DOI: 10.2478/auom-2022-0022
An. Şt. Univ. Ovidius Constanţa **Vol. 30(2),2022, 125–132**

Torsion subgroups of rational Mordell curves over some families of number fields

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 $[K : \mathbb{Q}] \in \{2p, 3p\}$. 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 on 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 $t$orsion 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

Key Words: Elliptic curves, Torsion group, Number fields
2010 Mathematics Subject Classification: Primary: 11G05, 11R16, 11R21; Secondary: 14H52
Received: 12.05.2021
Accepted: 24.01.2022

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 field K of degree d and E runs through all elliptic curves defined over K. Many number theorists have been studying these sets in last several years. Starting with the famous result of Mazur [24], we know that there are only 15 possibilities of torsion subgroups (up-to isomorphism) for any elliptic curve defined over the field of rational numbers. Later, Kamienny [20] and Kenku-Momose [21] independently addressed the case $d = 2$. Recently, Derickx, Etropolski, van Hoeij, Morrow and Zureick-Brown have determined $\Phi(3)$ in [9]. 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 [26] considered the set $\Phi_{\mathbb{Q}}(d) \subseteq \Phi(d)$ 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 $\Phi_{\mathbb{Q}}(d)$, for $d = 2, 3$. Later, the sets $\Phi_{\mathbb{Q}}(4)$ and $\Phi_{\mathbb{Q}}(p)$, for $p \geq 5$ is prime, have been determined in [14, 17, 26]. Moreover, in [17] it has been shown that $\Phi_{\mathbb{Q}}(7) = \Phi(1)$ and $\Phi_{\mathbb{Q}}(d) = \Phi(1)$ for any integer d not divisible by $2, 3, 5$ and 7. For $d = 6$, Daniels and González-Jiménez [8] and Guvi [18] have given a partial answer to the classification of $\Phi_{\mathbb{Q}}(6)$.

Apart from the aforementioned family, one can also make a similar study 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 [3],[4],[23]). In the case of CM-elliptic curves, we denote by $\Phi^{\text{CM}}(d)$ and $\Phi^{\text{CM}}_{\mathbb{Q}}(d)$ the analogue of the sets $\Phi(d)$ and $\Phi_{\mathbb{Q}}(d)$ respectively after restricting to CM-elliptic curves. In 1974, Olson [27] completely determined the set $\Phi^{\text{CM}}(1)$. In [25] and [12, 28], Müller et al. determined all possible torsion subgroups of elliptic curves with integral j-invariant over quadratic and cubic fields respectively. It is known that j-invariant of CM elliptic curves are also integral. For the higher classification problem, j-invariant do not identify CM case. Towards this direction, Clark [6] first classified the quadratic and cubic cases and it appeared in [7]. Moreover, in [7], Clark et al. have computed the sets $\Phi^{\text{CM}}(d)$ for $2 \leq d \leq 13$. Over odd degree number fields, torsion groups of CM elliptic curves have been determined by Bourdon and Pollack in [5].

Related to $\Phi^{\text{CM}}_{\mathbb{Q}}(d)$, we know the sets $\Phi^{\text{CM}}_{\mathbb{Q}}(2)$ and $\Phi^{\text{CM}}_{\mathbb{Q}}(3)$ which have been computed in [16] and [15], respectively.

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 $\Phi^{\mathrm{M}}(d)$ the set of all possible torsion subgroups of $E(K)_{\mathrm{tors}}$, 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 $\Phi^{\mathrm{M}}_{\mathbb{Q}}(d)$ to be the intersection $\Phi^{\mathrm{M}}(d) \cap \Phi_{\mathbb{Q}}(d)$. It is easy to note that $\Phi^{\mathrm{M}}_{\mathbb{Q}}(d) \subseteq \Phi^{CM}_{\mathbb{Q}}(d)$. The study of the sets $\Phi^{\mathrm{M}}(d)$ began long time ago by Fuerter through the determination of the set $\Phi^{\mathrm{M}}(1)$ in [13].

Recently, the set $\Phi^{\mathrm{M}}_{\mathbb{Q}}(d)$ was computed for $d = 2$ and for all $d \geq 5$ with $\gcd(d, 6) = 1$, in [10]; and for $d = 3$ in [11]* .In particular:

$$\Phi^{\mathrm{M}}_{\mathbb{Q}}(2) = \{C_m : m = 1, 2, 3, 6\} \cup \{C_2 \oplus C_{2m} : m = 1, 3\} \cup \{C_3 \oplus C_3\},$$

$$\Phi^{\mathrm{M}}_{\mathbb{Q}}(3) = \{C_m : m = 1, 2, 3, 6, 9\}.$$

Moreover, in [11] Dey and the second author determined the set $\Phi^{\mathrm{M}}(d)$ and $\Phi^{\mathrm{M}}_{\mathbb{Q}}(d)$ for $d = 3$ and 6.

Motivated by the above, in this paper we study the possible group structures of $E(K)_{\mathrm{tors}}$, where $[K : \mathbb{Q}] = 2p$ or $3p$ with $p \geq 5$ prime and E a Mordell curve defined over $\mathbb{Q}$. More precisely, we have determined the sets $\Phi^{\mathrm{M}}_{\mathbb{Q}}(2p)$ and $\Phi^{\mathrm{M}}_{\mathbb{Q}}(3p)$.

Theorem 1. *Let $p \geq 5$ be a prime number. Then $\Phi^{\mathrm{M}}_{\mathbb{Q}}(qp) = \Phi^{\mathrm{M}}_{\mathbb{Q}}(q)$ for $q = 2, 3$. That is:*

(i) $\Phi^{\mathrm{M}}_{\mathbb{Q}}(2p) = \{C_m : \ m = 1, 2, 3, 6\} \cup \{C_2 \oplus C_{2m} : \ m = 1, 3\} \cup \{C_3 \oplus C_3\}$,

(ii) $\Phi^{\mathrm{M}}_{\mathbb{Q}}(3p) = \{C_m : \ m = 1, 2, 3, 6, 9\}$.

We note that recently, for a prime number p, Bourdon and Chaos [2] characterized the groups that arise as torsion subgroups of an elliptic curve with complex multiplication defined over a number field of degree $2p$.

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.

*Note that $\Phi^{\mathrm{M}}_{\mathbb{Q}}(d)$ for $d = 2, 3$ has been independently obtained in [16] and [15] respectively.

2 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 *n-division field* of E. In other words, $K(E[n])$ is the smallest field over which the set $E[n]$ is defined. Let $P = (x(P), y(P))$ be an element in $E[n]$, we denote by $K(R)$ the field of definition of R, that is $K(R) = K(x(R), y(R))$. One of the main ingredients for proving Theorem 1 is the following result. It is a corollary obtained by combining [26,Proposition 1.15] in the special case $j = 0$ with [13, Theorem 3.6 and Table 1].

Theorem 2. *Let $E/\mathbb{Q}$ be an elliptic curve with $j(E) = 0$, p a prime number and $P \in E[p]$.*

(i) If $p = 2$, then $[\mathbb{Q}(P) : \mathbb{Q}] \in \{1, 2, 3\}$. Moreover, $[\mathbb{Q}(E[2]) : \mathbb{Q}] \in \{2, 6\}$.

(ii) If $p > 2$:

(a)If $p \equiv 1 \pmod 9$, then $[\mathbb{Q}(P) : \mathbb{Q}] \in \{2(p-1), (p-1)^2\}$.

(b) If $p \equiv 8 \pmod 9$, then $[\mathbb{Q}(P) : \mathbb{Q}] \in \{p^2 - 1\}$.

(c) If $p \equiv 4$ or $7 \pmod 9$, then $[\mathbb{Q}(P) : \mathbb{Q}] \in \{2(p-1), (p-1)^2, \frac{(p-1)^2}{2}, \frac{2(p-1)^2}{3}\}$.

(d) If $p \equiv 2$ or $5 \pmod 9$, then $[\mathbb{Q}(P) : \mathbb{Q}] \in \{p^2 - 1, \frac{p^2-1}{3}, 2\frac{(p^2-1)}{3}\}$.

(e) If $p = 3$, then $[\mathbb{Q}(P) : \mathbb{Q}] \in \{1, 2, 3, 4, 6\}$. Moreover, $[\mathbb{Q}(E[3]) : \mathbb{Q}] \in \{2, 4, 6, 12\}$.

Let $R^{\mathrm{M}}_{\mathbb{Q}}(d)$ be the set of all primes p such that there exists a number field K of degree d, a Mordell curve $E/\mathbb{Q}$ such that there exists a point of order p on $E(K)_{\mathrm{tors}}$.

Proposition 1. *Let $p \geq 5$ be a prime. Then $R^{\mathrm{M}}_{\mathbb{Q}}(qp) = \{2, 3\}$ for $q = 2, 3$.*

Proof. Suppose $E/\mathbb{Q}$ is a Mordell curve and K is a number field of degree $[K : \mathbb{Q}] = qp$, for some prime $p \geq 5$. Let $P_r \in E(K)_{\mathrm{tors}}$ be a point of order r, for some prime r. Assume $r \geq 5$. By Theorem 2, $[\mathbb{Q}(P_r) : \mathbb{Q}]$ is either divisible by 4 or $[\mathbb{Q}(P_r) : \mathbb{Q}] = \frac{(r-1)^2}{2}$ with $r \equiv 4$ or $7 \pmod 9$. In later case, $[\mathbb{Q}(P_r) : \mathbb{Q}] = \frac{(r-1)^2}{2}$ is divisible by 9. Since $\mathbb{Q}(P_r) \subseteq K$ and $[K : \mathbb{Q}] = qp$ is not divisible by 4 or 9, we obtain that $r < 5$. Thus $R^{\mathrm{M}}_{\mathbb{Q}}(qp) \subseteq \{2, 3\}$ for $q = 2, 3$. As we have previously mentioned, for $q = 2, 3$ we have $\{2, 3\} = R^{\mathrm{M}}_{\mathbb{Q}}(q) \subseteq R^{\mathrm{M}}_{\mathbb{Q}}(qp)$, which completes the proof. ∎

3 Proof of Theorem 1 (i)

By Proposition 1 we have that $R_{\mathbb{Q}}^{\mathrm{M}}(2p) = \{2, 3\}$. Therefore, in order to complete the proof of Theorem 1 (i), it remains to show that $E(K)_{\text{tors}}$ cannot contain a subgroup isomorphic to one of the following:

$$C_9,\ C_4,\ C_3 \oplus C_6.$$

- Let $P_9 \in E(K)$ be a point of order 9. Then $3P_9$ is a point of order 3 which we will denote by P_3. By [17, Proposition 4.6] it follows that $[\mathbb{Q}(P_9) : \mathbb{Q}(P_3)]$ divides 9 or 6. Furthermore, $[\mathbb{Q}(P_9) : \mathbb{Q}(P_3)]$ divides $[K : \mathbb{Q}] = 2p$. Therefore $[\mathbb{Q}(P_9) : \mathbb{Q}(P_3)] \in \{1, 2\}$. By Theorem 2 (e) it follows that $[\mathbb{Q}(P_3) : \mathbb{Q}] \in \{1, 2\}$. We conclude that $[\mathbb{Q}(P_9) : \mathbb{Q}] \in \{1, 2, 4\}$. If $[\mathbb{Q}(P_9) : \mathbb{Q}] = 4$, then 4 would divide $2p$, which is impossible. Hence we finally get that $[\mathbb{Q}(P_9) : \mathbb{Q}] \leq 2$, but C_9 is not a subgroup of any group in $\Phi_{\mathbb{Q}}^{\mathrm{M}}(2)$.
- 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 [17, Proposition 4.6.] we have $[\mathbb{Q}(P_4) : \mathbb{Q}(P_2)] \in \{1, 2, 4\}$. Additionally, by Theorem 2 (i), we have that $[\mathbb{Q}(P_2) : \mathbb{Q}] \in \{1, 2, 3\}$. We conclude that $[\mathbb{Q}(P_4) : \mathbb{Q}] \in \{1, 2, 3, 4, 6, 8, 12\}$. Since $[\mathbb{Q}(P_4) : \mathbb{Q}]$ divides $[K : \mathbb{Q}] = 2p$, we have $[\mathbb{Q}(P_4) : \mathbb{Q}] \in \{1, 2\}$, but C_4 is not a subgroup of any group in $\Phi_{\mathbb{Q}}^{\mathrm{M}}(2)$.
- Assume that $C_3 \oplus C_6 \subseteq E(K)$. By Theorem 2(e) it follows that $[\mathbb{Q}(E[3]) : \mathbb{Q}] \in \{2, 4, 6, 12\}$. Since $\mathbb{Q}(E[3]) \subseteq K$, we have that $[\mathbb{Q}(E[3]) : \mathbb{Q}]$ 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 can contain at most one quadratic subextension it follows that $\mathbb{Q}(P_2) \subseteq \mathbb{Q}(E[3])$. It follows that $C_3 \oplus C_6 \subseteq E(\mathbb{Q}(E[3]))$. But $C_3 \oplus C_6$ is not a subgroup of any group in $\Phi_{\mathbb{Q}}^{\mathrm{M}}(2)$.

4 Proof of Theorem 1 (ii)

Assume that $C_m \oplus C_m \subseteq E(K)_{\text{tors}}$. By the properties of the Weil pairing it follows that $\mathbb{Q}(\zeta_m) \subseteq K$, so $\phi(m) = [\mathbb{Q}(\zeta_m) : \mathbb{Q}]$ divides $[K : \mathbb{Q}] = 3p$. It follows that $m \in \{1, 2\}$.
By Proposition 1 we have that $R_{\mathbb{Q}}^{\mathrm{M}}(3p) = \{2, 3\}$. Therefore in order to complete the proof of Theorem 1 (ii), it remains to show that $E(K)_{\text{tors}}$ cannot contain a subgroup isomorphic to one of the following:

$$C_4,\ C_{18},\ C_{27},\ C_2 \oplus C_2.$$

- 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 $y(2P_4) = 0$ if and only if $(x(2P_4))^3 + a^3 = 0$. By [29, page-105], we know that $x(2P_4) = \frac{x(x^3-8c)}{4(x^3+c)}$. Using this, we obtain $x^6 + 20a^3x^3 - 8a^6 = 0$ if and only if $x^3 = -10a^3 \pm 6a^3\sqrt{3}$. 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 C_4 is not a subgroup of $E(K)_{\text{tors}}$.

- Assume that $P_{18} \in E(K)$ is a point of order 18. By [11, Proof of 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. By [5, Theorem 1.1] we have $E(K)_{\text{tors}} \cong \mathbb{Z}/27\mathbb{Z}$. Consider $\ell = 3$ and $n = 3$ in [5, Theorem 1.2] to obtain $\delta = 2$ and $\mathbb{Z}/27\mathbb{Z} = \mathbb{Z}/\ell^n\mathbb{Z}$ appears as the torsion subgroup of CM elliptic curve over an odd degree number field K with $[K : \mathbb{Q}] = d$ if and only if d is a multiple of $\ell^\delta = 9$. Therefore we conclude that this case is also impossible.

- Assume that $C_2 \oplus C_2 \subseteq E(K)_{\text{tors}}$. By Theorem 2 (i) we have $|G_E(2)| \in \{2, 6\}$. But since $|G_E(2)| = [\mathbb{Q}(E[2]) : \mathbb{Q}]$ divides $[K : \mathbb{Q}] = 3p$, we arrive to a contradiction.

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. We thank the referee for his/ her valuable suggestions.*

References

[1] W. Bosma, J. Cannon, and C. Playoust, The Magma algebra system. I. The user language, J. Symbolic Comput., 24 (1997), 235265.

[2] A. Bourdon and H. P. Chaos, *Torsion for CM elliptic curves defined over number fields of degree 2p, https://arxiv.org/abs/2110.07819v1.*

[3] A. Bourdon and P. L. Clark, *Torsion points and Galois representations on CM elliptic curves*, Pacific J. Math. 305 (2020), no. 1, 43-88.

[4] A. Bourdon and P. L. Clark, *Torsion points and isogenies on CM elliptic curves*, J. London Math. Soc. 102 (2020), no. 2, 580-622.

[5] 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.

[6] P. L. Clark, *Bounds for torsion on abelian varieties with integral moduli,* arXiv:math/0407264.

[7] 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.

[8] H. B. Daniels and E. González-Jiménez, *On the torsion of rational elliptic curves over sextic fields,* Math. Comp. 89 (321) (2020), 411-435.

[9] M. Derickx, A. Etropolski, M. V. Hoeij, J. S. Morrow and D. Zureick-Brown, *Sporadic Cubic Torsion,* Algebra & Number Theory 15 (7), 1837-1864.

[10] P. K. Dey, *Torsion groups of a family of elliptic curves over number fields,* Czechoslovak Math. J. 69 (144) (1) (2019), 161-171.

[11] P. K. Dey and B. Roy, *Torsion groups of Mordell curves over cubic and sextic fields,* Publicationes Mathematicae Debrecen 99/3-4 (13) (2021).

[12] 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.

[13] R. Fueter, *Ueber kubische diophantische Gleichungen,* Comment. Math. Helv. 2 (1930), no. 1, 6989.

[14] E. González-Jiménez, *Complete classification of the torsion structures of rational elliptic curves over quintic number fields,* J. Algebra. 478 (2017), 484-505.

[15] E. González-Jiménez, *Torsion growth over cubic fields of rational elliptic curves with complex multiplication,* Publicationes Mathematicae Debrecen 97/1-2, 63-76 (2020).

[16] E. González-Jiménez, *Explicit description of the growth of the torsion subgroup of rational elliptic curves with complex multiplication over quadratic fields,* Glas. Mat. Ser. III, 56(76)(2021), 47-61.

[17] E. González-Jiménez and F. Najman, *Growth of torsion groups of elliptic curves upon base change,* Math. Comp. 89 (323) (2020), 1457-1485.

[18] T. Guvi, *Torsion growth of rational elliptic curves in sextic number fields,* J. Number Theory 220 (2021), 330-345.

[19] T. Guvi, *Torsion of elliptic curves with rational j-invariant defined over number fields of prime degree,* Proc. Amer. Math. Soc. 149 (2021), 3261-3275.

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

[21] M. A. Kenku and F. Momose, *Torsion points on elliptic curves defined over quadratic fields,* Nagoya Math. J. 109 (1988), 125-149.

[22] A. W. Knapp, *Elliptic Curves,* Mathematical Notes, Vol. 40, Princeton Univ. Press, Princeton, 1992.

[23] A. Lozano-Robledo, *Galois representations attached to elliptic curves with complex multiplications*, arXiv: 1809.02584, Algebra & Number Theory (to appear).

[24] B. Mazur, *Modular curves and the Eisenstein ideal,* Inst. Hautes Études Sci. Publ. Math. 47 (1977), 33-186.

[25] 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), 100161.

[26] 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.

[27] L. D. Olson, *Points of finite order on elliptic curves with complex multiplication,* Manuscripta math. 14 (1974), 195-205.

[28] 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.

[29] J. H. Silverman, *The arithmetic of elliptic curves,* Graduate Texts in Mathematics, 106. Springer-Verlag, New York, 1986.

[30] D. J. Zywina, *On the possible images of the mod ℓ representations associated to elliptic curves over $\mathbb{Q}$, https://arxiv.org/abs/1508.07660.*

Tomislav Gužvić,
Department of Mathematics,
University of Zagreb,
Bijenička 30, 10 000 Zagreb, Croatia.
Email: tguzvic@math.hr

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