HYPERELLIPTIC MODULAR CURVES

By

N. Ishii and F. Momose

Let $N \geq 1$ be an integer, and $\Delta$ be a subgroup of $(\mathbb{Z}/N\mathbb{Z})^*$. Let $X_\Delta = X_\Delta(N)$ be the modular curve defined over $\mathbb{Q}$ associating to the modular group $\Gamma_\Delta = \Gamma_\Delta(N)$:

$$\Gamma_\Delta(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \mid c \equiv 0 \mod N, (a \mod N) \equiv \Delta \right\}.$$ 

Since $X_\Delta = X_{(\pm 1, \Delta)}$ [2], we always assume that $-1$ belongs to $\Delta$. For $\Delta = \{ \pm 1 \}$ (resp. $\Delta = (\mathbb{Z}/N\mathbb{Z})^*$), we denote $X_\Delta(N)$ by $X_\Delta(N)$ (resp. $X_\Delta(\mathbb{Q})$). Ogg [18] determined all the hyperelliptic modular curves of type $X_\Delta(N)$. This work aids the determination of the rational points on the modular curves $X_{sptet}(N)$ etc. [15, 16, 17] and that of the automorphism groups of $X_\Delta(N)$ [8], [19]. In this paper, we determine all the hyperelliptic modular curves of type $X_\Delta(N)$. There are nineteen hyperelliptic modular curves $X_\Delta(N)$ for $N = 22, 23, 26, 28, 29, 30, 31, 33, 35, 37, 39, 40, 41, 46, 47, 48, 50, 59$ and $71$ [18]. The modular curves $X_\Delta(N)$ are subcoverings of $X_\Delta(N) \rightarrow X_\Delta(N)$. Therefore it suffices to discuss the cases for the above nineteen integers $N$ and for the integers $N$ with genus of $X_\Delta(N)$ are 0 or 1 (i.e. $N = 17, 19, 20, 24, 27, 32, 36, 49; 13, 16, 18$ and 25). Our result is as follows.

**Theorem.** The hyperelliptic modular curves of type $X_\Delta(N)$ are the curves $X_\Delta(N)$ for the above nineteen integers $N$, and $X_\Delta(13), X_\Delta(16)$ and $X_\Delta(18)$.

By the above result and [18], we see that the hyperelliptic involutions of $X_\Delta(N)$ as above are represented by matrices belonging to $GL_2(\mathbb{Q})$, except for $X_\Delta(37)$ (see also [12]). Our result is used to determine the torsion points on elliptic curves defined over quadratic fields [17].

The automorphism groups Aut $X_\Delta(N)$ are determined for $X_\Delta(N)$, [3], [8], [19], and for all $\Delta$ with square free integers $N$ [13]. Except for $N = 37$ and 63 the automorphisms of $X_\Delta(N)$ with genera $\geq 2$ are represented by matrices belonging to $GL_2(\mathbb{Q})$ loc. cit.. In the final section, we determine the automorphism

Received October 31, 1990.
groups of the hyperelliptic modular curves as above.

**Notation.** Let \( Q_{p} \) denote the maximal unramified extension of \( Q_{p} \). For a positive integer \( n \), \( \zeta_{n} \) is a primitive \( n \)-th root of unity, and \( \mu_{n} \) is the group consisting of all the \( n \)-th roots of unity.

§ 1. Preliminaries

In this section, we give a review on modular curves and add the list of the hyperelliptic modular curves of type \( X_{0}(N) \) [18]. Let \( N \geq 1 \) be an integer, and \( \Delta \) be a subgroup of \( (Z/NZ)^{\times} \) containing \(-1\). Let \( X_{0}(N) \) be the modular curve defined over \( Q \) associating to the modular group \( (Z/NZ)^{\times} \)

\[
\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_{2}(Z) \mid c \equiv 0 \mod N, \; (a \mod N) \equiv \Delta \right\}
\]

Then \( X_{0}(N) \) is the coarse moduli space (over \( Q \)) of the isomorphism classes of the generalized elliptic curves \( E \) with a point \( P \mod \Delta \). We have the Galois covering

\[
X_{0}(N) \rightarrow X_{0}(N) \rightarrow X_{0}(N), \\
\langle E, \pm P \rangle \rightarrow \langle E, \Delta P \rangle \rightarrow \langle E, \langle P \rangle \rangle
\]

where \( \langle P \rangle \) is the cyclic subgroup generated by \( P \). Let \( g_{0}(N) \), \( g_{1}(N) \) and \( g_{d}(N) \) denote the genera of \( X_{0}(N) \), \( X_{1}(N) \) and \( X_{d}(N) \), respectively. Let \( Y_{0}(N) \), \( Y_{1}(N) \) and \( Y_{d}(N) \) be the open affine subschemes \( X_{0}(N) \setminus \{ \text{cusps} \} \), \( X_{1}(N) \setminus \{ \text{cusps} \} \), and \( X_{d}(N) \setminus \{ \text{cusps} \} \), respectively [2] VI (6.5). Then the covering \( Y_{1}(N) \rightarrow Y_{d}(N) \) ramifies at the points represented by the pairs \( (E, \langle P \rangle) \) with \( \text{Aut}(E, \langle P \rangle) \neq \{ \pm 1 \} \) and \( \text{Aut}(E, \pm P) = \{ \pm 1 \} \). The modular invariants of the ramification points on \( Y_{0}(N) \) are 0 or 1728.

(1.1) Let \( O = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \) and \( \infty = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \) be the \( Q \)-rational cusps on \( X_{0}(N) \) which are represented by the pairs \( (G_{m} \times Z/NZ, Z/NZ) \) and \( \{ G_{m}, \mu_{N} \} \), respectively [2] II. For a positive divisor \( d \) of \( N \) and for an integer \( i \) prime to \( d \), let \( \begin{pmatrix} i \\ d \end{pmatrix} \) denote the cusp on \( X_{0}(N) \) which is represented by \( (G_{m} \times Z/(N/d)Z, \langle \zeta_{K}, 1 \rangle) \). Then \( \begin{pmatrix} i \\ d \end{pmatrix} \) is defined over \( Q(\zeta_{n}) \) for \( n = \text{G.C.D. of } d \) and \( N/d \), and \( \begin{pmatrix} i \\ d \end{pmatrix} = \begin{pmatrix} j \\ d \end{pmatrix} \) if and only if \( i \equiv j \mod n \). The ramification index of the covering \( X_{0}(N) \rightarrow X_{0}(N) \) at the cusp \( \begin{pmatrix} i \\ d \end{pmatrix} \) is \( \text{G.C.D. of } d \) and \( N/d \). Let \( O_{i} \) (\( 1 \leq i \leq \#((Z/NZ)^{\times}/\Delta) \)) be the cusps on \( X_{0}(N) \) lying over the cusp \( O \) on \( X_{0}(N) \). Then \( O_{i} \) are all \( Q \)-rational.
We call them O-cusps.

Let $C_\infty = \left( \begin{smallmatrix} i \\ d \end{smallmatrix} \right)$ be a cusp on $X_d(N)$, and $C$ be a cusp on $X_{\Delta}(N)$ lying over $C_\infty$. We here discuss the field of definition of the cusp $C$. Put $N=d_1N_d$ for coprime divisors $d_1$ and $N_d$ such that $d$ and $d_1$ have same prime divisors. Put $\Delta_d = \{ a \mod d_1 | a \equiv 1 \mod N/d \}$, $\Delta_d' = \{ a \in (Z/d_1Z)\ast | a \equiv 1 \mod d \}$, and let $\Delta_d$ be the subgroup generated by $\Delta_d'$ and $\Delta_d'$.

**Lemma 1.2.** With the notation as above, let $k(\Delta, d)$ be the field associating to the subgroup $\Delta_d$ of $(Z/d_1Z)\ast$. Then $k(\Delta, d)$ is the field of definition of the cusp $C$. For $C = \infty$, we know $\Delta_d = \Delta$.

**Proof.** The cusp $C$ is represented by the pair

$$(G_m \times Z/(N/d)Z, (\zeta, 1) \mod \Delta)$$

for a primitive $d$-th root $\zeta = \zeta_d$ of unity (1.1). The subgroup $\Delta$ acts by $(\zeta, 1) \mapsto (\zeta^a, a)$ for $a \in \Delta$. Further, as a generalized elliptic curve, $\text{Aut}(G_m \times Z/(N/d)Z)$ is generated by $(x, i) \mapsto (\zeta x, x, i)$ and $(x, i) \mapsto (x^{-1}, -i)$ (see [2] 1).

Let $M \neq 1$ be a positive divisor of $N$ prime to $N/M$. The matrix

$$\begin{pmatrix} M & b \\ N & M \end{pmatrix}$$

for integers $a, b, c, d$ with $adM^2 - cdN = M$ defines an automorphism $w_M$ of $X_d(N)$. For a choice of a primitive $M$-th root $\zeta_M$ of unity, $w_M$ is defined by

$$(E, \pm P) \mapsto (E/P_M, \pm (P+Q_M) \mod P_M),$$

where $P_M = (N/M)P$ and $Q_M$ is a point of order $M$ such that $e_M(P_M, Q_M) = \zeta_M$ and $e_M : E_M \times E_M \to \mu_M$ is the $e_M$ (Weil)-pairing. Then $w_M$ induces the involution of $X_d(N)$ defined by

$$(E, A) \mapsto (E/A_M, (A+E_M)/A_M),$$

where $A_M$ is the cyclic subgroup of order $M$ of $A$. For an integer $i$ prime to $N$, let $[i]$ denote the automorphism of $X_d(N)$ represented by $g \in \Gamma_d(N)$ such that $g \equiv (i \ 0 \ \ast \ 0 \ 1) \mod N$, then $[i]$ acts as $(E, \pm P) \mapsto (E, \pm iP)$. We denote also by $w_M$ and $[i]$ the automorphisms of a subcovering $X_d(N)$ which are induced by $w_M$ and $[i]$, respectively.

(1.4) There are exactly nineteen values of $N$ for which $X_d(N)$ are hyperelliptic curves and they are listed in the table below [18]:
<table>
<thead>
<tr>
<th>$N$</th>
<th>genus</th>
<th>hyperelliptic involution</th>
</tr>
</thead>
<tbody>
<tr>
<td>22</td>
<td>2</td>
<td>$w_{11}$</td>
</tr>
<tr>
<td>23</td>
<td>2</td>
<td>$w_{23}$</td>
</tr>
<tr>
<td>26</td>
<td>2</td>
<td>$w_{26}$</td>
</tr>
<tr>
<td>28</td>
<td>2</td>
<td>$w_7$</td>
</tr>
<tr>
<td>29</td>
<td>2</td>
<td>$w_{29}$</td>
</tr>
<tr>
<td>30</td>
<td>3</td>
<td>$w_{15}$</td>
</tr>
<tr>
<td>31</td>
<td>2</td>
<td>$w_{31}$</td>
</tr>
<tr>
<td>33</td>
<td>3</td>
<td>$w_{11}$</td>
</tr>
<tr>
<td>35</td>
<td>3</td>
<td>$w_{25}$</td>
</tr>
<tr>
<td>37</td>
<td>2</td>
<td>$s \cdots (\ast)$</td>
</tr>
<tr>
<td>39</td>
<td>3</td>
<td>$w_{39}$</td>
</tr>
<tr>
<td>40</td>
<td>3</td>
<td>$\begin{pmatrix} -10 &amp; 1 \ -120 &amp; 10 \end{pmatrix}$</td>
</tr>
<tr>
<td>41</td>
<td>3</td>
<td>$w_{41}$</td>
</tr>
<tr>
<td>46</td>
<td>5</td>
<td>$w_{23}$</td>
</tr>
<tr>
<td>47</td>
<td>4</td>
<td>$w_{47}$</td>
</tr>
<tr>
<td>48</td>
<td>3</td>
<td>$\begin{pmatrix} -6 &amp; 1 \ -48 &amp; 6 \end{pmatrix}$</td>
</tr>
<tr>
<td>50</td>
<td>2</td>
<td>$w_{50}$</td>
</tr>
<tr>
<td>59</td>
<td>5</td>
<td>$w_{59}$</td>
</tr>
<tr>
<td>71</td>
<td>6</td>
<td>$w_{71}$</td>
</tr>
</tbody>
</table>

(\ast) $s$ is not represented by any $2 \times 2$ matrix [12] § 5, [18].

§ 2. **Hyperelliptic modular curves $X_\ell(N)$**

In this section, we determine the hyperelliptic modular curves of type $X_\ell(N)$. To determine the hyperelliptic modular curve $X_\ell(N)$ (of genus $g_\ell(N) \geq 2$), it suffices to discuss the following three cases (1), (2) and (3):

- **Case (1)** $g_\ell(N) \geq 2$ (see (1.4)).
- **Case (2)** $g_\ell(N) = 1$ ($N=17, 19, 20, 24, 27, 32, 36$ and 49)
- **Case (3)** $g_\ell(N) = 0$ ($N=13, 16, 18$ and 25)

**Theorem 2.1.** All the hyperelliptic modular curves $X_\ell(N)$ are the following twenty-two modular curves:

$$X_\ell(N) \quad \text{for the nineteen integers } N \text{ in (1.4),}$$

and
Hyperelliptic modular curves

\begin{center}
\begin{tabular}{|c|c|c|}
\hline
\text{genus} & \text{hyperelliptic involution } v \\
\hline
\text{X}_0(13) & 2 & [5] = [2]^3 \\
\text{X}_0(16) & 2 & [7] = [5]^2 \\
\text{X}_0(18) & 2 & w_2 \cdot [7] \\
\hline
\end{tabular}
\end{center}

\textbf{Proof.} Suppose that \( X_0 = X_0(N) \) has the hyperelliptic involution \( w \). Then \( w \) is defined over \( \mathbb{Q} \) and belongs to the center of \( \text{Aut} \ X_0(N) \). If moreover \( g_\delta(N) \geq 2 \), then \( w \) induces the hyperelliptic involution \( v \) of \( X_0(N) \).

\textbf{Case (1)} \( g_\delta(N) \geq 2 \): At first, we discuss the case when the hyperelliptic involutions \( v \) of \( X_0(N) \) are of type \( w_M \) (1.4). For \( N = 23, 26, 29, 31, 35, 39, 41, 47, 50, 59 \) and \( 71 \), \( v(O) = \infty \) and the cusps lying over \( \infty \) are defined over the fields associated with the subgroup \( \Delta \) of \( (\mathbb{Z}/N\mathbb{Z})^* \) by lemma 1.2. For \( N = 22, 28, 30, 33 \) and \( 46 \), by Lemma 1.2, we see that the cusps on \( X_0(N) \) lying over \( v(O) \) are not defined over \( \mathbb{Q} \) for \( \Delta \geq (\mathbb{Z}/N\mathbb{Z})^* \). Now we discuss the remaining case for \( N = 40, 48 \) and \( 37 \).

Case \( N = 40 \): The maximal subgroup of \( (\mathbb{Z}/40\mathbb{Z})^* = (\mathbb{Z}/8\mathbb{Z})^* \times (\mathbb{Z}/5\mathbb{Z})^* \) containing \( \pm 1 \) are \( \Delta_1 = \langle \pm 1, (3, 1), (-1, 1) \rangle \), \( \Delta_2 = \langle \pm 1, (3, 2) \rangle \) and \( \Delta_3 = \langle \pm 1, (1, 2) \rangle \). The hyperelliptic involution \( v \) of \( X_0(40) \) sends the cusp \( \infty \) to \( \left( \begin{smallmatrix} 1 \\ 4 \end{smallmatrix} \right) \) (1.4). The cusp \( C \) on \( X_0(40) \) lying over \( \left( \begin{smallmatrix} 1 \\ 4 \end{smallmatrix} \right) \) are all \( \mathbb{Q} \)-rational, and those lying over \( \infty \) are defined over the fields associated with the subgroups \( \Delta_i \) of \( (\mathbb{Z}/40\mathbb{Z})^* \), cf. Lemma 1.2.

Case \( N = 48 \): The maximal subgroups of \( (\mathbb{Z}/48\mathbb{Z})^* = (\mathbb{Z}/16\mathbb{Z})^* \times (\mathbb{Z}/3\mathbb{Z})^* \) are \( \Delta_1 = \langle \pm 1, (3, 1) \rangle \), \( \Delta_2 = \langle \pm 1, (9, 1), (1, -1) \rangle \) and \( \Delta_3 = \langle \pm 1, (3, -1) \rangle \). The hyperelliptic involution \( v \) of \( X_0(48) \) sends the cusp \( \infty \) to \( \left( \begin{smallmatrix} 1 \\ 8 \end{smallmatrix} \right) \) (1.4). Let \( P_t \) and \( Q_t \) be the cusps on \( X_0(48) \) lying over the cusp \( \infty \) and \( \left( \begin{smallmatrix} 1 \\ 8 \end{smallmatrix} \right) \), respectively. Then \( P_t \) are defined over real quadratic fields, cf. Lemma 1.2. But the cusp \( Q_t \) is defined over \( \mathbb{Q}(\sqrt{-2}) \), and the cusp \( Q_3 \) is defined over \( \mathbb{Q}(\sqrt{-1}) \). For \( \Delta_2 \), suppose that \( X_0(48) \) has the hyperelliptic involution \( v \), which induces the hyperelliptic involution \( w \) of \( X_0(48) \) represented by \( \left( \begin{smallmatrix} -6 & 1 \\ -48 & 6 \end{smallmatrix} \right) \) cf. (1.4). The matrix \( \left( \begin{smallmatrix} 1/0 & 1/2 \\ 0 & 1 \end{smallmatrix} \right) \) represents an automorphism \( u \) of \( X_0(48) \), and \( u \) does not commute with \( v \).

Case \( N = 37 \): The hyperelliptic involution \( s \) of \( X_0(37) \) sends the cusps to non cuspidal \( \mathbb{Q} \)-rational points, [12] §5, [18] Theorem 2. Further by [13], any automorphism of \( X_0(N) \) is represented by a matrix belonging to \( \text{GL}_3(\mathbb{R}) \) for
\[ \Delta = (\mathbb{Z}/37\mathbb{Z})^* \].

**Case (2)** \( g_\Delta(N) = 1 \): Let \( \Gamma_\Delta^*(N)/Q^* \) be the normalizer of \( \Gamma_\Delta(N)/\pm 1 \) in \( \text{PGL}_2(Q) \), and put \( B_\Delta = B_\Delta(N) = \Gamma_\Delta^*(N)/\Gamma_\Delta(N)Q^* \), which is a subgroup of \( \text{Aut} X_\Delta(N) \). For square free integers \( N \) with \( g_\Delta(N) \geq 2 \), \( B_\Delta(N) = \text{Aut} X_\Delta(N) \) except for \( X_\Delta(37) \) \[13\].

Case \( N = 17, 19 \) and \( 20 \): For \( \Delta = 1 \), \( g_\Delta(N) = 1 \). For \( N = 17 \) and \( 19 \), \( X_\Delta(N)(Q) \) consist of the \( O \)-cusps, and \( X_\Delta(20)(Q) \) consists of the \( O \)-cusps and ramified cusps \( C_1 \) and \( C_2 \) lying over the cusp \( \left( \frac{1}{2} \right) \) \[10\], Lemma 1.2. Suppose that \( X_\Delta(N) \) has the hyperelliptic involution \( v \). Then \( v \) induces an involution \( w \) of \( X_\Delta(N) \) such that \( X_\Delta(N)/\langle w \rangle \cong P_4 \), and \( w \) commutes with the automorphisms of type \( w_4 \) cf. \[1\] § 4. Then \( w \) fixes \( O \), and \( \left( \frac{1}{2} \right) \) for \( N = 20 \). For \( N = 17 \) and \( 19 \), there are not such involutions. The orbit of \( \{O, \left( \frac{1}{2} \right) \} \) under the subgroup \( \langle w_4, w \rangle \) is \( \{0, \infty, \left( \frac{1}{2} \right), \left( \frac{1}{4} \right), \left( \frac{1}{5} \right), \left( \frac{1}{10} \right) \} \), which consists of fixed points of \( w \).

This is a contradiction.

Case \( N = 21 \): The maximal subgroups of \( (\mathbb{Z}/21\mathbb{Z})^* = (\mathbb{Z}/3\mathbb{Z})^* \times (\mathbb{Z}/7\mathbb{Z})^* \) are \( \Delta_1 = \langle \pm 1, (1, -1) \rangle \), \( \Delta_2 = \langle \pm 1, (1, 2) \rangle \), and \( g_\Delta(21) = 3 \), \( g_{\Delta_2}(21) = 1 \). Suppose that \( X_\Delta \) has the hyperelliptic involution \( v \) for \( \Delta = \Delta_1 \). Then \( v \) induces the involution \( w = w_4 \) or \( w_{21} \) \[1\] § 4, \[24\] table 5. Since \( w_{21}(O) = \infty \), \( w \neq w_{21} \) cf. Lemma 1.2, hence \( w = w_4 \). But then \( v \) does not commute with \( w_4 \).

Case \( N = 24 \): Since \( X_\Delta(24)(Q) = \{ \text{cusps} \} \) \[24\] table 1, and \( \Gamma_\Delta(24)/\pm 1 \) has no elliptic element, any \( Q \)-rational automorphism of \( X_\Delta(24) \) belongs to \( B_\Delta(24) \). The maximal subgroups of \( (\mathbb{Z}/24\mathbb{Z})^* = (\mathbb{Z}/8\mathbb{Z})^* \times (\mathbb{Z}/3\mathbb{Z})^* \) are \( \Delta_1 = \langle \pm 1, (-1, 1) \rangle \), \( \Delta_2 = \langle \pm 1, (3, 1) \rangle \) and \( \Delta_3 = \langle \pm 1, (5, 1) \rangle \). For \( \Delta = \Delta_1 \) and \( \Delta_3 \), \( g_\Delta(24) = 3 \) and \( g_{\Delta_3}(24) = 1 \). Suppose \( X_\Delta \) has the hyperelliptic involution \( v \) for \( \Delta = \Delta_1 \) or \( \Delta_3 \). Since \( \left( \begin{smallmatrix} 1 & 1/2 \\ 0 & 1 \end{smallmatrix} \right) \mod \Gamma_\Delta(24) \) does not belong to \( \text{Aut} X_\Delta \), \( v \) induces the involution \( w = w_4 \) or \( w_{24} \) \[1\] § 4, \[24\] table 5. But \( w_4 \) and \( w_{24} \) are defined over \( Q(\sqrt{3}) \) for \( \Delta = \Delta_1 \). For \( \Delta = \Delta_3 \), \( w_{24} \) is defined over \( Q(\sqrt{-3}) \), hence \( w = w_4 \). Since \( X_\Delta(Q) \) consists of the \( O \)-cusps and ramified cusps \( C_1, C_3, C_5, C_4 \), \( w = w_4 \) must fix the \( O \)-cusps. This is a contradiction.

Case \( N = 27 \): For \( \Delta \neq \{ \pm 1 \} \), \( g_\Delta(27) = 1 \), and \( g_{\Delta_3}(27) = 3 \). Let \( \mathfrak{X} = \mathfrak{X}_i(27) \) be the normalization of the projective \( j \)-line in the function field of \( X_\Delta(27) \). Then
\#J'(F_5) \geq \#\{O\text{-cusps}\}=9, \text{ so that } X_i(27) \text{ is not hyperelliptic cf. } [18].

Case \(N=32\): \text{ For } \Delta'=\langle \pm 1, 1 \rangle, \ g_{\Delta'}(32)=5, \text{ and for } \Delta''=\langle \pm 1, 1+8 \rangle, \ g_{\Delta''}(32)=1. \text{ Let } J', J'' \text{ be the jacobian varieties of } X_{\Delta'}, \text{ and } X_{\Delta''} \text{ respectively. Then } J'=J''+A \text{ for an abelian variety } A/(Q) \text{ of dimension } 4. \text{ The involution [9] acts by } +1 \text{ on } J'', \text{ and by } -1 \text{ on } A. \text{ If } X_{\Delta'}, \text{ has the hyperelliptic involution } \nu, \text{ then } [9] \nu \text{ acts by } -1 \text{ on } J'', \text{ and } +1 \text{ on } A. \text{ But there is not such an involution. It is easily seen by Riemann-Hurwitz formula.}

Case \(N=36\): \text{ The maximal subgroups of } (\mathbb{Z}/36\mathbb{Z})^*=(\mathbb{Z}/4\mathbb{Z})^* \times (\mathbb{Z}/9\mathbb{Z})^* \text{ are } \Delta_1=\langle \pm 1, (1, 4) \rangle, \Delta_2=\langle \pm 1, (1, -1) \rangle, \text{ and } g_{\Delta_1}=3, g_{\Delta_2}=7. \text{ Suppose } X_h \text{ has the hyperelliptic involution } \nu. \text{ Then } \nu \text{ induces an involution } w \text{ of } X_i(36). \text{ At first, we discuss for } \Delta=\Delta_1. \text{ The set } X_{\Delta_1}(Q) \text{ consists of the } O\text{-cusps and ramified cusps } C_i, C_2 \text{ cf. } [24] \text{ table 1.2. Then } w \text{ fixes the set of } O\text{-cusps.}

The matrix \(\begin{pmatrix} 1 & 1/3 \\ 0 & 1 \end{pmatrix}\) represents an automorphism \(g \) of \(X_{\Delta_1}\), and the orbit of \(O\) under the subgroup \(\langle g, w, w^2 \rangle \) is \(S=\{0, \infty, (\pm 1, 3), (1, 4), (\pm 1, 12)\}\). \text{ Then } w \text{ must have more than } \#S=8 \text{ fixed points, which is a contradiction. Now consider the case for } \Delta=\Delta_2. \text{ The set } X_{\Delta_2}(Q) \text{ consists of the } O\text{-cusps and the cusps lying over the cusps } \left(\frac{1}{2}\right), \left(\frac{1}{4}\right), \text{ cf. Lemma 1.2. Then } \nu \text{ fixes a rational points on } X_{\Delta_2}, \text{ since } \#X_{\Delta_2}(Q)=9. \text{ The matrix } \begin{pmatrix} 1 & 1/2 \\ 0 & 1 \end{pmatrix} \text{ represents an automorphism } g \text{ of } X_{\Delta_2}, \text{ and the subgroup } \langle g, w, \gamma \rangle \text{ acts transitively on } X_{\Delta_2}(Q), \text{ where } \gamma \text{ is a generator of the covering group of } X_{\Delta_2} \to X_i(36). \text{ Thus } \nu \text{ fixes all the points belonging to } X_{\Delta_2}(Q) \text{ and } w_3(X_{\Delta_2}(Q)). \text{ This contradicts to } g_{\Delta_2}(36)=7.

Case \(N=49\): \text{ Let } \Delta_n \text{ be the maximal subgroups of } (\mathbb{Z}/49\mathbb{Z})^* \text{ of indices } n=3, 7. \text{ Let } X_\Delta \text{ be the normalization of the projective } j\text{-line } X_\Delta(1) \cong P_\delta \text{ in the function field of } X_\Delta. \text{ For } \Delta=\Delta_n, \text{ the cusps on } X_\Delta \text{ are all defined over } Q(\zeta), \text{ so that } \#X_\Delta(F_5) \geq 24. \text{ For } \Delta=\Delta_1, \#X_\Delta(F_5) \geq 7. \text{ Therefore } X_{\Delta_n} \text{ are not hyperelliptic cf. } [18].

Case (3) \(g_\delta(N)=0\): \text{ For } \Delta=\{\pm 1\}, \ X_\Delta=P_\delta. \text{ For } N=13, 16 \text{ and } 18, [5], [7] \text{ and } w_2[7] \text{ are the hyperelliptic involutions of } X_i(N), \text{ respectively. There remains the case for } N=25. \text{ Let } \Delta_n \text{ be the maximal subgroups of } (\mathbb{Z}/25\mathbb{Z})^* \text{ of index } n=2, 5. \text{ Then } g_{\Delta_2}(25)=0 \text{ and } g_{\Delta_5}(25)=4. \text{ We know that } X_{\Delta_2}(Q) \text{ consists of the } O\text{-cusps } [6]. \text{ Suppose that } X=X_{\Delta_2} \text{ has the hyperelliptic involution } \nu. \text{ Then } \nu \text{ fixes a } O\text{-cusp, hence } \nu \text{ fixes all the } O\text{-cusps. Then the divisor class } cl((O')-(O^*)) \text{ are of order } 2 \text{ for the } O\text{-cusps } O' \text{ and } O^*, \text{ } O' \neq O^*. \text{ But we know that the Mordell-Weil group of the jacobian variety of } X \text{ is isomorphic to}
§ 3. Automorphism groups of hyperelliptic curves $X_6(N)$

In this section, we determined the automorphism groups of hyperelliptic modular curves of type $X_6(N)$. For square free integers $N$, $\text{Aut } X_6(N)$ are determined [13], [19]. Hence it suffices to discuss for $X_6(16)$ and $X_6(18)$ cf. Theorem 2.1.

**Theorem 3.1.** The automorphisms of $X_6(16)$ and $X_6(18)$ are represented by $2 \times 2$ matrices.

**Proof.**

Case $N=18$: Let $X$ be the minimal model of $X_6(18) (\mathbb{Z})$. The special fibre $X \otimes \mathbb{F}_p$ has two irreducible components $Z, Z'$ which are isomorphic to $\mathbb{P}^1$ and intersect transversally at three supersingular points $S_1, S_2$ and $S_3$ [2]. Let $v=w_6[7]$ be the hyperelliptic involution of $X_6(18)$. Since the Jacobian variety $J_6(18)$ of $X_6(18)$ has stable reduction at the rational prime $2$ [2], any endomorphism of $J_6(18)$ is defined over $\mathbb{Q}$ [22] Lemma 1. Let $G$ be the subgroup of $\text{Aut } X_6(18)$ consisting of automorphisms $g$ which fix the irreducible component $Z$. Then we see that the representation of $G$ into the permutation group $S_3$ of the set $\{S_1, S_2, S_3\}$ is faithful. Thus we see that $G=\langle w_6, [7] \rangle$. Further $w_6$ exchanges $Z$ by $Z'$. Thus $\text{Aut } X_6(18)$ is generated by $w_6, w_9$ and [7].

Case $N=16$: The hyperelliptic involution $v=\tau^6$ for $\tau=[3]$. Put $X=X_6(16)$ and $Y=X/(\tau)$. Let $C_1, C_2$ (resp. $C_3, C_4$) be the cusps on $X$ lying over the cusp $\left(\frac{1}{2}\right)$ (resp. $\left(\frac{1}{8}\right)$). Then $C_i$ are the ramification points of the covering $X \rightarrow Y$. Let $P_1, P_2$ be the totally ramified cusps lying over $\left(\frac{1}{4}\right)$ and $\left(-\frac{1}{4}\right)$, respectively. Let $S_6$ be the set of the Weierstrass points of $X$: $S_6=\{P_1, P_2, C_1, C_2, C_3, C_4\}$, and let $S_8$ be the permutation group of the elements of $S_6$. Then $\langle \text{Aut } X \rangle/(\tau)$ becomes a subgroup of $S_8$.

**Lemma 3.2.** \(\{g \in \text{Aut } X \mid g \gamma g^{-1} = \gamma^{x_1}\} = \langle \gamma, w_{16} \rangle\).

**Proof.** We can take a local parameter $x$ along the cusp $\infty$ of $X_6(16)$ such that the modular invariant $j=F(x)/G(x)$ for $F(x)=x^8+2^4x^7+7.2^4x^6+7.2^4x^5+69.2^4x^4+13.2^4x^3+11.2^4x^2+2^3x+1$ and $G(x)=x(x+4)(x^8+4x+8)(x+2)^4$ [3] Kapitel IV. Further the values $x=0, -2, -2+2\sqrt{-1}, -2-2\sqrt{-1}$ and $-4$
corresponds to the cusps \( \infty, \left( \frac{1}{2} \right), \left( \frac{1}{4} \right), \left( -\frac{1}{4} \right) \) and \( \left( \frac{1}{8} \right) \), respectively. If \( g \gamma g^{-1} = \gamma \), then \( g \) induces an automorphism of \( h \) of \( X_0(16) = P^1(x) \), and \( h^* \) sends the set \( \{-4, -2\} \) and \( \{-2 \pm 2\sqrt{-1}\} \) to themselves. If \( h^*(-4) = -2 \), then \( w_{16} h^* \) fixes both \(-4\) and \(-2\). Changing \( g \) by \( gw_{16} \), if necessary, we may assume that \( h^* \) fixes both \(-4\) and \(-2\). Let \( \delta \) be the automorphism of \( P^1(x) \) defined by \( \delta^*(x) = x^4/x + 2 \), then \( \delta^*(-2 + 2\sqrt{-1}) = 1 - \sqrt{-1}, \delta^*(-2 - 2\sqrt{-1}) = 1 + \sqrt{-1}, \) and \((\delta h \delta^{-1})^*(x) = ax \) for some \( a \in \mathbb{C} \). If \( a \neq 1 \), then \( a(1 + \sqrt{-1}) = 1 - \sqrt{-1} \), so that \( a = -\sqrt{-1} \). But then \( 1 + \sqrt{-1} = (\delta h \delta^{-1})^*(1 - \sqrt{-1}) = (-\sqrt{-1})(1 - \sqrt{-1}) \). Therefore \( a = 1 \), i.e., \( h = id \) and \( g \) belongs to \( \langle \gamma \rangle \).

At first, we show that any 2-sylow subgroup \( H \) of \( G = \text{Aut} X \) containing \( \gamma \) and \( w_{16} \) is equal to the subgroup \( \langle w_{16}, \gamma \rangle \), which is a dihedral group with relation \( w_{16}^2 \gamma w_{16} = \gamma^{-1} \). If \( \#H \neq 8 \), then \( G \) has a subgroup \( K \) of order 16 containing \( \langle w_{16}, \gamma \rangle \). Then \( \langle \gamma \rangle \) is a normal subgroup of \( K \), since \( \langle \gamma \rangle \) is the unique cyclic subgroup of order 4 of \( \langle w_{16}, \gamma \rangle \). Then by Lemma 3.2, any \( g \in K \) belongs to \( \langle w_{16}, \gamma \rangle \). It is a contradiction. Now we show that \( G \) is a 2-group. The prime divisors of \( \#G \) are 2, 3 or 5. If \( g \in G \) is of order 5, then \( g \) fixes a Weierstrass point \( C \), which is defined over \( Q(\zeta_{15}) \). Let \( t \) be a local parameter along \( C \). Then \( g^*(t) = \zeta_t + a \theta t^2 + \cdots \) for a primitive 5-th root \( \zeta_t \) of unity, so that \( g \) is not defined over \( Q^\theta \). But we know that any endomorphism of the jacobian variety of \( X \) is defined over \( Q^\theta \) for any prime number \( p \neq 2 \) [2], [22] Lemma 1. Suppose that an automorphism \( g \in G \) is of order 3. By the same way as above, we see that \( g \) does not fix any Weierstrass point. Changing the induces of \( \{P_1\}, \{C_1, C_2\} \) and \( \{C_3, C_4\} \), if necessary, we may assume that \( (1) \ g(P_1) = P_2 \) or \( (2) \ g(P_2) = C_1 \).

Claim. \( g(P_1) \neq P_2 \).

We know that \( \gamma = C_1, C_2, C_3, C_4 \mod \langle v \rangle \). If \( g(P_1) = P_2 \), then \( g \gamma g \mod \langle v \rangle \) is of order 5, so that \( g(P_1) \neq P_2 \).

Put \( h = g \gamma g^{-1} \), which fixes the \( Q \)-rational cusp \( C_1 \). Let \( t \) be a local parameter along \( C_1 \). Then \( h^*(t) = \pm \sqrt{-1} t + \cdots \in Q(\sqrt{-1})[[t]] \), and \( h \) is defined over \( Q(\sqrt{-1}) \). For any \( \sigma \in \text{Gal}(\overline{Q}/Q) \), \( h^\sigma = h^{-1} \), so that \( g^\sigma g^{-1} \) belongs to \( \langle w_{16}, \gamma \rangle \) by Lemma 3.2. Since \( g^\sigma g^{-1} \) fixes the \( Q \)-rational cusp \( C_1 \), \( g^\sigma g^{-1} = v \). Then \( (g^\sigma)^2 = g^2 \). Since \( g \) is of order 3, \( g^\sigma = g \), so that \( g \) is defined over \( Q \). But we know that \( \text{End}_Q J_1(16) \otimes Q = Q(\sqrt{-1}) \) [14], [20, 21], where \( \text{End}_Q \cdots \) is the subring consisting of the endomorphisms defined over \( Q \). Thus \( \text{Aut} X \) is a 2-group. \( \square \)
References


Hyperelliptic modular curves

N. Ishii
Dokkyo Secondary High School
1-8, Sekiguchi, Bunkyo-ku
Tokyo 112, Japan

F. Momose
Department of Mathematics
Chuo University
1-13-27 Kasuga, Bunkyo-ku
Tokyo 112, Japan