Korean J. Math. **21** (2013), No. 3, pp. 305–309
http://dx.doi.org/10.11568/kjm.2013.21.3.305

# DEFINING EQUATIONS OF $X_1(2N)$

Daeyeol Jeon

Abstract. In this paper, we give a new method to get defining equations of modular curves $X_1(2N)$ which show the moduli problems.

## 1. Introduction

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

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

Then the modular curve $X_1(N)$ corresponding to $\Gamma_1(N)$ is related to moduli problems of elliptic curves with $N$-torsion points. Defining equations of a modular curve are any polynomials that yield an isomorphic function field of that modular curve(cf. [6]).

Baaziz [1], Ishida and Ishii [3], Reichert [5], and Yang [6] suggested some methods to find defining equations of $X_1(N)$. The purpose of this paper is to present a new method for obtaining equations of $X_1(N)$ for even integers $N$. The author, Kim and Lee [4] found defining equations

Received August 5, 2013. Revised August 16, 2013. Accepted August 16, 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).

of $X_1(20)$ and $X_1(24)$ whose degree in one of variables is 4 for obtaining infinitely many points over quartic number fields. We improve the method in [4] to get defining equations of $X_1(2N)$ for all $N$.

## 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. [2]). On the curve $E(b,c)$ we have the following by the chord-tangent method(cf. [5]):

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

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 $P$. Eq. (1) implies that

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

Without loss of generality, the cases $s=0$ and $s=1$ may be excluded. Then Eq. (2) becomes as follows:

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

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:

$$v^2+v=u^3-u^2.$$

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

Let $E$ be an elliptic curve with a $N$-torsion point $P$. Suppose $Q$ is a point of $E$ with $2Q = P$ and $Q \notin \langle P \rangle$. Then $Q$ is a $2N$-torsion point of $E$. The set of pairs $(E, P)$ defines $X_1(N)$, and so the set of pairs $(E, Q)$ does $X_1(2N)$. Thus it suffices to find a method to parametrize the pairs $(E, Q)$ for getting a defining equation of $X_1(2N)$.

Suppose $E$ is an elliptic curve defined by

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

and $P = (0, 0)$ is an $N$-torsion point of $E$. 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:

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

For simplicity, we write $E'$ by

$$y^2 = x^3 + Ax^2 + Bx + C,$$

where $A = \frac{(c-1)^2-4b}{4}, B = \frac{b(c-1)}{2}$, and $C = \frac{b^2}{4}$. Then $(0, -\frac{b}{2})$ is an $N$-torsion point of the curve $E'$.

Now consider a point $Q = (x_1, y_1)$ with $2Q = (0, -\frac{b}{2})$. Take $y = mx + \frac{b}{2}$ as the line through $(0, \frac{b}{2})$ tangent at the unknown point $Q$. Then the three roots of

$$x^3 + Ax^2 + Bx + C - \left(mx + \frac{b}{2}\right)^2 \tag{3}$$

are $0, x_1$ and $x_1$, i.e., $x_1$ is a double root of Eq. (3). Thus

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

and hence the discriminant of

$$x^2 + (A - m^2)x + (B - bm) \tag{4}$$

is equal to 0, i.e., $m$ satisfies the following quartic equation:

$$(z^2 - A)^2 + 4(bz - B) = 0. \tag{5}$$

Suppose $m_0$ is a root of Eq. (5). Then

$$x_1 = \frac{m_0^2 - A}{2}$$

is a double root of Eq. (4) and hence also of Eq. (3). Thus $2(x_1, m_0x_1 + \frac{b}{2}) = (0, -\frac{b}{2})$. In other words, $Q = (x_1, y_1)$ is a $2N$-torsion point of $E'$ where $y_1 = m_0x_1 + \frac{b}{2}$.

Now suppose $f_N(u, v) = 0$ is a defining eqution of $X_1(N)$. Then each common root of $f_N(u, v) = 0$ and Eq. (5) is corresponding to a pair of $(E', Q)$ where $Q$ is a $2N$-torsion point of an elliptic curve $E'$. Therefore we have the following result

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

$$\begin{cases} f_N(u, v) = 0, \\ (z^2 - A)^2 + 4(bz - B) = 0, \end{cases}$$

*where $f_N(u, v) = 0$ is a defining eqution of $X_1(N)$ and $b, A, B$ are defined as above.*

EXAMPLE 3.2. *A defining equation of $X_1(11)$ is*

$$v^2 + v = u^3 - u^2,$$

*and*

$$b = \frac{v(v+1)(v+u)}{u}, \quad c = \frac{v(v+u)}{u}.$$

*Therefore a defining equation of $X_1(22)$ is given by the following:*

$$X_1(22) : \begin{cases} v^2 + v = u^3 - u^2, \\ 16u^4z^4 - 8u^2(v^4 - 2uv^3 - 3(u^2 + 2u)v^2 - 6u^2v + u^2)z^2 \\ +64u^3v(v+1)(v+u)z + v^8 - 4uv^7 - 2u(u+6)v^6 \\ +4(3u-5)u^2v^5 + u^2(9u^2 - 4u + 6)v^4 + 4(u+9)u^3v^3 \\ +10(3u+2)u^3v^2 + 20u^4v + u^4 = 0. \end{cases}$$

## References


[1] H. Baaziz, *Equations for the modular curve $X_1(N)$ and models of elliptic curves with torsion points*, Math. Comp. **79** (2010), 2371-2386.

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

[3] N. Ishida and N. Ishii, *Generators and defining equation of the modular function field of the group $\Gamma_1(N)$*, Acta Arith. **101** (2002), 303–320.

[4] 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.

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

[6] Y. Yang, *Defining equations of modular curves*, Adv. Math. **204** (2006), 481–508.

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