FAMILIES OF ELLIPTIC CURVES OVER QUARTIC NUMBER FIELDS WITH PRESCRIBED TORSION SUBGROUPS

DAEYEOL JEON[1], CHANG HEON KIM[2] AND YOONJIN LEE[3]

ABSTRACT. We construct infinite families of elliptic curves with given torsion group structures over quartic number fields. Recently the first two authors and Park [2] determined all the group structures which occur infinitely often as the torsion of elliptic curves over quartic number fields. Our result presents explicit examples of their theoretical result. This paper also presents an efficient way of finding such families of elliptic curves with prescribed torsion group structures over quadratic or quartic number fields.

Key Words: elliptic curve, torsion, quadratic number field, quartic number field, modular curve

2000 Mathematics Subject classification. Primary: 11G05; Secondary: 11G18.

1. Introduction

It is an important research problem to determine all the torsion group structures of elliptic curves E over a number field and to find an infinite family of elliptic curves with a given torsion group structure. We briefly introduce some development on this research problem.

Over the rational number field $\mathbb{Q}$, Mazur [8] theoretically characterized all the possible torsion groups of elliptic curves, showing that the torsion group $E(\mathbb{Q})_{\text{tors}}$ of an elliptic curve E over $\mathbb{Q}$ is isomorphic to exactly one of the following 15 types:

$$\begin{array}{ll} \mathbb{Z}/N\mathbb{Z}, & N = 1-10, 12 \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N'\mathbb{Z}, & N' = 1-4. \end{array} \tag{1}$$

In fact, each of these groups in Eq. (1) appears infinitely often as a torsion group $E(\mathbb{Q})_{\text{tors}}$ of E over $\mathbb{Q}$. In other words, for each of the groups in Eq. (1) there are infinitely many absolutely non-isomorphic elliptic curves with such a torsion group structure over $\mathbb{Q}$. This follows from the fact that the modular curves $X_1(N)$ parametrizing elliptic curves with such a torsion structure are rational, so they have infinitely many $\mathbb{Q}$-rational points. Kubert [7,

The author[1] was supported by the Korea Science and Engineering Foundation(KOSEF) grant funded by the Korea government(MEST)(No. 2009-0060674), the author[2] by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education, Science and Technology (2009-0063182), and the author[3] by the Korea Science and Engineering Foundation(KOSEF) grant funded by the Korea government(MEST) (No. 2009-0059867).

Table 3] explicitly parametrized an infinite family of elliptic curves E with such a torsion group structure over $\mathbb{Q}$ for each of the 15 types in Eq. (1).

Over quadratic number fields, Kamienny and Mazur [4] theoretically determined all the possible torsion groups of elliptic curves as follows (total 26 types):

$$\begin{array}{ll} \mathbb{Z}/N\mathbb{Z}, & N = 1-16, 18 \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N'\mathbb{Z}, & N' = 1-6 \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3N''\mathbb{Z}, & N'' = 1-2 \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}. & \end{array} \tag{2}$$

Again, each of these 26 groups occurs infinitely often as $E(K)_{\mathrm{tors}}$, provided we allow the quadratic number field K to vary as well.

As mentioned previously, over the rational field or quadratic number fields, there was development on characterization of groups which appear infinitely often as torsion groups of elliptic curves. In this vein, it is very natural to investigate which groups would occur infinitely often as torsion groups of elliptic curves over quartic fields. Recently, the first two authors and Park [2] determined which groups occur infinitely often as torsion groups $E(K)_{\mathrm{tors}}$ when K varies over all quartic number fields and E varies over all elliptic curves over K. They proved that all the group structures occurring infinitely often as torsion groups $E(K)_{\mathrm{tors}}$ are exactly the following 38 types:

$$\begin{array}{ll} \mathbb{Z}/N_1\mathbb{Z}, & N_1 = 1-18, 20, 21, 22, 24 \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N_2\mathbb{Z}, & N_2 = 1-9 \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3N_3\mathbb{Z}, & N_3 = 1-3 \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4N_4\mathbb{Z}, & N_4 = 1-2 \\ \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}, & \\ \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}. & \end{array} \tag{3}$$

The main goal of this paper is constructing explicit examples of the theoretical result in [2], that is to say, the construction of infinite families of elliptic curves with the torsion groups in Eq. (3) over quartic number fields as Kubert did over $\mathbb{Q}$. While the subject of the torsion of elliptic curves over number fields of higher order has been studied by Kamienny and Mazur [4], Merel [9], Parent [12, 13], Zimmer et al. [11, 19] and Jeon et al. [2, 3], there has not been much development for finding elliptic curves with a given torsion group over number fields of higher order. It is known [3, Lemma 3.4] that if E is an elliptic curve over $\mathbb{Q}$ and E' an elliptic curve over a quadratic number field k, then for almost all quadratic number fields K we have $E(K)_{\mathrm{tors}} = E(\mathbb{Q})_{\mathrm{tors}}$, and for almost all quadratic number fields L of k we have $E'(L)_{\mathrm{tors}} = E'(k)_{\mathrm{tors}}$. Due to this fact, the group structure that already occurs over $\mathbb{Q}$ (respectively, quadratic number fields k) would appear infinitely often over suitable quadratic number fields K (respectively, quartic number fields L) without increasing the torsion.

In order to achieve our goal, according to the fact mentioned in the previous paragraph, it is sufficient to find infinite families of elliptic curves with prescribed torsion groups which do not occur over $\mathbb{Q}$ (respectively, quadratic number fields) but occur over quadratic number fields (respectively, quartic number fields). Therefore, over quadratic number fields, for each of the following 11 types in Eq. (4), we construct an explicit infinite family of elliptic curves with such a torsion group:

$$\begin{array}{ll}
\mathbb{Z}/N\mathbb{Z}, & N = 11, 13, 14, 15, 16, 18 \\
\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N'\mathbb{Z}, & N' = 5, 6 \\
\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}, & \\
\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}, & \\
\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}. &
\end{array} \tag{4}$$

On the other hand, over quartic number fields, for each of the following 12 types in Eq. (5), we obtain an explicit infinite family of elliptic curves with such a torsion group:

$$\begin{array}{ll}
\mathbb{Z}/N\mathbb{Z}, & N = 17, 20, 21, 22, 24 \\
\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N'\mathbb{Z}, & N' = 7, 8, 9 \\
\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z}, & \\
\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}, & \\
\mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}, & \\
\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}. &
\end{array} \tag{5}$$

We briefly explain the methods used in this paper. Regarding all the cyclic torsion group cases, we construct families of elliptic curves with the prescribed cyclic torsion by finding infinitely many quadratic points and quartic points on modular curves $X_1(N)$ for $N = 11, 13-18, 20, 21, 22, 24$. For achieving this, we need to search for proper forms of defining equations which yield such quadratic or quartic points. Reichert [14] calculated defining equations of the modular curves $X_1(N)$ for $N = 11, 13-16, 18$ by using the Tate normal form. Very recently, Sutherland [17] improved Reichert's result, so he obtained optimized forms (in terms of degree, number of terms, and coefficient size) for defining equations of $X_1(N)$ for $N \leq 50$. For all the cyclic torsion cases we consider except for $N = 24$, that is, for $N = 11, 13-18, 20-22$, the defining models $X_1(N)$ obtained by Sutherland [17, Table 6] are in proper form to use for our purpose. But, his model for $X_1(24)$ is not in proper form, so in this case of cyclic torsion $\mathbb{Z}/24\mathbb{Z}$, we use instead the *forgetful* map from $X_1(24)$ to $X_1(12)$ to construct our family of elliptic curves. On the other hand, for the non-cyclic torsion cases, we use the Kubert's families [7, Table 1 and Table 3] and some other methods such as Theorem 2.1 and Proposition 4.11.

This paper is organized as follows. We begin with some basic notions in Section 2. Section 3 presents infinite families of elliptic curves over quadratic number fields with torsion groups in Eq. (4), and in Section 4 we find infinite families of elliptic curves over quartic number fields with torsion groups in Eq. (5).

2. Preliminaries

In this section we introduce some basic notions on elliptic curves, and we can refer to [1, 6, 7, 16] for more details.

The general normal form of the cubic defining an elliptic curve passing through $P = (0, 0)$ is the following:

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x.$$

From the calculation of the derivative y' in the relation

$$(2y + a_1x + a_3)y' = 3x^2 + 2a_2x + a_4 - a_1y$$

we see that the slope of the tangent line at P is a_4/a_3 on E, so E is not singular at P if and only if $a_3 \neq 0$ or $a_4 \neq 0$.

Assume that E is nonsingular. Then P is of order 2 if and only if $a_3 = 0$ (and therefore $a_4 \neq 0$), i.e., E has the following equation:

$$y^2 + a_1xy = x^3 + a_2x^2 + a_4x.$$

If $a_3 \neq 0$, then by the admissible change of variables

$$(x, y) \to (X, Y + a_3^{-1}a_4X),$$

the curve E becomes

$$Y^2 + (a_1 + 2a_3^{-1}a_4)XY + a_3Y = X^3 + (a_2 - a_1a_3^{-1}a_4 - a_3^{-2}a_4^2)X^2,$$

which can be rewritten as

$$E' : y^2 + a_1xy + a_3y = x^3 + a_2x^2.$$

We have

$$-P = (0, -a_3), \quad 2P = (-a_2, a_1a_2 - a_3)$$

by the chord-tangent method [6, Chapter III], thus $3P = O$ (O denotes the point at infinity) if and only if $-P = 2P$, which implies that P is of order 3 if and only if $a_2 = 0$. Assume that P is not of order 2 or 3, that is, $a_2 \neq 0$ and $a_3 \neq 0$. Under the change of coordinates

$$(x, y) \to (X/u^2, Y/u^3) \ \text{ with } u = a_3^{-1}a_2,$$

and letting $b = -a_3^{-2}a_2^3$ and $c = 1 - a_3^{-1}a_1a_2$, we obtain the *Tate normal form* of an elliptic curve with $P = (0, 0)$ as follows:

$$E = E(b, c) : y^2 + (1 - c)xy - by = x^3 - bx^2,$$

and this is nonsingular if and only if $b \neq 0$. On the curve $E(b, c)$ we have the following by the chord-tangent method:

$$\begin{aligned}
P &= (0,\ 0),\\
2P &= (b,\ bc),\\
3P &= (c,\ b - c),\\
4P &= \big(r(r - 1),\ r^2(c - r + 1)\big)\,; \quad b = cr,\\
5P &= \big(rs(s - 1),\ rs^2(r - s)\big)\,; \quad c = s(r - 1),\\
6P &= \left(\frac{s(r - 1)(r - s)}{(s - 1)^2},\ \frac{s^2(r - 1)^2(rs - 2r + 1)}{(s - 1)^3}\right).
\end{aligned} \tag{6}$$

Table 1. Optimized form of $X_1(N) : f(u,v) = 0$

N	$f(u,v)$
11	$v^2 + (u^2+1)v + u$
13	$v^2 + (u^3+u^2+1)v - u^2 - u$
14	$v^2 + (u^2+u)v + u$
15	$v^2 + (u^2+u+1)v + u^2$
16	$v^2 + (u^3+u^2-u+1)v + u^2$
17	$v^4 + (u^3+u^2-u+2)v^3 + (u^3-3u+1)v^2 - (u^4+2u)v + u^3 + u^2$
18	$v^2 + (u^3-2u^2+3u+1)v + 2u$
19	$v^5 - (u^2+2)v^4 - (2u^3+2u^2+2u-1)v^3 + (u^5+3u^4+7u^3+6u^2+2u)v^2$ $-(u^5+2u^4+4u^3+3u^2)v + u^3 + u^2$
20	$v^3 + (u^2+3)v^2 + (u^3+4)v + 2$
21	$v^4 + (3u^2+1)v^3 + (u^5+u^4+2u^2+2u)v^2 + (2u^4+u^3+u)v + u^3$
22	$v^4 + (u^3+2u^2+u+2)v^3 + (u^5+u^4+2u^3+2u^2+1)v^2$ $+(u^5-u^4-2u^3-u^2-u)v - u^4 - u^3$
23	$v^7 + (u^5-u^4+u^3+4u^2+3)v^6 + (u^7+3u^5+u^4+5u^3+7u^2-4u+3)v^5$ $+(2u^7+3u^5-u^4-2u^3-u^2-8u+1)v^4$ $+(u^7-4u^6-5u^5-6u^4-6u^3-2u^2-3u)v^3$ $-(3u^6-5u^4-3u^3-3u^2-2u)v^2 + (3u^5+4u^4+u)v - u^2(u+1)^2$
24	$v^5 + (u^4+4u^3+3u^2-u-2)v^4 - (2u^4+8u^3+7u^2-1)v^3$ $-(2u^5+4u^4-3u^3-5u^2-u)v^2 + (2u^5+5u^4+2u^3)v + u^6 + u^5$

Very recently, by using the Tate normal form, Sutherland [17] found optimized forms for defining equations of the modular curves $X_1(N)$ for $N = 11, 13-50$. We use those defining equations for $N = 11, 13-24$, which are given in Table 1. We also need Table 2 for birational maps for $X_1(N)$ for our purpose.

TABLE 2. Birational maps φ for $X_1(N)$ from $f(u,v)=0$ to $F(r,s)=0$

N	φ	
11	$r = 1+uv,$	$s = 1-u$
12	$r = \frac{2u^2-2u+1}{u},$	$s = \frac{3u^2-3u+1}{u^2}$
13	$r = 1-uv,$	$s = \frac{1-uv}{v+1}$
14	$r = \frac{1-(u+v)}{(v+1)(u+v+1)},$	$s = \frac{1-u}{v+1}$
15	$r = \frac{1+(uv+v^2)}{(u^3+u^2v+u^2)},$	$s = \frac{1+v}{u^2+u}$
16	$r = \frac{u^2-uv+v^2+v}{u^2+u-v-1},$	$s = \frac{u-v}{u+1}$
17	$r = \frac{u^2+u-v}{u^2+uv+u-v^2-v},$	$s = \frac{u+1}{u+v+1}$
18	$r = \frac{u^2-uv-3u+1}{(u-1)^2(uv+1)},$	$s = \frac{u^2-2u-v}{u^2-uv-3u-v^2-2v}$
19	$r = \frac{1+u(u+v)(v-1)}{(u+1)(u^2-uv+2u-v^2+v)},$	$s = \frac{1+u(v-1)}{(u+1)(u-v+1)}$
20	$r = \frac{1+(u^3+uv+u)}{(u-1)^2(u^2-u+v+1)},$	$s = \frac{1+(u^2+v+1)}{(u-1)(u^2-u+v+2)}$
21	$r = \frac{1+(v^2+v)(uv+v+1)}{(uv+1)(uv-v^2+1)},$	$s = \frac{1+(v^2+v)}{uv+1}$
22	$r = \frac{u^2v+u^2+uv+v}{u^3+2u^2+v},$	$s = \frac{uv+v}{u^2+v}$
23	$r = \frac{u^2+u+v+1}{u^2-uv},$	$s = \frac{u+v+1}{u}$
24	$r = \frac{u^2+u-v+1}{u^2+uv-v^2+v},$	$s = \frac{u+1}{u+v}$

In fact, the condition $NP = O$ in $E(b,c)$ gives a defining equation for $X_1(N)$. For example, $11P = O$ implies $5P = -6P$, so

$$x_{5P} = x_{-6P} = x_{6P},$$

where x_{nP} denotes the x-coordinate of the n-multiple nP of P. Eq. (6) implies that

$$rs(s-1) = \frac{s(r-1)(r-s)}{(s-1)^2}. \tag{7}$$

Without loss of generality, the cases $s = 1$ and $s = 0$ may be excluded. Then Eq. (7) becomes as follows:

$$r^2 - 4sr + 3s^2r - s^3r + s = 0,$$

which is one of the equation $X_1(11)$, called the *raw form* of $X_1(11)$. By the coordinate changes $s = 1-u$ and $r = 1+uv$, we get the following equation:

$$v^2 + (u^2+1)v + u.$$

The following well-known theorem [6, Theorem 4.2] provides us with the condition for the divisibility of a given point on E by 2, and this result is very useful for studying torsion subgroups of the form $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N\mathbb{Z}$.

Theorem 2.1. *Let E be an elliptic curve defined over a field k of charateristic $\neq 2, 3$ given by*

$$y^2 = (x-\alpha)(x-\beta)(x-\gamma)$$

with α, β, γ in k. For (x_2, y_2) in $E(k)$ there exists (x_1, y_1) in $E(k)$ such that $2(x_1, y_1) = (x_2, y_2)$ if and only if $x_2 - \alpha,\ x_2 - \beta$ and $x_2 - \gamma$ are squares in k.

3. Torsion subgroups over quadratic number fields

Throughout this section, let K be a quadratic number field. Our goal of this section is to construct some families of elliptic curves with prescribed torsion over quadratic number fields which do not occur over $\mathbb{Q}$. Note that by finding the quadratic points of $X_1(N)$ we can find the elliptic curve with N-torsion point over quadratic number fields. For the cases of cyclic torsion, we obtain families of elliptic curve by calculating the quadratic points satisfying the equations of $X_1(N)$ in Table 1.

3.1. The case $E(K)_{\text{tors}} = \mathbb{Z}/11\mathbb{Z}$.

Theorem 3.1. *Put $d_t = t^4 + 2t^2 - 4t + 1$ with $t \in \mathbb{Q}$. Let E be an elliptic curve defined by the following equation:*

$$y^2 + (1-c)xy - by = x^3 - bx^2,$$

where

$$\begin{cases} b = \dfrac{t(t-1)(t^2+1-\sqrt{d_t})(t^3+t-2-t\sqrt{d_t})}{4}, \\ c = \dfrac{t(t-1)(t^2+1-\sqrt{d_t})}{2}. \end{cases}$$

Then the torsion subgroup of E over $\mathbb{Q}(\sqrt{d_t})$ is equal to $\mathbb{Z}/11\mathbb{Z}$.

Proof. Note that $(u, v) = (t, \frac{-t^2-1+\sqrt{t^4+2t^2-4t+1}}{2})$ satisfy the defining equation $v^2 + (u^2+1)v + u = 0$ of $X_1(11)$ in Table 1. From the birational map in Table 2, we know that b and c are expressed as

$$b = u(u-1)v(uv+1),\ c = u(u-1)v.$$

The result follows from the substitution $u = t$ and $v = \frac{-t^2-1+\sqrt{t^4+2t^2-4t+1}}{2}$. □

3.2. The case $E(K)_{\text{tors}} = \mathbb{Z}/13\mathbb{Z}$.

Theorem 3.2. *Put $d_t = t^6 + 2t^5 + t^4 + 2t^3 + 6t^2 + 4t + 1$ with $t \in \mathbb{Q}$. Let E be an elliptic curve defined by the following equation:*

$$y^2 + (1-c)xy - by = x^3 - bx^2,$$

where

$$\begin{cases} b = -\frac{t(t^4-t^2+t+1-(t-1)\sqrt{d_t})(t^3+t^2+1-\sqrt{d_t})(t^4+t^3+t+2-t\sqrt{d_t})}{4(t^3+t^2-1-\sqrt{d_t})} \\ c = -\frac{t(t^3+t^2+1-\sqrt{d_t})(t^4-t^2+t+1-(t-1)\sqrt{d_t})}{2(t^3+t^2-1-\sqrt{d_t})} \end{cases}$$

Then the torsion subgroup of E over $\mathbb{Q}(\sqrt{d_t})$ is equal to $\mathbb{Z}/13\mathbb{Z}$.

Proof. By the same method in Theorem 3.1 we are done. □

3.3. The case $E(K)_{\text{tors}} = \mathbb{Z}/14\mathbb{Z}$.

Theorem 3.3. *Put $d_t = t^4 + 2t^3 + t^2 - 4t$ with $t \in \mathbb{Q}$. Let E be an elliptic curve defined by the following equation:*

$$y^2 + (1 - c)xy - by = x^3 - bx^2,$$

where

$$\begin{cases} b = \frac{8(t-1)(t^2-t-\sqrt{d_t})(t^4+t^3-t^2-3t+2-(t^2-1)\sqrt{d_t})}{(t^2+t-2-\sqrt{d_t})^3(t^2-t-2-\sqrt{d_t})^2}, \\ c = \frac{4(t-1)(t^2-t-\sqrt{d_t})}{(t^2+t-2-\sqrt{d_t})^2(t^2-t-2-\sqrt{d_t})}. \end{cases}$$

Then the torsion subgroup of E over $\mathbb{Q}(\sqrt{d_t})$ is equal to $\mathbb{Z}/14\mathbb{Z}$.

Proof. By the same method in Theorem 3.1 we are done. □

3.4. The case $E(K)_{\text{tors}} = \mathbb{Z}/15\mathbb{Z}$.

Theorem 3.4. *Put $d_t = t^4 + 2t^3 - t^2 + 2t + 1$ with $t \in \mathbb{Q}$. Let E be an elliptic curve defined by the following equation:*

$$y^2 + (1 - c)xy - by = x^3 - bx^2,$$

where

$$\begin{cases} b = \frac{(t^2+t-1+\sqrt{d_t})(t^2+t+1-\sqrt{d_t})(t^2-t+1-\sqrt{d_t})(2t^3+t^2+t+1-\sqrt{d_t})}{4t^5(t+1)(t^2-t-1-\sqrt{d_t})^2}, \\ c = -\frac{(t^2-t+1-\sqrt{d_t})(t^2+t+1-\sqrt{d_t})(t^2+t-1+\sqrt{d_t})}{4t^3(t+1)(t^2-t-1-\sqrt{d_t})}. \end{cases}$$

Then the torsion subgroup of E over $\mathbb{Q}(\sqrt{d_t})$ is equal to $\mathbb{Z}/15\mathbb{Z}$.

Proof. By the same method in Theorem 3.1 we are done. □

3.5. The case $E(K)_{\text{tors}} = \mathbb{Z}/16\mathbb{Z}$.

Theorem 3.5. *Put $d_t = t^6 + 2t^5 - t^4 - t^2 - 2t + 1$ with $t \in \mathbb{Q}$. Let E be an elliptic curve defined by the following equation:*

$$y^2 + (1 - c)xy - by = x^3 - bx^2,$$

where

$$\begin{cases} b = \frac{t^2(t^3+t^2-t+1-\sqrt{d_t})(t^6+2t^5-t^3-2t^2-t+1-(t^3+t^2-1)\sqrt{d_t})(t^3+t^2+t+1-\sqrt{d_t})}{2(t^3+3t^2+t-1-\sqrt{d_t})^2}, \\ c = \frac{(t^6+2t^5-2t^2-t^3-t+1-(t^3+t^2-1)\sqrt{d_t})(t^3+t^2+t+1-\sqrt{d_t})}{2(t+1)(t^3+3t^2+t-1-\sqrt{d_t})}. \end{cases}$$

Then the torsion subgroup of E over $\mathbb{Q}(\sqrt{d_t})$ is equal to $\mathbb{Z}/16\mathbb{Z}$.

Proof. By the same method in Theorem 3.1 we are done. □

3.6. The case $E(K)_{\text{tors}} = \mathbb{Z}/18\mathbb{Z}$.

Theorem 3.6. *Put $d_t = t^6 - 4t^5 + 10t^4 - 10t^3 + 5t^2 - 2t + 1$ with $t \in \mathbb{Q}$. Let E be an elliptic curve defined by the following equation:*

$$y^2 + (1-c)xy - by = x^3 - bx^2,$$

where

$$\begin{cases} b = -\frac{t(t^3-t+1-\sqrt{d_t})(t^5-4t^4+9t^3-9t^2+4t-(t^2-2t+2)\sqrt{d_t})(t^4-2t^3+5t^2-5t+2-t\sqrt{d_t})}{(t-1)^4(t^6-4t^5+9t^4-10t^3+4t^2+t-1-(t^3-2t^2+2t-1)\sqrt{d_t})(t^4-2t^3+3t^2+t-2-t\sqrt{d_t})^2}, \\ c = \frac{t(t^5-4t^4+9t^3-9t^2+4t-(t^2-2t+2)\sqrt{d_t})(t^3-t+1-\sqrt{d_t})}{(t-1)^2(t^6-4t^5+9t^4-10t^3+4t^2+t-1-(t^3-2t^2+2t-1)\sqrt{d_t})(t^4-2t^3+3t^2+t-2-t\sqrt{d_t})}. \end{cases}$$

Then the torsion subgroup of E over $\mathbb{Q}(\sqrt{d_t})$ is equal to $\mathbb{Z}/18\mathbb{Z}$.

Proof. By the same method in Theorem 3.1 we are done. □

3.7. The case $E(K)_{\text{tors}} = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$.

Theorem 3.7. *Put $d_t = 8t^3 - 8t^2 + 1$ with $t \in \mathbb{Q}$. Let E be an elliptic curve defined by the following equation:*

$$y^2 + (1-c)xy - by = x^3 - bx^2,$$

where $b = \dfrac{t^3(2t^2-3t+1)}{(t^2-3t+1)^2}$ and $c = -\dfrac{t(2t^2-3t+1)}{t^2-3t+1}$. Then the torsion subgroup of E over $\mathbb{Q}(\sqrt{d_t})$ is equal to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$.

Proof. The elliptic curve defined by the form in the theorem has a $\mathbb{Q}$-rational torsion point $P = (0,0)$ of order 10. By the coordinate changes $x \to x$ and $y \to y + \frac{c-1}{2}x + \frac{b}{2}$, we get the following:

$$y^2 = x^3 + \frac{(c-1)^2 - 4b}{4}x^2 + \frac{b(c-1)}{2}x + \frac{b^2}{4}.$$

Since $5P$ is a $\mathbb{Q}$-rational point of order 2, the right hand side of the above equation should have a linear factor and a quadratic factor over $\mathbb{Q}$. By the simple calculation, one can show that the quadratic factor splits over the quadratic number field $\mathbb{Q}(\sqrt{d_t})$. □

3.8. The case $E(K)_{\text{tors}} = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$.

Theorem 3.8. *Put $d_t = \frac{t^2-1}{t^2+3}$ with $t \in \mathbb{Q}$. Let E be an elliptic curve defined by the following equation:*

$$y^2 + (1-c)xy - (c+c^2)y = x^3 - (c+c^2)x^2,$$

where $c = \dfrac{1-t^2}{t^4+3t^2}$. Then the torsion subgroup of E over $\mathbb{Q}\left(\sqrt{d_t}\right)$ is equal to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$.

Proof. The Tate normal form of an elliptic curve E with $\mathbb{Q}$-rational point $(0,0)$ of order 6 is the elliptic curve defined by

$$y^2 + (1-c)xy - (c+c^2) = x^3 - (c+c^2)x^2.$$

By the coordinate changes $x \to x$ and $y \to y + \frac{(c-1)}{2}x + \frac{(c^2+c)}{2}$, we get the following form:

$$y^2 = x^3 - \frac{3c^2+3c-1}{4}x^2 + \frac{c^3-c}{2}x + \frac{c^4+2c^3+c^2}{4}.$$

By substituting $c = \frac{10-2\alpha}{\alpha^2-9}$, we have

$$y^2 = \left(x + \frac{2(\alpha-1)^2}{(\alpha+3)^2(\alpha-3)}\right)\left(x + \frac{2(\alpha-5)}{(\alpha-3)(\alpha+3)}\right)\left(x + \frac{(\alpha-5)(\alpha-1)^2}{4(\alpha+3)(\alpha-3)^2}\right).$$

Note that the point $P = (0, \frac{c^2+c}{2})$ is of order 6 of the elliptic curve defined by the above equation. By Theorem 2.1, for a number field K, there exists a K-rational point Q with $2Q = P$ if and only if $\frac{2}{\alpha-3}$ and $\frac{\alpha-5}{\alpha+3}$ are square in K. Put $\alpha = 2t^2+3$. Then $c = \frac{1-t^2}{t^4+3t^2}$, and $\frac{2}{\alpha-3} = \frac{1}{t^2}$ and $\frac{\alpha-5}{\alpha+3} = \frac{t^2-1}{t^2+3}$ are squares in $\mathbb{Q}\left(\sqrt{d_t}\right)$. □

3.9. The case $E(K)_{\text{tors}} = \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$.

A one-parameter family of elliptic curves with points of order 3, called the *Hessian Family*, is given as follows [1, Ch. 4, Section 2]:

$$X^3 + Y^3 + Z^3 = 3\mu XYZ, \tag{8}$$

with μ in $\mathbb{Q}$. From [7, Table 1], we obtain the following:

Theorem 3.9. *Let $K = \mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\zeta_3)$ with a primitive cube root of unity ζ_3. Let E be an elliptic curve defined by the following equation:*

$$X^3 + Y^3 + Z^3 = 3tXYZ,$$

where $t \in \mathbb{Q}$ with $t^3 \neq 1$. Then the torsion subgroup of E over K is equal to $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$.

3.10. The case $E(K)_{\text{tors}} = \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$.

For finding a family of elliptic curves with $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$ as their torsion group, we begin with the curves in Eq. (8).

Theorem 3.10. *Let $K = \mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\zeta_3)$ with a primitive cube root of unity ζ_3. Let E be an elliptic curve defined by the following equation:*

$$X^3 + Y^3 + Z^3 = 3\mu XYZ,$$

where $\mu = \frac{2t^3+1}{3t^2}$ and $t \in \mathbb{Q}$ with $t \neq 0, 1, -\frac{1}{2}$. Then the torsion subgroup of E over K is equal to $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$.

Proof. We can refer to [7, Table 1]. □

3.11. The case $E(K)_{\text{tors}} = \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$.

Theorem 3.11. *Let $K = \mathbb{Q}(\sqrt{-1})$ and let E be an elliptic curve defined by the following equation:*

$$y^2 + xy - (\nu^2 - \frac{1}{16})y = x^3 - (\nu^2 - \frac{1}{16})x^2,$$

where $\nu = t^2$ and $t \in \mathbb{Q}$ with $t \neq 0, \pm\frac{1}{16}$. Then the torsion subgroup of E is equal to $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ over K.

Proof. We know that the curve $E : y^2 + xy - (\nu^2 - \frac{1}{16})y = x^3 - (\nu^2 - \frac{1}{16})x^2$ with a parameter ν has $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ as the torsion group over $\mathbb{Q}$ from [7, Table 1]. We note that $P = (0, 0)$ is a point of order 4 and $2P = (\nu^2 - \frac{1}{16}, 0)$. By Theorem 2.1, for another 2-torsion point $Q = (-\frac{1}{8} + \frac{\nu}{2}, \frac{(4\nu-1)^2}{32})$, there exist a K-rational point R with $2R = Q$ if and only if $(-\frac{1}{8} + \frac{\nu}{2}) - (-\frac{1}{8} - \frac{\nu}{2}) = \nu$ and $(-\frac{1}{8} + \frac{\nu}{2}) - (\nu^2 - \frac{1}{16}) = -\frac{(4\nu-1)^2}{16}$ are squares in K. It follows from taking $\nu = t^2$. □

4. Torsion subgroups over quartic number fields K

Throughout this section, K denotes a quartic number field. In this section we construct some families of elliptic curves with prescribed torsion structures given in Eq. (5) over quartic number fields; those torsion structures do not occur over $\mathbb{Q}$ and quadratic number fields.

A smooth projective curve X over an algebraically closed field is called *d-gonal* if there exists a finite morphism $f : X \to \mathbb{P}^1$ of degree d. For $d = 4$ we say that the curve is *tetragonal.* Also, the smallest possible d is called the *gonality* of the curve X and we denote it by $\text{Gon}(X)$. Sutherland [17] basically attempted to find a plane model $f_N(x, y) = 0$ of $X_1(N)$ which minimizes the degree d of one of its variables. Noting that $\text{Gon}(X_1(N)) = 3$ and $\text{Gon}(X_1(N)) = 4$ with $N = 17, 21, 22, 24$, for the cases $N = 17, 20, 21, 22$, Sutherland succeeded in finding plane models $f_N(x, y) = 0$ such that the degree in y of $f_N(x, y)$ is equal to $\text{Gon}(X_1(N))$. However, the case $N = 24$ has not been achieved by Sutherland.

In this section, for $N = 17, 21, 22$, using Sutherland's plane models for $X_1(N)$, we find infinite families of elliptic curves over quartic number fields whose torsion is $\mathbb{Z}/N\mathbb{Z}$. But, as mentioned before, for the case $N = 24$, we need to develop another method for this case, and this case is resolved in the subsection 4.5. Finally, for the case $N = 20$, we point out that we cannot use Sutherland's plane model for $X_1(20)$ since each degree of its variables in his model is not 4, but 3. We therefore need a proper model of $X_1(20)$ where the degree of one of its variables is exactly equal to 4, and we show how we resolve this case in the subsection 4.2.

4.1. The case $E(K)_{\text{tors}} = \mathbb{Z}/17\mathbb{Z}$.

Theorem 4.1. *Suppose that the polynomial* $f(x) = x^4 + (t^3 + t^2 - t + 2)x^3 + (t^3 - 3t + 1)x^2 - (t^4 + 2t)x + t^3 + t^2$ *is irreducible over* $\mathbb{Q}$ *for some* $t \in \mathbb{Q}$. *Let* α_t *be a zero of* $f(x)$. *Let* E *be an elliptic curve defined by the following equation:*

$$y^2 + (1 - c)xy - by = x^3 - bx^2,$$

where

$$\begin{cases} b = -\frac{(t+1)\alpha_t(\alpha_t-t)(\alpha_t-t^2-t)}{(\alpha_t+t+1)(\alpha_t{}^2-t\alpha_t+\alpha_t-t^2-t)^2}, \\ c = -\frac{(t+1)\alpha_t(\alpha_t-t)}{(\alpha_t+t+1)(\alpha_t{}^2-t\alpha_t+\alpha_t-t^2-t)}. \end{cases}$$

Then the torsion subgroup of E *over a quartic number field* $\mathbb{Q}(\alpha_t)$ *is equal to* $\mathbb{Z}/17\mathbb{Z}$.

Proof. From Table 1, we note that the points $(x, y) = (t, \alpha_t)$ satisfy the following:

$$f(x, y) = y^4 + (x^3 + x^2 - x + 2)y^3 + (x^3 - 3x + 1)y^2 - (x^4 + 2x)y + x^3 + x^2 = 0$$

which is an defining equation of $X_1(17)$. Also the coefficients b and c of E can be expressed by the following:

$$b = -\frac{(x+1)y(x-y)(x^2+x-y)}{(x+y+1)(x^2+xy+x-y^2-y)^2}, \quad c = -\frac{(x-y)y(x+1)}{(x+y+1)(x^2+xy+x-y^2-y)}.$$

The result follows from the substitution $x = t$ and $y = \alpha_t$. □

4.2. **The case** $E(K)_{\text{tors}} = \mathbb{Z}/20\mathbb{Z}$**.**

As explained in the beginning of this section, we need to find a plane model of $X_1(20)$ where the degree of one of its variables is equal to 4. For finding it, using the Reichert's method [14], we obtain the following:

Proposition 4.2. *The modular curve* $X_1(20)$ *has a plane model as follows:*

$$(x^2+2x+1)y^4-(x^2-1)y^3+(x^4+x^3-2x^2-3x)y^2+(x^4+4x^3+3x^2)y-x^5-2x^4-x^3 = 0.$$

Applying the same method used for the proof of Theorem 4.1 with the equation given in Propostion 4.2, we obtain the following result.

Theorem 4.3. *Suppose that the polynomial*

$$f(x) = (t^2 + 2t + 1)x^4 - (t^2 - 1)x^3 + (t^4 + t^3 - 2t^2 - 3t)x^2 + (t^4 + 4t^3 + 3t^2)x - t^5 - 2t^4 - t^3$$

is irreducible over $\mathbb{Q}$ *for some* $t \in \mathbb{Q}$. *Let* α_t *be a zero of* $f(x)$. *Let* E *be an elliptic curve defined by the following equation:*

$$y^2 + (1 - c)xy - by = x^3 - bx^2,$$

where

$$\begin{cases} b = \frac{\alpha_t(\alpha_t+1)(\alpha_t-t)(\alpha_t{}^2+\alpha_t-t)}{(t\alpha_t+\alpha_t-t)^2}, \\ c = \frac{\alpha_t(\alpha_t+1)(\alpha_t-t)}{(t\alpha_t+\alpha_t-t)}. \end{cases}$$

Then the torsion subgroup of E *over a quartic number field* $K = \mathbb{Q}(\alpha_t)$ *is equal to* $\mathbb{Z}/20\mathbb{Z}$.

4.3. **The case $E(K)_{\text{tors}} = \mathbb{Z}/21\mathbb{Z}$.**

Using the same method given for the proof of Theorem 4.1, we obtain the following result.

Theorem 4.4. *Suppose that the polynomial $f(x) = x^4 + (3t^2+1)x^3 + (t^5+t^4+2t^2+2t)x^2 + (2t^4+t^3+t)x + t^3$ is irreducible over $\mathbb{Q}$ for some $t \in \mathbb{Q}$. Let α_t be a zero of $f(x)$. Let E be an elliptic curve defined by the following equation:*

$$y^2 + (1-c)xy - by = x^3 - bx^2,$$

where

$$\begin{cases} b = \frac{\alpha_t(\alpha_t+1)(t\alpha_t+\alpha_t+1)(\alpha_t{}^2+t\alpha_t+\alpha_t+1)(\alpha_t{}^3+t^2\alpha_t{}^2+t\alpha_t{}^2+\alpha_t{}^2+2t\alpha_t+\alpha_t+1)}{(t\alpha_t+1)^3(\alpha_t{}^2-t\alpha_t-1)^2}. \\ c = -\frac{\alpha_t(\alpha_t+1)(t\alpha_t+\alpha_t+1)(\alpha_t{}^2+t\alpha_t+\alpha_t+1)}{(t\alpha_t+1)^2(\alpha_t{}^2-t\alpha_t-1)}. \end{cases}$$

Then the torsion subgroup of E over a quartic number field $K = \mathbb{Q}(\alpha_t)$ is equal to $\mathbb{Z}/21\mathbb{Z}$.

4.4. **The case $E(K)_{\text{tors}} = \mathbb{Z}/22\mathbb{Z}$.**

We obtain the following result by using the same method used for the proof of Theorem 4.1.

Theorem 4.5. *Suppose that the polynomial $f(x) = x^4 + (t^3+2t^2+t+2)x^3 + (t^5+t^4+2t^3+2t^2+1)x^2 + (t^5-t^4-2t^3-t^2-t)x - t^4 - t^3$ is irreducible over $\mathbb{Q}$ for some $t \in \mathbb{Q}$. Let α_t be a zero of $f(x)$. Let E be an elliptic curve defined by the following equation:*

$$y^2 + (1-c)xy - by = x^3 - bx^2,$$

where

$$\begin{cases} b = \frac{\alpha_t(t+1)t(t\alpha_t-t+\alpha_t-t^2)(t^2\alpha_t+t^2+t\alpha_t+\alpha_t)}{(t^2+\alpha_t)(t^3+2t^2+\alpha_t)^2}, \\ c = \frac{(t\alpha_t-t+\alpha_t-t^2)t\alpha_t(t+1)}{(t^2+\alpha_t)(t^3+2t^2+\alpha_t)}. \end{cases}$$

Then the torsion subgroup of E over a quartic number field $K = \mathbb{Q}(\alpha_t)$ is equal to $\mathbb{Z}/21\mathbb{Z}$.

4.5. **The case $E(K)_{\text{tors}} = \mathbb{Z}/24\mathbb{Z}$.**

In this subsection, we construct an infinite family of elliptic curves over quartic number fields whose torsion group is $\mathbb{Z}/24\mathbb{Z}$. Since there is a forgetful map of degree 4 from $X_1(24)$ to $X_1(12)$ which is rational, the points on $X_1(24)$ lying above each $\mathbb{Q}$-rational point on $X_1(12)$ are automatically defined over quartic number fields. It means that the elliptic curve corresponding to each $\mathbb{Q}$-rational point on $X_1(12)$ should have a 24-torsion point over a quartic number field. We explain the computation process explicitly in the proof of Theorem 4.6.

Theorem 4.6. *Put $f(x) = c_4(t)x^4 + c_2(t)x^2 + c_1(t)x + c_0(t)$, where*

$$\begin{aligned} c_4(t) &= 16t^{12} - 192t^{11} + 1056t^{10} - 3520t^9 + 7920t^8 - 12672t^7 + 14784t^6 - 12672t^5 + 7920t^4 - 3520t^3 \\ &\quad +1056t^2 - 192t + 16, \\ c_2(t) &= 96t^{14} - 1536t^{13} + 9888t^{12} - 36192t^{11} + 86400t^{10} - 144096t^9 + 174048t^8 - 154656t^7 + 100984t^6 \\ &\quad -47472t^5 + 15240t^4 - 2912t^3 + 168t^2 + 48t - 8, \\ c_1(t) &= -768t^{14} + 8064t^{13} - 39040t^{12} + 115520t^{11} - 233408t^{10} + 340544t^9 - 369664t^8 + 302720t^7 \\ &\quad -187264t^6 + 86528t^5 - 29056t^4 + 6720t^3 - 960t^2 + 64t, \\ c_0(t) &= 144t^{16} - 576t^{15} + 2112t^{14} - 9696t^{13} + 34016t^{12} - 82176t^{11} + 141936t^{10} - 181984t^9 + 177240t^8 \\ &\quad -132528t^7 + 76096t^6 - 33208t^5 + 10760t^4 - 2480t^3 + 376t^2 - 32t + 1. \end{aligned}$$

If $f(x)$ is irreducible over $\mathbb{Q}$ for some $t \in \mathbb{Q}$. Let α_t be a zero of $f(x)$. Let E be an elliptic curve defined by the following equation:

$$y^2 + (1-c)xy - by = x^3 - bx^2,$$

where

$$\begin{cases} b = \frac{t(2t-1)(3t^2-3t+1)(2t^2-2t+1)}{(t-1)^4}, \\ c = -\frac{t(2t-1)(3t^2-3t+1)}{(t-1)^3}. \end{cases}$$

Then the torsion subgroup of E over a quartic number field $K = \mathbb{Q}(\alpha_t)$ is equal to $\mathbb{Z}/24\mathbb{Z}$.

Proof. The elliptic curve defined as above has a $\mathbb{Q}$-rational torsion point $P = (0,0)$ of order 12. By the coordinate changes $x \to x$ and $y \to y + \frac{c-1}{2}x + \frac{b}{2}$, E is changed to the following form:

$$y^2 = x^3 + \frac{(c-1)^2 - 4b}{4}x^2 + \frac{b(c-1)}{2}x + \frac{b^2}{4}. \tag{9}$$

For simplicity, we write the curve in Eq. (9) by

$$y^2 = x^3 + Ax^2 + Bx + C, \tag{10}$$

where $A = \frac{(c-1)^2-4b}{4}, B = \frac{b(c-1)}{2}$, and $C = \frac{b^2}{4}$.

Let $P = (x_0, y_0)$ be a rational 12-torsion point of the curve in Eq. (10). Changing variables in x, we may assume $x_0 = 0$. Then

$$y_0^2 = c.$$

Now consider a point (x_1, y_1) with $2(x_1, y_1) = (0, y_0)$. Take $y = kx + y_0$ as the line through $(0, y_0)$ tangent at the unknown point (x_1, y_1). Then the three roots of

$$x^3 + Ax^2 + Bx + C - (kx + y_0)^2 \tag{11}$$

are $0, x_1$ and x_1, i.e., x_1 is a double root of Eq (11). Thus

$$\frac{x^3 + Ax^2 + Bx + C - (kx + y_0)^2}{x} = (x - x_1)^2,$$

and hence the discriminant of

$$x^2 + (A - k^2)x + (B - 2ky_0) \tag{12}$$

is equal to 0, i.e.,

$$(A - k^2)^2 - 4(B - 2ky_0) = 0, \tag{13}$$

which is a quartic equation in k.

Let k_0 be a root of Eq. (13) and K a quartic number field containing k_0. Then

$$x_1 = \frac{k_0^2 - A}{2}$$

is a double root of Eq. (12) and hence also of Eq. (11). Consequently $2(x_1, k_0x_1 + y_0) = (0, -y_0)$, and $2(x_1, -k_0x_1 - y_0) = (0, y_0)$. In other words, (x_1, y_1) is a K-rational 24-torsion point of E.

The computation process explained as above thus gives our result immediately. □

4.6. **The case $E(K)_{\text{tors}} = \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}$.**

Theorem 4.7. *Let $K = \mathbb{Q}(\zeta_5)$ with ζ_5 a primitive fifth root of unity, and let E be an elliptic curve over K defined by*

$$E : y^2 = x^3 - ax + b,$$

where

$$\begin{cases} a = \frac{t^{20}-228t^{15}+494t^{10}+228t^5+1}{48}, \\ b = \frac{t^{30}+522t^{25}-10005t^{20}-10005t^{10}-522t^5+1}{864}, \end{cases}$$

with t in $\mathbb{Q}$. Then $E(K)_{\text{tors}}$ is equal to $\mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}$.

Proof. The result follows from [15, Section 1.2]. □

4.7. **The case $E(K)_{\text{tors}} = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$.**

Theorem 4.8. *Put $d_t = t^4 + 2t^3 + t^2 - 4t$ with $t \in \mathbb{Q}$. Let E be an elliptic curve defined by the following equation:*

$$y^2 + (1 - c)xy - by = x^3 - bx^2,$$

where

$$\begin{cases} b = \frac{8(t-1)(t^2-t-\sqrt{d_t})(t^4+t^3-t^2-3t+2-(t^2-1)\sqrt{d_t})}{(t^2+t-2-\sqrt{d_t})^3(t^2-t-2-\sqrt{d_t})^2}, \\ c = \frac{4(t-1)(t^2-t-\sqrt{d_t})}{(t^2+t-2-\sqrt{d_t})^2(t^2-t-2-\sqrt{d_t})}. \end{cases}$$

Then the torsion subgroup of E over a quartic number field K is equal to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$ where $K = \mathbb{Q}(\sqrt{A_t + B_t\sqrt{d_t}})$ with

$$\begin{cases} A_t &= 2(t^2 - 1)^2(t^8 + 8t^7 + 24t^6 + 32t^5 + 4t^4 - 32t^3 - 24t^2 + 8t + 2), \\ B_t &= 2t(t^2 - 1)(t^7 + 7t^6 + 16t^5 + 10t^4 - 18t^3 - 26t^2 + 12). \end{cases}$$

Proof. The elliptic curve defined by the form in the theorem has a $\mathbb{Q}$-rational torsion point $P = (0, 0)$ of order 14. By the coordinate changes $x \to x$ and $y \to y + \frac{c-1}{2}x + \frac{b}{2}$, we get the following:

$$y^2 = x^3 + \frac{(c-1)^2 - 4b}{4}x^2 + \frac{b(c-1)}{2}x + \frac{b^2}{4}.$$

Since $7P$ is a $\mathbb{Q}$-rational point of order 2, the right hand side of the above equation should have a linear factor and a quadratic factor over $\mathbb{Q}$. By the simple calculation, one can show that the quadratic factor splits over the quadratic number field K. □

4.8. The case $E(K)_{\text{tors}} = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z}$.

Theorem 4.9. *Put $d_t = t^6 + 2t^5 - t^4 - t^2 - 2t + 1$ with $t \in \mathbb{Q}$. Let E be an elliptic curve defined by the following equation:*

$$y^2 + (1-c)xy - by = x^3 - bx^2,$$

where

$$\begin{cases} b = \frac{t^2(t^3+t^2-t+1-\sqrt{d_t})(t^6+2t^5-t^3-2t^2-t+1-(t^3+t^2-1)\sqrt{d_t})(t^3+t^2+t+1-\sqrt{d_t})}{2(t^3+3t^2+t-1-\sqrt{d_t})^2}, \\ c = \frac{(t^6+2t^5-2t^2-t^3-t+1-(t^3+t^2-1)\sqrt{d_t})(t^3+t^2+t+1-\sqrt{d_t})}{2(t+1)(t^3+3t^2+t-1-\sqrt{d_t})}. \end{cases}$$

Then the torsion subgroup of E over a quartic number field K is equal to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z}$ where $K = \mathbb{Q}(\sqrt{A_t + B_t\sqrt{d_t}})$ with

$$\begin{cases} A_t & = 2(t^2+2t-1)(t^2-2t-1)(t^{16}+8t^{15}+24t^{14}+32t^{13}+12t^{12}-24t^{11}-52t^{10}-48t^9-10t^8+24t^7+32t^6 \\ & \quad +16t^5-2t^4-8t^3-4t^2+1), \\ B_t & = -2(t+1)(t^2+2t-1)(t^2-2t-1)(t^4+2t^3-1)(t^8+4t^7+4t^6-2t^4-4t^3-2t^2+1). \end{cases}$$

Proof. The proof is the same as in Theorem 4.8. □

4.9. The case $E(K)_{\text{tors}} = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/18\mathbb{Z}$.

Theorem 4.10. *Put $d_t = t^6 - 4t^5 + 10t^4 - 10t^3 + 5t^2 - 2t + 1$ with $t \in \mathbb{Q}$. Let E be an elliptic curve defined by the following equation:*

$$y^2 + (1-c)xy - by = x^3 - bx^2,$$

where

$$\begin{cases} b = -\frac{t(t^3-t+1-\sqrt{d_t})(t^5-4t^4+9t^3-9t^2+4t-(t^2-2t+2)\sqrt{d_t})(t^4-2t^3+5t^2-5t+2-t\sqrt{d_t})}{(t-1)^4(t^6-4t^5+9t^4-10t^3+4t^2+t-1-(t^3-2t^2+2t-1)\sqrt{d_t})(t^4-2t^3+3t^2+t-2-t\sqrt{d_t})^2} \\ c = \frac{t(t^5-4t^4+9t^3-9t^2+4t-(t^2-2t+2)\sqrt{d_t})(t^3-t+1-\sqrt{d_t})}{(t-1)^2(t^6-4t^5+9t^4-10t^3+4t^2+t-1-(t^3-2t^2+2t-1)\sqrt{d_t})(t^4-2t^3+3t^2+t-2-t\sqrt{d_t})} \end{cases}$$

Then the torsion subgroup of E over a quartic number field K is equal to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/18\mathbb{Z}$ where $K = \mathbb{Q}(\sqrt{A_t + B_t\sqrt{d_t}})$, where A_t is given by

$$\begin{aligned} A_t \;=\; & 2(t-1)(t^2-t+1)(t^{81}-60t^{80}+1823t^{79}-37283t^{78}+575948t^{77}-7153345t^{76}+74270830t^{75}-661972936t^{74}+ \\ & 5162951498t^{73}-35748416786t^{72}+222220017978t^{71}-1251268732638t^{70}+6428384983229t^{69}-30312842608758t^{68}+ \\ & 131851626338239t^{67}-531250231119487t^{66}+1989823103024944t^{65}-6949508334581021t^{64}+22691031914247536t^{63}- \\ & 69421587124788592t^{62}+199398166568254427t^{61}-538599074700096200t^{60}+1370123432130051153t^{59} \\ & -3286607755162234569t^{58}+7442130833595477585t^{57}-15922314702385616367t^{56}+32211496441342160295t^{55} \\ & -61658320854407144771t^{54}+111732077832460006205t^{53}-191757358447486495265t^{52}+311783981857223273273t^{51}- \\ & 480377955812187198067t^{50}+701460096702393266510t^{49}-970828388582220808403t^{48}+1273499554107320498366t^{47}- \\ & 1583214470476057699882t^{46}+1865115992455672404654t^{45}-2081672644416495160786t^{44}+2200653935514819200850t^{43}- \\ & 2202900614029732113706t^{42}+2087342688173047087363t^{41}-1871469093808964236066t^{40}+1587010892862821302769t^{39}- \\ & 1272297692443572413697t^{38}+963823942575617496446t^{37}-689572852989653464007t^{36}+465685230414220170072t^{35}- \\ & 296668110710834337894t^{34}+178166673734004537624t^{33}-100794853955586974376t^{32}+53671606628550181752t^{31}- \\ & 26873929294396454432t^{30}+12639178841587420111t^{29}-5576323664562001728t^{28}+2304415519922916597t^{27} \\ & -890391919078266901t^{26}+320989515486805463t^{25}-107696232645654483t^{24}+33528606629383737t^{23}-9651448544386565t^{22}+ \\ & 2557905282500493t^{21}-620967067981855t^{20}+137230418386789t^{19}-27398950003547t^{18}+4895941157601t^{17}-773754511787t^{16}+ \end{aligned}$$

$$\begin{aligned}&106508074699t^{15} - 12516444275t^{14} + 1222390172t^{13} - 94746133t^{12} + 5272314t^{11} - 285040t^{10} + 36123t^{9} + 17014t^{8} - \\ &2203t^{7} - 2825t^{6} - 197t^{5} + 301t^{4} + 75t^{3} - 13t^{2} - 8t - 1),\end{aligned}$$

and B_t is given by

$$\begin{aligned}B_t \ = \ &-2(t-1)(t^2-t+1)(t^{78} - 58t^{77} + 1704t^{76} - 33702t^{75} + 503490t^{74} - 6046959t^{73} + 60699920t^{72} - 522929353t^{71} \\ &+ 3940918563t^{70} - 26356739261t^{69} + 158186387740t^{68} - 859569644802t^{67} + 4259404814230t^{66} - 19361594602200t^{65} \\ &+ 81132918428583t^{64} - 314714160514115t^{63} + 1134028075395685t^{62} - 3807324327193293t^{61} + 11940365012019310t^{60} \\ &- 35056812996275666t^{59} + 96539555039238846t^{58} - 249758967163209436t^{57} + 607888013075773385t^{56} \\ &- 1393565756338056381t^{55} + 3012092530860805936t^{54} - 6143427051448922789t^{53} + 11831916271965320454t^{52} \\ &- 21529969450924825288t^{51} + 37030874361408910140t^{50} - 60222036165664943643t^{49} + 92621203398649851311t^{48} \\ &- 134734395934473174400t^{47} + 185382543547282957200t^{46} - 241241935747139935962t^{45} + 296869812973936381290t^{44} \\ &- 345390717911773880952t^{43} + 379802067053070885010t^{42} - 394591051392115015200t^{41} + 387163287527891969172t^{40} \\ &- 358580348412681696084t^{39} + 313320640785305093519t^{38} - 258133725124201327476t^{37} + 200390095910550691472t^{36} \\ &- 146482677090320791692t^{35} + 100752870514167716130t^{34} - 65155408697205999195t^{33} + 39582254226841158336t^{32} \\ &- 22568926785727839867t^{31} + 12065466588240181737t^{30} - 6041011344235745169t^{29} + 2829101680897337178t^{28} \\ &- 1237413441787086082t^{27} + 504607238173621602t^{26} - 191458622895023160t^{25} + 67425601804317209t^{24} \\ &- 21975944178516265t^{23} + 6606041365002714t^{22} - 1823904224924193t^{21} + 460205086854590t^{20} - 105472707074592t^{19} \\ &+ 21792791183536t^{18} - 4021810727929t^{17} + 655195672587t^{16} - 92814616290t^{15} + 11201918849t^{14} - 1118622606t^{13} \\ &+ 89370166t^{12} - 5641950t^{11} + 134652t^{10} + 43891t^{9} + 19034t^{8} - 4317t^{7} - 3356t^{6} - 9t^{5} + 384t^{4} + 70t^{3} - 20t^{2} - 9t - 1).\end{aligned}$$

Proof. The proof is the same as in Theorem 4.8. □

4.10. The case $E(K)_{\text{tors}} = \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z}$.

We need the following result in [10, Proposition 3.1] for proving Theorem 4.12, which is useful for finding the divisibility condition of a given point on E by 3.

Proposition 4.11. *Let K be a number field whose characteristic is different from 3 and which contains a primitive third root of unity ζ_3. Let E be an elliptic curve over K with full 3-torsion given by $E : X^3 + Y^3 + Z^3 = 3\mu XYZ$, and $f_S = -27(\mu^3 - 1)\frac{{\zeta_3}^2 X + \zeta_3 Y + \mu Z}{X+Y+\mu Z}$ and $f_T = 9(\mu^2 + \mu + 1)\frac{X+\mu Y+Z}{X+Y+\mu Z}$ with $\mu^3 \neq 1$. Then for the following injection*

$$E(K)/3E(K) \to H^1(G, E[3]) \simeq K^*/K^{*3} \times K^*/K^{*3},$$

where $H^1(G, E[3])$ is the Galois cohomology group, $G = Gal(\bar{K}/K)$ and $E[3] = E[3](\bar{K})$, the pair (f_S, f_T) of rational functions on E gives its image in $H^1(G, E[3]) \simeq K^*/K^{*3} \times K^*/K^{*3}$ when evaluated at a point of $E(K)$.

Theorem 4.12. *Let $K = \mathbb{Q}(\sqrt{3t(4-t^3)}, \sqrt{-3})$ with $t \in \mathbb{Q}$, and let E be an elliptic curve defined by the following equation:*

$$X^3 + Y^3 + Z^3 = 3\mu XYZ$$

where $\mu = \zeta_3 + \frac{\left(3t^2 \pm \sqrt{3t(4-t^3)}\right)^3}{72\sqrt{-3}t^3}$ *with* $\mu^3 \neq 1$. *Then the torsion subgroup of* E *over a quartic number field* K *is equal to* $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z}$.

Proof. We use Proposition 4.11. We note that $P = (0; -1; 1)$ is a 3-torsion point from [1, Ch. 4, Section 2] so that we have $f_S = -27(\mu^2+\mu+1)(\mu-\zeta_3)$ and $f_T = -9(\mu^2+\mu+1)$ when f_S, f_T are evaluated at the point P. From Proposition 4.11, it suffices to find a condition of μ for which f_S and f_T are cubic in some quartic number fields. Note that $\dfrac{f_S}{f_T} = 3(\mu - \zeta_3)$. Setting $-3(\mu - \zeta_3) = x^3$ and $-3(\mu - \zeta_3^2) = y^3$ yields $f_T = -9(\mu - \zeta_3)(\mu - {\zeta_3}^2) = (-x)^3 y^3$. We also have $x^3 - y^3 = 3(\zeta_3 - \zeta_3^2) = 3\sqrt{-3}$, so

$$\left(-\frac{x}{\sqrt{-3}}\right)^3 - \left(-\frac{y}{\sqrt{-3}}\right)^3 = 1.$$

Let $X = -\dfrac{x}{\sqrt{-3}}$ and $Y = -\dfrac{y}{\sqrt{-3}}$, then we have $X^3 - Y^3 = 1$, and it is enough to show that the equation $X^3 - Y^3 = 1$ has infinitely many quadratic points. Let $X = Y + t$ then we have

$$3tY^2 + 3t^2Y + t^3 = 1.$$

Then

$$Y = \frac{-3t^2 \pm \sqrt{3t(4-t^3)}}{6t}.$$

Thus $X = Y + t$ and Y are defined over quadratic number fields K, so the result follows. □

4.11. **The case** $E(K)_{\text{tors}} = \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$.

Theorem 4.13. *Let* $K = \mathbb{Q}(\sqrt{-1}, \sqrt{4it^2+1})$ *with* $t \in \mathbb{Q}$ *and* $t \neq 0, \pm\frac{1}{16}$, *and let* E *be an elliptic curve defined by the following equation:*

$$y^2 + xy - (\nu^2 - \frac{1}{16})y = x^3 - (\nu^2 - \frac{1}{16})x^2,$$

where $\nu = it^2 + \frac{1}{4}$ *and* $t \neq 0, \pm\frac{1}{16}$. *Then the torsion subgroup of* E *over* K *is equal to* $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$.

Proof. Let E be defined as in subsection 3.11. Then the torsion subgroup of E over $\mathbb{Q}(i)$ is equal to $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$. Note that $P = (0, 0)$ is a point of order 4 and $2P = (\nu^2 - \frac{1}{16}, 0)$. There are two other 2-torsion points $(-\frac{1}{8} + \frac{\nu}{2}, \frac{(4\nu-1)^2}{32})$ and $(-\frac{1}{8} - \frac{\nu}{2}, \frac{(4\nu-1)^2}{32})$. Let $\alpha = \nu^2 - \frac{1}{16}$, $\beta = -\frac{1}{8} + \frac{\nu}{2}$ and $\gamma = -\frac{1}{8} - \frac{\nu}{2}$. By Theorem 2.1, there exist a K-rational point Q with $2Q = P$ if and only if $0 - \alpha = -(\nu^2 - \frac{1}{16})$, $0 - \beta = -(-\frac{1}{8} + \frac{\nu}{2})$, and $0 - \gamma = -(-\frac{1}{8} - \frac{\nu}{2})$ are all squares in K. This follows from taking $\nu = it^2 + \frac{1}{4}$. □

4.12. The case $E(K)_{\mathrm{tors}} = \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$.

Theorem 4.14. *Let $K = \mathbb{Q}(\sqrt{-3}, \sqrt{8t^3+1})$ with $t \in \mathbb{Q}$, and let E be an elliptic curve defined by the following equation:*

$$E_\mu : y^2 = x^3 - 27\mu(\mu^3+8)x + 54(\mu^6 - 20\mu^3 - 8),$$

where $\mu = \frac{2t^3+1}{3t^2}$ with $t \neq 0, 1, -\frac{1}{2}$. Then the torsion subgroup of E over K is equal to $\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$.

Proof. The curve given in Subsection 3.10 has the following Weierstrass model [15]

$$E_\mu : y^2 = x^3 - 27\mu(\mu^3+8)x + 54(\mu^6 - 20\mu^3 - 8).$$

If $\mu = \frac{2t^3+1}{3t^2}$, then E_μ has $\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$ as its full torsion group over $K = \mathbb{Q}(\sqrt{-3}, \sqrt{8t^3+1})$. We note that E_μ has the following 2-torsion points: $((8t^6 + 20t^3 - 1 \pm 3\sqrt{(8t^3+1)^3})/6t^4,\ 0)$, $(-(8t^6 + 20t^3 - 1)/3t^4,\ 0)$. □

Acknowledgments. We would like to thank KIAS (Korea Institute for Advanced Study) for its hospitality.

References

1. D. Husemöller, *Elliptic curves*, Second edition, Springer-Verlag, New York, 2004.
2. D. Jeon, C.H. Kim and E. Park, On the torsion of elliptic curves over quartic number fields, *J. London Math. Soc.* (2) **74** (2006), 1–12.
3. D. Jeon, C.H. Kim and A. Schweizer, On the torsion of elliptic curves over cubic number fields. *Acta Arith.* **113** (2004), 291–301.
4. S. Kamienny and B. Mazur, Rational torsion of prime order in elliptic curves over number fields. With an appendix by A. Granville. Columbia University Number Theory Seminar (New York, 1992). *Astérisque* No. 228 **1995**, 3, 81–100.
5. C.H. Kim and J.K. Koo, Generators of function fields of the modular curves $X_1(5)$ and $X_1(6)$, preprint.
6. A.W. Knapp, *Elliptic Curves*, Mathematical Notes 40, Princeton University Press, Princeton, NJ, 1992.
7. D.S. Kubert, Universal bounds on the torsion of elliptic curves, *Proc. London Math. Soc. (3)* **33** (1976), 193–237.
8. B. Mazur, Modular curves and the Eisenstein ideal, *Publ. Math. I.H.E.S.* **47** (1977), 33–168.
9. L. Merel, Bornes pour la torsion des courbes elliptiques sur les corps de nombres, *Invent. Math.* **124** (1996), no 1-3, 437-449.
10. C. O'Neil, Explicit descent over $X(3)$ and $X(5)$, arXiv:0201.5321 [math.NT] (2002).
11. A. Petho, T. Weis and H.G. Zimmer, Torsion groups of elliptic curves with integral j-invariant over general cubic number fields, *Internat. J. Algebra Comput.* **7** (1997), 353–413.
12. P. Parent, No 17-torsion on elliptic curves over cubic number fields, *J. Theor. Nombres Bordeaux* **15** (2003), 831–838.
13. P. Parent, Torsion des courbes elliptiques sur les corps cubiques, *Ann. Inst. Fourier (Grenoble)* **50** (2000), no. 3, 723–749.
14. M.A. Reichert, Explicit determination of nontrivial torsion structures of elliptic curves over quadratic number fields, *Math. Comp.* **46** (1986), 637–658.

15. K. Rubin abd A. Silverberg, Families of elliptic curves with constant mod p representations, *in Elliptic curves, modular forms, and Fermat's last theorem* (Hong Kong, 1993), 148–161, Ser. Number Theory, I, Int. Press, Cambridge, MA, 1995.
16. J. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, New York, 1986.
17. A.V. Sutherland, Constructing elliptic curves over finite fields with prescribed torsion, arXiv:0811.0296v2 [math.NT] (2008).
18. Y. Yang, Defining equations of modular curves, *Adv. in Math.* **204** (2006), 481–508.
19. H.G. Zimmer, Torsion groups of elliptic curves over cubic and certain biquadratic number fields, *Arithmetic geometry (Tempe, AZ, 1993),* 203–220, Comtemp. Math., 174, *Amer. Math. Soc., Providence, RI,* 1994.

Daeyeol Jeon
Department of Mathematics Education, Kongju National University, Kongju, Chungnam, South Korea
E-mail address: dyjeon@kongju.ac.kr

Chang Heon Kim
Department of Mathematics, Hanyang University, Seoul, South Korea
E-mail address: chhkim@hanyang.ac.kr

Yoonjin Lee
Department of Mathematics, Ewha Womans University, Seoul, South Korea
E-mail address: yoonjinl@ewha.ac.kr