MATHEMATICS OF COMPUTATION
Volume 80, Number 273, January 2011, Pages 579–591
S 0025-5718(10)02369-0
Article electronically published on May 12, 2010

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

DAEYEOL JEON, CHANG HEON KIM, AND YOONJIN LEE

Abstract. In this paper we construct infinite families of elliptic curves with given torsion group structures over cubic number fields. This result provides explicit examples of the theoretical result recently developed by the first two authors and A. Schweizer; they determined all the group structures which occur infinitely often as the torsion of elliptic curves over cubic number fields. In fact, this paper presents an efficient way of constructing such families of elliptic curves with prescribed torsion group structures over cubic number fields.

1. Introduction

The characterization of all torsion groups of elliptic curves E over a number field is certainly an important research problem. Mazur [8] determined all torsion groups of elliptic curves over the rational number field $\mathbb{Q}$: 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:

$$(1) \qquad \begin{array}{ll} \mathbb{Z}/N\mathbb{Z}, & N = 1, \ldots, 10, 12, \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N'\mathbb{Z}, & N' = 1, \ldots, 4. \end{array}$$

Each of these groups in (1) occurs 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 (1) there are infinitely many absolutely nonisomorphic elliptic curves with such a torsion group structure over $\mathbb{Q}$. This is mainly due to the fact that the modular curves $X_1(N)$ parametrizing elliptic curves with such a torsion structure are rational and hence have infinitely many $\mathbb{Q}$-rational points. Kubert [7, Table 3] found an explicit parametrization for an infinite family of elliptic curves E with such a torsion group structure over $\mathbb{Q}$ for each of the 15 types in(1).

Recently, the first two authors and Schweizer [3] determined torsion group structures of elliptic curves over cubic number fields by determining the modular curves $X_1(N)$ having infinitely many points defined over cubic number fields. In detail,

Received by the editor May 22, 2009 and, in revised form, October 3, 2009.

2010 *Mathematics Subject Classification.* Primary 11G05; Secondary 11G18.

Key words and phrases. Elliptic curve, torsion, cubic number field, modular curve.

The first named author was supported by the National Research Foundation of Korea (NRF) grant funded by the Korean government (MEST) (No. 20090060674).

The second named author was supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (No. 20090063182).

The third named author was supported by Priority Research Centers Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (No. 20090093827).

they proved that if K varies over all cubic number fields and E varies over all elliptic curves over K, the group structures which appear infinitely often as torsion groups $E(K)_{\text{tors}}$ are exactly the following 25 types:

$$\begin{array}{ll} \mathbb{Z}/N\mathbb{Z}, & N=1,\dots,16,18,20, \\ \mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2N'\mathbb{Z}, & N'=1,\dots,7. \end{array} \tag{2}$$

In fact, there are infinitely many cubic number fields K and elliptic curves E with $E(K)_{\text{tors}}=\mathbb{Z}/N\mathbb{Z}$ if and only if $X_1(N)$ is a triple cover of the projective line $\mathbb{P}^1$, and similarly with the modular curve $X_1(2N,2)$ for the torsion $\mathbb{Z}/2\mathbb{Z}\oplus 2N\mathbb{Z}$.

The main goal of this paper is constructing explicit examples of the theoretical result in [3]. As a matter of fact, there is no computational machinery developed for calculating torsion groups of elliptic curves over cubic number fields. Also even though 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 [11, 12], Zimmer et al. [10, 16], and Jeon et al. [2, 3], there has been little known for the examples of elliptic curves with a certain torsion group over number fields of higher order. For achieving our main goal, it suffices to find examples corresponding to the following ten types:

$$\begin{array}{ll} \mathbb{Z}/N\mathbb{Z}, & N=11,13,\dots,16,18,20, \\ \mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2N'\mathbb{Z}, & N'=5,6,7. \end{array} \tag{3}$$

In this paper, for each of the ten groups in (3), we construct an infinite family of elliptic curves E with such a torsion group structure over cubic number fields. This paper also presents an efficient way of constructing such families of elliptic curves with a prescribed torsion group structure over cubic number fields.

We briefly mention the methods used. Regarding all the cyclic torsion group cases, we construct such a family by using the defining equations of the modular curves $X_1(N)$ for $N=11,13,\dots,16,18,20$, which are obtained from the Tate normal form of elliptic curves; this approach basically follows Reichert's method [13]. On the other hand, for the non-cyclic torsion cases $\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2N\mathbb{Z}$ with $N=5,6$, we use the Kubert families [7, Table 3] and some standard methods, e.g. Theorem 2.2. Finally, the last noncyclic case corresponding to $\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/14\mathbb{Z}$ is a very hard task to deal with since no standard techniques can possibly be applied to this case. A completely new approach was therefore needed to solve this case. So far, there has not been even a single example found for an elliptic curve E with $E(K)_{\text{tors}}=\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/14\mathbb{Z}$. In this work, by resolving the moduli problem for $X_1(14,2)$, we construct an infinite family of elliptic curves that have $\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/14\mathbb{Z}$ as their torsion groups over cubic number fields.

This paper is organized as follows. We begin with the necessary basic notions in Section 2. Section 3 presents infinite families of elliptic curves with torsion groups in (3) except the case $\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/14\mathbb{Z}$, and in Section 4 we show our result for the final case $\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/14\mathbb{Z}$ with great detail.

2. Preliminaries

We recall some classical results on elliptic curves in this section, and we can refer to [1, 6, 7, 14] for details.

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

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

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:

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

By using the Tate normal form, Reichert [13] calculated defining equations of the modular curves $X_1(N)$ for $N = 11, 13, 14, 15, 16$, and 18 as follows:

Theorem 2.1. *For $N = 11, 13, 14, 15, 16$, and 18 the modular curves $X_1(N)$ are given by the following equations:*

(i) $X_1(11) : \ V^2 + V = U^3 - U^2$,

(ii) $X_1(13) : \ V^2 + (U^3 - U^2 - 1)V - U^2 + U = 0$,

(iii) $X_1(14) : \ V^2 = U^3 + U^2 - 8U + 16$,

(iv) $X_1(15) : \ V^2 + (U + 1)V = U^3 + U^2$,

(v) $X_1(16) : \ (2U^3 - 2U^2 - U + 1)V^2 + (2U^2 - 1)V - U^2 + U = 0$,

(vi) $X_1(18) : \ (U^2 - 2U + 1)V^2 + (-U^3 + U - 1)V + U^3 - U^2 = 0$.

In fact, the final formula for $X_1(14)$ given in [13] is $V^2+(U+1)V = U^3-U$, which is birationally equivalent to the above formula. We point out that regarding the formula for $X_1(16)$ the original formula given by Reichert [13] is not quite correct, so we calculated the formula for $X_1(16)$ as given above.

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} denote the x-coordinate of the n-multiple nP of P. Equation (4) implies that

$$rs(s-1) = -mt. \tag{5}$$

Without loss of generality, the cases $s = 1$ and $s = 0$ may be excluded. Reversing the substitutions made for calculating $6P$, i.e., $m = \frac{s(1-r)}{1-s}$, $t = \frac{r-s}{1-s}$, Equation (5) becomes

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

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

$$V^2 + V = U^3 - U^2.$$

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 2.2. *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 cubic number fields

In this section, we construct infinite families of elliptic curves with prescribed torsion groups given in (3) except the case $\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/14\mathbb{Z}$ over cubic number fields. For obtaining such families except the case $\mathbb{Z}/20\mathbb{Z}$, we basically use Theorem 2.1. For the case $\mathbb{Z}/20\mathbb{Z}$, we first find a defining equation for $X_1(20)$ by applying Reichert's method [13] as follows:

Proposition 3.1. *A defining equation of the modular curve $X_1(20)$ is given by the following equation:*

$$X_1(20): \; V^2U^3 + V^3U^2 - (V^3 - 4V^2 + 4V - 1)U - V^4 + 3V^3 - 3V^2 + V = 0.$$

Proof. In order to calculate the equation of $X_1(20)$, we set

$$9P = -11P.$$

For this we find the x-coordinates of nP with $n = 9, 11$. Let N_x and D_x denote the numerator and denominator of the x-coordinate, respectively.

$$\begin{aligned} x_{9P}: \; & N_x = 2mt^4 + (9m-5)mt^3 + (12m^2 - 16m + 4)mt^2 \\ & +(-13m^2 + 6m^3 + 8m - 1)mt + (-3m^3 + m^4 + 3m^2 - m)m, \\ & D_x = (m - t^2 - 1 + 2t)^2. \end{aligned}$$

$$\begin{aligned} x_{11P}: \ & N_x = -3mt^6 - (16m-9)mt^5 - (29m^2 - 39m + 10)mt^4 \\ & -(23m^3 - 57m^2 + 35m - 5)mt^3 - (8m^4 - 36m^3 + 41m^2 - 14m + 1)mt^2 \\ & -(m^5 - 10m^4 + 19m^3 - 12m^2 + 2m)mt - (-m^5 + 3m^4 - 3m^3 + m^2)m, \\ & D_x = (t^3 - t^2 + 2mt + m^2 - m)^2. \end{aligned}$$

From the equality $x_{9P} = x_{-11P} = x_{11P}$, we obtain

$$\begin{aligned} & m(m-1+t)(m^2 - m + 3mt - t + t^2)(t + m + m^5 + 35t^5 - 20t^6 + 7m^4t + 20m^3t^2 \\ & +33m^2t^3 - 5m^2t^4 - 20mt^5 + 44mt^4 + 5t^6m + t^5m^2 - 54mt^3 - 47m^2t^2 - 35t^4 \\ & +21t^3 - 4m^2 - 7t^2 + 6m^3 - 4m^4 + 34mt^2 + 24m^2t - 22m^3t - 10mt + 5t^7) = 0. \end{aligned}$$

Without loss of generality, we can exclude the case that the first three factors are equal to zero. Then the raw form of $X_1(20)$ is given by

$$\begin{aligned} & 5t^7 + (5m - 20)t^6 + (m^2 + 35 - 20m)t^5 + (-5m^2 + 44m - 35)t^4 \\ & +(21 - 54m + 33m^2)t^3 + (-7 - 47m^2 + 20m^3 + 34m)t^2 \\ & +(24m^2 + 1 + 7m^4 - 10m - 22m^3)t + m + 6m^3 - 4m^2 - 4m^4 + m^5 = 0. \end{aligned}$$

Transforming this equation birationally by means of the transformation

$$m = \frac{V^3 + UV^2 - V + 1}{U+1}, \qquad t = -\frac{(V-1)(V+U)}{U+1},$$

we obtain the following defining equation of $X_1(20)$:

$$X_1(20) : V^2U^3 + V^3U^2 - (V^3 - 4V^2 + 4V - 1)U - V^4 + 3V^3 - 3V^2 + V = 0.$$

□

3.1. The case $E(K)_{\mathbf{tors}} = \mathbb{Z}/N\mathbb{Z}$ with $N = 11, 13, \ldots, 16, 18, 20$.

Theorem 3.2. *For each $N = 11, 13, \ldots, 16, 18, 20$, choose $t \in \mathbb{Q}$ such that the corresponding polynomial $f_N(x)$ in Table 1 is irreducible over $\mathbb{Q}$. Let α_t be a zero of $f_N(x)$. Let E be an elliptic curve defined by the equation*

$$y^2 + (1 - c_N)xy - b_Ny = x^3 - b_Nx^2.$$

Then the torsion subgroup of E over a cubic number field $\mathbb{Q}(\alpha_t)$ is equal to $\mathbb{Z}/N\mathbb{Z}$ for almost all t.

Remark. In the above theorem, there are indeed infinitely many values $t \in \mathbb{Q}$ such that the polynomial $f_N(x)$ is irreducible over $\mathbb{Q}$ by Hilbert's irreducibility theorem.

Proof. We first prove this theorem for the case $N = 11$. From the formula in (i) of Theorem 2.1, we note that the points $(U, V) = (\alpha_t, t)$ satisfy

$$V^2 + V = U^3 - U^2,$$

which is a defining equation of $X_1(11)$. Also the coefficients b and c of $E(b, c)$ can be expressed by the following:

$$b = \frac{V(V+1)(U+V)}{U}, \qquad c = \frac{V(U+V)}{U}.$$

Substituting $U = \alpha_t$ and $V = t$, we obtain the curve E over $\mathbb{Q}(\alpha_t)$ that contains a point of order 11. But, in fact, this curve E over $\mathbb{Q}(\alpha_t)$ has no other torsion points for almost all t since Jeon et al. [3] determined all the possible torsion structures that occur infinitely often over cubic fields.

Table 1. Polynomials $f_N(x)$ and Coefficients b_N, c_N

N	Polynomials $f_N(x)$ and Coefficients b_N, c_N
11	$f_{11}(x) = x^3 - x^2 - t^2 - t$ $\begin{cases} b_{11} = \frac{t(t+1)(\alpha_t+t)}{\alpha_t} \\ c_{11} = \frac{t(\alpha_t+t)}{\alpha_t} \end{cases}$
13	$f_{13}(x) = tx^3 - (t+1)x^2 + x + t^2 - t$ $\begin{cases} b_{13} = \frac{\alpha_t^2(\alpha_t-1)(\alpha_t^3-\alpha_t+t)(\alpha_t^3-\alpha_t^2+t)}{t^2(\alpha_t^2-\alpha_t+t)} \\ c_{13} = \frac{\alpha_t^2(\alpha_t-1)(\alpha_t^3-\alpha_t+t)}{t(\alpha_t^2-\alpha_t+t)} \end{cases}$
14	$f_{14}(x) = x^3 + x^2 - 8x - t^2 + 16$ $\begin{cases} b_{14} = -\frac{8(3\alpha_t-t-4)(\alpha_t^2-2\alpha_t-2t+8)(\alpha_t^2+2\alpha_t-2t-8)}{(\alpha_t-4)^3(\alpha_t^2-2\alpha_t-2t-8)^2} \\ c_{14} = -\frac{8(3\alpha_t-t-4)(\alpha_t^2+2\alpha_t-2t-8)}{\alpha_t(\alpha_t-4)^2(\alpha_t^2-2\alpha_t-2t-8)} \end{cases}$
15	$f_{15}(x) = x^3 + x^2 - tx - t^2 - t$ $\begin{cases} b_{15} = -\frac{\alpha_t(\alpha_t^3+t\alpha_t^2-t\alpha_t-t^2)(\alpha_t^3+t\alpha_t^2-t^2)}{(\alpha_t^2+\alpha_t-t)(\alpha_t^3+\alpha_t^2+t\alpha_t^2+t\alpha_t-t^2)^2} \\ c_{15} = -\frac{\alpha_t(\alpha_t^3+t\alpha_t^2-t\alpha_t-t^2)}{(\alpha_t^2+\alpha_t-t)(\alpha_t^3+\alpha_t^2+t\alpha_t^2+t\alpha_t-t^2)} \end{cases}$
16	$f_{16}(x) = 2t^2x^3 + (-2t^2 + 2t - 1)x^2 + (-t^2 + 1)x + t^2 - t$ $\begin{cases} b_{16} = \frac{t(t-1)\alpha_t(\alpha_t-t)(t^2\alpha_t+\alpha_t-t)}{(t\alpha_t+\alpha_t-t)^3} \\ c_{16} = \frac{t(t-1)\alpha_t(\alpha_t-t)}{(t\alpha_t+\alpha_t-t)^2} \end{cases}$
18	$f_{18}(x) = (-t + 1)x^3 + (t^2 - 1)x^2 + (-2t^2 + t)x + t^2 - t$ $\begin{cases} b_{18} = -\frac{t(\alpha_t-t)(\alpha_t^2+t)(\alpha_t^2-t\alpha_t+t)}{(\alpha_t^2-t^2+t)(\alpha_t^2+t\alpha_t-t^2+t)^2} \\ c_{18} = -\frac{t(\alpha_t-t)(\alpha_t^2-t\alpha_t+t)}{(\alpha_t^2-t^2+t)(\alpha_t^2+t\alpha_t-t^2+t)} \end{cases}$
20	$f_{20}(x) = t^2x^3 + t^3x^2 - (t^3 - 4t^2 + 4t - 1)x - t^4 + 3t^3 - 3t^2 + t$ $\begin{cases} b_{20} = \frac{t((t^2-t+1)\alpha_t+t^3-t^2+1)((t-1)\alpha_t+t^2-t)(t^2\alpha_t+t^3-t+1)}{(t\alpha_t+t^2-t+1)(\alpha_t+1)^2} \\ c_{20} = \frac{((t-1)\alpha_t+t^2-t)(t^2\alpha_t+t^3-t+1)}{(t\alpha_t+t^2-t+1)(\alpha_t+1)} \end{cases}$

The other cases can be proved by using the formulas of Theorem 2.1 and Proposition 3.1 and applying the same method as the case $N = 11$. □

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

Theorem 3.3. *Choose $t \in \mathbb{Q}$ such that the polynomial $f(x) = 8x^3 - 8x^2 + 1 - t^2$ is irreducible over $\mathbb{Q}$. Let α_t be a zero of $f(x)$. Let E be an elliptic curve defined by the equation*

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

where

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

Then the torsion subgroup of E over a cubic number field $\mathbb{Q}(\alpha_t)$ is equal to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$ for almost all t.

Proof. We first note that the elliptic curve E defined as above satisfies the parametrization given in [7, Table 3] for having $\mathbb{Z}/10\mathbb{Z}$ as its torsion subgroups. We thus have that $P = (0, 0)$ is a torsion point on E of order 10. By the coordinate change $x \to x$ and $y \to y + \frac{c-1}{2}x + \frac{b}{2}$, the curve E becomes

$$y^2 = x^3 + \frac{(c-1)^2 - 4b}{4}x^2 + \frac{b(c-1)}{2}x + \frac{b^2}{4}. \tag{6}$$

Since $5P$ is a $\mathbb{Q}(\alpha_t)$-rational point of order 2, the right hand side of (6) should have a linear factor and a quadratic factor over $\mathbb{Q}(\alpha_t)$. By a simple calculation, one can show that the quadratic factor splits over $\mathbb{Q}(\sqrt{8\alpha_t^3 - 8\alpha_t^2 + 1})$, and this implies that E has two more 2-torsion points over $\mathbb{Q}(\sqrt{8\alpha_t{}^3 - 8\alpha_t{}^2 + 1})$. In fact, $\mathbb{Q}(\sqrt{8\alpha_t{}^3 - 8\alpha_t{}^2 + 1})$ is equal to $\mathbb{Q}$ since α_t satisfies $8\alpha_t^3 - 8\alpha_t^2 + 1 = t^2$. Therefore, E has the torsion subgroup $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$ over $\mathbb{Q}(\alpha_t)$. □

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

Theorem 3.4. *Choose $t \in \mathbb{Q}$ such that the polynomial $f(x) = x^3 - 4x^2 + 6x - 3 - t^2$ is irreducible over $\mathbb{Q}$. Let α_t be a zero of $f(x)$. Let E be an elliptic curve defined by the equation*

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

where $c = -\frac{(\alpha_t - 1)(\alpha_t - 2)^2}{\alpha_t^2(\alpha_t^2 - 3\alpha_t + 3)}$. Then the torsion subgroup of E over a cubic number field $\mathbb{Q}(\alpha_t)$ is equal to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$ for almost all t.

Proof. From [7, Table 3] we see that the Tate normal form

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

defines an elliptic curve having a $\mathbb{Q}$-rational point $(0, 0)$ of order 6. The coordinate changes given by $x \to x$ and $y \to y + \frac{(c-1)}{2}x + \frac{(c^2+c)}{2}$ yield the following form:

$$y^2 = x^3 - \frac{3c^2 + 3c - 1}{4}x^2 + \frac{c^3 - c}{2}x + \frac{c^4 + 2c^3 + c^2}{4}. \tag{7}$$

By substituting $c = \frac{10-2k}{k^2-9}$ into (7), the cubic polynomial of the right hand side of (7) splits as follows:

$$y^2 = \left(x + \frac{2(k-1)^2}{(k+3)^2(k-3)}\right)\left(x + \frac{2(k-5)}{(k-3)(k+3)}\right)\left(x + \frac{(k-5)(k-1)^2}{4(k+3)(k-3)^2}\right). \tag{8}$$

Note that the elliptic curve defined by (8) has the point $P = (0, -\frac{c^2+c}{2})$ of order 6. By Theorem 2.2, for a number field K, there exists a K-rational point Q with $2Q = P$ if and only if both $\frac{2}{k-3}$ and $\frac{k-5}{k+3}$ are squares in K. Set $k = 2l^2 + 3$; then $\frac{2}{k-3} = \frac{1}{l^2}$ and $\frac{k-5}{k+3} = \frac{l^2-1}{l^2+3}$ are squares in $\mathbb{Q}\left(\sqrt{\frac{l^2-1}{l^2+3}}\right)$ and $c = \frac{1-l^2}{l^4+3l^2}$. Thus the elliptic curve defined by $y^2 + (1-c)xy - (c + c^2)y = x^3 - (c + c^2)x^2$ with $c = \frac{1-l^2}{l^4+3l^2}$ contains $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$ as its torsion group over the field $\mathbb{Q}\left(\sqrt{\frac{l^2-1}{l^2+3}}\right)$. Now we need to find an l such that l generates a cubic number field $\mathbb{Q}(l)$ and $\frac{l^2-1}{l^2+3}$ is a square in

$\mathbb{Q}(l)$; the latter condition is equivalent to $(l^2-1)(l^2+3)$ being a square in $\mathbb{Q}(l)$. Consider the following equation:

$$Y^2 = (X^2-1)(X^2+3) = X^4 + 2X^2 - 3. \tag{9}$$

Substituting $X = \frac{x}{x-2}$ and $Y = \frac{4y}{(x-2)^2}$, (9) becomes

$$y^2 = x^3 - 4x^2 + 6x - 3. \tag{10}$$

Since α_t is a zero of $f(x)$, the point $(x,y) = (\alpha_t, t)$ satisfy (10). Then the point $(X,Y) = (\frac{\alpha_t}{\alpha_t-2}, \frac{4t}{(\alpha_t-2)^2})$ satisfies (9). Thus we can take l to be $\frac{\alpha_t}{\alpha_t-2}$, and then $c = -\frac{(\alpha_t-1)(\alpha_t-2)^2}{\alpha_t^2(\alpha_t^2-3\alpha_t+3)}$. The result follows as desired. □

4. Moduli problem and the case $E(K)_{\mathrm{tors}} = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$

Let $X_1(2N,2)$ be the modular curve belonging to the congruence subgroup $\Gamma_1(2N) \cap \Gamma(2)$. When K is a number field, the K-rational points on the curve $X_1(2N,2)$ parametrize elliptic curves E over K such that $E(K)_{\mathrm{tors}}$ contains a subgroup $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N\mathbb{Z}$. There are *forgetful* maps from $X_1(2N,2)$ to $X_1(2N)$ which send (E,P,R) to (E,P) where P (resp. R) is a K-rational $2N$ (resp. 2) torsion point.

In order to find the elliptic curves with noncyclic torsion groups $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N\mathbb{Z}$ as their torsion subgroups over K, we use forgetful maps from $X_1(2N,2)$ to $X_1(2N)$. For example, in the case $N=3$, consider the forgetful map $X_1(6,2) \to X_1(6)$. It follows from the Tate normal form that there is a canonical bijection $\mathbb{P}^1 \to X_1(6)$ which sends $t \mapsto (E_t, P_t)$, where

$$E_t : y^2 + (1+t)xy + (t-t^2)y = x^3 + (t-t^2)x^2, \quad P_t = (0,0).$$

Viewed as a modular function, $t(z)$ has the following q-expansion [5]:

$$\frac{1}{9}(1 - 8q + 24q^2 - 24q^3 - 40q^4 + 144q^5 + \cdots).$$

Meanwhile, the curve $X_1(6,2)$ has genus 0, and thus its function field over $\mathbb{Q}$ is equal to $\mathbb{Q}(f)$, where $f(z)$ is the Hauptmodul for $\Gamma_1(6,2)$ with the q-expansion

$$f(z) = q^{-\frac{1}{2}} + 2q^{\frac{1}{2}} + q^{\frac{3}{2}} - 2q^{\frac{7}{2}} - 2q^{\frac{9}{2}} + \cdots.$$

Comparing q-expansions of $t(z)$ and $f(z)$, we obtain $t = \frac{f^2-9}{9(f^2-1)}$. Thus we see that

$$E_f : y^2 + (1+t)xy + (t-t^2)y = x^3 + (t-t^2)x^2, \quad \text{where } t = \frac{f^2-9}{9(f^2-1)}$$

gives a family of elliptic curves which have torsion subgroups $E_f(\mathbb{Q})_{\mathrm{tors}} = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$.

Now, in order to settle our problem, we need to construct the forgetful map from $X_1(14,2)$ to $X_1(14)$ by following the above method. But the situation is quite different from the previous case. Note that $X_1(14,2)$ (resp. $X_1(14)$) has genus 4 (resp. genus 1). Since the modular curve $X_1(14,2)$ has genus greater than 0, the function field generators for the curve are not uniquely determined. Since $X_1(14)$ is an elliptic curve over $\mathbb{Q}$, it is parametrized by modular functions. The modularity of $X_1(14,2)$ is heavily affected by the choice of function field generators and the modular parametrizations.

In the following we construct the forgetful map from $X_1(14,2)$ to $X_1(14)$ which reflects the correct modularity. For this purpose, we need to consider the modular curves $X_\Delta(N)$. Let Δ be a subgroup of $(\mathbb{Z}/N\mathbb{Z})^*$ that contains -1. We write $X_\Delta(N)$ for the modular curve belonging to the group

$$\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \ : \ N|c \text{ and } a \in \Delta \right\}.$$

Note that for $\Delta = \{\pm 1\}$ this is just $X_1(N)$. Let $\Delta = \{\pm 1, \pm(2N+1)\}$. Then we observe that $X_\Delta(4N)$ is the modular curve corresponding to the subgroup $\Gamma_0(4N) \cap \Gamma_1(2N)$. Conjugating the group $\Gamma_1(2N, 2)$ with the matrix $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 2 \end{smallmatrix}\right)$, we obtain a birational map, defined over $\mathbb{Q}$, from $X_1(2N, 2)$ to $X_\Delta(4N)$. In the moduli interpretation this corresponds to dividing an elliptic curve with a distinguished subgroup $\mathbb{Z}/2N\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ by the 2-torsion point that generates $\mathbb{Z}/2\mathbb{Z}$ and obtaining an elliptic curve with a cyclic $4N$-isogeny and a distinguished underlying $2N$-torsion point.

The first two authors and Schweizer [3] calculate a defining equation of $X_\Delta(28)$ by using the modular forms of weight 2 corresponding to $\Gamma_\Delta(28)$ as follows:

$$(x^2-1)(y^3-9y) + (x^3+2x^2-9x-2)(y^2-1) = 0. \tag{11}$$

Note that the defining equation of the modular curve $X_1(14)$ is as follows:

$$X_1(14): \ v^2 + uv + v = u^3 - u. \tag{12}$$

Now we construct the forgetful map from $X_1(14, 2)$ to $X_1(14)$ by finding the corresponding map between the curves defined by the equations in (11) and (12). For this purpose, we need to know the q-expansions of modular functions on $X_\Delta(28)$ and $X_1(14)$.

Yang [15] developed a method to find the equations of modular curves by using the generalized Dedekind η-functions. More precisely, he devised an algorithm to generate modular functions from the generalized Dedekind η-functions and then obtained an equation of modular curves by finding two modular functions satisfying some conditions of the orders of the pole at infinity. The generalized Dedekind η-functions are defined by

$$E_g(\tau) = q^{\frac{NB(\frac{g}{N})}{2}} \prod_{m=1}^{\infty} \left(1 - q^{(m-1)N+g}\right)\left(1 - q^{mN-g}\right) \tag{13}$$

where N is a fixed positive integer, g is not congruent to 0 modulo N, $q = e^{2\pi i \tau}$, and $B(x) = x^2 - x + \frac{1}{6}$.

In particular, the equation of $X_1(14)$ in (12) can be computed by the following two modular functions:

$$\begin{aligned} u &= \frac{E_5 E_6}{E_1 E_2}, \\ v &= -\frac{E_5 E_6}{E_1 E_2} - \frac{E_6^2 E_7}{E_1 E_2^2} - 1. \end{aligned} \tag{14}$$

Using the infinite product in (13), we can obtain q-expansions of u and v as follows:

$$\begin{aligned} u &= \frac{1}{q^2} + \frac{1}{q} + 2 + 2q + 3q^2 + 2q^3 + 2q^4 + q^5 - 2q^7 - 3q^8 - 4q^9 - 4q^{10} + \cdots, \\ v &= -\frac{1}{q^3} - \frac{2}{q^2} - \frac{4}{q} - 6 - 8q - 9q^2 - 10q^3 - 8q^4 - 6q^5 - q^6 + 5q^7 + 12q^8 + \cdots. \end{aligned}$$

Also we can get the q-expansions of modular functions x and y which give the equation in (11) as follows:

$$\begin{array}{rcl} x & = & 1-2q+2q^4-2q^6+4q^9-2q^{10}-2q^{11}+4q^{14}-4q^{15}-2q^{17}+4q^{18}+\cdots, \\ y & = & -\dfrac{2}{q}-1+2q^2-2q^4-2q^5+2q^{10}+2q^{11}-2q^{12}-4q^{13}-2q^{14}+4q^{15}+\cdots. \end{array}$$

Now we are ready to construct the forgetful map. An algorithm for finding such a map is as follows:

Algorithm.

(1) *Put*

$$u=\frac{f_1(x,y)}{f_2(x,y)},\quad v=\frac{g_1(x,y)}{g_2(x,y)}$$

where $f_i(x,y), g_i(x,y) \in \mathbb{Z}[x,y]$ *with* $i=1,2$.

(2) *Input the* q*-expansions of* $u, v, x,$ *and* y *in the following two equations:*

$$f_1(x,y)=uf_2(x,y), \qquad g_1(x,y)=vg_2(x,y).$$

(3) *Compare the coefficients, and set two systems of linear equations.*

(4) *Find* $f_i(x,y)$ *and* $g_i(x,y)$ *with* $i=1,2$ *by solving the above systems of linear equations.*

Following this algorithm, we obtain the following result.

Proposition 4.1. *The forgetful map from* $X_\Delta(28)$ *to* $X_1(14)$ *is given as follows:*

$$\begin{aligned} u &= \frac{-2+2y}{3+x+y-xy}, \\ v &= \frac{-y-3y^2-x-4xy+xy^2-x^2+x^2y}{1+4y+y^2+3x+2xy-xy^2-2x^2y}.\%endarray \end{aligned} \tag{15}$$

Proof. First of all, we need to introduce a defining equation of $X_1(14,2)$ which shows its modularity explicitly. Each point (u,v) on $X_1(14)$ corresponds to the elliptic curve $E(b,c)$ with a torsion point $P=(0,0)$ of order 14, where

$$\begin{array}{rcl} b & = & \dfrac{(v-u^2+u)(-v-1+u^2)(-v+u-1)}{(-v-u-1+u^2)^2(u-1)^3}, \\ c & = & \dfrac{(v-1-u^2)(-v+u-1)}{(-v-u-1+u^2)u(u-1)^2}. \end{array} \tag{16}$$

By replacing y by $y+\frac{(c-1)}{2}x+\frac{b}{2}$ in the equation of $E(b,c)$, we have the following form:

$$E: \ y^2=x^3+\frac{1}{4}(c^2-2c+1-b)x^2+\frac{1}{2}b(c-1)x+\frac{b^2}{4}. \tag{17}$$

Note that $7P$ is of order 2 and the x-coordinate of $7P$ is as follows:

$$x_{7P}=-\frac{(-v+u-1)u(u^2-u-v)}{(-v-u-1+u^2)(u-1)^4}.$$

The cubic polynomial in the right hand side of (17) is divisible by $x-x_{7P}$, and we have a quadratic factor $q(x)$. Then the torsion subgroup of the elliptic curve E defined over the field $K=\mathbb{Q}(u,v)$ contains the group $\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/14\mathbb{Z}$ if and only if the quadratic factor $q(x)$ splits over K, and it holds if and only if the discriminant $\Delta(u,v)$ of $q(x)$ is a square in K. Since the denominator of $\Delta(u,v)$ is a square, it is equivalent to the numerator of $\Delta(u,v)$, say $d(u,v)$, being a square in K. Note that $d(u,v)$ is given by

$$d(u,v) = v^8+(8+8u+12u^2-20u^3)v^7+(28-56u+96u^2-132u^3-6u^4+8u^5+6u^6)v^6+(56-168u+324u^2-372u^3-136u^4+324u^5-300u^6+252u^7-88u^8+12u^9)v^5+(70-280u+600u^2-580u^3-584u^4+1404u^5-1182u^6+288u^7+u^1 2+767u^8-832u^9+336u^{10}-56u^{11})v^4+(56-280u+660u^2-540u^3-1096u^4+2560u^5-1668u^6-1188u^7+3288u^8-1908u^9-652u^{10}-584u^{12}+108u^{13}-4u^{14}+1248u^{11})v^3+(28-168u+432u^2-300u^3-1054u^4+2376u^5-1006u^6-2748u^7+4368u^8-740u^9-3350u^{10}+2684u^{11}+44u^{12}-996u^{13}+532u^{14}-108u^{15}+6u^{16})v^2+(8-56u+156u^2-92u^3-512u^4+1116u^5-200u^6-2056u^7+2432u^8+780u^9-3348u^{10}+1464u^{11}+1508u^{12}-1624u^{13}+212u^{14}+412u^{15}-252u^{16}+56u^{17}-4u^{18})v+(1-8u-12u^3+24u^2-100u^4+212u^5+14u^6-532u^7+498u^8+456u^9-1006u^{10}+128u^{11}+837u^{12}-524u^{13}-242u^{14}+364u^{15}-77u^{16}-72u^{17}+50u^{18}-12u^{19}+u^{20}).$$

Therefore a defining equation of the modular curve $X_1(14,2)$ is given by

$$\begin{cases} w^2 = d(u,v), \\ v^2+uv+v = u^3-u. \end{cases} \tag{18}$$

It is enough to show that each point (x,y) on $X_\Delta(28)$ is sent via the map in (15) to a point (u,v) on $X_1(14)$ such that $d(u,v)$ is a square.

By using the q-expansions of u and v, we have the followig q-expansion of $d(u,v)$:

$$d(u,v) = \frac{1}{q^{40}} + \frac{24}{q^{39}} + \frac{304}{q^{38}} + \frac{2696}{q^{37}} + \frac{18764}{q^{36}} + \frac{109000}{q^{35}} + \frac{549060}{q^{34}} + \frac{2461000}{q^{33}} + \cdots .$$

Consider the function $w(u,v)$ which satisfies

$$w(u,v)^2 = d(u,v).$$

Using the computer algebra system MAPLE, we can obtain the q-expansion of $w(u,v)$ as follows:

$$w(u,v) = \frac{1}{q^{20}} + \frac{12}{q^{19}} + \frac{80}{q^{18}} + \frac{388}{q^{17}} + \frac{1526}{q^{16}} + \frac{5148}{q^{15}} + \frac{15402}{q^{14}} + \frac{41748}{q^{13}} + \frac{104015}{q^{12}} + \cdots .$$

By using the algorithm to find our forgetful map, we can express $w(u,v)$ as a function of x and y, say $w(x,y)$. Then $w(x,y)$ is given by the following:

$$w(x,y) = (383853934x-54063026260x^3+1379413578y-123255399692x^4-167914xy^9-31428348264x^2y+19230671876x^2y^2+694312x^2y^7+492414x^2y^8+159008209164x^6y^2+16065416x^4y^6-106840989252x^5y+158946584916x^5y^2-22472013304x^7y^3-24523541364x^8y^2-84492576104x^3y+62620354220x^3y^2+2949480x^3y^6-1947000x^3y^7+759365284x^5y^4-165655676x^5y^5+140747568536x^6y-4784831510xy+932698396xy^2-179242xy^8-10900521880x^6y^3+1867038484x^6y^4+133076830500x^4y^2-53533212x^4y^5+218660344216x^7y-65277977844x^7y^2-99647268612x^4y-12427018434x^2-177287357856x^6-604790904y^2+65277977844x^7-169528920088x^5+24523541364x^8-167914y^9+321578392)/(28-130978226x+14284x^1 0+333488x^9y-596841706x^2y+1066214497x^2y^2-148235x^2y^7+33555x^2y^8-719758869x^2-2265027x^8y+16714462667x^6y^2+5196294278x^7+2446411x^4y^6-12468749230x^5y+8576723560x^5y^2-220632x^9-1877501054x^3-2069563299x^7y^3-2277572804x^8y^2-5239206172x^3y+2181375376x^3y^2-1831371x^3y^6+14015x^3y^7-19137109x^5y^4-14969541x^5y^5+5310496290x^6y-609156369xy+14356616xy^2-33555xy^8-18535760799x^6-207071073x^6y^3+191054373x^6y^4-7419757485x^4+8645284145x^4y^2-575703x^4y^5+20304995860x^7y-5205074905x^7y^2+2278124061x^8-4555739890x^4y-8833344818x^5)\ .$$

We can also express $d(u,v)$ as a function of x and y by using the map in (15), say $d(x,y)$. Then one can check that $d(x,y)$ and $w(x,y)^2$ define the same function on $X_\Delta(28)$. Therefore we can finally conclude that the map in (15) is the forgetful map. □

In the following theorem, we obtain an infinite family of elliptic curves over cubic number fields whose torsions are $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$.

Theorem 4.2. *Choose $t \in \mathbb{Q}$ such that the polynomial*

$$f(x) = (t^2-1)x^3 + (t^3+2t^2-9t-2)x^2 - 9(t^2-1)x - t^3 - 2t^2 + 9t + 2$$

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

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

where b is given by

$$b = (5+13\alpha_t-{\alpha_t}^3+16t-12{\alpha_t}^2t+5{\alpha_t}^2t^2+{\alpha_t}^3t^2-4\alpha_tt-13\alpha_tt^2-{\alpha_t}^2-9t^2-4t^3+4\alpha_tt^3)(-3-t-\alpha_t+\alpha_tt)^2(-5-12\alpha_t+4{\alpha_t}^3-25t+{\alpha_t}^4+26{\alpha_t}^2t+26{\alpha_t}^2t^2+8{\alpha_t}^3t-12{\alpha_t}^3t^2-24\alpha_tt+28\alpha_tt^2-{\alpha_t}^4t^2-{\alpha_t}^4t-4{\alpha_t}^2-25t^2+17t^3+6t^4+16\alpha_tt^3-8t^4\alpha_t-18t^3{\alpha_t}^2+2{\alpha_t}^2t^4+{\alpha_t}^4t^3)(-5t^4+7t^4\alpha_t-3{\alpha_t}^2t^4+{\alpha_t}^3t^4+6t^3{\alpha_t}^2-4\alpha_tt^3-4{\alpha_t}^3t^3-15t^3+{\alpha_t}^4t^3+3t^2+8{\alpha_t}^2t^2+10\alpha_tt^2-3{\alpha_t}^4t^2-2{\alpha_t}^3t^2+10{\alpha_t}^2t-36\alpha_tt+3{\alpha_t}^4t+12{\alpha_t}^3t-37t-10-7{\alpha_t}^3-{\alpha_t}^4-21{\alpha_t}^2-41\alpha_t)/[(1+8\alpha_t+4{\alpha_t}^3-5t+{\alpha_t}^4+6{\alpha_t}^2t+30{\alpha_t}^2t^2+4{\alpha_t}^3t-4{\alpha_t}^3t^2-20\alpha_tt-4\alpha_tt^2-{\alpha_t}^4t^2-{\alpha_t}^4t+2{\alpha_t}^2-37t^2+5t^3+4t^4+20\alpha_tt^3-4t^4\alpha_t-6t^3{\alpha_t}^2-4{\alpha_t}^3t^3+{\alpha_t}^4t^3)^2(-1-4t-t^2-3\alpha_t-2\alpha_tt+\alpha_tt^2+2{\alpha_t}^2t)(t-5-\alpha_t+\alpha_tt)^3],$$

and c is given by

$$c = (5+12\alpha_t-4{\alpha_t}^3+25t-{\alpha_t}^4-26{\alpha_t}^2t-26{\alpha_t}^2t^2-8{\alpha_t}^3t+12{\alpha_t}^3t^2+24\alpha_tt-28\alpha_tt^2+{\alpha_t}^4t^2+{\alpha_t}^4t+4{\alpha_t}^2+25t^2-17t^3-6t^4-16\alpha_tt^3+8t^4\alpha_t+18t^3{\alpha_t}^2-2{\alpha_t}^2t^4-{\alpha_t}^4t^3)(-3-t-\alpha_t+\alpha_tt)^2(5+13\alpha_t-{\alpha_t}^3+16t-12{\alpha_t}^2t+5{\alpha_t}^2t^2+{\alpha_t}^3t^2-4\alpha_tt-13\alpha_tt^2-{\alpha_t}^2-9t^2-4t^3+4\alpha_tt^3)/[(1+8\alpha_t+4{\alpha_t}^3-5t+{\alpha_t}^4+6{\alpha_t}^2t+30{\alpha_t}^2t^2+4{\alpha_t}^3t-4{\alpha_t}^3t^2-20\alpha_tt-4\alpha_tt^2-{\alpha_t}^4t^2-{\alpha_t}^4t+2{\alpha_t}^2-37t^2+5t^3+4t^4+20\alpha_tt^3-4t^4\alpha_t-6t^3{\alpha_t}^2-4{\alpha_t}^3t^3+{\alpha_t}^4t^3)(3t-3t^2-t^3-\alpha_tt-3\alpha_tt^2+\alpha_tt^3+2{\alpha_t}^2t^2+1+3\alpha_t-2{\alpha_t}^2t)(t-5-\alpha_t+\alpha_tt)^2].$$

Then the torsion subgroup of E over a cubic number field $\mathbb{Q}(\alpha_t)$ is equal to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$ for almost all t.

Proof. Substituting $y = t$ into the defining equation of $X_\Delta(28)$, we have a cubic polynomial $f(x)$ as above. For the irreducible cubic polynomial $f(x)$ with a rational number t and its root α_t, the point (α_t, t) on $X_\Delta(28)$ is defined over the cubic number field $\mathbb{Q}(\alpha_t)$.

If the point (α_t, t) is mapped via the forgetful map of Proposition 4.1 to a point Q on $X_1(14)$, then the elliptic curve $E(b,c)$ corresponding to this point Q has the torsion subgroup $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$ over a cubic number field $\mathbb{Q}(\alpha_t)$. □

Example 4.3. Let $t = 0$. Then $f(x) = -x^3 - 2x^2 + 9x + 2$. If we let $\alpha = \alpha_0$, then b and c are given by

$$b = -\frac{73}{128}\alpha^2 - \frac{149}{128}\alpha + \frac{357}{64}, \qquad c = \frac{13}{32}\alpha^2 + \frac{25}{32}\alpha - \frac{65}{16}.$$

Then the cubic equation in (17) splits over $\mathbb{Q}(\alpha)$ as follows:

$$\frac{(16x - 47 + 10\alpha + 5\alpha^2)(2048x - 1190 + 163\alpha + 207\alpha^2)(4x + 18 - 3\alpha - 2\alpha^2)}{131072}.$$

Therefore the torsion subgroup of $E(b,c)$ should be $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$ over $\mathbb{Q}(\alpha)$.

Acknowledgments

We would like to thank KIAS (Korea Institute for Advanced Study) for its hospitality, Y. Yang for providing the formula (14), and A. Schweizer, J. Silverman, and J. Ahn for their valuable comments during the writing of this paper. We appreciate the referees' helpful comments, which improved the clarity of this paper.

References

1. D. Husemoller, *Elliptic curves*, second edition, Springer-Verlag, New York, 2004. MR2024529 (2005a:11078)
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. MR2254548 (2007m:11079)
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. MR2069117 (2005f:11112)
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. MR1330929 (96c:11058)
5. C.H. Kim and J.K. Koo, Generators of function fields of the modular curves $X_1(5)$ and $X_1(6)$, Math. Comp. **79** (2010), 1047–1066.
6. A.W. Knapp, *Elliptic curves*, Mathematical Note, 40, Princeton University Press, Princeton, NJ, 1992. MR1193029 (93j:11032)
7. D.S. Kubert, Universal bounds on the torsion of elliptic curves, *Proc. London Math. Soc. (3)* **33** (1976), 193–237. MR0434947 (55:7910)
8. B. Mazur, Modular curves and the Eisenstein ideal, *Publ. Math. I.H.E.S.* **47** (1977), 33-168. MR488287 (80c:14015)
9. L. Merel, Bornes pour la torsion des courbes elliptiques sur les corps de nombres, *Invent. Math.* **124** (1996), no 1-3, 437-449. MR1369424 (96i:11057)
10. 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 MR1448331 (98e:11069)
11. P. Parent, No 17-torsion on elliptic curves over cubic number fields, *J. Theor. Nombres Bordeaux* **15** (2003), 831–838. MR2142238 (2006a:11071)
12. P. Parent, Torsion des courbes elliptiques sur les corps cubiques, *Ann. Inst. Fourier (Grenoble)* **50** (2000), no. 3, 723–749. MR1779891 (2001i:11067)
13. M.A. Reichert, Explicit determination of nontrivial torsion structures of elliptic curves over quadratic number fields, *Math. Comp.* **46** (1986), 637–658. MR829635 (87f:11039)
14. J. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, New York, 1986. MR817210 (87g:11070)
15. Y. Yang, Defining equations of modular curves, *Adv. in Math.* **204** (2006), 481–508. MR2249621 (2007e:11068)
16. H.G. Zimmer, Torsion groups of elliptic curves over cubic and certain biquadratic number fields, *Arithmetic geometry (Tempe, AZ, 1993),* 203–220, Contemp. Math., 174, *Amer. Math. Soc., Providence, RI,* 1994. MR1299744 (95i:11056)

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

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

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