Czechoslovak Mathematical Journal

Jerome Tomagan Dimabayao

The torsion subgroup of a family of elliptic curves over the maximal abelian extension of $\mathbb{Q}$

Czechoslovak Mathematical Journal, Vol. 70 (2020), No. 4, 979–995

Persistent URL: http://dml.cz/dmlcz/148406

Czechoslovak Mathematical Journal, 70 (145) (2020), 979–995

THE TORSION SUBGROUP OF A FAMILY OF ELLIPTIC CURVES OVER THE MAXIMAL ABELIAN EXTENSION OF $\mathbb{Q}$

Jerome Tomagan Dimabayao, Quezon City

Received February 25, 2019. Published online April 2, 2020.

Abstract. We determine explicitly the structure of the torsion group over the maximal abelian extension of $\mathbb{Q}$ and over the maximal p-cyclotomic extensions of $\mathbb{Q}$ for the family of rational elliptic curves given by $y^2 = x^3 + B$, where B is an integer.

Keywords: torsion group; elliptic curve; cyclotomic field

MSC 2020: 14H52, 11R18

1. Introduction

Let E be an elliptic curve defined over a number field K. The Mordell-Weil theorem states that the set $E(K)$ of K-rational points on E is a finitely generated abelian group. That is, $E(K)$ is isomorphic to a direct sum of the form $\mathbb{Z}^r \oplus E(K)_{\rm tors}$ for some nonnegative integer r (called the *rank* of E) and finite group $E(K)_{\rm tors}$, called the *torsion subgroup* of $E(K)$. Over the last few decades the characterization of the possible structures of $E(K)_{\rm tors}$ has been of considerable interest. The case $K = \mathbb{Q}$ was given by Mazur, see [17], while the case of quadratic fields ($[K : \mathbb{Q}] = 2$) was completed by Kamienny, see [12] and Kenku and Momose, see [14]. The past few years saw development in the classification of the torsion structure over number fields of higher degree for elliptic curves defined over $\mathbb{Q}$. These were provided by Najman, see [18] for cubic fields, by González-Jiménez and Lozano-Robledo, see [11] for quartic fields and by González-Jiménez, see [10] for quintic number fields. Results were also obtained for the torsion subgroup of specific families of rational elliptic curves over arbitrary number fields. More recently, Dey in [4] and [5] studied the possible

The research has been supported by the OVCRD PhD Incentive Award Project No. 171725 PhDIA.

DOI: 10.21136/CMJ.2020.0082-19

structures of $E(K)_{\text{tors}}$ for rational CM-elliptic curves E that lie in the families $y^2 = x^3 + B$ and $y^2 = x^3 + Ax$, where $A, B \in \mathbb{Q}$.

When K is an infinite extension of $\mathbb{Q}$, the Mordell-Weil theorem no longer applies. In particular there is no guarantee for the finiteness of the torsion subgroup of $E(K)$. For instance, if for a fixed integer $d \geqslant 1$ we write $\mathbb{Q}(d^\infty)$ for the compositum of all field extensions $K/\mathbb{Q}$ of degree d, then $E(\mathbb{Q}(d^\infty))$ is not finitely generated for elliptic curves E over $\mathbb{Q}$ (see [6] and [9]). But even so, the torsion subgroup can be finite. The possible torsion structures have been classified by Laska and Lorenz, see [15] and Fujita, see [7], [8] for $d = 2$, and by Daniels, Lozano-Robledo, Najman and Sutherland, see [3] for $d = 3$.

A result of Ribet, see [13] states that if K is a number field and $K(\mu_\infty)$ is the field extension of K obtained by adjoining all the roots of unity then for any elliptic curve E over K, $E(K(\mu_\infty))_{\text{tors}}$ is finite. In particular, for an elliptic curve E defined over $\mathbb{Q}$, the torsion subgroup of E over the maximal abelian extension $\mathbb{Q}^{\text{ab}}$ of $\mathbb{Q}$ is finite.

In this paper, we study the family of rational elliptic curves $E_B\colon\ y^2 = x^3 + B$, where $B \in \mathbb{Q}$. Note that by performing a rational transformation, we may assume that B is an integer that is sixth power-free. For this family of elliptic curves, we determine the structure of the torsion subgroup of the group of rational points of E_B over $\mathbb{Q}^{\text{ab}}$ and over the maximal p-cyclotomic extension $\mathbb{Q}(\zeta_{p^\infty})$ of $\mathbb{Q}$, where p is a prime number. The proofs indicate the coordinates of the points that belong to the torsion subgroup, see [5].

2. Statements of results

Let n be a positive integer. The nth cyclotomic extension $\mathbb{Q}(\zeta_n)$ is the splitting field of the polynomial $x^n - 1$ over $\mathbb{Q}$. Here, ζ_n denotes a primitive nth root of unity. The field $\mathbb{Q}(\zeta_n)$ is a Galois extension over $\mathbb{Q}$ with the cyclic Galois group isomorphic to the unit group $(\mathbb{Z}/n\mathbb{Z})^\times$. Let p be a prime number. If p is an odd prime, then $\mathbb{Q}(\zeta_{p^n})$ has a unique quadratic subfield given by $\mathbb{Q}(\sqrt{p^*})$, where $p^* = (-1)^{(p-1)/2}p$. If $p = 2$, we have $\mathbb{Q}(\zeta_2) = \mathbb{Q}$, $\mathbb{Q}(\zeta_4) = \mathbb{Q}(\mathrm{i})$, and for $n \geqslant 3$, $\mathbb{Q}(\zeta_{2^n})$ has 3 quadratic subfields given by $\mathbb{Q}(\mathrm{i})$, $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{-2})$. The p^nth cyclotomic extensions $(n \geqslant 1)$ form an increasing tower

$$\mathbb{Q}(\zeta_{p^n}) \subseteq \mathbb{Q}(\zeta_{p^{n+1}}), \quad n \geqslant 1.$$

We define the maximal p-cyclotomic extension $\mathbb{Q}(\zeta_{p^\infty})$ to be the union

$$\mathbb{Q}(\zeta_{p^\infty}) = \bigcup_{n \geqslant 1} \mathbb{Q}(\zeta_{p^n}).$$

The field $\mathbb{Q}(\zeta_{p^\infty})$ is Galois over $\mathbb{Q}$ with the Galois group

$$\mathrm{Gal}(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q}) = \varprojlim_n (\mathbb{Z}/p^n\mathbb{Z})^\times = \mathbb{Z}_p^\times \simeq \begin{cases} \mathbb{Z}_p \oplus (\mathbb{Z}/p\mathbb{Z})^\times & \text{if } p \neq 2, \\ \mathbb{Z}_p \oplus \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z} & \text{if } p = 2. \end{cases}$$

The Kronecker-Weber theorem states that any abelian extension of $\mathbb{Q}$ is contained in some nth cyclotomic extension. The maximal abelian extension $\mathbb{Q}^{\mathrm{ab}}$ of $\mathbb{Q}$ is the union of all the nth cyclotomic extensions, as n runs through the set of all positive integers. Equivalently, $\mathbb{Q}^{\mathrm{ab}}$ is the composite field of all the maximal p-cyclotomic extensions, as p runs through the set of primes. We have

$$\mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q}) \simeq \widehat{\mathbb{Z}}^\times \simeq \prod_p \mathbb{Z}_p^\times.$$

In this paper we prove the following classification of the torsion subgroup of the elliptic curve $y^2 = x^3 + B$ over the maximal abelian extension $\mathbb{Q}^{\mathrm{ab}}$ of $\mathbb{Q}$ and over the maximal p-cyclotomic extensions $\mathbb{Q}(\zeta_{p^\infty})$ for each prime p.

Theorem 2.1. *Let $E_B\colon\ y^2 = x^3 + B$ be an elliptic curve, where B is a nonzero sixth power-free integer. We have*

$$E_B(\mathbb{Q}^{\mathrm{ab}})_{\mathrm{tors}} = \begin{cases} \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z} & \text{if } B = 2t^3, \text{ where } t \in \mathbb{Z}, \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z} & \text{if } B = s^3, \text{ where } s \in \mathbb{Z}, \\ \mathbb{Z}/3\mathbb{Z} & \text{otherwise.} \end{cases}$$

Theorem 2.2. *Let $E_B\colon\ y^2 = x^3 + B$ be an elliptic curve, where B is a sixth power-free integer. For a prime p, let $T_{B,p}$ be the torsion subgroup of $E_B(\mathbb{Q}(\zeta_{p^\infty}))$. Then $T_{B,p}$ is given by the following tables.*

$T_{B,p}$ $(p > 3)$	*conditions*
$\mathbb{Z}/6\mathbb{Z}$	$B = 1$ *or* $(p^*)^3$
$\mathbb{Z}/2\mathbb{Z}$	$B = t^3$ *(where* $t \neq 1,\ p^*$*)*
$\mathbb{Z}/3\mathbb{Z}$	$B = -432, -432(p^*)^3, 16(p^*)^3$, *or* $B = s^2$ *(where* $s \neq \pm 1$*) or* $B = p^* s^2$ *(where* $s \neq \pm p^*$*)*
$\{\mathcal{O}\}$	*otherwise*
$T_{B,3}$	
$\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z}$	$B = 16, -432$
$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$	$B = 1, -27$
$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$	$B = t^3$ *(where* $t \neq 1, -3$*)*
$\mathbb{Z}/3\mathbb{Z}$	$B = s^2$ *(where* $s \neq \pm 1 \pm 4$*), or* $B = -3s^2$ *(where* $s \neq \pm 3 \pm 12$*)*
$\{\mathcal{O}\}$	*otherwise*

$T_{B,2}$	*conditions*
$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$	$B = \pm 1, \pm 8$
$\mathbb{Z}/2\mathbb{Z}$	$B = t^3$ *(where* $t \neq \pm 1, \pm 2$*)*
$\mathbb{Z}/3\mathbb{Z}$	$B = \pm 54, \pm 432$, *or* $B = \pm s^2$ *(where* $t \neq 1$*), or* $B = \pm 2s^2$ *(where* $t \neq 2$*)*
$\{\mathcal{O}\}$	*otherwise*

3. Preliminary observations

Let E be an elliptic curve over $\mathbb{Q}$ and K a field extension of $\mathbb{Q}$. For an integer n, we write

$$E(K)[n] := \{P \in E(K)\colon\ nP = \mathcal{O}\} \cup \{\mathcal{O}\}.$$

For a prime q, we introduce

$$E(K)[q^\infty] := \bigcup_{n \in \mathbb{N}} E(K)[q^n],$$

called the *q-primary part of* $E(K)$. The torsion subgroup is a direct sum of its q-primary parts:

$$E(K)_{\text{tors}} = \bigoplus_{q\colon \text{prime}} E(K)[q^\infty].$$

In order to determine the torsion subgroup of $E(K)$, it helps to know the possible primes that give nontrivial contributions to the direct sum. To do this, we need the following facts.

Proposition 3.1 ([4], Proposition 4)**.** *Let K be a number field and $E\colon\ y^2 = x^3 + Ax + B$ be an elliptic curve for some integers A and B. Let T be the torsion subgroup of $E(K)$. Write $\mathcal{O}_K$ for the ring of integers in K. Let $\mathcal{P}$ be a prime ideal in $\mathcal{O}_K$ lying above an odd prime p. If E has good reduction at $\mathcal{P}$, we let Φ be the reduction map on T. Then Φ is an injective homomorphism except for finitely many prime ideals $\mathcal{P}$.*

Lemma 3.2 ([5], Corollary 1)**.** *Let $E_B\colon\ y^2 = x^3 + B$ be an elliptic curve for some nonzero integer B with discriminant Δ. Let $p \equiv 2 \pmod 3$ be an odd prime such that $p \nmid \Delta$. Write $\overline{E}_B$ for the reduction of E modulo p. Then*

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

Proposition 3.3. *Let $E_B\colon\ y^2 = x^3 + B$ be an elliptic curve for some nonzero integer B and $n \in \mathbb{N}$. If q is a prime divisor of the order of $E_B(\mathbb{Q}(\zeta_n))_{\mathrm{tors}}$ then $q = 2$ or 3.*

P r o o f. This result is known for $n = 1, 2$ so we assume henceforth that $n \geqslant 3$. Assume that q is a prime greater than 3 such that q divides the order of $E_B(\mathbb{Q}(\zeta_n))_{\mathrm{tors}}$. Dirichlet's theorem on primes in arithmetic progression allows us to choose a prime l relatively prime to q and n of good reduction with

$$l \equiv -1 \pmod{n} \quad \text{and} \quad l \equiv 1 \pmod{q}, \quad \text{if } 3 \mid n,$$
$$l \equiv 1 \pmod{n} \quad \text{and} \quad l \equiv q^2 + 1 \pmod{3q}, \quad \text{otherwise.}$$

The ideal generated by l in the ring of integers $\mathbb{Z}[\zeta_n]$ decomposes as

$$l\mathbb{Z}[\zeta_n] = \mathfrak{l}_1^e \ldots \mathfrak{l}_g^e,$$

where the $\mathfrak{l}_j$'s are distinct prime ideals in $\mathbb{Z}[\zeta_n]$ lying above l and e is the common ramification index for the $\mathfrak{l}_j$'s. Since $\mathbb{Q}(\zeta_n)$ is Galois over $\mathbb{Q}$ we also have the fundamental identity in algebraic number theory: $efg = [\mathbb{Q}(\zeta_n) : \mathbb{Q}]$, where f is the common residue degree for the $\mathfrak{l}_j$, namely, the integer f such that $\#(\mathcal{O}_{\mathbb{Q}(\zeta_n)}/\mathfrak{l}_j) = l^f$. For cyclotomic extensions $\mathbb{Q}(\zeta_n)$, it is known that f is the order of l modulo n (see for instance, [16], Theorem 26). We take a prime ideal $\mathfrak{l}_j$ and consider the reduction $\overline{E}_B$ of E_B modulo $\mathfrak{l}_j$. In any case we have $l \equiv 2 \pmod{3}$. Lemma 3.2 implies

$$\#\overline{E}_B(\mathcal{O}_K/\mathfrak{l}_j) = \begin{cases} (l+1)^2 & \text{if } 3 \mid n, \\ l+1 & \text{otherwise.} \end{cases}$$

From Proposition 3.1 we see that in any case

$$l + 1 \equiv 0 \pmod{q}.$$

But as $l \equiv 1 \pmod{q}$ we also have

$$l + 1 \equiv 2 \pmod{q}.$$

This is absurd since $q > 3$. This proves the lemma. □

Corollary 3.4. *Let $q > 3$ be an odd prime. Then we have*

$$E_B(\mathbb{Q}^{\mathrm{ab}})[q^\infty] = \{\mathcal{O}\}.$$

Consequently,

$$E_B(\mathbb{Q}(\zeta_{p^\infty}))[q^\infty] = \{\mathcal{O}\}$$

for any prime p.

Proof. Note that $E_B(\mathbb{Q}^{\mathrm{ab}})[q]$ is a subset of the finite group $E_B(\mathbb{C})[q]$. Then there exists $n \in \mathbb{N}$ such that

$$E_B(\mathbb{Q}^{\mathrm{ab}})[q] = E_B(\mathbb{Q}(\zeta_n))[q].$$

By Proposition 3.3 we have $E_B(\mathbb{Q}^{\mathrm{ab}})[q] = \{\mathcal{O}\}$, since $q > 3$. If $m > 1$ and $\mathcal{O} \neq P \in E_B(\mathbb{Q}^{\mathrm{ab}})[q^m]$ then $q^{m-1}P$ is a nontrivial element of $E_B(\mathbb{Q}^{\mathrm{ab}})[q]$, which is absurd. The result follows. □

Corollary 3.4 implies that the torsion subgroup of E_B over $\mathbb{Q}^{\mathrm{ab}}$ is completely determined by its 2-primary and 3-primary parts. The determination of the possible structures of the 2-primary and 3-primary parts will be covered by the next three sections.

4. Points whose order is a power of 2

Lemma 4.1. *Let K be a Galois extension of $\mathbb{Q}$ (possibly of infinite degree) whose Galois group does not have a quotient isomorphic to S_3. Then*

$$E_B(K)[2] = \begin{cases} \{\mathcal{O}, (-t,0), (-t\zeta_3,0), (-t\zeta_3^2,0)\} & \text{if } B = t^3,\ \exists\, t \in \mathbb{Z} \text{ and } \sqrt{-3} \in K, \\ \{\mathcal{O}, (\sqrt[3]{B}, 0)\} & \text{if } B = t^3,\ \exists\, t \in \mathbb{Z} \text{ but } \sqrt{-3} \notin K, \\ \{\mathcal{O}\} & \text{otherwise.} \end{cases}$$

Proof. Let $P = (x, y)$ be a point of order 2 in $E_B(K)$. Then $y = 0$ and x is a solution of $X^3 + B = 0$. Observe that

$$X^3 + B = \big(X + \sqrt[3]{B}\big)\big(X + \sqrt[3]{B}\zeta_3\big)\big(X + \sqrt[3]{B}\zeta_3^2\big).$$

If B is a perfect cube of an integer and $\sqrt{-3} \in K$ then all the three roots belong to K. If B is a perfect cube of an integer and $\sqrt{-3} \notin K$ then only $-\sqrt[3]{B}$ belongs to K. Suppose B is not a cube of an integer. Then $X^3 + B$ is irreducible over $\mathbb{Q}$. Since K is Galois over $\mathbb{Q}$, if one of its roots belongs to K then all the three must be in K. This implies that $\mathbb{Q}(\sqrt[3]{B}, \zeta_3)$ is a subfield of K, contrary to our assumption.

□

Lemma 4.2. *Let K be a Galois extension of $\mathbb{Q}$ (possibly of infinite degree) whose Galois group does not have a quotient isomorphic to S_3. Then $E_B(K)$ has no element of order 4.*

P r o o f. If $E_B(K)$ has an element of order 4, then it has an element of order 2. The previous lemma implies that $B = t^3$ for some nonzero square-free integer t.

Let $P = (x, y) \in E_B(K)$ be an element of order 4. Then $y(2P) = 0$. By the duplication formula we have

$$x^6 + 20t^3x^3 - 8t^6 = 0.$$

Thus

$$x^3 = (-10 \pm 6\sqrt{3})t^3 = (-1 \pm \sqrt{3})^3 t^3.$$

If $\sqrt{3} \in K$ then

$$x = (-1 \pm \sqrt{3})t \in \mathbb{Z}[\sqrt{3}] \subseteq K$$

and $E_B(K)$ has no point of order 4 if $\sqrt{3} \notin K$.

Suppose $\sqrt{3} \in K$. As $x \in \mathbb{Z}[\sqrt{3}]$ and $y^2 = x^3 + t^3 \in \mathbb{Z}[\sqrt{3}]$, we have $y \in \mathbb{Z}[\sqrt{3}]$. We write $y = a + b\sqrt{3}$ for some $a, b \in \mathbb{Z}$. From the relation $y^2 = x^3 + t^3$, we obtain the equations

$$a^2 + 3b^2 = -9t^3 \quad \text{and} \quad ab = \pm 3t^3.$$

From these we get $a^2+3b^2 \pm 3ab = 0$. If we put $c := a/b \in \mathbb{Q}$, we see that $c^2 \pm 3c + 3 = 0$ so that

$$c = \frac{\mp 3 \pm \sqrt{-3}}{2} \notin \mathbb{Q},$$

a contradiction. Therefore there is no point of order 4 in $E_B(K)$ even if $\sqrt{3} \in K$. $\square$

The previous lemmas give the following result.

Proposition 4.3. *Let K be a Galois extension of $\mathbb{Q}$ (possibly of infinite degree) whose Galois group does not have a quotient isomorphic to S_3. Then*

$$E_B(K)[2^\infty] = \begin{cases} \{\mathcal{O}, (-t, 0), (-t\zeta_3, 0), (-t\zeta_3^2, 0)\} & \text{if } B = t^3,\ \exists t \in \mathbb{Z} \text{ and } \sqrt{-3} \in K, \\ \{\mathcal{O}, (\sqrt[3]{B}, 0)\} & \text{if } B = t^3,\ \exists t \in \mathbb{Z} \text{ but } \sqrt{-3} \notin K, \\ \{\mathcal{O}\} & \text{otherwise.} \end{cases}$$

Now let p be a prime and consider $\mathbb{Q}(\zeta_{p^\infty})$. The Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q})$ is abelian; and thus does not have a quotient isomorphic to S_3. If p is odd, then $\mathbb{Q}(\sqrt{p^*})$ is the unique quadratic subfield of $\mathbb{Q}(\zeta_{p^\infty})$. On the other hand, $\mathbb{Q}(\zeta_{2^\infty})$ has three quadratic subfields: $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2})$, and $\mathbb{Q}(\sqrt{-2})$. In particular we have $\sqrt{-3} \in \mathbb{Q}(\zeta_{p^\infty})$ if and only if $p = 3$. From Proposition 4.3, we have the following result.

Proposition 4.4. *Let p be a prime. Then we have*

$$E_B(\mathbb{Q}(\zeta_{p^\infty}))[2^\infty] = \begin{cases} \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} & \text{if } B = t^3 \text{ for some integer } t \text{ and } p = 3, \\ \mathbb{Z}/2\mathbb{Z} & \text{if } B = t^3 \text{ for some integer } t \text{ and } p \neq 3, \\ \{\mathcal{O}\} & \text{otherwise.} \end{cases}$$

Moreover,

$$E_B(\mathbb{Q}^{\mathrm{ab}})[2^\infty] = \begin{cases} E(\mathbb{Q}(\sqrt{-3}))[2^\infty] \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} & \text{if } B = t^3 \text{ for some integer } t, \\ E(\mathbb{Q})[2^\infty] = \{\mathcal{O}\} & \text{otherwise.} \end{cases}$$

5. Points of order 3

Let $P = (x, y) \in E_B(K)$ be a point of order 3. Then $P \neq \mathcal{O}$ and $2P = -P$. In particular, $x(2P) = x(-P) = (x, -y)$. By the duplication formula

$$\frac{x^4 - 8Bx}{4(x^3 + B)} = x.$$

Equivalently, x is a solution of the polynomial equation

$$X(X^3 + 4B) = 0. \tag{5.1}$$

We use this observation in the succeeding lemma, which generalizes Lemmas 5 and 6 of [5].

Lemma 5.1. *Let K be a Galois extension of $\mathbb{Q}$ (possibly of infinite degree) whose Galois group does not have a quotient isomorphic to S_3. If $B \neq 2t^3$ for any integer t then*

$$E_B(K)[3] = \begin{cases} \{\mathcal{O}, (0, \pm\sqrt{B})\} & \text{if } \sqrt{B} \in K, \\ \{\mathcal{O}\} & \text{otherwise.} \end{cases}$$

On the other hand, if $B = 2t^3$ for some square-free integer t then $E_B(K)[3]$ is given by the following table:

$E(K)[3]$	*conditions*
$\{\mathcal{O},(0,\pm 4)\}$	*if* $t=2$ *and* $\sqrt{-3}\notin K$
$\{\mathcal{O},(0,\pm 4),(-4,\pm 4\sqrt{-3}),$ $(-4\zeta_3,\pm 4\sqrt{-3}),(-4\zeta_3^2,\pm 4\sqrt{-3})\}$	*if* $t=2$ *and* $\sqrt{-3}\in K$
$\{\mathcal{O},(12,\pm 36)\}$	*if* $t=-6$ *and* $\sqrt{-3}\notin K$
$\{\mathcal{O},(0,\pm 12\sqrt{-3}),(12,\pm 36),$ $(12\zeta_3,\pm 36),(12\zeta_3^2,\pm 36)\}$	*if* $t=-6$ *and* $\sqrt{-3}\in K$
$\{\mathcal{O},(0,\pm t\sqrt{2t})\}$	*if* $t\neq 2$, $\sqrt{2t}\in K$ *and* $\sqrt{-6t}\notin K$
$\{\mathcal{O},(-2t,\pm t\sqrt{-6t})\}$	*if* $t\neq -6$, $\sqrt{-6t}\in K$ *and* $\sqrt{2t}\notin K$
$\{\mathcal{O},(0,\pm t\sqrt{2t}),(-2t,\pm t\sqrt{-6t}),$ $(-2t\zeta_3,\pm t\sqrt{-6t}),(-2t\zeta_3^2,\pm t\sqrt{-6t})\}$	*if* $t\neq 2,-6$ *and* $\sqrt{-6t},\sqrt{2t}\in K$
$\{\mathcal{O}\}$	*otherwise*

P r o o f. If $P=(x,y)$ is a point of order 3 then x is a solution of equation (5.1). Consider the polynomial X^3+4B. If X^3+4B is reducible over $\mathbb{Q}$ then there exists an integer α such that $\alpha^3=4B$. But this implies $B=2t^3$ for some integer t, a contradiction. If X^3+4B is irreducible over $\mathbb{Q}$ but reducible over K then it splits over K, so that $\mathbb{Q}(\sqrt[3]{4B},\zeta_3)\subseteq K$, a contradiction. Therefore X^3+4B is irreducible over K which tells us that $x=0$ and $y=\pm\sqrt{B}$.

If $\sqrt{B}\in K$ then $(0,\pm\sqrt{B})$ are the only points of order 3 in $E_B(K)$. Otherwise, there is no point of order 3 in $E_B(K)$.

Now suppose that $B=2t^3$ for some square-free integer t. We consider once again equation (5.1). If $x=0$ then $y=\pm\sqrt{B}=\pm t\sqrt{2t}$. If $t\neq 2$ then $2t$ is not a square and $(0,\pm t\sqrt{2t})$ are points of order 3 in $E_B(K)$ if and only if K contains the quadratic field $\mathbb{Q}(\sqrt{2t})$. If $t=2$ then we see that $(0,\pm 4)$ are points of order 3 in $E_B(\mathbb{Q})$, hence in $E_B(K)$.

If $x\neq 0$, then $x^3=-4B=-8t^3=(-2t)^3$. So x is one of $-2t$, $-2t\zeta_3$, or $-2t\zeta_3^2$. For this case we have $y=\pm t\sqrt{-6t}$. If $t=2$, then $(-4,\pm 4\sqrt{-3}),(-4\zeta_3,\pm 4\sqrt{-3})$, and $(-4\zeta_3^2,\pm 4\sqrt{-3})$ are points of order 3 in $E_B(K)$ if and only if $\sqrt{-3}\in K$. If $t=-6$ then $(12,\pm 36)$ are points of order 3 in $E_B(\mathbb{Q})$, hence in $E_B(K)$. Moreover, the points $(0,\pm 12\sqrt{-3})$, $(12\zeta_3,\pm 36)$, and $(12\zeta_3^2,\pm 36)$ are points of order 3 in $E_B(K)$ if and only if $\sqrt{-3}\in K$. If $t\neq -6$ then $-6t$ is not a square and $(-2t,\pm t\sqrt{-6t})$ are points of order 3 in $E_B(K)$ if and only if K contains the quadratic field $\mathbb{Q}(\sqrt{-6t})$. If this is the case, the points $(-2t\zeta_3,\pm t\sqrt{-6t})$ and $(-2t\zeta_3^2,\pm t\sqrt{-6t})$ are also contained in $E_B(K)$ if and only if $\sqrt{-3}$ (equivalently $\sqrt{2t}$) belongs to K. $\square$

Since $\mathbb{Q}^{\mathrm{ab}}$ contains all the quadratic extensions of $\mathbb{Q}$, we obtain the following statement.

Proposition 5.2. *We have*

$$E_B(\mathbb{Q}^{\mathrm{ab}})[3] = \begin{cases} \{\mathcal{O}, (0, \pm\sqrt{B})\} & \text{if } B \neq 2t^3 \text{ for any integer } t, \\ \{\mathcal{O}, (0, \pm t\sqrt{2t}), (-2t, \pm t\sqrt{-6t}), & \\ (-2t\zeta_3, \pm t\sqrt{-6t}), & \\ (-2t\zeta_3^2, \pm t\sqrt{-6t})\} & \text{if } B = 2t^3 \text{ for some square-free } t. \end{cases}$$

For the p-cyclotomic extensions $\mathbb{Q}(\zeta_{p^\infty})$, the subgroup of 3-torsion points is given as follows.

Proposition 5.3. *Let $p > 3$ be a prime. Then*

$$E_B(\mathbb{Q}(\zeta_{p^\infty}))[3] = \begin{cases} \{\mathcal{O}, (0, \pm s)\} & \text{if } B = s^2, \text{ where } s \in \mathbb{Z}, \\ \{\mathcal{O}, (0, \pm s\sqrt{p^*})\} & \text{if } B = p^* s^2, \text{ where } s \in \mathbb{Z}, \\ \{\mathcal{O}, (0, \pm 4p^*\sqrt{p^*})\} & \text{if } B = 16(p^*)^3, \\ \{\mathcal{O}, (12, \pm 36)\} & \text{if } B = -432, \\ \{\mathcal{O}, (12p^*, \mp 36p^*\sqrt{p^*})\} & \text{if } B = -432(p^*)^3, \\ \{\mathcal{O}\} & \text{otherwise.} \end{cases}$$

Furthermore we have

$$E_B(\mathbb{Q}(\zeta_{3^\infty}))[3] = \begin{cases} \{\mathcal{O}, (0, \pm 4), (-4, \pm 4\sqrt{-3}), & \\ (-4\zeta_3, \pm 4\sqrt{-3}), & \\ (-4\zeta_3^2, \pm 4\sqrt{-3})\} & \text{if } B = 16, \\ \{\mathcal{O}, (0, \pm 12\sqrt{-3}), (12, \pm 36), & \\ (12\zeta_3, \pm 36), (12\zeta_3^2, \pm 36)\} & \text{if } B = -432, \\ \{\mathcal{O}, (0, \pm s)\} & \text{if } B = s^2, \text{ where } s \neq \pm 4, \\ \{\mathcal{O}, (0, \pm s\sqrt{-3})\} & \text{if } B = -3s^2, \text{ where } s \neq \pm 12, \\ \{\mathcal{O}\} & \text{otherwise,} \end{cases}$$

and

$$E_B(\mathbb{Q}(\zeta_{2^\infty}))[3] = \begin{cases} \{\mathcal{O}, (0, \pm\sqrt{B})\} & \text{if } B = \pm s^2 \text{ or } \pm 2s^2, \text{ where } s \in \mathbb{Z}, \\ \{\mathcal{O}, (-2t, \pm t\sqrt{-6t})\} & \text{if } B = 2t^3, \text{ where } t = \pm 3, \pm 6, \\ \{\mathcal{O}\} & \text{otherwise.} \end{cases}$$

Proof. We write $K_p := \mathbb{Q}(\zeta_{p^\infty})$. Suppose that $p > 3$. Recall that $\mathbb{Q}(\sqrt{p^*})$ is the unique quadratic subfield of K_p. If $B \neq 2t^3$ for any integer t then $\sqrt{B} \in K_p$ if and only if $B = s^2$ or $p^* s^2$ for some cube-free integer s. In the former case, we have $E_B(K_p) = \{\mathcal{O}, (0, \pm s)\}$, while $E_B(K_p) = \{\mathcal{O}, (0, \pm s\sqrt{p^*})\}$ in the latter case by Lemma 5.1. Suppose $B = 2t^3$ for some square-free integer t. We apply Lemma 5.1 to this case. Note that if both $\sqrt{-6t}$ and $\sqrt{2t}$ lie in K_p then $\sqrt{-3} \in K_p$, which is absurd. We have $\sqrt{2t} \in K_p$ if and only if $t = 2$ or $2p^*$. If $t = 2$, then $B = 16$ and $E_B(K_p) = \{\mathcal{O}, (0 \pm 4)\}$. If $t = 2p^*$ then $B = 16(p^*)^3$ and $E_B(K_p) = \{\mathcal{O}, (0 \pm 4p^*\sqrt{p^*})\}$. Moreover, $\sqrt{-6t} \in K_p$ if and only if $t = -6$ or $t = -6p^*$. In the first case we have $B = -432$ and $E_B(K_p) = \{\mathcal{O}, (12, \pm 36)\}$. In the second case, $B = -432(p^*)^3$ and $E_B(K_p) = \{\mathcal{O}, (12p^*, \pm 36p^*\sqrt{p^*})\}$. If the above forms for B are not satisfied, $E_B(K_p)$ is trivial. By doing a similar case work, we obtain the corresponding results for $p = 2, 3$. We just keep in mind that $\mathbb{Q}(\sqrt{-3})$ is the unique quadratic subfield of K_3, while K_2 has three distinct quadratic subfields given by $\mathbb{Q}(\mathrm{i})$, $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{-2})$. □

6. Points whose order is a power of 3

Proposition 6.1. *The group $E_B(\mathbb{Q}^{\mathrm{ab}})$ has a point of order 9 if and only if $B = 2t^3$ for some square-free integer t. In this case, we have*

$$E_B(\mathbb{Q}^{\mathrm{ab}})[9] = E_B\big(\mathbb{Q}\big(\zeta_9, \sqrt{-12\theta^2 - 4\theta + 35}, \sqrt{3B}\big)\big)[9] \simeq \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z},$$

where $\theta = \zeta_9 + \zeta_9^{-1}$.

Consequently, $E_B(\mathbb{Q}(\zeta_{p^\infty}))$ has a point of order 9 if and only if $p = 3$ and $B = 16$ or -432. In this case, we have $E_B(\mathbb{Q}(\zeta_{3^\infty}))[9] \simeq \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z}$.

Proof. Suppose that $E_B(\mathbb{Q}^{\mathrm{ab}})$ has a point $P = (x, y)$ of order 9. Then $E_B(\mathbb{Q}^{\mathrm{ab}})$ has a point of order 3 given by $3P$. The addition formula in E_B shows that the x-coordinate of $3P$ is given by:

$$x(3P) = \frac{x^9 - 96Bx^6 + 48B^2x^3 + 64B^3}{(3x^4 + 12Bx)^2}. \tag{6.1}$$

We consider the following cases:

Case 1: Assume that $x(3P) = 0$. Put $f(X) = X^9 - 96BX^6 + 48B^2X^3 + 64B^3$ and consider the equation

$$f(X) = 0. \tag{6.2}$$

The substitution $Y = X^3/4B$ gives rise to the equation

$$Y^3 - 24Y^2 + 3Y + 1 = 0.$$

With the aid of Magma, see [1], we find that this cubic splits in the field $\mathbb{Q}(\theta)$, where $\theta := \zeta_9 + \zeta_9^{-1}$. The roots are given by

$$X_1 = -9\theta^2 - 3\theta + 26 = (-\theta^2 + 3)^3, \tag{6.3}$$

$$X_2 = 3\theta^2 - 6\theta + 2 = (-\theta + 1)^3, \tag{6.4}$$

$$X_3 = 6\theta^2 + 9\theta - 4 = (\theta^2 + \theta - 1)^3. \tag{6.5}$$

From these we obtain the 9 roots of equation (6.2):

$$\begin{gathered} X_{1,j} = \sqrt[3]{4B}(-\theta^2 + 3)\zeta_3^j, \quad X_{2,j} = \sqrt[3]{4B}(-\theta + 1)\zeta_3^j, \\ X_{3,j} = \sqrt[3]{4B}(\theta^2 + \theta - 1)\zeta_3^j, \end{gathered} \tag{6.6}$$

where $j \in \{0, 1, 2\}$. From this, we see that the splitting field of $f(x)$ over $\mathbb{Q}$ is

$$\begin{cases} \mathbb{Q}(\zeta_9) & \text{if } B = 2t^3 \text{ for some square-free } t, \\ \mathbb{Q}(\theta, \zeta_3, \sqrt[3]{4B}) & \text{otherwise}, \end{cases} \tag{6.7}$$

with the latter satisfying $\mathrm{Gal}(\mathbb{Q}(\theta, \zeta_3, \sqrt[3]{4B})/\mathbb{Q}(\theta)) \simeq S_3$. Hence, $E_B(\mathbb{Q}^{\mathrm{ab}})$ has no point of order 9 if $B \neq 2t^3$ for any integer t.

Assume $B = 2t^3$. Then

$$\begin{gathered} X_{1,j}^3 + B = 3B(-12\theta^2 - 4\theta + 35), \quad X_{2,j}^3 + B = 3B(4\theta^2 - 8\theta + 3), \\ X_{3,j}^3 + B = 3B(8\theta^2 + 12\theta - 5). \end{gathered}$$

Put $\alpha := \sqrt{-12\theta^2 - 4\theta + 35}$. Its irreducible polynomial over $\mathbb{Q}$ is

$$p(x) = x^6 - 33x^4 + 27x^2 - 3.$$

The splitting field $\mathbb{Q}(\alpha)$ of $p(x)$ is an abelian extension of degree 6 over $\mathbb{Q}$ that contains $\mathbb{Q}(\theta)$ as a subfield. The conjugates of α are $-\alpha, \pm\sqrt{4\theta^2 - 8\theta + 3}$ and $\pm\sqrt{8\theta^2 + 12\theta - 5}$. Since $\mathbb{Q}(\zeta_9)$, $\mathbb{Q}(\alpha)$ and $\mathbb{Q}(\sqrt{3B})$ are all abelian extensions of $\mathbb{Q}$, then so is their compositum $\mathbb{Q}(\zeta_9, \alpha, \sqrt{3B})$. So an element P of $E_B(\mathbb{Q}^{\mathrm{ab}})$ of order 9 such that the x-coordinate of $3P$ equals 0 must be one of the following 18 points:

$$\begin{gathered} \big(X_{1,j}, \pm\sqrt{3B(-12\theta^2 - 4\theta + 35)}\big), \quad \big(X_{2,j}, \pm\sqrt{3B(4\theta^2 - 8\theta + 3)}\big), \\ \big(X_{3,j}, \pm\sqrt{3B(8\theta^2 + 12\theta - 5)}\big), \end{gathered}$$

where $j \in \{0, 1, 2\}$.

Case 2: Suppose $P = (x, y) \in E_B(\mathbb{Q}^{\mathrm{ab}})$ is a point of order 9 such that $x(3P) \neq 0$. Then $B = 2t^3$ for some square-free t and P satisfies $x(3P) = -2t$, $-2t\zeta_3$ or $-2t\zeta_3^2$. Then we have the following polynomial equations from equation (6.1):

$$x^9 + 18t\zeta_3^j x^8 - 192t^3x^6 + 288\zeta_3^j t^4x^5 + 192t^6x^3 + 1152\zeta_3^j t^7x^2 + 512t^9 = 0 \tag{6.8}$$

for $j = 0, 1, 2$. For each j, we write

$$f_j(X) := X^9 + 18t\zeta_3^j X^8 - 192t^3X^6 + 288\zeta_3^j t^4X^5 + 192t^6X^3 + 1152\zeta_3^j t^7X^2 + 512t^9.$$

The change of variable $Y = X/2t$ gives the polynomials

$$g_j(Y) := Y^9 + 9\zeta_3^j Y^8 - 24Y^6 + 18\zeta_3^j Y^5 + 3Y^3 + 9\zeta_3^j Y^2 + 1$$

for $j = 0, 1, 2$. With the aid of Magma, see [1], we verify that each g_j is irreducible over $\mathbb{Q}(\sqrt{-3})$. The splitting field L_j of g_j over $\mathbb{Q}(\sqrt{-3})$ is a degree 18 Galois extension of $\mathbb{Q}$ listed in the following table.

j	defining polynomial for L_j over $\mathbb{Q}$
0	$x^{18} + 27x^{17} + 279x^{16} + 1476x^{15} + 4914x^{14} + 11934x^{13} + 23166x^{12}$ $+37260x^{11} + 51840x^{10} + 61182x^9 + 59049x^8 + 41310x^7 + 19197x^6$ $+5103x^5 + 8019x^4 + 13122x^3 + 10935x^2 + 4374x + 729$
1 and 2	$x^{18} - 9x^{17} + 81x^{16} - 48x^{15} + 198x^{14} + 324x^{13} + 582x^{12} + 396x^{11}$ $+486x^{10} - 142x^9 + 153x^8 + 324x^7 - 39x^6 - 45x^5$ $+81x^4 + 6x^3 - 9x^2 + 1$

Each extension L_j has a nonabelian Galois group. From this we conclude that in this case $E_B(\mathbb{Q}^{\mathrm{ab}})$ has no point P of order 9 that satisfies the conditions specified for $x(3P)$. This completes the proof of our claim for $E_B(\mathbb{Q}^{\mathrm{ab}})$.

Now consider $E_B(\mathbb{Q}(\zeta_{p^\infty}))$. Case 2 above shows that if $E_B(\mathbb{Q}(\zeta_{p^\infty}))$ has a point P of order 9 then the x-coordinate of $3P$ must be zero. If this is the case then the result indicated by (6.7) implies that $E_B(\mathbb{Q}(\zeta_{p^\infty}))$ has no point of order 9 when $p \neq 3$. On the other hand, if $p = 3$, then the 9 points in (6.6) are in $\mathbb{Q}(\zeta_{3^\infty})$ if and only if $4B$ is the cube of an integer. But at the same time, Proposition 5.3 requires that B is also square in $\mathbb{Q}(\sqrt{-3})$. Hence, $B = 16$ or -432.

If $B = 16$ then we have the following 18 points in $E_B(\mathbb{Q}(\zeta_{3^\infty}))$ of order 9 whose triple has the x-coordinate equal to 0:

$$(X_{1,j}, \pm(16\zeta_9^5 + 8\zeta_9^4 + 8\zeta_9^2 - 8\zeta_9 - 12)), \tag{6.9}$$

$$(X_{2,j}, \pm(8\zeta_9^5 - 8\zeta_9^4 + 16\zeta_9^2 - 16\zeta_9 + 12)), \tag{6.10}$$

$$(X_{3,j}, \pm(8\zeta_9^5 + 16\zeta_9^4 - 8\zeta_9^2 + 8\zeta_9 + 12)) \tag{6.11}$$

for $j = 0, 1, 2$.

Finally, for $B=-432$ we have the following 18 points in $E_B(\mathbb{Q}(\zeta_{3^\infty}))$ of order 9 whose triple has x-coordinate equal to 0:

$$(X_{1,j}, \pm(72\zeta_9^4+72\zeta_9^3+72\zeta_9^2+72\zeta_9+36)), \tag{6.12}$$
$$(X_{2,j}, \pm(72\zeta_9^5-72\zeta_9^4+72\zeta_9^3+36)), \tag{6.13}$$
$$(X_{3,j}, \pm(72\zeta_9^5-72\zeta_9^3+72\zeta_9^2+72\zeta_9-36)) \tag{6.14}$$

for $j=0,1,2$. This concludes the proof of Proposition. □

To account for possible points of order 27, we apply the following result.

Lemma 6.2 ([2], Theorem 2.6). *Let $E/\mathbb{C}$ be an $\mathcal{O}_K$-CM elliptic curve for some imaginary quadratic field K. Let $M\subset E(\mathbb{C})$ be a finite $\mathcal{O}_K$-submodule. Write* $\operatorname{ann} M$ *for the annihilator of M. Then $M=E[\operatorname{ann} M]\simeq_{\mathcal{O}_K}\mathcal{O}_K/(\operatorname{ann} M)$ and thus the orders of M and* $\operatorname{ann} M$ *are equal.*

Proposition 6.3. *The group $E_B(\mathbb{Q}^{\mathrm{ab}})$ has no element of order* 27.

Proof. If $E_B(\mathbb{Q}^{\mathrm{ab}})$ has an element of order 27 then it has a point of order 9 and Proposition 6.1 implies that we have $E_B(\mathbb{Q}^{\mathrm{ab}})[27]\simeq\mathbb{Z}/3\mathbb{Z}\oplus\mathbb{Z}/27\mathbb{Z}$. The elliptic curve $y^2=x^3+B$ has CM by the maximal order $\mathcal{O}_K$ of the quadratic number field $K=\mathbb{Q}(\sqrt{-3})$. The prime 3 ramifies in K, so $3\mathcal{O}_K=\mathfrak{p}^2$ for some prime ideal $\mathfrak{p}$ in $\mathcal{O}_K$. Now Lemma 6.2 implies that

$$E_B[27]:=E_B(\mathbb{C})[27]\simeq\mathcal{O}_K/\mathfrak{p}^6\simeq_{\mathbb{Z}}\mathbb{Z}/27\mathbb{Z}\oplus\mathbb{Z}/27\mathbb{Z}.$$

The ideals of $\mathcal{O}_K/\mathfrak{p}^6$ are of the form $I/\mathfrak{p}^6$, where I is an ideal of $\mathcal{O}_K$ such that $\mathfrak{p}^6\subseteq I$. Since $\mathcal{O}_K$ is a Dedekind domain, $I=\mathfrak{p}^a$ for some $0\leqslant a\leqslant 6$. Consequently, any $\mathcal{O}_K$-submodule of $E_B[27]$ must be of the form $\mathfrak{p}^a/\mathfrak{p}^6$ for some $0\leqslant a\leqslant 6$. The torsion subgroup of $E_B(\mathbb{Q}^{\mathrm{ab}})$ is an $\mathcal{O}_K$-submodule of $E_B(\mathbb{C})$. Thus,

$$\mathfrak{p}^a/\mathfrak{p}^6\simeq E_B(\mathbb{Q}^{\mathrm{ab}})[27]\simeq_{\mathbb{Z}}\mathbb{Z}/3\mathbb{Z}\oplus\mathbb{Z}/27\mathbb{Z}.$$

Hence

$$\mathcal{O}_K/\mathfrak{p}^a\simeq(\mathcal{O}_K/\mathfrak{p}^6)/(\mathfrak{p}^a/\mathfrak{p}^6)\simeq_{\mathbb{Z}}\mathbb{Z}/9\mathbb{Z}.$$

So $a=2$. However, $\mathcal{O}_K/\mathfrak{p}^2$ is isomorphic to $\mathbb{Z}/3\mathbb{Z}\oplus\mathbb{Z}/3\mathbb{Z}$ as an additive group. Therefore, $E_B(\mathbb{Q}^{\mathrm{ab}})$ has no element of order 27. □

The results of Propositions 5.2, 5.3, 6.1 and Corollary 6.3 combine to give the 3-primary part of E_B.

Corollary 6.4. *We have*

$$E_B(\mathbb{Q}^{\mathrm{ab}})[3^\infty] = \begin{cases} \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z} & \text{if } B = 2t^3, \text{ where } t \in \mathbb{Z}, \\ \mathbb{Z}/3\mathbb{Z} & \text{otherwise.} \end{cases}$$

If $p > 3$, *we have*

$$E_B(\mathbb{Q}(\zeta_{p^\infty}))[3^\infty] = \begin{cases} \mathbb{Z}/3\mathbb{Z} & \text{if } B = -432, -432(p^*)^3, 16(p^*)^3, s^2 \text{ or } p^* s^2 \text{ with } s \in \mathbb{Z}, \\ \{\mathcal{O}\} & \text{otherwise.} \end{cases}$$

Moreover,

$$E_B(\mathbb{Q}(\zeta_{3^\infty}))[3^\infty] = \begin{cases} \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z} & \text{if } B = 16 \text{ or } -432, \\ \mathbb{Z}/3\mathbb{Z} & \text{if } B = s^2 \text{ for } s \neq \pm 4 \text{ or } B = -3s^2 \text{ for } s \neq \pm 12, \\ \{\mathcal{O}\} & \text{otherwise,} \end{cases}$$

and

$$E_B(\mathbb{Q}(\zeta_{2^\infty}))[3^\infty] = \begin{cases} \mathbb{Z}/3\mathbb{Z} & \text{if } B = \pm 54, \pm 432, \pm s^2 \text{ or } \pm 2s^2 \text{ for } s \in \mathbb{Z}, \\ \{\mathcal{O}\} & \text{otherwise.} \end{cases}$$

7. Proofs of the main results

We are now ready to give the proof of our results for the torsion subgroup of $E_B: Y^2 = X^3 + B$ over $\mathbb{Q}^{\mathrm{ab}}$ and $\mathbb{Q}(\zeta_{p^\infty})$. This is carried out by combining Corollary 3.4, Proposition 4.4, and Corollary 6.4.

Proof of Theorem 2.1. By Corollary 3.4, any prime divisor of the order of $E_B(\mathbb{Q}^{\mathrm{ab}})_{\mathrm{tors}}$ has to be less than 5. So the torsion subgroup is determined by Proposition 4.4 and Corollary 6.4. We only note that by the unique factorization of integers, if $B = 2t^3$ for some square-free integer t, then $B \neq s^3$ for any square-free integer s. The result follows. □

Proof of Theorem 2.2. By Proposition 3.3, the structure of $T_{B,p}$ is completely determined by its 2-primary and 3-primary parts.

Assume $p > 3$. If $B = t^3$ for some square-free integer t then the 2-primary part of $T_{B,p}$ is a cyclic group of order 2 by Proposition 4.4. Moreover, $T_{B,p}$ has a point of order 3 if and only if $B = 1$ or $B = (p^*)^3$ by Corollary 6.4. Thus $T_{B,p} \simeq \mathbb{Z}/6\mathbb{Z}$ if $B = 1$ or $B = (p^*)^3$ and $T_{B,p} \simeq \mathbb{Z}/2\mathbb{Z}$ if $B = t^3$ with $t \neq 1, p^*$. If $B \neq t^3$ for any integer t then the 2-primary part of $T_{B,p}$ is trivial and so $T_{B,p}$ is nontrivial if and only if it has a point of order 3. Corollary 6.4 implies that $T_{B,p} \simeq \mathbb{Z}/3\mathbb{Z}$ if $B = -432, -432(p^*)^3, 16(p^*)^3, s^2$ (with $s \neq \pm 1$), or $p^* s^2$ (with $s \neq \pm p^*$).

Let $p = 3$. If $B = t^3$ for some square-free integer t then the 2-primary part of $T_{B,3}$ is isomorphic to the Klein-4 group by Proposition 4.4. By Corollary 6.4, $T_{B,3}$ has a point of order 3 if and only if $B = s^2$ or $-3s^2$ for some integer s. Since t is square-free, we obtain $B = 1$ or -27. So $T_{B,3} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$ if $B = 1$ or -27, while $T_{B,3} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ if $B = t^3$ (with $t \neq 1, -3$). Suppose $B \neq t^3$ for any integer t. Then $T_{B,3}$ has no point of order 2 and Corollary 6.4 gives the structure of $T_{B,3}$.

Finally we consider the case where $p = 2$. If $B = t^3$ for some square-free integer t then the 2-primary part of $T_{B,2}$ is a cyclic group of order 2 by Proposition 4.4. By Corollary 6.4, $T_{B,2}$ has a point of order 3 if and only if $B = \pm s^2$ or $B = \pm 2s^2$ for some integer s. Since B is sixth-power free, we get $B = \pm 1$ or $B = \pm 8$. So $T_{B,2} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$ if $B = \pm 1, \pm 8$; while $T_{B,2} \simeq \mathbb{Z}/2\mathbb{Z}$ if $B = t^3$ with $t \neq \pm 1, \pm 2$. If $B \neq t^3$ for any integer t then $T_{B,2}$ has no point of order 2. In this case Corollary 6.4 gives the structure of $T_{B,2}$. $\square$

Acknowledgements. The author would like to express his sincere gratitude to Pallab Kanti Dey for providing him with the copies of [4] and [5].

References

[1] *W. Bosma, J. Cannon, C. Playoust*: The Magma algebra system. I. The user language. J. Symb. Comput. *24* (1997), 235–265. zbl MR doi

[2] *A. Bourdon, P. L. Clark*: Torsion points and Galois representations on CM elliptic curves. Pac. J. Math. *305* (2020), 43–88. zbl MR doi

[3] *H. B. Daniels, Á. Lozano-Robledo, F. Najman, A. V. Sutherland*: Torsion subgroups of rational elliptic curves over the compositum of all cubic fields. Math. Comput. *87* (2018), 425–458. zbl MR doi

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

[5] *P. K. Dey*: Torsion groups of a family of elliptic curves over number fields. Czech. Math. J. *69* (2019), 161–171. zbl MR doi

[6] *G. Frey, M. Jarden*: Approximation theory and the rank of abelian varieties over large algebraic fields. Proc. Lond. Math. Soc., III. Ser. *28* (1974), 112–128. zbl MR doi

[7] *Y. Fujita*: Torsion subgroups of elliptic curves with non-cyclic torsion over $\mathbb{Q}$ in elementary abelian 2-extensions of $\mathbb{Q}$. Acta Arith. *115* (2004), 29–45. zbl MR doi

[8] *Y. Fujita*: Torsion subgroups of elliptic curves in elementary abelian 2-extensions of $\mathbb{Q}$. J. Number Theory *114* (2005), 124–134. zbl MR doi

[9] *I. Gal, R. Grizzard*: On the compositum of all degree d extensions of a number field. J. Théor. Nombres Bordx. *26* (2014), 655–672. zbl MR doi

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

[11] *E. González-Jiménez, Á. Lozano-Robledo*: On the torsion of rational elliptic curves over quartic fields. Math. Comput. *87* (2018), 1457–1478. zbl MR doi
[12] *S. Kamienny*: Torsion points on elliptic curves and q-coefficients of modular forms. Invent. Math. *109* (1992), 221–229. zbl MR doi
[13] *N. M. Katz, S. Lang*: Finiteness theorems in geometric classfield theory. Enseign. Math., II. Sér.; Appendix by K. Ribet: Torsion points on abelian varieties in cyclotomic extensions *27* (1981), 285–319. zbl MR doi
[14] *M. A. Kenku, F. Momose*: Torsion points on elliptic curves defined over quadratic fields. Nagoya Math. J. *109* (1988), 125–149. zbl MR doi
[15] *M. Laska, M. Lorenz*: Rational points on elliptic curves over $\mathbb{Q}$ in elementary abelian 2-extensions of $\mathbb{Q}$. J. Reine Angew. Math. *355* (1985), 163–172. zbl MR doi
[16] *D. A. Marcus*: Number Fields. Universitext, Springer, New York, 1977. zbl MR doi
[17] *B. Mazur*: Modular curves and the Eisenstein ideal. Publ. Math., Inst. Hautes Étud. Sci. *47* (1978), 33–186. zbl MR
[18] *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

Author's address: Jerome Tomagan Dimabayao, Institute of Mathematics, College of Science, University of the Philippines-Diliman, C.P. Garcia Ave, Diliman, Quezon City, 1101, Philippines, e-mail: `jdimabayao@math.upd.edu.ph`.