JOURNAL OF THE
CHUNGCHEONG MATHEMATICAL SOCIETY
Volume **26**, No. 3, August 2013

DEFINING EQUATIONS OF CERTAIN MODULAR CURVES

Daeyeol Jeon*

Abstract. In this paper, we explain how to get defining equations of the modular curves $X_1(2,2N)$ which show the moduli problems and present defining equations of $X_1(2,2N)$ for $N = 2,3,\ldots,8$.

1. Introduction

For positive integers $M|N$, consider the congruence subgroup $\Gamma_1(M,N)$ of $\mathrm{SL}_2(\mathbb{Z})$ defined by

$$\Gamma_1(M,N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \bmod N,\ M \mid b \right\}.$$

Then the modular curve $X_1(M,N)$ corresponding to $\Gamma_1(M,N)$ is related to moduli problems of elliptic curves containing a subgroup which is isomorphic to $\mathbb{Z}/M\mathbb{Z} \bigoplus \mathbb{Z}/N\mathbb{Z}$. If $M = 1$, then $X_1(M,N)$ is the same as $X_1(N)$ which is the coarse moduli space of elliptic curves with N-torsion points.

It is not much known for the defining equations of $X_1(M,N)$, in particular, the equations which show the moduli problems of $X_1(M,N)$. But recently, the author with C. H. Kim and Y. Lee [2] found a defining equation of $X_1(2,14)$ which enables us to construct a family of elliptic curves over cubic number fields with the torsion subgroups $\mathbb{Z}/2\mathbb{Z} \bigoplus \mathbb{Z}/14\mathbb{Z}$.

In this paper, we explain how to get defining equations of $X_1(2,2N)$ which show the moduli problems and present defining equations of $X_1(2,2N)$ for some N by following the method in [2].

Received April 15, 2013; Revised June 13, 2013; Accepted July 22, 2013.

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

Key words and phrases: defining equations, modular curves, elliptic curves.

This work was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education, Science and Technology (2010-0023942).

2. Preliminaries

The Tate normal form of an elliptic curve with $P = (0, 0)$ is given as follows:

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

and this is nonsingular if and only if $b \neq 0$. In this case, P is not of order 2 or 3(cf. [1]). On the curve $E(b, c)$ we have the following by the chord-tangent method(cf. [3]):

(2.1)

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

The condition $NP = O$ in $E(b, c)$ gives a defining equation for $X_1(N)$. For example, $10P = O$ implies $4P = -6P$, so

$$x_{4P} = x_{-6P} = x_{6P},$$

where x_{nP} denote the x-coordinate of the n-multiple nP of P. Eq. (2.1) implies that

$$r(r-1) = -mt. \tag{2.2}$$

Without loss of generality, the cases $r = 1$ and $s = 1$ may be excluded. Reversing the substitutions made for calculating $6P$: $m = \frac{s(1-r)}{1-s}$, $t = \frac{r-s}{1-s}$, Eq. (2.2) becomes as follows:

$$r - 3rs + rs^2 + s^2 = 0,$$

which is one of the equations $X_1(10)$.

By using the above method and Sutherland's calculation [4] we have the following defining equations of the modular curves $X_1(2N)$ for $N = 2, 3, \ldots, 8$ as follows:

Theorem 2.1. *For $N = 2, 3, ..., 8$ the modular curves $X_1(2N)$ are given by the following equations:*

(1) $X_1(4) :\ v - u = 0,$
(2) $X_1(6) :\ v - u^2 - u = 0,$
(3) $X_1(8) :\ uv - 2u + 1 = 0,$

TABLE 1. The relations between b, c and u, v

$2N$	The relations between b, c and u, v
4	$\begin{cases} b = v \\ c = u \end{cases}$
6	$\begin{cases} b = v \\ c = u \end{cases}$
8	$\begin{cases} b = u(u-1)v \\ c = (u-1)v \end{cases}$
10	$\begin{cases} b = v(v-1)u \\ c = (v-1)u \end{cases}$
12	$\begin{cases} b = \frac{v(v+1)(v+u)}{u^2} \\ c = \frac{v(v+1)}{u} \end{cases}$
14	$\begin{cases} b = \frac{(u-1)(v+u)(v^2+uv+v+1)}{(v+1)^3(v+u+1)^2} \\ c = \frac{(u-1)(v+u)}{(v+1)^2(v+u+1)} \end{cases}$
16	$\begin{cases} b = -\frac{(v+1)(v-u)(v-u+1)(v^2-uv+v+u^2)}{(u+1)(v-u^2-u+1)^2} \\ c = -\frac{(v+1)(v-u)(v-u+1)}{(u+1)(v-u^2-u+1)} \end{cases}$

(4) $X_1(10): \ (u^2 - 3u + 1)v + u^2 = 0,$
(5) $X_1(12): \ v - u^2 + 3u - 2 = 0,$
(6) $X_1(14): \ v^2 + (u^2 + u)v - u = 0,$
(7) $X_1(16): \ v^2 + (u^3 + u^2 - u + 1)v + u^2 = 0.$

In the above theorem, for each point (u, v) satisfying the defining equation $f_{2N}(u, v) = 0$ of $X_1(2N)$, the corresponding elliptic curve $E(b, c)$ is defined over the number field $K = \mathbb{Q}(u, v)$ and has the torsion subgroup containing $\mathbb{Z}/2N\mathbb{Z}$. In Table 1, we list the relations between b, c and u, v.

3. Defining equations of $X_1(2, 2N)$

There are *forgetful* maps from $X_1(2, 2N)$ to $X_1(2N)$ which send (E, P, R) to (E, P) where P (resp. R) is a torsion point of order $2N$ (resp. 2) of E. In order to find the defining equations of $X_1(2, 2N)$, we use forgetful maps from $X_1(2, 2N)$ to $X_1(2N)$.

Let $f_{2N}(u, v) = 0$ be a defining equation of $X_1(2N)$. Each point (u, v) on $X_1(2N)$ corresponds to the elliptic curve $E(b, c)$ with a torsion point $P = (0, 0)$ of order $2N$ where b, c can be expressed by u, v. By replacing

TABLE 2. Defining equations of $X_1(2, 2N)$

$X_1(2,2N)$	Defining equations of $X_1(2,2N)$
$X_1(2,4)$	$\begin{cases} w^2 = (u-1)(u^3 - 19u^2 - 13u - 1) \\ v - u = 0 \end{cases}$
$X_1(2,6)$	$\begin{cases} w^2 = (u+1)(9u+1) \\ v - u^2 - u = 0 \end{cases}$
$X_1(2,8)$	$\begin{cases} w^2 = (8u^2 - 8u + 1) \\ uv - 2u + 1 = 0 \end{cases}$
$X_1(2,10)$	$\begin{cases} w^2 = (2u-1)(4u^2 - 2u - 1) \\ (u^2 - 3u + 1)v - u^2 = 0 \end{cases}$
$X_1(2,12)$	$\begin{cases} w^2 = (u^2 - 6u + 6)(u^2 - 2u + 2) \\ v - u^2 + 3u - 2 = 0 \end{cases}$
$X_1(2,14)$	$\begin{cases} w^2 = -(u-1)(u+1)(u^8v + 7u^7v + 16u^6v + 10u^5v \\ -18u^4v - 26u^3v + 12uv + u^7 + 6u^6 + 10u^5 + u^4 \\ -14u^3 - 7u^2 + 4u + 1) \\ v^2 + (u^2+u)v - u = 0 \end{cases}$
$X_1(2,16)$	$\begin{cases} w^2 = -(u^2 + 2u - 1)(u^2 - 2u - 1)(u^{13}v + 7u^{12}v + 18u^{11}v \\ +20u^{10}v + 5u^9v - 26u^7v - 15u^8v - 18u^6v - u^5v + 9u^4v \\ +8u^3v + 2u^2v - uv - v + u^{12} + 6u^{11} + 13u^{10} + 12u^9 + u^8 \\ -12u^7 - 16u^6 - 8u^5 + 2u^4 + 6u^3 + 3u^2 - 1) \\ v^2 + (u^3 + u^2 - u + 1)v + u^2 = 0 \end{cases}$

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

$$E: \ y^2 = x^3 + \frac{1}{4}(c^2 - 2c + 1 - 4b)x^2 + \frac{1}{2}b(c-1)x + \frac{b^2}{4}. \tag{3.1}$$

Note that NP is of order 2. The cubic polynomial in the right hand side of Eq. (3.1) is divisible by $x - x_{NP}$, 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 $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N\mathbb{Z}$ if and only if the quadratic factor $q(x)$ splits over K, and it holds if and only if the discriminant $d_{2N}(u, v)$ of $q(x)$ is a square in K. Therefore we have the following result:

THEOREM 3.1. *A defining equation of the modular curve $X_1(2, 2N)$ is given by*

$$\begin{cases} w^2 = d_{2N}(u, v), \\ f_{2N}(u, v) = 0. \end{cases} \tag{3.2}$$

In Table 2, we list defining equations of $X_1(2,2N)$ only for $N = 2,3,\ldots,8$ because those are very complicated for $N \geq 9$. We omit a defining equation of $X_1(2,2)$ for it has no model obtaining from the Tate normal form. We note that $d_{2N}(u,v)$ in Table 2 is not the exact discriminant but the same as a multiple by a square factor.

Example 3.2. *A defining equation of* $X_1(10)$ *is*

$$(u^2-3u+1)v+u^2=0,$$

and

$$d_{10}(u,v)=\frac{(4u^2-2u-1)(2u-1)^5}{16(u^2-3u+1)^4}.$$

Therefore a defining equation of $X_1(2,10)$ *is as follows:*

$$X_1(2,10):\begin{cases} w^2=(2u-1)(4u^2-2u-1), \\ (u^2-3u+1)v-u^2=0. \end{cases}$$

References

[1] D. Husemoller, *Elliptic curves*, Second edition, Springer-Verlag, New York, 2004.

[2] D. Jeon, C. H. Kim, and Y. Lee, *Families of elliptic curves over cubic number fields with prescribed torsion subgroups*, Math. Comp. **80** (2011), 579-591.

[3] M. A. Reichert, *Explicit determination of nontrivial torsion structures of elliptic curves over quadratic number fields*, Math. Comp. **46** (1986), 637–658.

[4] A. V. Sutherland, *Constructing elliptic curves over finite fields with prescribed torsion*, Math. Comp. **81** (2012), 1131-1147.

*

Department of Mathematics Education
Kongju National University
Kongju 314-701, Republic of Korea
E-mail: dyjeon@kongju.ac.kr