OVER NUMBER FIELDS OF HIGHER DEGREE

TOMISLAV GUŽVIĆ AND BIDISHA ROY

Abstract. Mordell curves over a number field $K$ are elliptic curves of the form $y^2 = x^3 + c$, where $c \in K \setminus \{0\}$. Let $p \geq 5$ be a prime number, $K$ a number field such that $[K : \mathbb{Q}] \in \{2p, 3p\}$ and let $E$ be a Mordell curve defined over $K$. We classify all the possible torsion subgroups $E(K)_{\text{tors}}$ for all Mordell curves $E$ defined over $\mathbb{Q}$ when $[K : \mathbb{Q}] \in \{2p, 3p\}$.

1. Introduction

Let $K$ be a number field and let $E/K$ be an elliptic curve. The set of all $K$-rational points of the elliptic curve is denoted by $E(K)$. By a celebrated theorem of Mordell and Weil, it is known that $E(K)$ is a finitely generated abelian group. If we invoke the structure theorem of finitely generated abelian groups on $E(K)$, we get $E(K) \cong E(K)_{\text{tors}} \oplus \mathbb{Z}^r$, where $r \geq 0$ is an integer, called the rank of the elliptic curve $E$ over $K$. The group $E(K)_{\text{tors}}$ is called the torsion subgroup of $E(K)$. The study of the possible torsion subgroups of a given family of elliptic curve is a well researched topic in algebraic number theory.

It is well known that the possible torsion subgroups are of the form $C_m \oplus C_n$, where $m$ and $n$ are positive integers such that $m$ divides $n$. It is natural to try to classify the possibilities of all $E(K)_{\text{tors}}$, where $K$ runs through all number fields of fixed degree and $E$ runs through all elliptic curves defined over $K$. The focus of this paper is to study the growth of $E(K)_{\text{tors}}$, when $[K : \mathbb{Q}] \in \{2p, 3p\}$ for prime number $p \geq 5$ and for some particular infinite family of elliptic curves.

Before going into more details, we introduce some notations for our convenience and we briefly mention the relevant history. If we fix an integer $d \geq 1$, then by $\Phi(d)$ we will denote the set of all possible torsion subgroups $E(K)_{\text{tors}}$, where $K$ runs through all number fields of degree $d$ and $E$ runs through all elliptic curves defined over $K$. The famous result of Mazur [20], we know that

$$\Phi(1) = \{C_n : n = 1, \ldots, 10, 12\} \cup \{C_2 \oplus C_{2n} : n = 1, \ldots, 4\}.$$ 

In other words, if we fix the number field as the set of all rational numbers, then there are only 15 possibilities of torsion subgroups (up-to isomorphism) for any elliptic curve defined over the set of rational numbers. Later, Kamienny [16] and Kenku-Momose [17] independently addressed the case $d = 2$. More precisely, they showed that

$$\Phi(2) = \{C_n : n = 1, \ldots, 16, 18\} \cup \{C_2 \oplus C_{2n} : n = 1, \ldots, 6\} \cup \{C_3 \oplus C_{3n} : n = 1, 2\} \cup \{C_2 \oplus C_4\}.$$ 

2010 Mathematics Subject Classification. Primary: 11G05, 11R16, 11R21; Secondary: 14H52. 

Keywords and phrases. Elliptic curves, Torsion group, Number fields.
Recently, Derickx, Etropolski, Hoeij, Morrow and Zureick-Brown have determined $\Phi(3)$ in [7]. In general, the set $\Phi(d)$, for $d \geq 4$ is not known.

Since the sets $\Phi(d)$ are not known explicitly, one can think of reducing the family of elliptic curve to a subfamily. In this notion, Najman [22] considered the set $\Phi_Q(d) \subseteq \Phi(d)$ which is the set of all possible torsion subgroups of $E(K)_{\text{tors}}$, where $K$ runs through all number fields of degree $d$ and $E$ runs through all elliptic curves defined over $\mathbb{Q}$. For this subfamily, he completely classified the sets $\Phi_Q(d)$, for $d = 2, 3$. Later, the sets $\Phi_Q(4)$ and $\Phi_Q(p)$, for $p \geq 5$ is prime, have been determined in [11, 13, 22]. Moreover, in [13] it has been shown that $\Phi_Q(7) = \Phi(1)$ and $\Phi_Q(d) = \Phi(1)$ for any integer $d$ not divisible by 2, 3, 5 and 7. For the sextic number fields, H.B. Daniels and González-Jiménez [6] and T. Gužvić [14] have given a partial answer to the classification of $\Phi_Q(6)$.

Apart from the aforementioned family, one can also study a similar thing for another family of elliptic curves, namely the family of elliptic curves with complex multiplication (CM). Moreover, torsion groups of CM elliptic curves have been studied by many mathematicians in the past several years (see for instance [2, 3, 19]). In the case of CM-elliptic curves, we denote by $\Phi_{\text{CM}}(d)$ and $\Phi_{\text{CM}}^Q(d)$ the analogue of the sets $\Phi(d)$ and $\Phi_Q(d)$ respectively after restricting to CM-elliptic curves. In 1974, Olson [23] completely determined the set $\Phi_{\text{CM}}(1)$. The sets $\Phi_{\text{CM}}(2)$ and $\Phi_{\text{CM}}(3)$ were determined as a special case in a paper by Müller et al. [21] and by Zimmer et al. [10, 24] respectively. Recently, Clark et al. [5] have computed the sets $\Phi_{\text{CM}}(d)$ for $4 \leq d \leq 13$. Over odd degree number fields, torsion groups of CM elliptic curves have been determined by Bourdon and Pollack in [4].

Next, we consider a particular subfamily of CM elliptic curves, namely the set of Mordell curves. The family of all Mordell curves over a number field $K$ consists of elliptic curves that are of the form $y^2 = x^3 + c$, for some $c \in K$. In the case of Mordell curves, we denote by $\Phi_{\text{M}}(d)$ the set of all possible torsion subgroups of $E(K)_{\text{tors}}$, where $K$ runs through all number fields of degree $d$ and $E$ runs through all Mordell curves defined over $K$. We also define the set $\Phi_{\text{M}}^Q(d)$ to be the intersection $\Phi_{\text{M}}(d) \cap \Phi_Q(d)$ . The study of the sets $\Phi_{\text{M}}(d)$ began long time ago by Knapp through the determination of the set $\Phi_{\text{M}}(1)$ in [18]. Recently, in [8], the set $\Phi_{\text{M}}^Q(d)$ was computed for $d = 2$ and for all $d \geq 5$ with gcd$(d,6) = 1$.

Recently, in [9] Dey and the second author determined the set $\Phi_{\text{M}}(d)$ and $\Phi_{\text{M}}^Q(d)$ completely for $d = 3$ and 6. Moreover, for a chosen torsion subgroup from the sets $\Phi_{\text{M}}^Q(3), \Phi_{\text{M}}(6)$ and $\Phi_{\text{M}}^Q(3)$, the conditions of arising that subgroup have been completely determined. The determination of the set $\Phi_{\text{M}}(6)$ was earlier established as a particular case in [5].

Motivated by the above, in this paper we study the possible group structures of $E(K)_{\text{tors}}$, where $[K : \mathbb{Q}] = 2p$ with prime $p \geq 5$ and $E$ a Mordell curve defined over $\mathbb{Q}$. More precisely, we have determined the sets $\Phi_{\text{M}}^Q(2p)$ and $\Phi_{\text{M}}^Q(3p)$. The techniques we have used here are completely different from the techniques used in [9]. All the computations in this paper were done in Magma [1].

**Remark 1.** Every elliptic curve $E/K$ with $j(E) = 0$ can be written as a Mordell curve and vice versa. Therefore, the classification of torsion groups of Mordell curves is actually the classification of torsion groups of elliptic curves with $j$-invariant equal to 0.
2. Main Results

First we consider the family of Mordell curves of the form \( y^2 = x^3 + c \) with \( c \in \mathbb{Q} \). Next we observe that it is enough to assume that \( c \) is an integer. For this family of elliptic curves, we find all the possibilities for torsion subgroup of \( E(K) \) where \( K \) is a number field such that \([K : \mathbb{Q}] \in \{2p, 3p\}\).

For an elliptic curve \( E : y^2 = x^3 + c \) with \( c \in \mathbb{Z} \), we write \( c = c_1t^6 \) for some sixth power-free integer \( c_1 \) and for some nonzero integer \( t \). Then \((x, y)\) is a point on the elliptic curve \( E_1 : y^2 = x^3 + c_1 \) if and only if \((t^2x, t^3y)\) is a point on \( E \). Thus, it is enough to assume that \( c \) is a sixth power-free integer. Here we prove the following results.

**Theorem 1.** Let \( p \) be a prime number such that \( p \geq 5 \) and \( K \) be any number field of degree \( 2p \). Also let \( E : y^2 = x^3 + c \) be a Mordell curve, for any 6th power-free element \( c \) in \( \mathbb{Q} \). Then

\[
E(K)_{\text{tors}} \in \Phi_M^M(2p) = \{C_m, m = 1, 2, 3, 6\} \cup \{C_2 \oplus C_{2m}, m = 1, 3\} \cup \{C_3 \oplus C_3\}.
\]

**Theorem 2.** Let \( p \) be a prime number such that \( p \geq 5 \) and \( K \) be any number field of degree \( 3p \). Also let \( E : y^2 = x^3 + c \) be a Mordell curve, for any 6th power-free element \( c \) in \( \mathbb{Q} \). Then

\[
E(K)_{\text{tors}} \in \Phi_M^M(3p) = \{C_m, m = 1, 2, 3, 6, 9\}.
\]

3. Preliminaries

Let \( E \) be an elliptic curve defined over a number field \( K \) and \( n \) be a positive integer. Let \( \overline{K} \) be a fixed algebraic closure of \( K \). The \( n \)-torsion subgroup of \( E(\overline{K}) \) is denoted by \( E[n] \). More precisely, \( E[n] = \{P \in E(\overline{K}) : nP = \mathcal{O}\} \), where the point at infinity, \( \mathcal{O} \) is known as the identity of the group \( E(\overline{K}) \). We adjoin all the \( x \) and \( y \) coordinates of the elements in \( E[n] \) to \( K \) and obtain the number field \( K(E[n]) \). This number field is called **field of definition of the \( n \)-torsion points**. In other words, \( K(E[n]) \) is the smallest field over which the set \( E[n] \) is defined. The absolute Galois group \( \text{Gal}(\overline{K}/K) \) acts on \( E[n] \) by the map \( \sigma(x, y) \mapsto (\sigma(x), \sigma(y)) \), for each \( \sigma \in \text{Gal}(\overline{K}/K) \). This induces a mod \( n \) Galois representation attached to \( E \) as follows

\[
\rho_{E,n} : \text{Gal}(\overline{K}/K) \longrightarrow \text{Aut}(E[n]).
\]

It is well known that \( E[n] \) is a free \( \mathbb{Z}/n\mathbb{Z} \) module of rank 2. After fixing a basis \( \{P, Q\} \) of \( E[n] \), we can identify \( \text{Aut}(E[n]) \) with \( \text{GL}_2(\mathbb{Z}/n\mathbb{Z}) \). It follows that the aforementioned map can now be seen as follows

\[
\rho_{E,n} : \text{Gal}(\overline{K}/K) \longrightarrow \text{GL}_2(\mathbb{Z}/n\mathbb{Z}).
\]

The image of the above map, \( \rho_{E,n}(\text{Gal}(\overline{K}/K)) \) is a subgroup of \( \text{GL}_2(\mathbb{Z}/n\mathbb{Z}) \) and we denote it by \( G_E(n) \).
We note that $K(E[n]) = \{x, y : (x, y) \in E[n]\}$ is a Galois extension over $K$ and since $\ker \rho_{E,n} = \text{Gal}(K/K(E[n]))$, we get that $\rho_{E,n}(\text{Gal}(K/K)) = G_E(n) \cong \frac{\text{Gal}(K/K)}{\ker \rho_{E,n}} = \text{Gal}(K(E[n])/K)$. Let $R = (x(R), y(R))$ be an element in $E[n]$. We obviously have $K(R) = K(x(R), y(R)) \subseteq K(E[n])$. By Galois theory, there exists a subgroup $\mathcal{H}_R$ of $\text{Gal}(K(E[n])/K)$ such that $K(R) = K(E[n])^{\mathcal{H}_R}$, the fixed field of $\mathcal{H}_R$. Now we take the image of $\mathcal{H}_R$ in $\text{GL}_2(\mathbb{Z}/n\mathbb{Z})$ and denote it by $H_R$. Thus, we have

$$[K(R) : K] = [G_E(n) : H_R].$$

Now we state an important observation.

**Observation 1.** Let $E/K$ be an elliptic curve and let $n$ be a positive integer. Let $R \in E[n]$ be a point of order $n$. Then $[K(R) : K]$ divides $|G_E(n)|$.

From the above discussion, it is clear that for a given conjugacy class of $G_E(n)$ in $\text{GL}_2(\mathbb{Z}/n\mathbb{Z})$, we can deduce some relevant arithmetic properties of $K(E[n])$. Since $E[n]$ is a free $\mathbb{Z}/n\mathbb{Z}$ module of rank 2, after fixing a basis $\{P, Q\}$ for $E[n]$, we can identify the $n$-torsion points with $(a, b) \in (\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})$. For any $R \in E[n]$, there exists $a, b \in \mathbb{Z}/n\mathbb{Z}$ such that $R = aP + bQ$. Therefore, it is easy to check that $H_R$ is the stabilizer of $(a, b)$ by the action of $G_E(n)$ on $(\mathbb{Z}/n\mathbb{Z})^2$.

Let $p$ be an odd prime and $\epsilon = -1$, for $p \equiv 3 \pmod{4}$ otherwise let $\epsilon \geq 2$ be the smallest integer such that $(\frac{2}{p}) = -1$. We recall the well-known subgroups of $\text{GL}_2(\mathbb{Z}/p\mathbb{Z})$ as follows.

$$D(a, b) = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}, \quad M_\epsilon(a, b) = \begin{bmatrix} a & b \\ \epsilon b & a \end{bmatrix}, \quad T = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad J = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad B = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix},$$

where $a, b \in \mathbb{F}_p^\times$.

Using the above matrices, we define the following subgroups of $\text{GL}_2(\mathbb{F}_p)$.

$$B(p) = \{D(a, 1), D(1, a), B : a \in \mathbb{F}_p^\times\},$$

$$C_s(p) = \{D(a, b) : a, b \in \mathbb{F}_p^\times\},$$

$$C_s^+(p) = \{D(a, b), T \cdot D(a, b) : a, b \in \mathbb{F}_p^\times\},$$

$$C_{ns}(p) = \{M_\epsilon(a, b) : (a, b) \in \mathbb{F}_p^2, (a, b) \neq (0, 0)\}$$

and

$$C_{ns}^+(p) = \{M_\epsilon(a, b), J \cdot M_\epsilon(a, b) : (a, b) \neq (0, 0)\}.$$

If $E/\mathbb{Q}$ is a CM elliptic curve and $p$ is a prime, then the theory of complex multiplication gives us a lot of information about $G_E(p) \subseteq \text{GL}_2(\mathbb{F}_p)$. In the CM case, the possibilities for $G_E(p)$ are completely understood. We list all the possibilities for $G_E(p)$, where $E/\mathbb{Q}$ is a CM elliptic curve with $j(E) = 0$. The following theorem is obtained by combining [13 Theorem 3.6] and [28 Proposition 1.15]. It is one of the main ingredients for proving Theorem [1] and Theorem [2].
Theorem 3. Let $E/\mathbb{Q}$ be a CM elliptic curve and $p$ be a prime. The ring of endomorphisms of $E_{\mathbb{Q}}$ is an order of conductor $f$ in the ring of integers of an imaginary quadratic field of discriminant $-D$.

(i) If $p = 2$, then $G_E(2) = \text{GL}_2(\mathbb{F}_2)$ or is conjugate in $\text{GL}_2(\mathbb{F}_2)$ to $B(2)$.
(ii) If $p > 2$ and $(D, f) = (3, 1)$

(a) If $p \equiv 1 \pmod{9}$, then $G_E(p)$ is conjugate in $\text{GL}_2(\mathbb{F}_p)$ to $C^+_s(p)$.
(b) If $p \equiv 8 \pmod{9}$, then $G_E(p)$ is conjugate in $\text{GL}_2(\mathbb{F}_p)$ to $C^+_n(p)$.
(c) If $p \equiv 4$ or $7 \pmod{9}$, then $G_E(p)$ is conjugate in $\text{GL}_2(\mathbb{F}_p)$ to $C^+_s(p)$ or to the subgroup $G^3(p) = \{D(a, ab^3), T \cdot D(a, ab^3) : a, b \in \mathbb{F}_p^*\} \subseteq C^+_s(p)$.
(d) If $p \equiv 2$ or $5 \pmod{9}$, then $G_E(p)$ is conjugate in $\text{GL}_2(\mathbb{F}_p)$ to $C^+_n(p)$ or to the subgroup $G_0(p)$ of $C^+_n(p)$.
(e) If $p = 3$, then $G_E(p)$ is conjugate in $\text{GL}_2(\mathbb{F}_3)$ to $3C_{s.1.1}$, $C_s(3)$, $3B_{1.1}$, $3B_{1.2}$ or $B(3)$, where

$$3C_{s.1.1} = \langle \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} \rangle, \quad 3B_{1.1} = \langle \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \rangle,$$

$$3B_{1.2} = \langle \begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \rangle.$$ 

All the cases occur.

The following lemmas (mentioned in [13]) give us useful information regarding the arithmetic structure of $G_E(p)$ which will be needed to prove our results.

Lemma 1. Let $E/K$ be an elliptic curve over a number field and $p$ a prime such that $G_E(p) \cong C^+_n(p)$. Then for a point $P \in E(\overline{K})$ of order $p$, we have $[\mathbb{Q}(P) : \mathbb{Q}] = p^2 - 1$.

Lemma 2. Let $E/K$ be an elliptic curve over a number field and $p$ a prime such that $G_E(p)$ is a conjugate to $C^+_s(p)$ in $\text{GL}_2(\mathbb{F}_p)$. Then for a point $P \in E(\overline{K})$ of order $p$, we have $[\mathbb{Q}(P) : \mathbb{Q}] \in \{(p-1)^2, 2(p-1)\}$; both cases can occur.

Lemma 3. [13] Theorem 5.6. Let $E$ be an elliptic curve defined over $\mathbb{Q}$ and let $p$ be a prime number and let $P \in E(\overline{K})$ be a point of order $p$. If $p \equiv 1 \pmod{3}$ and $G_E(p) \cong G^3(p)$, then

$$[\mathbb{Q}(P) : \mathbb{Q}] \in \left\{ 2(p-1), \frac{(p-1)^2}{3}, \frac{2(p-1)^2}{3} \right\}.$$

If $p \equiv 2 \pmod{3}$ and $G_E(p) \cong G_0(p)$ then

$$[\mathbb{Q}(P) : \mathbb{Q}] \in \left\{ \frac{(p-1)^2}{2}, \frac{2(p-1)^2}{3} \right\}.$$

The classification of $\Phi^M_\mathbb{Q}(3)$ is one of many parts handled by González-Jiménez [12] very recently during classification for $\Phi^\text{CM}_\mathbb{Q}(3)$ for all 13 imaginary quadratic discriminants of class number 1.

We record $\Phi^M_\mathbb{Q}(2)$ in the following theorem.

Theorem 4. [8] Let $E/\mathbb{Q}$ be a Mordell curve and let $K$ be a quadratic number field. Then

$$E(K)_{\text{tors}} \in \Phi^M_\mathbb{Q}(2) = \{C_m, m = 1, 2, 3, 6\} \cup \{C_2 \oplus C_{2m}, m = 1, 3\} \cup C_3 \oplus C_3.$$
Another part of this article is to determine torsion subgroups of Mordell curves over number fields of degree 3p. In order to determine this, we will need the description of the set \( \Phi^M_Q(3) \) as mentioned below.

**Theorem 5.** \([9]\) Let \( E/\mathbb{Q} \) be a Mordell curve and let \( K \) be a cubic number field. Then \( E(K)_{\text{tors}} \in \Phi^M_Q(3) = \{C_m, m = 1, 2, 3, 6, 9\} \).

As we mentioned earlier, the sets \( \Phi^M_Q(2) \) and \( \Phi^M_Q(3) \) have been completely classified in \([8]\) and \([9]\), respectively. In this paper, we merely find the set of all possible torsion groups.

4. **Proof of Theorem 1**

Let \( R_\mathbb{Q}(d) \) be the set of all primes \( p \) such that there exists a number field \( K \) of degree \( d \), an elliptic curve \( E/\mathbb{Q} \) such that there exists a point of order \( p \) on \( E(K)_{\text{tors}} \).

Moreover, we will need the following result.

**Lemma 4.** \([15]\) Lemma 1 \([15]\) For any prime number \( p \geq 7 \), we have \( R_\mathbb{Q}(2p) = \{2, 3, 5, 7\} \). Moreover, we have \( R_\mathbb{Q}(10) = \{2, 3, 5, 7, 11\} \).

It order to complete the proof of Theorem 1, it remains to show that \( E(K)_{\text{tors}} \) cannot contain a subgroup isomorphic to one of the following:

\[ C_{11}, C_7, C_5, C_9, C_4, C_3 \oplus C_6. \]

**Proof of Theorem 1**

- Assume that \( P_{11} \in E(K) \) is a point of order 11. By Theorem 3 we obtain that \( G_E(11) \) is conjugate to \( C_{11}^{ns}(11) \) or to \( G_0(11) \). In any case, by Lemma 1 and Lemma 3 we get that \( [\mathbb{Q}(P_{11}) : \mathbb{Q}] \) is divisible by 4. This is not possible because \( [\mathbb{Q}(P_{11}) : \mathbb{Q}] \) divides \( [K : \mathbb{Q}] = 2p \) which is not divisible by 4.
- Assume that \( P_7 \in E(K) \) is a point of order 7. By Theorem 3 we have that \( G_E(7) \) is conjugate to \( C_7^{+}(7) \) or to \( C_3^{+}(7) \). By Lemma 3 we have that \( [\mathbb{Q}(P_7) : \mathbb{Q}] \) is divisible by 4. But \( \mathbb{Q}(P_7) \subseteq K \) and \( [K : \mathbb{Q}] = 2p \) is not divisible by 4, a contradiction.
- Let \( P_5 \in E(K) \) be a point of order 5. From Theorem 3(ii)(d), we get that \( G_E(5) \) is either conjugate to \( C_{ns}^{+}(5) \) or to the subgroup \( G_0(5) \) of \( C_{ns}^{+}(5) \). In any case, by Lemma 1 and Lemma 3 we get that \( [\mathbb{Q}(P_5) : \mathbb{Q}] \) is divisible by 4 which is not possible because \( [\mathbb{Q}(P) : \mathbb{Q}] \) divides \( [K : \mathbb{Q}] = 2p \).
- Let \( P_3 \in E(K) \) be a point of order 9. Then \( 3P_3 \) is a point of order 3 which we will denote by \( P_3 \). By \([15]\) Proposition 4.6.] it follows that \([\mathbb{Q}(P_3) : \mathbb{Q}(P_3)] \) divides 9 or 6. Furthermore, \([\mathbb{Q}(P_3) : \mathbb{Q}(P_3)] \) divides \([K : \mathbb{Q}] = 2p \). We conclude that \([\mathbb{Q}(P_3) : \mathbb{Q}(P_3)] \in \{1, 2, 3\} \). By Theorem 3(ii)(e) and \([15]\) Table 1, it follows that \([\mathbb{Q}(P_3) : \mathbb{Q}] \in \{1, 2, 3\} \). Finally, we conclude that \([\mathbb{Q}(P_3) : \mathbb{Q}] \in \{1, 2, 4\} \). If \([\mathbb{Q}(P_3) : \mathbb{Q}] = 4 \), then 4 would divide \( 2p \), which is impossible. Hence we finally get that \([\mathbb{Q}(P_3) : \mathbb{Q}] \leq 2 \), which contradicts Theorem 1.
- Let \( P_4 \in E(K) \) be a point of order 4. It follows that \( 2P_4 \) is a point of order 2, which will be denoted by \( P_2 \). As in the previous case, by \([15]\) Proposition 4.6.] we have \([\mathbb{Q}(P_2) : \mathbb{Q}(P_2)] \in \{1, 2, 4\} \). Additionally, by Theorem 3(i), we have that \( G_E(2) \) is conjugate to either \( GL_2(F_2) \) or \( B(2) \). By \([15]\) Table 1 and \([13]\) Lemma 5.1] it follows that \([\mathbb{Q}(P_2) : \mathbb{Q}] \in \{1, 2, 3\} \). We conclude that \([\mathbb{Q}(P_3) : \mathbb{Q}] \in \{1, 2, 3\} \).
\{1, 2, 3, 4, 6, 8, 12\}. Since \( \mathbb{Q}(P_4) : \mathbb{Q} \) divides \( [K : \mathbb{Q}] = 2p \), we have \( \mathbb{Q}(P_4) : \mathbb{Q} \in \{1, 2\} \), which is impossible by Theorem 4.

- Assume that \( C_3 \oplus C_6 \subseteq E(K) \). By Theorem 3 (ii)(e) and Table 1, it follows that \( \mathbb{Q}(E[3]) : \mathbb{Q} \in \{2, 4, 6, 12\} \). Obviously we have \( \mathbb{Q}(E[3]) \subseteq K \), so \( \mathbb{Q}(E[3]) : \mathbb{Q} \) divides \( [K : \mathbb{Q}] = 2p \). Therefore, we must have \( \mathbb{Q}(E[3]) : \mathbb{Q} = 2 \). Let \( P_2 \in E(K) \) be a point of order 2. As in the previous case, we conclude that \( \mathbb{Q}(P_2) : \mathbb{Q} \in \{1, 2\} \). Since \( K \) contains at most one quadratic subextension it follows that \( \mathbb{Q}(P_2) \subseteq \mathbb{Q}(E[3]) \). It follows that \( C_3 \oplus C_6 \subseteq E(K) \). This is not possible by Theorem 4.

Now we show that each group \( G \) contained in \( \Phi_\mathbb{Q}^M(3) \) is also contained in \( \Phi_\mathbb{Q}^M(3p) \) by giving a concrete examples of elliptic curve \( E/\mathbb{Q} \) with \( j(E) = 0 \) and a number field \( L \) such that \( [L : \mathbb{Q}] = 2p \) that satisfy \( E(L)_{\text{tors}} \cong G \).

- Let \( E : y^2 = x^3 - 108 \) be an elliptic curve. We have \( E(\mathbb{Q})_{\text{tors}} \cong \mathcal{O} \). Let \( L \) be a number field such that \( [L : \mathbb{Q}] = 2p \) and \( L \cap \mathbb{Q}(E[2], E[3]) = \mathbb{Q} \). It follows that \( E(L) \) does not contain a point of order 2 or a point of order 3. By what we have previously shown, we get \( E(L)_{\text{tors}} \cong \mathcal{O} \).

- Let \( E : y^2 = x^3 + 27 \) be an elliptic curve and \( K = \mathbb{Q}(\sqrt{2}) \) a number filed. Then by \[8\] Theorem 1, we get \( E(K)_{\text{tors}} \cong C_2 \). Let \( L \) be a number field such that \( L \) contains \( K \), \( [L : \mathbb{Q}] = 2p \) and \( L \cap \mathbb{Q}(E[3]) = \mathbb{Q} \). We conclude that \( E(L) \) does not contain a point of order 3. In order to prove that \( E(L)_{\text{tors}} \cong C_2 \), we need to show that \( E(L)_{\text{tors}} \not\cong C_2 \oplus C_2 \). If \( E(L)_{\text{tors}} \cong C_2 \oplus C_2 \), then the polynomial \( x^3 + 27 \) would split into linear factors over \( L \) which means that \( \zeta_3 \in L \), a contradiction. Therefore, \( E(L)_{\text{tors}} \cong C_2 \).

- Let \( E : y^2 = x^3 + 16 \) be an elliptic curve and \( K = \mathbb{Q}(\sqrt{2}) \) a number filed. Then by \[8\] Theorem 1, we get \( E(K)_{\text{tors}} \cong C_3 \). Let \( L \) be a number field such that \( L \) contains \( K \), \( [L : \mathbb{Q}] = 2p \) and \( L \cap \mathbb{Q}(E[2]) = \mathbb{Q} \). We conclude that \( E(L) \) does not contain a point of order 2. In order to prove that \( E(L)_{\text{tors}} \cong C_3 \), we need to show that \( E(L)_{\text{tors}} \not\cong C_3 \oplus C_3 \). If \( E(L)_{\text{tors}} \cong C_3 \oplus C_3 \), then by the properties of Weil pairing we have \( \zeta_3 \in L \), but this contradicts the construction of \( L \). Therefore, \( E(L)_{\text{tors}} \cong C_3 \).

- Let \( E : y^2 = x^3 + 1 \) be an elliptic curve, \( K = \mathbb{Q}(\sqrt{2}) \) and \( L \) be a number filed that contains \( K \) and \( [L : \mathbb{Q}] = 2p \). By \[8\] Theorem 1, we get \( E(K)_{\text{tors}} \cong C_6 \). From the aforementioned discussion, we have \( E(L)_{\text{tors}} \subseteq \{C_6, C_2 \oplus C_6\} \). If \( E(L)_{\text{tors}} \cong C_2 \oplus C_6 \), then \( x^3 + 1 \) should split completely in \( L \) which is not possible because \( \sqrt{-3} \notin L \). Hence \( E(L)_{\text{tors}} \cong C_6 \).

- Let \( E : y^2 = x^3 - 1 \) be an elliptic curve, \( K = \mathbb{Q}(\zeta_3) \) and \( L \) a number field that contains \( K \), satisfies \( [L : \mathbb{Q}] = 2p \) and \( L \cap \mathbb{Q}(E[3]) = \mathbb{Q} \). We immediately get that \( E(L) \) does not contain a point of order 3. We conclude that \( E(L)_{\text{tors}} \cong C_2 \oplus C_2 \).

- The elliptic curves \( E_1 : y^2 = x^3 - 27 \) and \( E_2 : y^2 + y = x^3 \) satisfy \( E_1(\mathbb{Q}(\zeta_3))_{\text{tors}} \cong C_2 \oplus C_6 \) and \( E_2(\mathbb{Q}(\zeta_3))_{\text{tors}} \cong C_3 \oplus C_3 \).

\( \square \)

5. Proof of Theorem 2

In order to prove Theorem 2, we first need to narrow down the possible set of prime numbers \( p \) for which there exists a Mordell curve \( E/\mathbb{Q} \) and a number field \( L \) of degree
It order to complete the proof of Theorem 2, first we will show that contain a subgroup isomorphic to one of the following:

\[ \text{Proof of Theorem 2:} \]

Let \( E/L \) contains a point of order \( p \). We do this with the help of the following lemma.

**Lemma 5.** Let \( p \neq 3 \) be a prime number. Then \( R_\mathbb{Q}(3p) = \{2, 3, 5, 7\} \cup \{19, 43, 67, 163\} \).

**Proof.** We know that for all positive integers \( n \) and \( d \) we have \( R_\mathbb{Q}(d) \subseteq R_\mathbb{Q}(nd) \). Since \( R_\mathbb{Q}(1) = \{2, 3, 5, 7\} \), we have \( R_\mathbb{Q}(1) \subseteq R_\mathbb{Q}(3p) \), for any \( p \geq 5 \).

By [13, Theorem 5.8.], we can see that the only possible elements of \( R_\mathbb{Q}(3p) \), other than \( R_\mathbb{Q}(1) \) lie in the set \( \{19, 43, 67, 163\} \). This is obtained by using the fact that if \( P \in E(K) \) is a point of order \( p \), then \([Q(P) : \mathbb{Q}] \) must divide \([K : \mathbb{Q}] = 3p\). Hence the proof follows. \( \square \)

By \( R_M^M(d) \), we denote the set of all primes \( p \) such that there exits a number field \( K \) of degree \( d \), a Mordell curve \( E/\mathbb{Q} \) such that there exists a point of order \( p \) on \( E(K) \). In the following lemma, we determine \( R_M^M(3p) \), where \( p \geq 5 \) is a prime number.

**Lemma 6.** Let \( p \geq 5 \) be a prime. Then \( R_M^M(3p) = \{2, 3\} \).

**Proof.** Let \( E/\mathbb{Q} \) be a Mordell curve and let \( P_p \in E(K) \) be a point of order \( p \).

- \( p \in \{7, 43, 67\} \): By Theorem 3 we get that \( G_E(p) \) is conjugate in \( GL_2(\mathbb{F}_p) \) to \( C^+_{10}(p) \) or to the subgroup \( G^3(p) = \{D(a, ab^3), T : D(a, ab^3) : a, b \in \mathbb{F}_p^\times \} \subseteq C^+_{10}(p) \).
  - In any case, by Lemma 1 and Lemma 3 we have that \([Q(P_p) : \mathbb{Q}] \) is even. This is impossible because \([Q(P) : \mathbb{Q}] \) must divide \([K : \mathbb{Q}] = 3p\).
- \( p = 5 \): By Theorem 3(iii)(d), we get that \( G_E(5) \) is either conjugate to \( C^+_{10}(5) \) or to the subgroup \( C_0(5) \) of \( C^+_{10}(5) \). In any case, by Lemma 1 and Lemma 3 we have that \([Q(P_5) : \mathbb{Q}] \) is even, which is impossible.
- \( p \in \{19, 163\} \): By Theorem 3(iii)(a), we get \( G_E(p) \) is conjugate to \( C^+_{10}(p) \). Thus, using Lemma 1 we can see that \([Q(P_p) : \mathbb{Q}] \) is always divisible by \( 4 \), which is not possible.

Assume that \( C_m \subset E(K)_{\text{tors}} \). By the properties of the Weil pairing it follows that \( \mathbb{Q}(\zeta_m) \subset K \), so \( \phi(m) = [\mathbb{Q}(\zeta_m) : \mathbb{Q}] \) divides \([K : \mathbb{Q}] = 3p\). It follows that \( m \in \{1, 2\} \).

It order to complete the proof of Theorem 2, first we will show that \( E(K)_{\text{tors}} \) cannot contain a subgroup isomorphic to one of the following:

\[ C_4, C_{18}, C_{27}, C_2 \oplus C_2. \]

**Proof of Theorem 2:**

- Assume that \( P_4 = (x, y) \in E(K) \) is a point of order \( 4 \). Then \( E(K)_{\text{tors}} \) has an element of order 2, which forces \( c \) to be a cube, so \( c = a^3 \) for some \( a \in K \). Now we observe that \( y(2P) = 0 \iff (x(2P))^3 + a^3 = 0 \). By [23, page-105], we know that \( x(2P) = \frac{x(x^3 - 8a)}{4(x^3 + a)} \). Using this, we obtain \( x^6 + 20a^3x^3 - 8a^6 = 0 \iff x^3 = -10a^3 \pm 6a^3\sqrt{3} \). Since \( a \in K \), we see that \( \sqrt{3} \in K \), which is a contradiction as \( K \) is a number field of odd degree. This concludes that \( E(K)_{\text{tors}} \neq C_4 \).
- Assume that \( P_{18} \in E(K) \) is a point of order 18. By [9, Lemma 4.9.], we get that \( 9 \) divides \([K : \mathbb{Q}] = 3p\) which is not possible because \( p \geq 5 \).
• Assume that $P_{27} \in E(K)$ is a point of order 27. Let $\ell = 3$ and $n = 3$. By [4, Theorem 1.2], we have that $\delta = 2$ and $\mathbb{Z}/27\mathbb{Z} = \mathbb{Z}/\ell^m\mathbb{Z}$ appears as the torsion subgroup of $CM$ elliptic curve over an odd degree number field $K$ such that $[K : \mathbb{Q}] = d$ if and only if $d$ is a multiple of 9. Therefore we conclude that this case is also impossible.

• Assume that $C_2 \oplus C_2 \subseteq E(K)_{\text{tors}}$. By [20] Proposition 1.15, we have $G_E(2)$ is conjugate to $GL_2(F_2)$ or $B(2)$. It follows that $|G_E(2)| \in \{2, 6\}$. But since $|G_E(2)| = |\mathbb{Q}(E[2]) : \mathbb{Q}|$ divides $[K : \mathbb{Q}] = 3p$, we arrive at the contradiction.

Now, for each group $G \in \Phi^M_3(3)$, we need to show that it is contained in $\Phi^M_3(3p)$. We do this in the same manner as we did in the proof of Theorem 1.

• Consider the elliptic curve $E : y^2 = x^3 - 108$. Let $L$ be a number field such that $[L : \mathbb{Q}] = 3p$ and $L \cap \mathbb{Q}(E[2], E[3]) = \mathbb{Q}$. It follows that $E(L)$ does not contain a point of order 2 nor a point of order 3. By what we have previously shown, we get $E(L)_{\text{tors}} \cong \mathcal{O}$.

• Let $E : y^2 = x^3 + 27$ be an elliptic curve over $\mathbb{Q}$. We choose a cubic number field $K$ such that 4·27 and 108 are not cubes in $K$. Then, by [9] Theorem 2.1, we know that $E(K)_{\text{tors}} \cong C_2$. Let $L$ be a number field of degree 3p that contains $K$. As we have shown earlier, $E(L)_{\text{tors}} \subseteq \{\mathcal{O}, C_2, C_3, C_6, C_9\}$. Thus we can conclude $E(L)_{\text{tors}} \subseteq \{C_2, C_6\}$. If $E(L)_{\text{tors}} \cong C_6$, then $E(L)_{\text{tors}}$ has a point $P_3 = (x, y)$ of order 3. By [25, page-105], the 3rd-division polynomial of $E$ has two factors, namely $x$ and $x^3 + 108$. By the construction of $K$, $x^3 + 108$ remains irreducible over $L$. Thus we conclude $E(L)_{\text{tors}} \cong C_2$.

• Consider an elliptic curve $E : y^2 = x^3 + 4$. We have $E(\mathbb{Q})_{\text{tors}} \cong C_3$. Let $L$ be a number field such that $[L : \mathbb{Q}] = 3p$ and $L \cap \mathbb{Q}(E[2]) = \mathbb{Q}$. This immediately gives us that $E(L)_{\text{tors}} \neq C_6$. In order to conclude that $E(L)_{\text{tors}} = C_3$, it remains to show that $E(L)_{\text{tors}} \neq C_9$. Consider the 9th primitive division polynomial (i.e. a polynomial whose roots are precisely the $x$-coordinates of points of order 9 on $E$) $f_{E,9}(x)$ of $E$. The irreducible factors of $f_{E,9}(x)$ are of degrees 9 and 27. Since $[L : \mathbb{Q}] = 3p$, we know that these irreducible factors cannot have a root in $L$. Hence, $E(L)_{\text{tors}} \neq C_9$. Thus we conclude that $E(L)_{\text{tors}} \cong C_3$.

• Consider the elliptic curves $E_1 : y^2 = x^3 + 16$, $E_2 : y^2 = x^3 + 1$ and a number field $M := \mathbb{Q}(x_0)$, where $x_0$ is a root of the irreducible polynomial $x^3 - 3x^2 + 1 = 0$. We have $E_1(M)_{\text{tors}} \cong C_9$ and $E_2(M)_{\text{tors}} \cong C_6$. Let $L$ be a number field containing $M$ such that $[L : \mathbb{Q}] = 3p$. We have previously shown that $E_1(L)_{\text{tors}}$ and $E_2(L)_{\text{tors}}$ are both contained in the set $\{\mathcal{O}, C_2, C_3, C_6, C_9\}$. Therefore, we conclude that $E_1(L)_{\text{tors}} \cong C_9$ and $E_2(L)_{\text{tors}} \cong C_6$.

\[\square\]

Acknowledgement. The first author gratefully acknowledges 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. The second author would like to sincerely thank the Department of Mathematics, University of Zagreb where the project was initiated. The second author thanks also IMPAN for providing appropriate support to conclude this project.
References

[1] Wieb Bosma, John Cannon, and Catherine Playoust, The Magma algebra system. I. The user language, J. Symbolic Comput., 24 (1997), 235–265.
[2] A. Bourdon and P. L. Clark, Torsion points and Galois representations on CM elliptic curves, Pacific J. Math. 305 (2020), no. 1, 43-88.
[3] A. Bourdon and P. L. Clark, Torsion points and isogenies on CM elliptic curves, J. London Math. Soc. 102 (2020), no. 2, 580-622.
[4] A. Bourdon and P. Pollack, Torsion subgroups of CM elliptic curves over odd degree number fields, Math. Res. Not. IMRN (2017), no. 16, 4923-4961.
[5] P. L. Clark, P. Corn, A. Rice and J. Stankewicz, Computation on elliptic curves with complex multiplication, LMS J. Comput. Math. 17 (1) (2014), 509-535.
[6] H. B. Daniels and E. González-Jiménez, On the torsion of rational elliptic curves over sextic fields, Math. Comp. 89 (321) (2020), 411-435.
[7] M. Derickx, A. Etropolski, M. V. Hoeij, J. S. Morrow and D. Zureick-Brown, Sporadic Cubic Torsion, Accepted for publication in Algebra and Number Theory
[8] P. K. Dey, Torsion groups of a family of elliptic curves over number fields, Czechoslovak Math. J. 69 (144) (1) (2019), 161-171.
[9] P. K. Dey and B. Roy, Torsion groups of Mordell curves over cubic and sextic fields, Pub. Math Deb (to appear).
[10] 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 (1) (1990), 12-45.
[11] E. González-Jiménez, Complete classification of the torsion structures of rational elliptic curves over quintic number fields, J. Algebra. 478 (2017), 484-505.
[12] E. González-Jiménez, Torsion growth over cubic fields of rational elliptic curves with complex multiplication, Publicationes Mathematicae Debrecen 97/1-2, 63-76 (2020)
[13] E. González-Jiménez and F. Najman, Growth of torsion groups of elliptic curves upon base change, Math. Comp. 89 (323) (2020), 1457-1485.
[14] T. Gužvić, Torsion growth of rational elliptic curves in sextic number fields, J. Number Theory 220 (2021), 330-345
[15] T. Gužvić, Torsion of elliptic curves with rational $j$-invariant defined over number fields of prime degree, Accepted for publication in Proceedings of the AMS.
[16] S. Kamienny, Torsion points on elliptic curves and q-coefficients of modular forms, Invent. Math. 109 (2) (1992), 221-229.
[17] M. A. Kenku and F. Momose, Torsion points on elliptic curves defined over quadratic fields, Nagoya Math. J. 109 (1988), 125-149.
[18] A. W. Knapp, Elliptic Curves, Mathematical Notes, Vol. 40, Princeton Univ. Press, Princeton, 1992.
[19] A. Lozano-Robledo, Galois representations attached to elliptic curves with complex multiplications, arXiv: 1809.02684.
[20] B. Mazur, Modular curves and the Eisenstein ideal, Inst. Hautes Études Sci. Publ. Math. 47 (1977), 33-186.
[21] H. H. Müller, H. Ströher, and H. G. Zimmer, Torsion groups of elliptic curves with integral $j$-invariant over quadratic fields, J. Reine Angew. Math. 397 (1989), 100–161.
[22] F. Najman, Torsion of rational elliptic curves over cubic fields and sporadic points on $X_1(n)$, Math. Res. Letters. 23 (1) (2016), 245-272.
[23] L. D. Olson, Points of finite order on elliptic curves with complex multiplication, Manuscripta math. 14 (1974), 195-205.
[24] A. Pethő, T. Weis, and H. Zimmer, Torsion groups of elliptic curves with integral $j$-invariant over general cubic number fields, Int. J. Algebra Comput. 7 (1997) 353-413.
[25] J. H. Silverman, The arithmetic of elliptic curves, Graduate Texts in Mathematics, 106. Springer-Verlag, New York, 1986.
[26] D. J. Zywina, On the possible images of the mod $\ell$ representations associated to elliptic curves over $\mathbb{Q}$, arxiv:1508.07660
TORSION GROUPS OF MORDELL CURVES OVER NUMBER FIELDS OF HIGHER DEGREE

Tomislav Gužvić, University of Zagreb, Faculty of Science, Department of Mathematics, Zagreb, Croatia
Email address: tguzvic@math.hr

Bidisha Roy, Institute of Mathematics of the Polish Academy of Sciences, Jana i Jędrzeja Śniadeckich 8, Warsaw 00-656, Poland
Email address: brroy123456@gmail.com