JOURNAL OF THE
CHUNGCHEONG MATHEMATICAL SOCIETY
Volume **28**, No. 1, February 2015
http://dx.doi.org/10.14403/jcms.2015.28.1.97

ARITHMETIC OF A CERTAIN MODULAR CURVE

Daeyeol Jeon*

Abstract. In this work, we study some arithmetic properties of an intermediate modular curve $X_\Delta(21)$.

1. Introduction

Let N be a positive integer and Δ a subgroup of $(\mathbb{Z}/N\mathbb{Z})^*$ which contains ± 1. Let $X_\Delta(N)$ be the modular curve defined over $\mathbb{Q}$ associated to the congruence subgroup

$$\Gamma_\Delta(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1) := \mathrm{SL}_2(\mathbb{Z}) \mid a \pmod N \in \Delta, N \mid c \right\}.$$

Then all the intermediate modular curves between $X_1(N)$ and $X_0(N)$ are of the form $X_\Delta(N)$.

There is a very interesting modular curve $X_\Delta(21)$ where $\Delta = \{\pm 1, \pm 8\}$ which is the only hyperelliptic intermediate modular curve with $\{\pm 1\} \subsetneq \Delta \subsetneq (\mathbb{Z}/N\mathbb{Z})^*$.

A smooth, projective curve X with the genus $g(X) \geq 2$ is called *hyperelliptic* if it admits a surjective morphism $\phi : X \to \mathbb{P}^1$ of degree 2. If X is a hyperelliptic curve, there exists a unique involution ν, called a *hyperelliptic involution*, such that $X/\langle \nu \rangle$ is a rational curve. A hyperelliptic involution is contained in the center of the automorphism group $\mathrm{Aut}(X)$, and it is defined over $\mathbb{Q}$.

In fact, Ishii and Momose [2] asserted that there exist no hyperelliptic modular curves $X_\Delta(N)$ with $\{\pm 1\} \subsetneq \Delta \subsetneq (\mathbb{Z}/N\mathbb{Z})^*$. But the author and Kim [4] proved that $X_\Delta(21)$ is hyperelliptic, and it is the unique one.

Received October 02, 2014; Accepted January 12, 2015.
2010 Mathematics Subject Classification: Primary 11G18, 11G30.
Key words and phrases: hyperelliptic, modular curve.
The author 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).

In this paper, we study some arithmetic properties of $X_\Delta(21)$. Firstly we give a new proof for that $X_\Delta(21)$ is hyperelliptic by using the computations in [5]. Secondly we compute the full automorphism group $\mathrm{Aut}(X_\Delta(21))$ of $X_\Delta(21)$. Finally we find the explicit expressions of all the automorphisms of $X_\Delta(21)$.

2. Preliminaries

Let $\mathbb{H}$ be the complex upper half plane and $\mathbb{H}^* = \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$, and let

$$\Gamma_1(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1) \mid a \equiv d \equiv 1 \pmod{N},\ c \equiv 0 \pmod{N} \right\}.$$

Then $\Gamma_1(N)$ acts on $\mathbb{H}^*$ by the linear fractional transformation, and then the compact Riemann surface $X_1(N) = \Gamma_1(N)\backslash\mathbb{H}^*$ is called a *modular curve.*

The points of $\Gamma_1(N)\backslash\mathbb{H}$ are in one-to-one correspondence with the equivalent classes of elliptic curves E together with a specified point P of exact order N. Let $L_\tau = [\tau, 1]$ be the lattice in $\mathbb{C}$ with basis τ and 1. Then $[\tau] \in \Gamma_1(N)\backslash\mathbb{H}$ corresponds to $\left[\mathbb{C}/L_\tau, \frac{1}{N} + L_\tau\right]$. Thus $\Gamma_1(N)\backslash\mathbb{H}$ is a moduli space for the moduli problem of determining equivalence classes of pairs (E, P), where E is an elliptic curve defined over $\mathbb{C}$, and $P \in E$ is a point of exact order N. Two pairs (E, P) and (E', P') are equivalent if there is an isomorphism $E \simeq E'$ which sends P to P'.

Now we note that

$$\begin{aligned}\left[\mathbb{C}/L_\tau,\, \frac{1}{N} + L_\tau\right] &= \left[y^2 = 4x^3 - g_2(\tau)x - g_3(\tau),\, \left(\wp\left(\frac{1}{N}, \tau\right), \wp'\left(\frac{1}{N}, \tau\right)\right)\right] \\ &= \left[y^2 + (1 - c(\tau))xy - b(\tau)y = x^3 - b(\tau)x^2,\, (0,0)\right],\end{aligned}$$

where $\wp(z, \tau) := \wp(z, L_\tau)$ is the Weierstrass elliptic function. From [1], it follows that

$$b(\tau) = -\frac{(\wp(\frac{1}{N}, \tau) - \wp(\frac{2}{N}, \tau))^3}{\wp'(\frac{1}{N}, \tau)^2},\ c(\tau) = -\frac{\wp'(\frac{2}{N}, \tau)}{\wp'(\frac{1}{N}, \tau)} \tag{2.1}$$

are modular functions on $\Gamma_1(N)$ and generate the function field of $X_1(N)$, where the derivative is with respect to z. Furthermore, the function field of $X_1(N)$ can be generated by x, y satisfying the defining equation $f_N(x, y) = 0$ of $X_1(N)$ for $N \le 30$ in Table 6 of [6], where x, y are considered as functions of τ via the rational maps of Table 7 of [6], Eq. (2.1) and the following relations:

$$b = cr, c = s(r - 1). \tag{2.2}$$

3. Hyperelliptic modular curves

We consider the automorphisms on $X_\Delta(N)$. Note that $X_\Delta(N) \to X_0(N)$ is a Galois covering with Galois group $\Gamma_0(N)/\Gamma_\Delta(N)$ which gives automorphisms on $X_\Delta(N)$. For an integer a prime to N, let $[a]$ denote the automorphism of $X_\Delta(N)$ represented by $\gamma \in \Gamma_0(N)$ such that $\gamma \equiv \left(\begin{smallmatrix} a & * \\ 0 & * \end{smallmatrix}\right) \mod N$. Sometimes we regard $[a]$ as a matrix.

For each divisor $d|N$ with $(d, N/d) = 1$, consider the matrices of the form $\begin{pmatrix} dx & y \\ Nz & dw \end{pmatrix}$ with $x, y, z, w \in \mathbb{Z}$ and determinant d. Then these matrices define a unique involution on $X_0(N)$ which is called the *Atkin-Lehner involution* and denoted by W_d. We denote by W_d a matrix of the above form. In general, W_d may not define an automorphism of $X_\Delta(N)$.

Note that $X_\Delta(21)$ is isomorphic to the quotient space $X_1(21)/\langle[8]\rangle$. Take $[8] = \left(\begin{smallmatrix} 8 & -3 \\ 21 & -8 \end{smallmatrix}\right)$ then one can compute that

$$
\begin{aligned}
b([8]\tau) &= -\frac{\left(\wp\left(\frac{8}{21}, \tau\right) - \wp\left(\frac{16}{21}, \tau\right)\right)^3}{\wp'\left(\frac{8}{21}, \tau\right)^2}, \\
c([8]\tau) &= -\frac{\wp'\left(\frac{16}{21}, \tau\right)}{\wp'\left(\frac{8}{21}, \tau\right)}.
\end{aligned} \tag{3.1}
$$

From the q-expansions of $\wp(z,\tau)$ and $\wp'(z,\tau)$, the author with Kim and Lee [5] compute the q-expansions $x(\tau)$ and $y(\tau)$ by using Eq. (2.1), (2.2) and Table 7 of [6] where $q = e^{2\pi i\tau}$. Also they compute the q-expansions of $x([8]\tau)$ and $y([8]\tau)$ from Eq. (3.1). Then the functions $u := x + x \circ [8]$ and $v := y + y \circ [8]$ are generators for the function field of $X_1(21)/\langle[8]\rangle$. By using the q-expansions of x, y, $x \circ [8]$, $y \circ [8]$, they compute a defining equation of $X_1(21)/\langle[8]\rangle$ as follows:

(3.2)
$$
\begin{aligned}
f(u,v) :=& -2 + 4v - u + u^4v^2 + u^5v + u^5v^2 + 3u^2v^2 - 3u^2v + 5uv^2 - 3u^3v \\
&+ 2u^4v - 5u^3v^2 + 3u^2v^3 - u^2 - 6v^2 + u^3 - 4v^3 + u^4 + v^4 = 0.
\end{aligned}
$$

Thus this equation is also a defining equation of $X_\Delta(21)$.

Firstly, we give a new proof for the hyperellipticity of $X_\Delta(21)$ by using a computer algebra system Maple. Maple can compute the Weierstrass form of hyperelliptic curves by using the following commands:

```
> with(algcurves):
> Weierstrassform(f(u,v),u,v,x,y);
```

Let α be a root of the polynomial $g(x) := x^4 - 4x^3 - 6x^2 + 4x - 2$. Then we have a defining equation $y^2 = ch(x)$ for $X_\Delta(21)$ where

$$\begin{aligned} c =& 351440727601040\alpha^3 + 355787816740356\alpha^2 - 269886886283168\alpha \\ & + 141066103901184, \end{aligned}$$

and

$$h(x) = x^8 + a_7x^7 + a_6x^6 + a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0,$$

$$\begin{aligned} a_7 &= -\frac{1}{58619}(14280\alpha^3 - 86540\alpha^2 + 3616\alpha + 24712) \\ a_6 &= -\frac{1}{58619}(202860\alpha^3 - 856974\alpha^2 - 1052048\alpha + 433812) \\ a_5 &= -\frac{1}{5329}(32712\alpha^3 - 125696\alpha^2 - 209104\alpha + 19136) \\ a_4 &= -\frac{1}{58619}(200536\alpha^3 - 672780\alpha^2 - 1522508\alpha - 624892) \\ a_3 &= \frac{1}{5329}(3456\alpha^3 - 19332\alpha^2 - 13240\alpha + 70896) \\ a_2 &= \frac{1}{58619}(72172\alpha^3 - 275150\alpha^2 - 502432\alpha + 284760) \\ a_1 &= \frac{1}{58619}(18272\alpha^3 - 54248\alpha^2 - 139080\alpha + 2984) \\ a_0 &= -\frac{1}{58619}(120\alpha^3 - 4668\alpha^2 - 1940\alpha + 9567) \end{aligned}$$

Therefore one can conclude that $X_\Delta(21)$ is a hyperelliptic curve of genus 3.

Now we compute $\mathrm{Aut}(X_\Delta(21))$ by using the computer algebra system MAGMA. MAGMA can compute the full automorphism group of hyperelliptic curves of genus 2 or 3. One can use the following commands:

```
> R<x> := PolynomialRing(Integers());
> K<y> := NumberField(g(x));
> P<x> := PolynomialRing(K);
> k := c*h(x);
> C := HyperellipticCurve(k);
> GeometricAutomorphismGroup(C);
```

Then one can get the order of $\mathrm{Aut}(X_\Delta(21))$ to be 12. In fact, the author, Im and Kim [3] prove that the quotient group $\mathfrak{N}_\Delta(21)/\Gamma_\Delta(21)$ is isomorphic to the dihedral group of order 12 where $\mathfrak{N}_\Delta(21)$ is the normalizer of $\Gamma_\Delta(21)$ in $\mathrm{PSL}_2(\mathbb{R})$. Since $\mathfrak{N}_\Delta(21)/\Gamma_\Delta(21)$ can be consider a subgroup of $\mathrm{Aut}(X_\Delta(21))$, one can conclude that $\mathrm{Aut}(X_\Delta(21))$ is the dihedral group of order 12.

Now we find the explicit expressions on Eq. (3.2) of all the automorphsims of $X_\Delta(21)$. For that it suffices to find explicit expressions of the generators of $\mathrm{Aut}(X_\Delta(21))$ which are $[2]W_3$ and W_{21}. Note that W_3 is the hyperelliptic involution on $X_\Delta(21)$ whose expression can be obtained from the computations in [5] as follows:

$$
\begin{aligned}
(3.3)\quad u\circ W_3 &= \frac{-1+5v+3u^2-9uv+6v^2-3uv^2+v^3+2u^3v+3u^2v}{-2+v-3uv-v^3+u^3v},\\
v\circ W_3 &= -\frac{-1+3u-4v-3uv+3v^2+3u^2v+v^3+2u^3v}{1-2v+6v^2-v^3+u^3v-3u^2v^2}.
\end{aligned}
$$

Now consider the automorphism $[2]$ whose action on u and v are $u\circ[2] = x\circ[2]+x\circ[16]$ and $v\circ[2] = y\circ[2]+y\circ[16]$. By using the q-expansions of u, v, $u\circ[2]$ and $v\circ[2]$, one can find the following expressions:

$$
\begin{aligned}
&(3.4)\\
&u\circ[2] = \frac{-1+2v^2-v^3-2uv-u^2v^2+u^3v}{-1+v-2v^2-uv+u^2v^2},\\
&v\circ[2] = -\frac{4v+2v^2-v^3-u-uv+uv^2+uv^3+u^2-2u^2v-2u^2v^2+u^3+u^3v}{-1+v-2v^2+u-3uv+uv^2+uv^3+u^2+u^2v+u^2v^2+u^3v}.
\end{aligned}
$$

By the exact same method, one can get the expression of the action by W_{21} as follows:

$$
\begin{aligned}
&u\circ W_{21}\\
&= \{2+3\zeta-3\zeta^6+3\zeta^8+(4-3\zeta+3\zeta^6-3\zeta^8)u+(3\zeta^3-3\zeta^4-3\zeta^{11})u^2-(1+3\zeta-3\zeta^6+3\zeta^8)u^3\\
&\quad -(7+3\zeta-6\zeta^3+6\zeta^4-3\zeta^6+3\zeta^8+6\zeta^{11})v+(2+3\zeta-6\zeta^3+6\zeta^4-3\zeta^6+3\zeta^8+6\zeta^{11})uv\\
&\quad +(5+3\zeta^3-3\zeta^4-3\zeta^{11})u^2v-(1+3\zeta-3\zeta^6+3\zeta^8)u^3v-(4+3\zeta-3\zeta^6+3\zeta^8)v^2\\
&\quad -(3\zeta^3-3\zeta^4-3\zeta^{11})uv^2+(4-3\zeta^4-3\zeta^{11}+3\zeta^3)u^2v^2+(4-3\zeta+3\zeta^3-3\zeta^4+3\zeta^6-3\zeta^8-3\zeta^{11})v^3\}\\
&\quad /(-5+2u-3u^2+u^3-2v+uv-2u^2v-8v^2+3uv^2-v^3),\\
&v\circ W_{21}\\
&= \{-76-76\zeta^3+76\zeta^4-26\zeta^6+26\zeta^8+76\zeta^{11}+26\zeta+(-285-224\zeta^3+224\zeta^4-103\zeta^6+103\zeta^8+224\zeta^{11}\\
&\quad +103\zeta)u+(30+23\zeta^3-23\zeta^4+10\zeta^6-10\zeta^8-23\zeta^{11}-10\zeta)u^2+(-42-23\zeta^3+23\zeta^4-16\zeta^6+16\zeta^8\\
&\quad +23\zeta^{11}+16\zeta)u^3+(102+79\zeta^3-79\zeta^4+38\zeta^6-38\zeta^8-79\zeta^{11}-38\zeta)u^4+(314+277\zeta^3-277\zeta^4\\
&\quad +107\zeta^6-107\zeta^8-277\zeta^{11}-107\zeta)v+(225+163\zeta^3-163\zeta^4+86\zeta^6-86\zeta^8-163\zeta^{11}-86\zeta)uv\\
&\quad +(-171-146\zeta^3+146\zeta^4-61\zeta^6+61\zeta^8+146\zeta^{11}+61\zeta)u^2v+(-241-182\zeta^3+182\zeta^4-88\zeta^6+88\zeta^8\\
&\quad +182\zeta^{11}+88\zeta)u^3v+(-522-418\zeta^3+418\zeta^4-185\zeta^6+185\zeta^8+418\zeta^{11}+185\zeta)v^2+(-72-55\zeta^3\\
&\quad +55\zeta^4-26\zeta^6+26\zeta^8+55\zeta^{11}+26\zeta)uv^2+(261-93\zeta+93\zeta^6+207\zeta^3-93\zeta^8-207\zeta^{11}-207\zeta^4)u^2v^2\\
&\quad +(25-9\zeta+9\zeta^6+21\zeta^3-9\zeta^8-21\zeta^{11}-21\zeta^4)v^3\}/\{44+32\zeta^3-32\zeta^4+16\zeta^6-16\zeta^8-32\zeta^{11}-16\zeta\\
&\quad +(63+43\zeta^3-43\zeta^4+23\zeta^6-23\zeta^8-43\zeta^{11}-23\zeta)u+(237+191\zeta^3-191\zeta^4+85\zeta^6-85\zeta^8-191\zeta^{11}\\
&\quad -85\zeta)u^2+(-105-86\zeta^3+86\zeta^4-37\zeta^6+37\zeta^8+86\zeta^{11}+37\zeta)u^3+(-66-47\zeta^3+47\zeta^4-25\zeta^6
\end{aligned}
$$

$+ 25\zeta^8 + 47\zeta^{11} + 25\zeta)u^4 + (119 + 88\zeta^3 - 88\zeta^4 + 47\zeta^6 - 47\zeta^8 - 88\zeta^{11} - 47\zeta)v + (-759 - 602\zeta^3$
$+ 602\zeta^4 - 274\zeta^6 + 274\zeta^8 + 602\zeta^{11} + 274\zeta)uv + (333 + 262\zeta^3 - 262\zeta^4 + 119\zeta^6 - 119\zeta^8 - 262\zeta^{11}$
$- 119\zeta)u^2v + (164 + 130\zeta^3 - 130\zeta^4 + 59\zeta^6 - 59\zeta^8 - 130\zeta^{11} - 59\zeta)u^3v + (369 + 302\zeta^3 - 302\zeta^4$
$+ 130\zeta^6 - 130\zeta^8 - 302\zeta^{11} - 130\zeta)v^2 + (-165 - 133\zeta^3 + 133\zeta^4 - 59\zeta^6 + 59\zeta^8 + 133\zeta^{11} + 59\zeta)uv^2 + v^3\},$
where ζ is a primitive 21-th root of unity.

References

[1] H. Baaziz, *Equations for the modular curve $X_1(N)$ and models of elliptic curves with torsion points*, Math. Comp. **79** (2010), no. 272, 2371-2386.

[2] N. Ishii and F. Momose, *Hyperelliptic modular curves,* Tsukuba J. Math. **15** (1991), 413-423.

[3] B. Im, D. Jeon, and C. H. Kim, *Normalizers of intermediate congruence subgroups of the Hecke subgroups,* preprint.

[4] D. Jeon and C. H. Kim, *On the arithmetic of certain modular curves.* Acta Arith. **130** (2007), 138-193.

[5] D. Jeon, C. H. Kim, and Y. Lee, *Families of elliptic curves with prescribed torsion subgroups over dihedral quartic fields,* J. Number Theory. **147** (2015), 342-363.

[6] 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, Republic of Korea
E-mail: dyjeon@kongju.ac.kr