Automorphism groups of hyperelliptic modular curves

By Daeyeol JEON

Department of Mathematics Education, Kongju National University, Kongju, Chungnam 305-701, South Korea

(Communicated by Shigefumi MORI, M.J.A., June 12, 2015)

Abstract: In this paper, we determine the automorphism groups of the hyperelliptic modular curves $X_1(N)$, and determine explicit forms for the actions of all automorphisms on certain defining equations of $X_1(N)$.

Key words: Modular curve; automorphism group; hyperelliptic curve; hyperelliptic involution.

1. Introduction. Let $\Gamma(1) = \mathrm{SL}_2(\mathbf{Z})$ be the full modular group. For any integer $N \geq 1$, we have subgroups $\Gamma_1(N)$ and $\Gamma_0(N)$ of $\Gamma(1)$ defined by matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ that are congruent modulo N to $\left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right)$, respectively. We let $X_1(N)$ and $X_0(N)$ be the modular curves defined over $\mathbf{Q}$ associated with $\Gamma_1(N)$ and $\Gamma_0(N)$, respectively. There are some more modular curves $X_\Delta(N)$ associated with the subgroups $\Gamma_\Delta(N)$ of $\Gamma_0(N)$ defined by matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ with $a \in \Delta$, where Δ is a subgroup of $(\mathbf{Z}/N\mathbf{Z})^*$ that contains -1. For $\Delta = \{\pm 1\}$, this is $X_1(N)$.

For an integer $N \geq 2$, the modular curve $X_1(N)$ (with cusps removed) parameterizes isomorphism classes of pairs (E, P), where E is an elliptic curve and P a torsion point of order N on E. Reichert [9], Sutherland [10], and Baaziz [1] derived defining equations for $X_1(N)$. One can recover explicit forms for the pairs (E, P) from the corresponding points whose coordinates satisfy these defining equations of $X_1(N)$.

Let $N(\Gamma_1(N))$ be the normalizer of $\Gamma_1(N)$ in $\mathrm{PSL}_2(\mathbf{R}) \cong \mathrm{GL}_2^+(\mathbf{R})/\mathbf{R}^*$. Then, the quotient group $N(\Gamma_1(N))/\pm\Gamma_1(N)$ can be viewed as a subgroup of the automorphism group $\mathrm{Aut}(X_1(N))$ of $X_1(N)$ consisting of all automorphisms of $X_1(N)$ defined over $\mathbf{C}$. Kim and Koo [4] and Lang [5] compute $N(\Gamma_1(N))$ independently.

The main theorem of an unpublished paper by Momose [8] is that, for any square-free integer N and modular curve $X_\Delta(N)$ of genus $g \geq 2$, $\mathrm{Aut}(X_\Delta(N))$ is equal to $N(\Gamma_\Delta(N))/\Gamma_\Delta(N)$, except for $X_0(37)$. However, the author with Kim and Schweizer [3] found a counterexample for the case of $X_\Delta(37)$ where $\Delta = \{\pm 1, \pm 6, \pm 8, \pm 10, \pm 11, \pm 14\}$. We do not want to use Momose's result in this paper.

In [2], the authors determined the group structures of $\mathrm{Aut}(X_1(N))$ for $N = 13, 16, 18$. In this paper, we give a new proof for this result.

Let C be a smooth, projective curve over an algebraically closed field k of genus $g(C) \geq 2$. Then C is said to be *hyperelliptic* if it admits a map $\phi : C \to \mathbf{P}^1$ of degree 2 defined over k. If C is a hyperelliptic curve, then there exists an involution ν, called a *hyperelliptic involution*, such that $C/\langle\nu\rangle$ is a rational curve. Mestre [7] showed that the modular curve $X_1(N) \otimes_{\mathbf{Q}} \mathbf{C}$ is hyperelliptic only for $N = 13, 16, 18$.

The main goal of this paper is to compute the automorphism groups $\mathrm{Aut}(X_1(N))$ of the hyperelliptic modular curves $X_1(N)$ and derive explicit forms of the actions of all automorphisms on the defining equations of these $X_1(N)$. For this purpose, we use the recent results of Baaziz [1], which enable us to solve the moduli problems. In fact, $\mathrm{Aut}(X_1(N))$ is equal to $N(\Gamma_1(N))/\pm\Gamma_1(N)$ for the hyperelliptic curves $X_1(N)$.

We concentrate on hyperelliptic cases for the following reasons: First, the automorphism groups of the curves $X_1(N)$ of genus $g \leq 1$ are infinite; second, the full classification of $\mathrm{Aut}(X_1(N))$ is not yet known; and third, the method of calculating explicit forms of all automorphisms from $N(\Gamma_1(N))/\Gamma_1(N)$ can be applied to the other cases.

2. Preliminaries. The *Tate normal form* of an elliptic curve with a point $P = (0, 0)$ is

$$E = E(b, c) : Y^2 + (1 - c)XY - bY = X^3 - bX^2,$$

and this is nonsingular if and only if $b \neq 0$. On the

2010 Mathematics Subject Classification. Primary 14H37; Secondary 11G18.

doi: 10.3792/pjaa.91.95

curve $E(b,c)$, we can use the chord-tangent method to derive the following

$$
\begin{aligned}
(1)\qquad P &= (0,0),\\
2P &= (b,\ bc),\\
3P &= (c,\ b-c),\\
4P &= \big(r(r-1),\ r^2(c-r+1)\big); \quad b = cr,\\
5P &= \big(rs(s-1),\ rs^2(r-s)\big); \quad c = s(r-1),\\
6P &= \left(\frac{s(r-1)(r-s)}{(s-1)^2},\right.\\
&\qquad \left.\frac{s^2(r-1)^2(rs-2r+1)}{(s-1)^3}\right),\\
7P &= \left(\frac{rs(s-1)(r-1)(sr-2r+1)}{(r-s)^2},\right.\\
&\qquad \left.\frac{(s-1)^2(r-1)^2(r-s^2+s-1)}{(r-s)^3}\right).
\end{aligned}
$$

The condition $NP = O$ in $E(b,c)$ gives a defining equation for $X_1(N)$. For example, $13P = O$ implies $6P = -7P$, so

$$X_{6P} = X_{-7P} = X_{7P},$$

where X_{nP} denotes the X-coordinate of the n-multiple nP of P. Eq. (1) implies that

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

Without loss of generality, the cases $s = 0, 1,\ r = 1, s$ may be excluded. Then, Eq. (2) becomes

$$
\begin{aligned}
F_{13}(r,s) := r^3 - 2r^2 + 5s^3r^2 - s^4r^2 - 9s^2r^2 + 4sr^2\\
- s^3r - 3sr + 6s^2r + r - s^3 = 0,
\end{aligned}
$$

which is one of the equations for $X_1(13)$, called the *raw form* of $X_1(13)$. By the coordinate changes $r = 1 - xy$ and $s = 1 - \frac{xy}{y+1}$, we have that

$$f_{13}(x,y) := y^2 + (x^3 + x^2 + 1)y - x^2 - x = 0.$$

This solves the moduli problem of $X_1(13)$. If we pick $x_0 = 1$, and set $y_0 = -\frac{3}{2} + \frac{\sqrt{17}}{2}$, then (x_0, y_0) is a K-rational point on $X_1(13)$ satisfying $f_{13}(x_0,y_0) = 0$, where $K = \mathbf{Q}(\sqrt{17})$ is a quadratic number field. If we apply the formulas in Table II and Eq. (1) with $x = x_0$ and $y = y_0$, we obtain

$$
\begin{aligned}
b_0 &:= b(x_0,y_0) = -\frac{13}{4} + \frac{3\sqrt{17}}{4},\\
c_0 &:= c(x_0,y_0) = -\frac{7}{8} + \frac{\sqrt{17}}{8}.
\end{aligned}
$$

Table I. Defining equations of $X_1(N) : f_N(x,y) = 0$

N	$f_N(x,y)$
13	$y^2 + (x^3 + x^2 + 1)y - x^2 - x$
16	$y^2 + (x^3 + x^2 - x + 1)y + x^2$
18	$(x^2 - 2x + 1)y^2 + (-x^3 + x - 1)y + x^3 - x^2$

Table II. Birational maps φ for $X_1(N)$ from $f_N(x,y) = 0$ to $F_N(r,s) = 0$

N	φ	
13	$r = 1 - xy,$	$s = 1 - \frac{xy}{y+1}$
16	$r = \frac{x^2 - xy + y^2 + y}{x^2 + x - y - 1},$	$s = \frac{x-y}{x+1}$
18	$r = \frac{x^2 + y}{x^2 + y + xy - y^2},$	$s = \frac{x^2 + y - xy}{x^2 + y - y^2}$

Then, the elliptic curve $E(b_0, c_0)$ over K contains the point $(0,0)$ of order 13, and in fact its torsion subgroup is $\mathbf{Z}/13\mathbf{Z}$.

From [9] and [10], we obtain the defining equations of $X_1(N)$ in Table I and birational maps φ for $X_1(N)$ from $f_N(x,y) = 0$ to $F_N(r,s) = 0$ in Table II for $N = 13, 16, 18$, where $F_N(r,s) = 0$ denotes the raw form of $X_1(N)$.

Let $\mathbf{H}$ be the complex upper half plane and $\mathbf{H}^* = \mathbf{H} \cup \mathbf{P}^1(\mathbf{Q})$. Then, $\Gamma_1(N)$ acts on $\mathbf{H}^*$ under linear fractional transformations, and $X_1(N)(\mathbf{C})$ can be viewed as a Riemann surface $\Gamma_1(N)\backslash\mathbf{H}^*$.

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

Note that

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

where $g_2(\tau) = 60G_4(\tau)$, $g_3(\tau) = 140G_6(\tau)$ for the Eisenstein series $G_{2k}(\tau)$ of weight $2k$, $\wp(z,\tau) := \wp(z, L_\tau)$ is the Weierstrass elliptic function, and $b(\tau)$, $c(\tau)$ are the coefficients of the Tate normal form contained in $[\mathbf{C}/L_\tau,\ \frac{1}{N} + L_\tau]$. Note that each equivalence class of pairs (E, P) contains a unique Tate normal form [1, Proposition 1.3], and hence $b(\tau)$ and $c(\tau)$ induce well-defined functions on $\Gamma_1(N)\backslash\mathbf{H}$. From [1], it follows that

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

$$c(\tau) = -\frac{\wp'(\frac{2}{N},\tau)}{\wp'(\frac{1}{N},\tau)}$$

are modular functions on $\Gamma_1(N)$ and generate the function field of $X_1(N)$, where $\wp'$ is the derivative with respect to z.

3. Automorphism groups. In this section, we determine the full automorphism groups of $X_1(N)$ with $N = 13, 16, 18$.

Since $\Gamma_0(N)/\{\pm 1\}$ is contained in $N(\Gamma_1(N))$, every $\gamma \in \Gamma_0(N)$ induces an automorphism of $X_1(N)$. For an integer a that is prime to N, let $[a]$ denote the automorphism of $X_1(N)$ represented by $\gamma \in \Gamma_0(N)$ such that $\gamma \equiv \left(\begin{smallmatrix} a & * \\ 0 & * \end{smallmatrix}\right) \bmod N$. In some instances, we regard $[a]$ as a matrix.

For each divisor $d|N$ with $(d, N/d) = 1$, consider matrices of the form $W_d = \begin{pmatrix} dx & y \\ Nz & dw \end{pmatrix}$ with $x, y, z, w \in \mathbf{Z}$ and determinant d. Such matrices define a unique involution on $X_0(N)$ that is called the *Atkin–Lehner involution*. However, this is not true for $X_1(N)$. Furthermore, W_d does not, in general, give an involution on $X_1(N)$.

We now fix a matrix W_d that belongs to the normalizer $N(\Gamma_1(N))$, and define an automorphism of $X_1(N)$. Kim and Koo [4] and Lang [5] proved that $N(\Gamma_1(N))$ is generated by $\Gamma_0(N)$ and the W_d when $N \neq 4$.

First, we compute $N(\Gamma_1(N))/\pm\Gamma_1(N)$ with $N = 13, 16, 18$. For each $N = 13, 16$, or 18, we consider the following exact sequence:

$$(4)\quad 1 \to \Gamma_0(N)/\pm\Gamma_1(N) \to N(\Gamma_1(N))/\pm\Gamma_1(N) \to N(\Gamma_1(N))/\Gamma_0(N) \to 1.$$

If $N = 13, 16$, then $N(\Gamma_1(N))/\Gamma_0(N)$ is a cyclic group of order 2 that is generated by W_N. One can easily check that

$$(5)\qquad [a]W_N \equiv W_N[a^{-1}] \bmod \pm\Gamma_1(N)$$

for all a prime to N, and hence W_N is of order 2 in $N(\Gamma_1(N))/\pm\Gamma_1(N)$. Thus, the exact sequence in Eq. (4) can be split, and so $N(\Gamma_1(N))/\pm\Gamma_1(N)$ is a semidirect product of $\Gamma_0(N)/\pm\Gamma_1(N)$ and $N(\Gamma_1(N))/\Gamma_0(N)$. Note that $\Gamma_0(N)/\pm\Gamma_1(N)$ is isomorphic to $(\mathbf{Z}/N\mathbf{Z})^*/\{\pm 1\}$. From Eq. (5), we can conclude that $N(\Gamma_1(N))/\pm\Gamma_1(N)$ are $\langle [2], W_{13}\rangle$ and $\langle [3], W_{16}\rangle$, which are isomorphic to the dihedral groups D_6, D_4 for $N = 13, 16$ respectively.

Let us now consider $N = 18$. Choose a matrix $W_2 = \begin{pmatrix} 4 & -1 \\ 18 & -4 \end{pmatrix}$. For any a prime to 18, the $(1,1)$-entry $W_2[a]W_2^{-1}[1,1]$ of the matrix $W_2[a]W_2^{-1}$ satisfies the following

$$W_2[a]W_2^{-1}[1,1] \equiv a^{-1} \equiv a \pmod 2,$$
$$W_2[a]W_2^{-1}[1,1] \equiv a \pmod 9.$$

Thus, W_2 commutes with $[a]$ for any a prime to 18. Choose $W_9 = \begin{pmatrix} 9 & -5 \\ 18 & -9 \end{pmatrix}$. Then,

$$W_9[a]W_9^{-1}[1,1] \equiv a \equiv a^{-1} \pmod 2,$$
$$W_9[a]W_9^{-1}[1,1] \equiv a^{-1} \pmod 9,$$

for any a prime to N. Thus

$$(6)\qquad [a]W_9 \equiv W_9[a^{-1}] \bmod \pm\Gamma_1(18).$$

One can easily check that $W_2W_9 \equiv W_9W_2 \bmod \pm\Gamma_1(18)$. Note that $N(\Gamma_1(18))/\Gamma_0(18)$ is the Klein 4-group, and the matrices W_2, W_9 generate a subgroup of $N(\Gamma_1(18))/\pm\Gamma_1(18)$ that is also the Klein 4-group. Thus, the exact sequence in Eq. (4) can be split when $N = 18$, and hence $N(\Gamma_1(18))/\pm\Gamma_1(18)$ is the semidirect product of $\Gamma_0(18)/\pm\Gamma_1(18)$ and $N(\Gamma_1(18))/\Gamma_0(18)$. Since $\Gamma_0(18)/\pm\Gamma_1(18)$ is a cyclic group of order 3 and W_2 commutes with $[a]$ for any a prime to 18, $\Gamma_0(18)/\pm\Gamma_1(18)$ and W_2 generate a cyclic group of order 6. From Eq. (6), we can conclude that $N(\Gamma_1(18))/\pm\Gamma_1(18) = \langle [5]W_2, W_9\rangle$ is isomorphic to the dihedral group D_6.

Note that for $N = 13, 16, 18$, $X_1(N)$ are hyperelliptic curves of genus 2. The computer algebra system MAGMA can compute the full automorphism group of hyperelliptic curves of genus 2 or 3. Using MAGMA, we can compute that $\mathrm{Aut}(X_1(N))$ is isomorphic to D_6, D_4, D_6 for $N = 13, 16, 18$, respectively. Therefore, we conclude that $\mathrm{Aut}(X_1(N))$ are the same as $N(\Gamma_1(N))/\pm\Gamma_1(N)$ for $N = 13, 16, 18$.

Theorem 3.1. *For $N = 13, 16, 18$, the full automorphism groups* $\mathrm{Aut}(X_1(N))$ *are the same as* $N(\Gamma_1(N))/\pm\Gamma_1(N)$*, which are the dihedral groups* D_6, D_4, D_6 *respectively.*

4. Explicit forms. In this section, we derive explicit forms of the actions of all automorphisms on the defining equations of the hyperelliptic curves $X_1(N)$ in Table I. For this purpose, it suffices to know the forms of the generators of $N(\Gamma_1(N))/\pm\Gamma_1(N)$.

Let us consider $N = 13$. The group $\mathrm{Aut}(X_1(13))$ is generated by $[2]$ and W_{13}. If we take $[2] = \left(\begin{smallmatrix} 2 & 1 \\ 13 & 7 \end{smallmatrix}\right)$, then $[2]$ acts on $X_1(13)$ as $[2]\tau = \frac{2\tau+1}{13\tau+7}$. In this case, we have the following

$$\begin{aligned}\wp\left(\frac{1}{13}, [2]\tau\right) &= (13\tau+7)^2\wp\left(\frac{13\tau+7}{13}, \tau\right)\\ &= (13\tau+7)^2\wp\left(\frac{7}{13}, \tau\right),\end{aligned}$$

and

$$\begin{aligned}\wp'\left(\frac{1}{13}, [2]\tau\right) &= (13\tau+7)^3\wp'\left(\frac{13\tau+7}{13}, \tau\right)\\ &= (13\tau+7)^3\wp'\left(\frac{7}{13}, \tau\right).\end{aligned}$$

Similarly, we have the following

$$\begin{aligned}\wp\left(\frac{2}{13}, [2]\tau\right) &= (13\tau+7)^2\wp\left(\frac{1}{13}, \tau\right),\\ \wp'\left(\frac{2}{13}, [2]\tau\right) &= (13\tau+7)^3\wp'\left(\frac{1}{13}, \tau\right).\end{aligned}$$

Thus, from Eq. (3), we obtain the following

$$\begin{aligned}b([2]\tau) &= -\frac{\left(\wp\left(\frac{7}{13}, \tau\right) - \wp\left(\frac{1}{13}, \tau\right)\right)^3}{\wp'\left(\frac{7}{13}, \tau\right)^2},\\ c([2]\tau) &= -\frac{\wp'\left(\frac{1}{13}, \tau\right)}{\wp'\left(\frac{7}{13}, \tau\right)}.\end{aligned} \tag{7}$$

From Eq. (1) and Table 7 of [10], we have that the generators x, y of the function field of $X_1(13)$ satisfying $f_{13}(x, y) = 0$ can be expressed as the following functions of b, c:

$$\begin{aligned}x &= \frac{(b-c^2-c)(b-c)}{b^2-bc-c^3},\\ y &= -\frac{b^2-bc-c^3}{c(b-c^2-c)}.\end{aligned} \tag{8}$$

From the formulas in Proposition 3 of [6, p. 46], we can determine the q-expansions for $\wp(z, \tau)$ and $\wp'(z, \tau)$, where $q = e^{2\pi i\tau}$. Using these q-expansions and Eqs. (3), (7), and (8), we arrive at the following q-expansions of $x(\tau)$, $y(\tau)$, $x([2]\tau)$, and $y([2]\tau)$:

$$\begin{aligned}x(\tau) &= (-2-\omega^2-\omega^3-\omega^4-\omega^6-\omega^7-\omega^9\\ &\quad -\omega^{10}-\omega^{11}) + O(q),\\ y(\tau) &= (10+10\omega^2+\omega^3+8\omega^4+3\omega^5+6\omega^6+6\omega^7\\ &\quad +3\omega^8+8\omega^9+\omega^{10}+10\omega^{11}) + O(q),\\ x([2]\tau) &= (-1+\omega^4+\omega^6+\omega^7+\omega^9) + O(q),\\ y([2]\tau) &= (-2\omega^2-4\omega^3-7\omega^4-9\omega^5-10\omega^6-9\omega^8\\ &\quad -10\omega^7-7\omega^9-4\omega^{10}-2\omega^{11}) + O(q),\end{aligned}$$

where ω is a 13th primitive root of 1.

Using the computer algebra system Maple, we can express $x \circ [2]$ and $y \circ [2]$ as functions of x and y from their q-expansions as follows:

$$\begin{aligned}x \circ [2] &= -\frac{1}{1+x},\\ y \circ [2] &= -\frac{x-y}{x+x^2-y},\end{aligned}$$

which is the explicit form of the action of $[2]$ on the defining equation $f_{13}(x, y) = 0$ of $X_1(13)$.

If we take $W_{13} = \left(\begin{smallmatrix} 0 & -1 \\ 13 & 0 \end{smallmatrix}\right)$, then W_{13} acts on $X_1(13)$ as $W_{13}\tau = -\frac{1}{13\tau}$. In this case, we have the following

$$\begin{aligned}\wp\left(\frac{a}{13}, W_{13}\tau\right) &= (13\tau)^2\wp(a\tau, 13\tau),\\ \wp'\left(\frac{a}{13}, W_{13}\tau\right) &= (13\tau)^3\wp'(a\tau, 13\tau),\end{aligned}$$

where $a = 1, 2$. Thus, it follows that:

$$\begin{aligned}b(W_{13}\tau) &= -\frac{(\wp(\tau, 13\tau) - \wp(2\tau, 13\tau))^3}{\wp'(\tau, 13\tau)^2},\\ c(W_{13}\tau) &= -\frac{\wp'(2\tau, 13\tau)}{\wp'(\tau, 13\tau)}.\end{aligned} \tag{9}$$

Using Eqs. (8) and (9), we obtain the following q-expansions of $x(W_{13}\tau)$ and $y(W_{13}\tau)$:

$$\begin{aligned}x(W_{13}\tau) &= -1+q-q^2+q^5+O(q^6),\\ y(W_{13}\tau) &= -q+2q^2-3q^3+5q^4-8q^5+O(q^6).\end{aligned}$$

Using Maple, again, we can express $x \circ W_{13}$ and $y \circ W_{13}$ as the following functions of x and y from their q-expansions:

$$\begin{aligned}x \circ W_{13} &= \frac{-1+\omega^4+\omega^7+\omega^6+\omega^9-x}{1+(\omega^4+\omega^6+\omega^7+\omega^9)x},\\ y \circ W_{13} &= \frac{k_1+k_2x+k_3x^2+k_4y}{k_5+k_6x+k_7x^2+k_8y},\end{aligned} \tag{10}$$

where

$$(11)\quad \begin{aligned} k_1 &= 12 + 3\omega^2 - 5\omega^3 + 2\omega^4 - 2\omega^5 - 4\omega^6 - 4\omega^7 \\ &\quad - 2\omega^8 + 2\omega^9 - 5\omega^{10} + 3\omega^{11}, \\ k_2 &= -8 - 2\omega^2 - \omega^3 + 3\omega^4 - 3\omega^5 - 6\omega^6 - 6\omega^7 \\ &\quad - 3\omega^8 + 3\omega^9 - \omega^{10} - 2\omega^{11}, \\ k_3 &= -16 - 4\omega^2 + 11\omega^3 + 6\omega^4 + 7\omega^5 + \omega^6 + \omega^7 \\ &\quad + 7\omega^8 + 6\omega^9 + 11\omega^{10} - 4\omega^{11}, \\ k_4 &= 13, \\ k_5 &= -14 + 3\omega^2 + 8\omega^3 + 2\omega^4 - 2\omega^5 - 4\omega^6 - 4\omega^7 \\ &\quad - 2\omega^8 + 2\omega^9 + 8\omega^{10} + 3\omega^{11}, \\ k_6 &= 5 + 11\omega^2 + 12\omega^3 + 16\omega^4 + 10\omega^5 + 20\omega^6 \\ &\quad + 20\omega^7 + 10\omega^8 + 16\omega^9 + 12\omega^{10} + 11\omega^{11}, \\ k_7 &= 10 + 9\omega^2 - 2\omega^3 + 6\omega^4 - 6\omega^5 + \omega^6 + \omega^7 \\ &\quad - 6\omega^8 + 6\omega^9 - 2\omega^{10} + 9\omega^{11}, \\ k_8 &= -26 - 13\omega^2 - 13\omega^4 - 13\omega^5 - 26\omega^6 - 26\omega^7 \\ &\quad - 13\omega^8 - 13\omega^9 - 13\omega^{11}. \end{aligned}$$

Eq. (10) is the explicit form of the action of W_{13} on the defining equation $f_{13}(x,y) = 0$ of $X_1(13)$. In fact, the defining field of W_{13} is $\mathbf{Q}(\omega)$.

Using exactly the same method, we can derive explicit forms of the actions of the generators of $\mathrm{Aut}(X_1(N))$ on the defining equations $f_N(x,y) = 0$ of $X_1(N)$ for $N = 16, 18$.

Theorem 4.1. *The explicit forms of the actions of the automorphisms on the defining equations $f_N(x,y) = 0$ in Table I for the hyperelliptic curves $X_1(N)$ can be written as follows*:

(i) *The case $N = 13$*:

$$x \circ [2] = -\frac{1}{1+x},$$

$$y \circ [2] = -\frac{x-y}{x+x^2-y},$$

$$x \circ W_{13} = \frac{-1+\omega^4+\omega^7+\omega^6+\omega^9-x}{1+(\omega^4+\omega^6+\omega^7+\omega^9)x},$$

$$y \circ W_{13} = \frac{k_1 + k_2 u + k_3 u^2 + k_4 y}{k_5 + k_6 u + k_7 u^2 + k_8 y}.$$

(ii) *The case $N = 16$*:

$$x \circ [3] = -\frac{1}{x},$$

$$y \circ [3] = -\frac{1+y}{x^2+y},$$

$$x \circ W_{16} = \frac{(1+\omega^2-\omega^6)(1-\omega^2+\omega^6-x)}{1+\omega^2-\omega^6-x},$$

$$y \circ W_{16} = \frac{l_1 + l_2 x + l_3 x^2 + l_4 y + l_5 xy}{l_6 + l_7 x + l_8 x^2 + l_9 y + l_{10} xy}.$$

The case $N = 18$:

$$x \circ [5]W_2 = \frac{1}{1-x},$$

$$y \circ [5]W_2 = \frac{x-y}{1-y+xy},$$

$$x \circ W_9 = \frac{(1-\omega^4+\omega^5)(1-\omega-\omega^2+\omega^4-x)}{1-\omega^4+\omega^5-x},$$

$$y \circ W_9 = (2+2\omega+2\omega^2-\omega^4-\omega^5) \times \frac{2-\omega-\omega^2+2\omega^4-\omega^5-y}{2+2\omega+2\omega^2-\omega^4-\omega^5-y}.$$

For each case, ω is a primitive N-th root of unity, the k_i are as given in Eq. (11), *and*

$$\begin{aligned} l_1 &= -1 + \omega - \omega^2 + \omega^6 - \omega^7, \\ l_2 &= -4 + 5\omega - 4\omega^2 + 2\omega^3 - 2\omega^5 + 4\omega^6 - 5\omega^7, \\ l_3 &= -5 + 4\omega - 3\omega^2 + 2\omega^3 - 2\omega^5 + 3\omega^6 - 4\omega^7, \\ l_4 &= -\omega + 2\omega^2 - 2\omega^3 + 2\omega^5 - 2\omega^6 + \omega^7, \\ l_5 &= \omega - 2\omega^2 + 2\omega^3 - 2\omega^5 + 2\omega^6 - \omega^7, \\ l_6 &= 9 - 8\omega + 6\omega^2 - 3\omega^3 + 3\omega^5 - 6\omega^6 + 8\omega^7, \\ l_7 &= -4 + 2\omega - \omega^3 + \omega^5 - 2\omega^7, \\ l_8 &= 1, \\ l_9 &= 8 - 6\omega + 4\omega^2 - 3\omega^3 + 3\omega^5 - 4\omega^6 + 6\omega^7, \\ l_{10} &= 4 - 4\omega + 4\omega^2 - 3\omega^3 + 3\omega^5 - 4\omega^6 + 4\omega^7. \end{aligned}$$

Corollary 4.2. *The hyperelliptic involutions of the hyperelliptic curves $X_1(N)$ are* $[5], [7], W_2$ *for $N = 13, 16, 18$, respectively. The explicit forms of the hyperelliptic involutions on the defining equation $f_N(x,y) = 0$ in Table I for the hyperelliptic modular curves $X_1(N)$ are as follows*:

N	*explicit form*
13	$x \circ [5] = x, \quad y \circ [5] = \frac{x(x-y)}{x-y-x^2y}$
16	$x \circ [7] = x, \quad y \circ [7] = \frac{x^2}{y}$
18	$x \circ W_2 = x, \quad y \circ W_2 = \frac{1-y+xy}{1-x+xy}$

Acknowledgement. This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (2014R1A1A2056390).

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), no. 2, 413–423.

[3] D. Jeon, C. H. Kim and A. Schweizer, Bielliptic intermediate modular curves. (Preprint).

[4] C. H. Kim and J. K. Koo, The normalizer of $\Gamma_1(N)$ in $\mathrm{PSL}_2(\mathbf{R})$, Comm. Algebra **28** (2000), no. 11, 5303–5310.

[5] M.-L. Lang, Normalizer of $\Gamma_1(m)$, J. Number Theory **86** (2001), no. 1, 50–60.

[6] S. Lang, *Elliptic functions*, 2nd ed., Graduate Texts in Mathematics, 112, Springer, New York, 1987.

[7] J.-F. Mestre, Corps euclidiens, unités exceptionnelles et courbes élliptiques, J. Number Theory **13** (1981), no. 2, 123–137.

[8] F. Momose, Automorphism groups of the modular curves $X_1(N)$. (Preprint).

[9] M. A. Reichert, Explicit determination of nontrivial torsion structures of elliptic curves over quadratic number fields, Math. Comp. **46** (1986), no. 174, 637–658.

[10] A. V. Sutherland, Constructing elliptic curves over finite fields with prescribed torsion, Math. Comp. **81** (2012), no. 278, 1131–1147.