Czechoslovak Mathematical Journal, 69 (144) (2019), 161–171

TORSION GROUPS OF A FAMILY OF ELLIPTIC CURVES OVER NUMBER FIELDS

Pallab Kanti Dey, Allahabad

Received May 8, 2017. Published online July 24, 2018.

Abstract. We compute the torsion group explicitly over quadratic fields and number fields of degree coprime to 6 for a family of elliptic curves of the form $E\colon y^2 = x^3 + c$, where c is an integer.

Keywords: torsion group; elliptic curve; number field

MSC 2010: 14H52, 11R04

1. Introduction

Let K be a number field and E be an elliptic curve defined over K. Then by the Mordell-Weil theorem, the group $E(K)$ of K-rational points is a finitely generated abelian group. We have $E(K) \cong T \oplus \mathbb{Z}^r$ for some nonnegative integer r and for some torsion subgroup T. When $K = \mathbb{Q}$, by Mazur's theorem, see [9], it is well-known that the torsion subgroup of $E(\mathbb{Q})$ is either cyclic of order m for some integer $1 \leqslant m \leqslant 10$ or $m = 12$, or of the form $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z}$ for some integer $1 \leqslant m \leqslant 4$.

If K is a quadratic field, then, by a result of Kamienny in [6] and Kenku, Momose in [7], the torsion subgroup is isomorphic to one of $\mathbb{Z}/m\mathbb{Z}$ for $1 \leqslant m \leqslant 18$, $m \neq 17$ or one of $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z}$ for $1 \leqslant m \leqslant 6$ or one of $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3m\mathbb{Z}$ for $m = 1, 2$ or $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$. Moreover in [5], it has been proved that if we let the quadratic fields vary, then all of the 26 torsion subgroups described above appear infinitely often. However, when we fix a quadratic field, it is still unknown which of the 26 listed groups are actually appearing as torsion subgroup. Najman in [11] and [10] determined all possible torsion subgroups of $E(K)$ when K is a quadratic cyclotomic field, i.e. $K = \mathbb{Q}(\mathrm{i})$ or $\mathbb{Q}(\sqrt{-3})$.

Recently, Najman in [12] found all possible torsion subgroups of $E(K)$ for cubic field K and Enrique González-Jiménez [4] found all possible torsion subgroups of $E(K)$ for quintic number field K whenever E is defined over $\mathbb{Q}$.

The subject of torsion points on CM elliptic curves begins with a result of Olson, see [13]. He showed that the torsion subgroup of $E(\mathbb{Q})$ is isomorphic to one of: the trivial group, $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/6\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ for any CM elliptic curve E over $\mathbb{Q}$. Then in [2], Bourdon, Clark and Stankewicz computed the torsion subgroup for CM elliptic curves defined over number fields of odd degree.

In this paper, we deal with a family of CM elliptic curves of the form $y^2 = x^3 + c$, where $c \in \mathbb{Q}$. By a rational transformation, it is enough to assume that c is an integer. For this family of curves, we derive precise torsion subgroup of $E(K)$ for any quadratic field K and for any number field K of degree coprime to 6.

2. The main results

For an elliptic curve $E\colon\ y^2 = x^3 + c$ with $c \in \mathbb{Z}$, we write $c = c_1 t^6$ for some sixth power-free integer c_1 and for some nonzero integer t. Then (x, y) is a point on the elliptic curve $E_1\colon\ y^2 = x^3 + c_1$ 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 to compute the torsion subgroup of $E(K)$ for some number field K. We prove the following results.

Theorem 1. *Let $E\colon\ y^2 = x^3 + c$ be an elliptic curve for some sixth power-free integer c and let $\mathbb{Q}(\sqrt{d})$ be a quadratic field for some square-free integer d. If T is the torsion subgroup of $E(\mathbb{Q}(\sqrt{d}))$, then T is isomorphic to one of the following groups.*

(1) $\mathbb{Z}/6\mathbb{Z} \begin{cases} \text{if } c = 1 \text{ and } d \neq -3, \\ \text{or } c = a^3 \text{ with } a \neq 1, -3 \text{ for some } a \in \mathbb{Z} \text{ and } d = a; \end{cases}$

(2) $\mathbb{Z}/3\mathbb{Z} \begin{cases} \text{if } c = 2t^3 \text{ with } t \neq 2, -6 \text{ for some } t \in \mathbb{Z} \text{ and} \\ \qquad d \text{ is square-free part of } 2t \text{ or } -6t, \\ \text{or } c = b^2 \neq 1, 16 \text{ for some } b \in \mathbb{Z}, \\ \text{or } c = 16, -432 \text{ and } d \neq -3, \\ \text{or } c \text{ is neither a cube nor a square, } c \neq 2t^3 \text{ for any } t \in \mathbb{Z} \text{ and} \\ \qquad d \text{ is square-free part of } c; \end{cases}$

(3) $\mathbb{Z}/2\mathbb{Z}$ *if* $c = a^3$ *with* $a \neq 1$ *for some* $a \in \mathbb{Z}$ *and* $d \neq a$;

(4) $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ *if* $c = 1, -27$ *and* $d = -3$;

(5) $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ *if* $c = 16, -432$ *and* $d = -3$;

(6) $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ *if* $c = a^3$ *with* $a \neq 1, -3$ *for some* $a \in \mathbb{Z}$ *and* $d = -3$;

(7) $\{\mathcal{O}\}$, *otherwise.*

Theorem 2. *Let $E\colon\ y^2 = x^3 + c$ be an elliptic curve for some sixth power-free integer c and let K be a number field of degree coprime to 6. If T is the torsion subgroup of $E(K)$, then T is isomorphic to one of the following groups.*

(1) $\mathbb{Z}/6\mathbb{Z}$ *if* $c = 1$,
(2) $\mathbb{Z}/3\mathbb{Z}$ *if* $c \neq 1$ *is a square, or* $c = -432$,
(3) $\mathbb{Z}/2\mathbb{Z}$ *if* $c \neq 1$ *is a cube,*
(4) $\{\mathcal{O}\}$, *otherwise.*

3. Preliminaries

In this section, we provide some useful tools which are essential to prove the main results.

For any elliptic curve E over field L and for any positive integer n define

$$E(L)[n] = \{P = (x, y) \in E(L)\colon\ nP = \mathcal{O}\} \cup \{\mathcal{O}\}.$$

Remark 1. Let E be an elliptic curve defined over a number field K. Also let E^d be the d-quadratic twist of E for some $d \in K^*/(K^*)^2$. Then it is well-known that, for any odd positive integer n,

$$E(K(\sqrt{d}))[n] \cong E(K)[n] \times E^d(K)[n].$$

Proposition 1 ([4], Lemma 5)**.** *Let E be an elliptic curve defined over $\mathbb{Q}$ and let $R \in E(\mathbb{C})$ be a point of order n for some positive integer n. Then $[\mathbb{Q}(R) : \mathbb{Q}]$ divides $|\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})|$, where $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ is the set of all 2×2 invertible matrices over $\mathbb{Z}/n\mathbb{Z}$ and the field $\mathbb{Q}(R)$ is the smallest field containing $\mathbb{Q}$, $x(R), y(R)$.*

Proposition 2 ([8], Lemma 5.12, page 149)**.** *Let $E\colon\ y^2 = x^3 + c$ be an elliptic curve for some nonzero integer c. Let $p \equiv 2 \pmod 3$ be an odd prime such that $p \nmid \Delta$, where Δ is the discriminant of E. Then we have*

$$|\overline{E}(\mathbb{F}_p)| = p + 1,$$

where $\overline{E}$ is the elliptic curve obtained by reducing E modulo p.

Proposition 3 ([14], Theorem 4.12, page 103)**.** *For any prime p let $|E(\mathbb{F}_p)| = p + 1 - a$ with $|a| \leqslant 2\sqrt{p}$. Let $X^2 - aX + p = (X - \alpha)(X - \beta)$ be a quadratic equation for some complex numbers α, β. Then*

$$|E(\mathbb{F}_{p^n})| = p^n + 1 - (\alpha^n + \beta^n)$$

for all $n \geqslant 1$.

Corollary 1. *Let $E\colon\ y^2 = x^3 + c$ be an elliptic curve for some nonzero integer c. Let $p \equiv 2 \pmod 3$ be an odd prime such that $p \nmid \Delta$, where Δ is the discriminant of E. Then we have*

$$|\overline{E}(\mathbb{F}_{p^n})| = \begin{cases} p^n + 1 & \text{if } n \text{ is odd},\\ (p^{n/2}+1)^2 & \text{if } n \equiv 2 \pmod 4. \end{cases}$$

P r o o f. We know that $|\overline{E}(\mathbb{F}_p)| = p + 1 - a$ for some integer a with $|a| \leqslant 2\sqrt{p}$. Hence, by Proposition 2, we have $a = 0$ as $p \equiv 2 \pmod 3$. Consider the factorization of the quadratic equation over $\mathbb{C}$ as

$$X^2 + p = (X - \mathrm{i}\sqrt{p})(X + \mathrm{i}\sqrt{p}).$$

By setting $\alpha = \mathrm{i}\sqrt{p}$ and $\beta = -\mathrm{i}\sqrt{p}$ and by Proposition 3, we have

$$|\overline{E}(\mathbb{F}_{p^n})| = \begin{cases} p^n + 1 & \text{if } n \text{ is odd},\\ (p^{n/2}+1)^2 & \text{if } n \equiv 2 \pmod 4. \end{cases}$$

□

Proposition 4 ([3], Proposition 4)**.** *Let $E\colon\ y^2 = x^3 + bx + c$ be an elliptic curve for some integers b and c. Let T be the torsion subgroup of $E(K)$ for some number field K. Also let $\mathcal{O}_K$ be the ring of integers in K and $\mathcal{P}$ be a prime ideal lying above odd prime p in $\mathcal{O}_K$. If E has good reduction at $\mathcal{P}$, then let φ be the reduction modulo $\mathcal{P}$ map on T. Then the reduction map φ is an injective homomorphism except for finitely many prime ideals $\mathcal{P}$.*

Proposition 5 ([8], Theorem 5.3, page 134)**.** *Let $E\colon\ y^2 = x^3 + c$ be an elliptic curve for some sixth power-free integer c. If T is the torsion subgroup of $E(\mathbb{Q})$, then T is isomorphic to one of the following groups.*

(1) *$\mathbb{Z}/6\mathbb{Z}$ if $c = 1$,*
(2) *$\mathbb{Z}/3\mathbb{Z}$ if $c \neq 1$ is a square, or $c = -432$,*
(3) *$\mathbb{Z}/2\mathbb{Z}$ if $c \neq 1$ is a cube,*
(4) *$\{\mathcal{O}\}$, otherwise.*

4. Proof of Theorem 1

To prove Theorem 1, we need to formulate several lemmas.

Lemma 1. *There does not exist any element of order* 4 *in* T.

Proof. Let P be an element of order 4 in T. In that case, T contains an element of order 2 which forces c to be a cube, say, a^3 for some nonzero integer a.

Note that if $P = (x, y)$ is an element of order 4, then $y(2P) = 0 \Leftrightarrow x^6 + 20cx^3 - 8c^2 = 0 \Leftrightarrow x^3 = -10c \pm 6c\sqrt{3}$. Hence, for $d = 3$ we have $x = (-1 \pm \sqrt{3})a \in \mathbb{Z}[\sqrt{3}]$. Therefore for $d \neq 3$ there does not exist any element of order 4.

For $d = 3$, since $x \in \mathbb{Z}[\sqrt{3}]$ and $y^2 = x^3 + c \in \mathbb{Z}[\sqrt{3}]$, we have $y \in \mathbb{Z}[\sqrt{3}]$. Let $y = t_1 + t_2\sqrt{3}$ for some nonzero integers t_1 and t_2. Since $y^2 = x^3 + c$, we get two relations which are $t_1^2 + 3t_2^2 = -9c$ and $t_1t_2 = \pm 3c$. These two relations together imply $t_1^2 + 3t_2^2 \mp 3t_1t_2 = 0$. Putting $t = t_1/t_2 \in \mathbb{Q}$, we have

$$t^2 \mp 3t + 3 = 0 \implies t = \frac{\pm 3 \pm \sqrt{-3}}{2},$$

a contradiction as $t \in \mathbb{Q}$. Hence, we conclude that there does not exist any element of order 4 in T. $\square$

Lemma 2. *Let* $q > 3$ *be any prime. Then there does not exist any element of order* q *in* T.

Proof. From Proposition 5 we see that $E(\mathbb{Q})$ does not have any element of order q. Therefore $E(\mathbb{Q})[q] = \{\mathcal{O}\}$. Now, we consider the d-quadratic twist of E which is $E^d\colon y^2 = x^3 + cd^3$. Again by Proposition 5, $E^d(\mathbb{Q})$ does not have any element of order q. Therefore $E^d(\mathbb{Q})[q] = \{\mathcal{O}\}$. Hence, by Remark 1, we have $E(\mathbb{Q}(\sqrt{d}))[q] = \{\mathcal{O}\}$, which proves the lemma. $\square$

Lemma 3. *There does not exist any element of order* 9 *in* T.

Proof. From Proposition 5 we see that $E(\mathbb{Q})$ does not have any element of order 9. Therefore $E(\mathbb{Q})[9] \cong \mathbb{Z}/3\mathbb{Z}$ or $E(\mathbb{Q})[9] = \{\mathcal{O}\}$. Also by Proposition 5, $E^d(\mathbb{Q})$ does not have any element of order 9. Therefore $E^d(\mathbb{Q})[9] \cong \mathbb{Z}/3\mathbb{Z}$ or $E^d(\mathbb{Q})[9] = \{\mathcal{O}\}$. Hence, by Remark 1, we conclude that $E(\mathbb{Q}(\sqrt{d}))[9]$ is isomorphic to one of $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$ and $\{\mathcal{O}\}$. Thus, there does not exist any element of order 9 in T. $\square$

Lemma 4. *Let $P=(x,y)$ be a point of order 2 in $T\subseteq E(\mathbb{Q}(\sqrt{d}))$. Then $c=a^3$ for some nonzero square-free integer a and*

$$P=\begin{cases}(-a,0) & \text{for } d\neq -3,\\ (-a,0),(-a\omega,0),(-a\omega^2,0) & \text{for } d=-3,\end{cases}$$

where ω is a cube root of unity.

Proof. Note that $P=(x,y)$ is a point of order 2 in $T\Leftrightarrow P\neq\mathcal{O}$ and $2P=\mathcal{O}$ $\Leftrightarrow P\neq\mathcal{O}$ and $P=-P\Leftrightarrow y=0\Leftrightarrow x^3+c=0$. Hence, $[\mathbb{Q}(x):\mathbb{Q}]\leqslant 3$. Since $x\in\mathbb{Q}(\sqrt{d})$ and $[\mathbb{Q}(\sqrt{d}):\mathbb{Q}]=2$, we conclude that $[\mathbb{Q}(x):\mathbb{Q}]\leqslant 2$. Hence the polynomial x^3+c is reducible over $\mathbb{Q}$ and so it has an integer root. Therefore $c=a^3$ for some nonzero integer a.

Then $(-a,0)$ is the only point of order 2 in T for $d\neq -3$. For $d=-3$, $(-a,0)$, $(-a\omega,0)$ and $(-a\omega^2,0)$ are the only points of order 2 in T. Hence the lemma. □

Lemma 5. *Let $P=(x,y)$ be a point of order 3 in $T\subseteq E(\mathbb{Q}(\sqrt{d}))$. If $c\neq 2t^3$ for any integer t, then*

$$P=\begin{cases}(0,\pm\sqrt{c}) & \text{if } c \text{ is a square},\\ (0,\pm\sqrt{c}) & \text{if } c \text{ is not a square and } d \text{ is square-free part of } c.\end{cases}$$

Proof. Note that $P=(x,y)$ is a point of order 3 in $T\Leftrightarrow P\neq\mathcal{O}$ and $3P=\mathcal{O}\Leftrightarrow P\neq\mathcal{O}$ and $2P=-P$.

Hence, if P is a point of order 3 in T, then

$$x(2P)=x(-P)\ \Leftrightarrow\ \frac{x(x^3-8c)}{4(x^3+c)}=x\ \Leftrightarrow\ x(x^3+4c)=0.$$

If $x^3+4c=0$, then $[\mathbb{Q}(x):\mathbb{Q}]\leqslant 3$. Since $x\in\mathbb{Q}(\sqrt{d})$ and $[\mathbb{Q}(\sqrt{d}):\mathbb{Q}]=2$, we see that $[\mathbb{Q}(x):\mathbb{Q}]\leqslant 2$. Hence the polynomial x^3+4c is reducible over $\mathbb{Q}$ and so it has an integer root. Therefore $4c=z^3$ for some nonzero integer z. Hence, we conclude that $c=2t^3$ for some nonzero square-free integer t, which is a contradiction. So, $x^3+4c\neq 0$. Therefore $x=0$ and $y=\pm\sqrt{c}$.

If c is a square, say $c=b^2$ for some nonzero integer b, then $(0,\pm b)$ are the only points of order 3 in T for any d. If c is not a square, then $(0,\pm\sqrt{c})$ are the only points of order 3 in T when d is square-free part of c. Hence the lemma. □

Lemma 6. *Let $P = (x, y)$ be a point of order 3 in $T \subseteq E(\mathbb{Q}(\sqrt{d}))$. If $c = 2t^3$ for some square-free integer t, then*

$$P = \begin{cases} (0, \pm 4) \quad \text{if } t = 2 \text{ and } d \neq -3, \\ (0, \pm 4),\ (-4, \pm 4\sqrt{-3}),\ (-4\omega, \pm 4\sqrt{-3}) \\ \qquad \text{and } (-4\omega^2, \pm 4\sqrt{-3}) \quad \text{if } t = 2 \text{ and } d = -3, \\ (12, \pm 36) \quad \text{if } t = -6 \text{ and } d \neq -3, \\ (0, \pm 12\sqrt{-3}),\ (12, \pm 36),\ (12\omega, \pm 36) \\ \qquad \text{and } (12\omega^2, \pm 36) \quad \text{if } t = -6 \text{ and } d = -3, \\ (0, \pm t\sqrt{2t}) \quad \text{if } t \neq 2 \text{ and } d \text{ is square-free part of } 2t, \\ (-2t, \pm t\sqrt{-6t}) \quad \text{if } t \neq -6 \text{ and } d \text{ is square-free part of } -6t. \end{cases}$$

Proof. Note that if P is a point of order 3 in T, then $x(x^3 + 4c) = 0$. If $x = 0$, then $y = \pm\sqrt{c} = \pm t\sqrt{2t}$. If $2t$ is a square, then $t = 2$ as t is square-free. In this case, $(0, \pm 4)$ are points of order 3 for any d. Though for $d = -3$ we have 8 points of order 3. If $2t$ is not a square, then $(0, \pm t\sqrt{2t})$ are the only points of order 3 when d is square-free part of $2t$.

If $x \neq 0$, then $x^3 = -4c = -8t^3$ and hence x is one of $-2t$, $-2t\omega$, $-2t\omega^2$, where ω is a cube root of unity. In this case, $y = \pm t\sqrt{-6t}$. If $-6t$ is a square, then $t = -6$ as t is square-free. In this case, $(12, \pm 36)$ are points of order 3 for any d. Though for $d = -3$ we have 8 points of order 3. If $-6t$ is not a square, then $(12, \pm t\sqrt{-6t})$ are the only points of order 3 when d is square-free part of $-6t$. □

Now we are ready to prove Theorem 1.

Proof of Theorem 1. By Lemma 1, Lemma 2 and Lemma 3 we see that the only possible orders for the nontrivial torsion points in T are $2, 3$ and 6.

Case 1. c is a cube and a square.

In this case, $c = 1$ as c is sixth power-free.

If $d \neq -3$, then $(0, \pm 1)$ are the only points of order 3 by Lemma 5 and $(1, 0)$ is the only point of order 2 by Lemma 4. Since T is abelian, it has an element of order 6. Hence, $T \cong \mathbb{Z}/6\mathbb{Z}$.

If $d = -3$, then $(0, \pm 1)$ are the only points of order 3 by Lemma 5 and $(1, 0)$, $(\omega, 0)$, $(\omega^2, 0)$ are the only points of order 2 in T by Lemma 4. Since T is abelian, it has an element of order 6. Hence, $T \cong \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Case 2. c is a cube, but not a square.

Write $c = a^3$ for some nonzero square-free integer $a \neq 1$.

For $d = -3$, $(-a, 0)$, $(-a\omega, 0)$, $(-a\omega^2, 0)$ are the only points of order 2 in T by Lemma 4. If $a \neq -3$, then there does not exist any element of order 3 for $d = -3$

by Lemma 5. Hence, $T \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. If $a = -3$, then $c = -27$. In that case, $(0, \pm 3\sqrt{-3})$ are the only points of order 3 for $d = -3$ by Lemma 5. Since T is abelian, it has an element of order 6. Hence, $T \cong \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

For $d \neq -3$, $(-a, 0)$ is the only point of order 2 in T by Lemma 4. If $-3 \neq d = a$, then $(0, \pm a\sqrt{a})$ are the only points of order 3 by Lemma 5. Since T is abelian, it has an element of order 6. Hence, $T \cong \mathbb{Z}/6\mathbb{Z}$. If $-3 \neq d \neq a$, then there does not exist any element of order 3 in T by Lemma 5. Hence, $T \cong \mathbb{Z}/2\mathbb{Z}$.

Case 3. c is a square, but not a cube.

If $c = 2t^3$ for some square-free integer t, then $c = 16$ as c is a square. In this case, there does not exist any element of order 2 in T by Lemma 4. For $d = -3$, T has 8 points of order 3 by Lemma 6. Hence, $T \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. For $d \neq -3$, $(0, \pm 4)$ are the only points of order 3 by Lemma 6. Hence, $T \cong \mathbb{Z}/3\mathbb{Z}$.

If $c \neq 2t^3$ for any integer t, then write $c = a^2$ for some integer a. Therefore $(0, \pm a)$ are the only points of order 3 in T by Lemma 5. Also there does not exist any element of order 2 by Lemma 4. Hence, $T \cong \mathbb{Z}/3\mathbb{Z}$.

Case 4. c is neither a square nor a cube.

If $c = 2t^3$ for some square-free integer t, then $t \neq 2$ as c is not a square. Hence there does not exist any element of order 2 in T by Lemma 4. Now by Lemma 6, we conclude that for $t = -6$, $T \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ for $d = -3$ and $T \cong \mathbb{Z}/3\mathbb{Z}$ for $d \neq -3$. Also for $t \neq -6$, $T \cong \mathbb{Z}/3\mathbb{Z}$ if d is square-free part of $2t$ or $-6t$ by Lemma 6.

If $c \neq 2t^3$ for any integer t, then there does not exist any element of order 2 in T by Lemma 4 and $(0, \pm\sqrt{c})$ are the only points of order 3 in T when d is square-free part of c by Lemma 5. Hence, $T \cong \mathbb{Z}/3\mathbb{Z}$.

Thus, combining all the cases, Theorem 1 follows. □

5. Proof of Theorem 2

Throughout this section, we denote by $\mathcal{O}_K$ a ring of integers in K. To prove Theorem 2, we require the following lemmas.

Lemma 7. *For any odd prime $q > 3$ there does not exist any element of order q in T.*

Proof. Suppose there exists an element of order q in T. Hence, q divides $|T|$. Then, by Dirichlet theorem on primes in arithmetic progression [1], we can choose a good prime p with $p \equiv q^2 + 1 \pmod{3q}$ as $(q^2 + 1, 3q) = 1$. Let $p\mathcal{O}_K = \mathcal{P}_1^{e_1}\mathcal{P}_2^{e_2} \ldots \mathcal{P}_r^{e_r}$ be the ideal decomposition in $\mathcal{O}_K$, where $\mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_r$ are prime ideals in $\mathcal{O}_K$ lying above p and e_i's are ramification indices for $\mathcal{P}_i$'s. Also, we know that $\sum\limits_{i=1}^{r} e_i f_i = n$, where f_i's are residual degrees for $\mathcal{P}_i$'s.

Since n is odd, there exists at least one f_i which is odd. Let $\mathcal{P}_i$ be the corresponding prime ideal and consider the reduction modulo $\mathcal{P}_i$ map. Since $|\mathcal{O}_K/\mathcal{P}_i| = p^{f_i}$ and f_i is odd, we have $|\overline{E}(\mathcal{O}_K/\mathcal{P}_i)| = p^{f_i} + 1$ by Corollary 1 as $p \equiv 2 \pmod 3$. Hence by Proposition 4, we conclude that $q \mid p^{f_i} + 1$. But we also have $p \equiv 1 \pmod q$, which implies $p^{f_i} + 1 \equiv 2 \pmod q$, which is a contradiction as $q \nmid 2$. Hence the lemma. $\square$

Lemma 8. *There does not exist any element of order* 4 *in* T.

Proof. Suppose there exists an element of order 4 in T. Then 4 divides $|T|$. Therefore, by Dirichlet theorem on primes in arithmetic progression, see [1], we can choose a good prime p with $p \equiv 5 \pmod{12}$. Let $p\mathcal{O}_K = \mathcal{P}_1^{e_1}\mathcal{P}_2^{e_2}\dots\mathcal{P}_r^{e_r}$ be the ideal decomposition in $\mathcal{O}_K$, where $\mathcal{P}_1, \mathcal{P}_2, \dots, \mathcal{P}_r$ are prime ideals in $\mathcal{O}_K$ lying above p and e_i's are ramification indices for $\mathcal{P}_i$'s. Also, we know that $\sum\limits_{i=1}^{r} e_i f_i = n$, where f_i's are residual degrees for $\mathcal{P}_i$'s.

Since n is odd, there exists at least one f_i which is odd. Let $\mathcal{P}_i$ be the corresponding prime ideal and consider the reduction modulo $\mathcal{P}_i$ map. Since $|\mathcal{O}_K/\mathcal{P}_i| = p^{f_i}$ and f_i is odd, we have $|\overline{E}(\mathcal{O}_K/\mathcal{P}_i)| = p^{f_i} + 1$ by Corollary 1 as $p \equiv 2 \pmod 3$. Hence by Proposition 4, we conclude that $4 \mid p^{f_i} + 1$. But we also have $p \equiv 1 \pmod 4$, which implies $p^{f_i} + 1 \equiv 2 \pmod 4$, which is a contradiction. Therefore there does not exist any element of order 4 in $|T|$. $\square$

Lemma 9. *Let* $P = (x, y)$ *be a point of order* 2 *in* T. *Then* $c = a^3$ *for some nonzero square-free integer* a *and* $P = (-a, 0)$.

Proof. If $P = (x, y)$ is a point of order 2, then $x(P) = x(-P) \Leftrightarrow y = 0 \Leftrightarrow x^3 + c = 0$. Hence, $[\mathbb{Q}(x) : \mathbb{Q}] \leqslant 3$. Since $x \in K$ and $[K : \mathbb{Q}]$ is coprime to 6, we conclude that x is an integer. Hence, $c = a^3$ for some nonzero square-free integer a. In this case, $(-a, 0)$ is the only point of order 2 in T. Hence the lemma. $\square$

Lemma 10. *Let* $P = (x, y)$ *be a point of order* 3 *in* T. *Then*

$$P = \begin{cases} (0, \pm\sqrt{c}) & \text{if } c \text{ is a square,} \\ (12, \pm 36) & \text{if } c = -432. \end{cases}$$

Proof. If P is a point of order 3 in T, then

$$x(2P) = x(-P) \ \Leftrightarrow\ \frac{x(x^3 - 8c)}{4(x^3 + c)} = x \ \Leftrightarrow\ x(x^3 + 4c) = 0.$$

If $x = 0$, then $y = \pm\sqrt{c}$. Since K is a number field of odd degree, we see that y must be an integer and hence c is a square.

If $x \neq 0$, then $x^3 + 4c = 0$. Hence, $[\mathbb{Q}(x) : \mathbb{Q}] \leqslant 3$. Since $x \in K$ and $[K : \mathbb{Q}]$ is coprime to 6, we conclude that x is an integer. Hence $c = 2t^3$ for some nonzero square-free integer t. Therefore $y = \pm t\sqrt{-6t}$. Since $y \in K$ and K is a number field of odd degree, we conclude that y must be an integer. Hence, $-6t$ must be a square. Since t is a square-free integer, we have $t = -6$. Hence, for $c = -432$, $(12, \pm 36)$ are the only points of order 3 in T. Hence the lemma. $\square$

Lemma 11. *There does not exist any element of order* 9 *in* T.

P r o o f. Let $P = (x, y)$ be a point of order 9 in T. By Proposition 1, $[\mathbb{Q}(P) : \mathbb{Q}]$ divides $|\mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z})| = 3^5(3^2 - 1)(3 - 1) = 2^4 3^5$, which is a contradiction because $\mathbb{Q}(P)$ is a subfield of K and $[K : \mathbb{Q}]$ is coprime to 6. $\square$

Now we are ready to prove Theorem 2.

P r o o f of Theorem 2. By Lemma 7, Lemma 8 and Lemma 11, we see that the only possible orders for the nontrivial torsion points in T are $2, 3$ and 6.

Case 1. c is a cube and a square.

In this case, $c = 1$ as c is sixth power-free. Hence, $(0, \pm 1)$ are the only points of order 3 in T by Lemma 10 and $(1, 0)$ is the only point of order 2 in T by Lemma 9. Since T is abelian, it has an element of order 6. Hence, $T \cong \mathbb{Z}/6\mathbb{Z}$.

Case 2. c is a cube, but not a square.

Write $c = a^3$ for some nonzero square-free integer $a \neq 1$. In this case, $(-a, 0)$ is the only point of order 2 in T by Lemma 9. There does not exist any element of order 3 in T by Lemma 10. Hence, $T \cong \mathbb{Z}/2\mathbb{Z}$.

Case 3. c is a square, but not a cube.

Suppose $c = a^2$ for some nonzero integer $a \neq 1$. In this case, there does not exist any element of order 2 in T by Lemma 9. Also $(0, \pm a)$ are the only points of order 3 in T by Lemma 10. Hence, $T \cong \mathbb{Z}/3\mathbb{Z}$.

Case 4. c is neither a square, nor a cube.

In this case, there does not exist any element of order 2 in T by Lemma 9. If $c = -432$, then $(12, \pm 36)$ are the only points of order 3 in T by Lemma 10. Hence, $T \cong \mathbb{Z}/3\mathbb{Z}$ for $c = -432$. If $c \neq -432$, then there does not exist any element of order 3 in T by Lemma 10. Hence, $T = \{\mathcal{O}\}$ for $c \neq -432$.

Thus, combining all the cases, Theorem 2 follows. $\square$

References

[1] *R. Ayoub*: An Introduction to the Analytic Theory of Numbers. Mathematical Surveys 10, American Mathematical Society, Providence, 1963. zbl MR doi

[2] *A. Bourdon, P. L. Clark, J. Stankewicz*: Torsion points on CM elliptic curves over real number fields. Trans. Am. Math. Soc. *369* (1996), 8457–8496. zbl MR doi

[3] *P. K. Dey*: Elliptic curves with rank 0 over number fields. Funct. Approximatio, Comment. Math. *56* (2017), 25–37. zbl MR doi

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

[5] *D. Jeon, C. H. Kim, E. Park*: On the torsion of elliptic curves over quartic number fields. J. Lond. Math. Soc., II. Ser. *74* (2006), 1–12. zbl MR doi

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

[7] *M. A. Kenku, F. Momose*: Torsion points on elliptic curves defined over quadratic fields. Nagoya Math. J. *109* (1988), 125–149. zbl MR doi

[8] *A. W. Knapp*: Elliptic Curves. Mathematical Notes (Princeton) 40, Princeton University Press, Princeton, 1992. zbl MR

[9] *B. Mazur*: Modular curves and the Eisenstein ideal. Publ. Math., Inst. Hautes Étud. Sci. *47* (1977), 33–186. zbl MR doi

[10] *F. Najman*: Complete classification of torsion of elliptic curves over quadratic cyclotomic fields. J. Number Theory *130* (2010), 1964–1968. zbl MR doi

[11] *F. Najman*: Torsion of elliptic curves over quadratic cyclotomic fields. Math. J. Okayama Univ. *53* (2011), 75–82. zbl MR

[12] *F. Najman*: Torsion of rational elliptic curves over cubic fields and sporadic points on $X_1(n)$. Math. Res. Lett. *23* (2016), 245–272. zbl MR doi

[13] *L. D. Olson*: Points of finite order on elliptic curves with complex multiplication. Manuscr. Math. *14* (1974), 195–205. zbl MR doi

[14] *L. C. Washington*: Elliptic Curves. Number Theory and Cryptography. Chapman and Hall/CRC, Boca Raton, 2008. zbl MR doi

Author's address: Pallab Kanti Dey, Harish-Chandra Research Institute, Chhatnag Road, Jhunsi, Allahabad – 211019, India, e-mail: `pallabkantidey@gmail.com`.