TSUKUBA J. MATH.
Vol. 15 Nol 2 (1991), 413–423

HYPERELLIPTIC MODULAR CURVES

By

N. ISHII and F. MOMOSE

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

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

Since $X_{\Delta}=X_{\langle\pm 1,\Delta\rangle}$ [2], we always assume that -1 belongs to Δ. For $\Delta=\{\pm 1\}$ (resp. $\Delta=(\boldsymbol{Z}/N\boldsymbol{Z})^{\times}$), we denote $X_{\Delta}(N)$ by $X_1(N)$ (resp. $X_0(N)$). Ogg [18] determined all the hyperelliptic modular curves of type $X_0(N)$. This work aids the determination of the rational points on the modular curves $X_{split}(N)$ etc. [15, 16, 17] and that of the automorphism groups of $X_0(N)$ [8], [19]. In this paper, we determine all the hyperelliptic modular curves of type $X_{\Delta}(N)$. There are nineteen hyperelliptic modular curves $X_0(N)$ 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 $X_1(N)\rightarrow X_0(N)$. Therefore it suffices to discuss the cases for the above nineteen integers N and for the integers N with genus of $X_0(N)$ 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 $X_0(N)$ for the above nineteen integers N, and $X_1(13)$, $X_1(16)$ and $X_1(18)$.*

By the above result and [18], we see that the hyperelliptic involutions of $X_{\Delta}(N)$ as above are represented by matrices belonging to $\mathrm{GL}_2^+(\boldsymbol{Q})$, except for $X_0(37)$ (see also [12]). Our result is used to determine the torsion points on elliptic curves defined over quadratic fields [17].

The automorphism groups $\mathrm{Aut}\,X_{\Delta}(N)$ are determined for $X_0(N)$, [3], [8], [19], and for all Δ with square free integers N [13]. Except for $N=37$ and 63 the automorphisms of $X_0(N)$ with genera $\geqq 2$ are represented by matrices belonging to $\mathrm{GL}_2^+(\boldsymbol{Q})$ 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^{ur} denote the maximal unramified extension of Q_p. For a positive integer n, ζ_n is a primitive n-th root of unity, and μ_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 $N \geqq 1$ be an integer, and Δ be a subgroup of $(Z/NZ)^\times$ containing -1. Let $X_\Delta = X_\Delta(N)$ be the modular curve defined over Q associating to the modular group $\Gamma_\Delta(N)$:

$$\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(Z) \mid c \equiv 0 \bmod N,\ (a \bmod N) \in \Delta\right\}$$

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

$$X_1(N) \longrightarrow X_\Delta(N) \longrightarrow X_0(N),$$

$$(E, \pm P) \longmapsto (E, \Delta P) \longmapsto (E, \langle P \rangle)$$

where $\langle P \rangle$ is the cyclic subgroup generated by P. Let $g_\Delta(N)$, $g_1(N)$ and $g_0(N)$ denote the genera of $X_\Delta(N)$, $X_1(N)$ and $X_0(N)$, respectively, Let $Y_\Delta(N)$, $Y_1(N)$ and $Y_0(N)$ be the open affine subschemes $X_\Delta(N) \setminus \{\text{cusps}\}$ $X_1(N) \setminus \{\text{cusps}\}$, and $X_0(N) \setminus \{\text{cusps}\}$, respectively [2] VI (6.5). Then the covering $Y_1(N) \to Y_0(N)$ ramifies at the points represented by the pairs $(E, \langle P \rangle)$ with $\mathrm{Aut}(E, \langle P \rangle) \neq \{\pm 1\}$ and $\mathrm{Aut}(E, \pm P) = \{\pm 1\}$. The modular invariants of the remification points on $Y_0(N)$ are 0 or 1728.

(1.1) Let $\mathbf{0} = \binom{0}{1}$ and $\infty = \binom{1}{0}$ 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 $\binom{i}{d}$ denote the cusp on $X_0(N)$ which is represented by $(G_m \times Z/(N/d)Z, \langle \zeta_N^i, 1 \rangle)$. Then $\binom{i}{d}$ is defined over $Q(\zeta_n)$ for $n =$ G.C.D. of d and N/d, and $\binom{i}{d} = \binom{j}{d}$ if and only if $i \equiv j \bmod n$. The ramification index of the covering $X_1(N) \to X_0(N)$ at the cusp $\binom{i}{d}$ is G.C.D. of d and N/d. Let $\mathbf{0}_i$ $(1 \leqq i \leqq \#((Z/NZ)^\times/\Delta))$ be the cusps on $X_\Delta(N)$ lying over the cusp $\mathbf{0}$ on $X_0(N)$. Then $\mathbf{0}_i$ are all Q-rational.

We call them **0**-cusps.

Let $C_0=\binom{i}{d}$ be a cusp on $X_0(N)$, and C be a cusp on $X_\Delta(N)$ lying over C_0. We here discuss the field of definition of the cusp C. Put $N=d_1\cdot N_d$ for coprime divisors d_1 and N_d such that d and d_1 have same prime divisors. Put $\Delta_d'=\{a \bmod d_1 \mid a\in\Delta,\ a\equiv 1 \bmod N/d\}$, $\Delta_d''=\{a\in(\boldsymbol{Z}/d_1\boldsymbol{Z})^\times \mid a\equiv 1 \bmod d\}$, and let Δ_d be the subgroup generated by Δ_d' and Δ_d''.

LEMMA 1.2. *With the notation as above, let $k(\Delta, d)$ be the field associating to the subgroup Δ_d of $(\boldsymbol{Z}/d_1\boldsymbol{Z})^\times$. 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

$$(\mathbf{G}_m\times \boldsymbol{Z}/(N/d)\boldsymbol{Z},\ (\zeta, 1) \bmod \Delta)$$

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

(1.3) Let $M\neq 1$ be a positive divisor of N prime to N/M. The matrix $\begin{pmatrix} Ma & b \\ Nc & Md\end{pmatrix}$ for integers a, b, c, d with $adM^2-cdN=M$ defines an automorphism w_M of $X_1(N)$. For a choice of a primitive M-th root ζ_M of unity. w_M is defined by

$$(E, \pm P)\longmapsto(E/\langle P_M\rangle,\ \pm(P+Q_M) \bmod \langle P_M\rangle)\,,$$

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 $X_0(N)$ defined by

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

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 $X_1(N)$ represented by $g\in\Gamma_0(N)$ such that $g\equiv\begin{pmatrix} i & * \\ 0 & *\end{pmatrix} \bmod N$, then $[i]$ acts as $(E, \pm P)\mapsto(E, \pm iP)$. We denote also by w_M and $[i]$ the automorphisms of a subcovering $X_\Delta(N)$ which are induced by w_M and $[i]$, respectively.

(1.4) There are exactly nineteen values of N for which $X_0(N)$ are hyperelliptic curves and they are listed in the table below [18]:

N	genus	hyperelliptic involution
22	2	w_{11}
23	2	w_{23}
26	2	w_{26}
28	2	w_7
29	2	w_{29}
30	3	w_{15}
31	2	w_{31}
33	3	w_{11}
35	3	w_{35}
37	2	$s \cdots (*)$
39	3	w_{39}
40	3	$\begin{pmatrix} -10 & 1 \\ -120 & 10 \end{pmatrix}$
41	3	w_{41}
46	5	w_{23}
47	4	w_{47}
48	3	$\begin{pmatrix} -6 & 1 \\ -48 & 6 \end{pmatrix}$
50	2	w_{50}
59	5	w_{59}
71	6	w_{71}

(*) s is not represented by any 2×2 matrix [12] §5, [18].

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

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

Case (1) $g_0(N)\geqq 2$ (see (1.4)).

Case (2) $g_0(N)=1$ (N=17, 19, 20, 24, 27, 32, 36 and 49)

Case (3) $g_0(N)=0$ (N=13, 16, 18 and 25)

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

$X_0(N)$ *for the nineteen integers N in* (1.4),

and

	genus	hyperelliptic involution v
$X_1(13)$	2	$[5]=[2]^3$
$X_1(16)$	2	$[7]=[5]^2$
$X_1(18)$	2	$w_2\circ[7]$

PROOF. Suppose that $X_\Delta=X_\Delta(N)$ has the hyperelliptic involution w. Then w is defined over $\boldsymbol{Q}$ and belongs to the center of Aut $X_\Delta(N)$. If moreover $g_0(N)\geqq 2$, then w induces the hyperelliptic involution v of $X_0(N)$.

CASE (1) $g_0(N)\geqq 2$: 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, $v(\mathbf{0})=\infty$ and the cusps lying over ∞ are defined over the fields associated with the subgroup Δ of $(\boldsymbol{Z}/N\boldsymbol{Z})^\times$ by lemma 1.2. For $N=22$, 28, 30, 33 and 46, by Lemma 1.2, we see that the cusps on $X_\Delta(N)$ lying over $v(\mathbf{0})$ are not defined over $\boldsymbol{Q}$ for $\Delta\neq(\boldsymbol{Z}/N\boldsymbol{Z})^\times$. Now we discuss the remaining case for $N=40$, 48 and 37.

Case $N=40$: The maximal subgroup of $(\boldsymbol{Z}/40\boldsymbol{Z})^\times=(\boldsymbol{Z}/8\boldsymbol{Z})^\times\times(\boldsymbol{Z}/5\boldsymbol{Z})^\times$ containing ± 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 ∞ to $\left(\frac{1}{4}\right)$ (1.4). The cusp C on X_{Δ_i} lying over $\left(\frac{1}{4}\right)$ are all $\boldsymbol{Q}$-rational, and those lying over ∞ are defined over the fields associated with the subgroups Δ_i of $(\boldsymbol{Z}/40\boldsymbol{Z})^\times$, cf. Lemma 1.2.

Case $N=48$: The maximal subgroups of $(\boldsymbol{Z}/48\boldsymbol{Z})^\times=(\boldsymbol{Z}/16\boldsymbol{Z})^\times\times(\boldsymbol{Z}/3\boldsymbol{Z})^\times$ are $\Delta_1=\langle\pm 1, (3, 1)\rangle$, $\Delta_2=\langle\pm 1, (9, 1), (1, -1)\rangle$ and $\Delta_3=\langle\pm 1, (3, -1)\rangle$. Tne hyperelliptic involution v of $X_0(48)$ sends the cusp ∞ to $\left(\frac{1}{8}\right)$ (1.4). Let P_i and Q_i be the cusps on X_{Δ_i} lying over the cusp ∞ and $\left(\frac{1}{8}\right)$, respectively. Then P_i are defined over real quadratic fields, cf. Lemma 1.2. But the cusp Q_1 is defined over $\boldsymbol{Q}(\sqrt{-2})$, and the cusp Q_3 is defined over $\boldsymbol{Q}(\sqrt{-1})$. For Δ_2, suppose that X_{Δ_2} has the hyperelliptic involution v, which induces the hyperelliptic involution w of $X_0(48)$ represented by $\begin{pmatrix}-6 & 1\\ -48 & 6\end{pmatrix}$ cf. (1.4). The matrix $\begin{pmatrix}1 & 1/2\\ 0 & 1\end{pmatrix}$ represents an automorphism u of X_{Δ_2}, and u does not commute with v.

Case $N=37$: The hyperelliptic involution s of $X_0(37)$ sends the cusps to non cuspidal $\boldsymbol{Q}$-rational points, [12] § 5, [18] Theorem 2. Further by [13], any automorphism of $X_\Delta(N)$ is represented by a matrix belonging to $\mathrm{GL}_2^+(\boldsymbol{R})$ for

$\Delta\neq(\boldsymbol{Z}/37\boldsymbol{Z})^{\times}$.

Case (2) $g_0(N)=1$: Let $\Gamma_{\Delta}^{*}(N)/\boldsymbol{Q}^{\times}$ be the normalizer of $\Gamma_{\Delta}(N)/\pm1$ in $\mathrm{PGL}_2^{+}(\boldsymbol{Q})$, and put $B_{\Delta}=B_{\Delta}(N)=\Gamma_{\Delta}^{*}(N)/\Gamma_{\Delta}(N)\boldsymbol{Q}^{\times}$, which is a subgroup of $\mathrm{Aut}\,X_{\Delta}(N)$. For square free integers N with $g_{\Delta}(N)\geqq 2$, $B_{\Delta}(N)=\mathrm{Aut}\,X_{\Delta}(N)$ except for $X_0(37)$ [13].

Case $N=17$, 19 and 20: For $\Delta\neq\{\pm1\}$, $g_{\Delta}(N)=1$. For $N=17$ and 19, $X_1(N)(\boldsymbol{Q})$ consist of the $\boldsymbol{O}$-cusps, and $X_1(20)(\boldsymbol{Q})$ consists of the $\boldsymbol{O}$-cusps and ramified cusps C_1 and C_2 lying over the cusp $\binom{1}{2}$ [10], Lemma 1.2. Suppose that $X_1(N)$ has the hyperelliptic involution v. Then v induces an involution w of $X_0(N)$ such that $X_0(N)/\langle w\rangle\simeq \boldsymbol{P}^1_{\boldsymbol{Q}}$, and w commutes with the automorphisms of type w_M cf. [1] §4. Then w fixes $\mathbf{O}$, and $\binom{1}{2}$ for $N=20$. For $N=17$ and 19, there are not such involutions. The orbit of $\left\{\mathbf{O},\binom{1}{2}\right\}$ under the subgroup $\langle w_4, w_5\rangle$ is $\left\{\mathbf{O}, \infty, \binom{1}{2}, \binom{1}{4}, \binom{1}{5}, \binom{1}{10}\right\}$, which consists of fixed points of w. This is a contradiction.

Case $N=21$: The maximal subgroups of $(\boldsymbol{Z}/21\boldsymbol{Z})^{\times}=(\boldsymbol{Z}/3\boldsymbol{Z})^{\times}\times(\boldsymbol{Z}/7\boldsymbol{Z})^{\times}$ are $\Delta_1=\langle\pm1, (1, -1)\rangle$, $\Delta_2=\langle\pm1, (1, 2)\rangle$, and $g_{\Delta_1}(21)=3$, $g_{\Delta_2}(21)=1$. Suppose that X_{Δ} has the hyperelliptic involution v for $\Delta=\Delta_1$. Then v induces the involution $w=w_3$ or w_{21} [1] §4, [24] table 5. Since $w_{21}(\mathbf{O})=\infty$, $w\neq w_{21}$ cf. Lemma 1.2, hence $w=w_3$. But then v dose not commutes with w_7.

Case $N=24$: Since $X_0(24)(\boldsymbol{Q})=\{\text{cusps}\}$ [24] table 1, and $\Gamma_0(24)/\pm1$ has no elliptic element, any $\boldsymbol{Q}$-rational automorphism of $X_0(24)$ belongs to $B_0(24)$. The maximal subgroups of $(\boldsymbol{Z}/24\boldsymbol{Z})^{\times}=(\boldsymbol{Z}/8\boldsymbol{Z})^{\times}\times(\boldsymbol{Z}/3\boldsymbol{Z})^{\times}$ are $\Delta_1=\langle\pm1, (-1, 1)\rangle$, $\Delta_2=\langle\pm1, (3, 1)\rangle$ and $\Delta_3=\langle\pm1, (5, 1)\rangle$. For $\Delta=\Delta_1$ and Δ_2, $g_{\Delta}(24)=3$ and $g_{\Delta_3}(24)=1$. Suppose X_{Δ} has the hyperelliptic involution v for $\Delta=\Delta_1$ or Δ_2. Since $\begin{pmatrix}1 & 1/2\\ 0 & 1\end{pmatrix}$ $\bmod \Gamma_{\Delta}(24)$ does not belong to $\mathrm{Aut}\,X_{\Delta}$, v induces the involution $w=w_8$ or w_{24} [1] §4, [24] table 5. But w_8 and w_{24} are defined over $\boldsymbol{Q}(\sqrt{2})$ for $\Delta=\Delta_1$. For $\Delta=\Delta_2$, w_{24} is defined over $\boldsymbol{Q}(\sqrt{-3})$, hence $w=w_8$. Since $X_{\Delta}(\boldsymbol{Q})$ consisits of the $\mathbf{O}$-cusps and ramified cusps C_1, C_2, C_3, C_4, $w=w_8$ must fix the $\mathbf{O}$-cusps. This is a contradiction.

Case $N=27$: For $\Delta\neq\{\pm1\}$, $g_{\Delta}(27)=1$, and $g_1(27)=3$. Let $\mathscr{X}=\mathscr{X}_1(27)$ be the normalization of the projective j-line in the function field of $X_1(27)$. Then

$\#\mathscr{X}(\boldsymbol{F}_2)\geqq\#\{\mathrm{O}\text{-cusps}\}=9$, so that $X_1(27)$ is not hyperelliptic cf. [18].

Case $N=32$: For $\Delta'=\langle\pm1, 1+16\rangle$, $g_{\Delta'}(32)=5$, and for $\Delta''=\langle\pm1, 1+8\rangle$, $g_{\Delta''}(32)=1$. Let J', J'' be the jacobian varieties of $X_{\Delta'}$ and $X_{\Delta''}$ respectively. Then $J'=J''+A$ for an abelian variety $A(/\boldsymbol{Q})$ of dimension 4. The involution [9] acts by $+1$ on J'', and by -1 on A. If $X_{\Delta'}$ has the hyperelliptic involution v, then [9] v acts by -1 on J'', and $+1$ on A. But there is not such an involution. It is easily seen by Riemann-Hurwitz formula.

Case $N=36$: The maximal subgroups of $(\boldsymbol{Z}/36\boldsymbol{Z})^\times=(\boldsymbol{Z}/4\boldsymbol{Z})^\times\times(\boldsymbol{Z}/9\boldsymbol{Z})^\times$ are $\Delta_1=\langle\pm1, (1, 4)\rangle$, $\Delta_2=\langle\pm1, (1, -1)\rangle$, and $g_{\Delta_1}=3$, $g_{\Delta_2}=7$. Snppose X_Δ has the hyperelliptic involution v. Then v induces an involution w of $X_0(36)$. At first, we discuss for $\Delta=\Delta_1$. The set $X_{\Delta_1}(\boldsymbol{Q})$ consists of the O-cusps and ramified cusps C_1, C_2 cf. [24] table 1, Lemma 1.2. Then w fixes the set of O-cusps. The matrix $\begin{pmatrix}1 & 1/3\\ 0 & 1\end{pmatrix}$ represents an automorphism g of X_{Δ_1}, and the orbit of O under the subgroup $\langle g, w_4, w_9\rangle$ is $S=\left\{\mathrm{O}, \infty, \begin{pmatrix}\pm1\\ 3\end{pmatrix}, \begin{pmatrix}1\\ 9\end{pmatrix}, \begin{pmatrix}1\\ 4\end{pmatrix}, \begin{pmatrix}\pm1\\ 12\end{pmatrix}\right\}$. Then w must have more than $\#S=8$ fixed points, which is a contradiction. Now consider the case for $\Delta=\Delta_2$. The set $X_{\Delta_2}(\boldsymbol{Q})$ consists of the O-cusps and the cusps lying over the cusps $\begin{pmatrix}1\\ 2\end{pmatrix}, \begin{pmatrix}1\\ 4\end{pmatrix}$, cf. Lemma 1.2. Then v fixes a rational points on X_{Δ_2}, since $\#X_{\Delta_2}(\boldsymbol{Q})=9$. The matrix $\begin{pmatrix}1 & 1/2\\ 0 & 1\end{pmatrix}$ represents an automorphism g of X_{Δ_2}, and the subgroup $\langle g, w_4, \gamma\rangle$ acts transitively on $X_{\Delta_2}(\boldsymbol{Q})$, where γ is a generator of the covering group of $X_{\Delta_2}\to X_0(36)$. Thus v fixes all the points belonging to $X_{\Delta_2}(\boldsymbol{Q})$ and $w_9(X_{\Delta_2}(\boldsymbol{Q}))$. This contradicts to $g_\Delta(36)=7$.

Case $N=49$: Let Δ_n be the maximal subgroups of $(\boldsymbol{Z}/49\boldsymbol{Z})^\times$ of indices $n=3, 7$. Let $\mathscr{X}_\Delta$ be the normalization of the projective j-line $\mathscr{X}_0(1)\cong\boldsymbol{P}^1_{\boldsymbol{Q}}$ in the function field of X_Δ. For $\Delta=\Delta_3$, the cusps on X_Δ are all defined over $\boldsymbol{Q}(\zeta_7)$, so that $\#\mathscr{X}_\Delta(\boldsymbol{F}_8)\geqq24$. For $\Delta=\Delta_7$, $\#\mathscr{X}_\Delta(\boldsymbol{F}_2)\geqq7$. Therefore X_{Δ_n} are not hyperelliptic cf. [18].

Case (3) $g_0(N)=0$: For $\Delta\neq\{\pm1\}$, $X_\Delta=\boldsymbol{P}^1_{\boldsymbol{Q}}$. For $N=13$, 16 and 18, [5], [7] and w_2[7] are the hyperelliptic involutions of $X_1(N)$, respectively. There remains the case for $N=25$. Let Δ_n be the maximal subgroups of $(\boldsymbol{Z}/25\boldsymbol{Z})^\times$ of index $n=2, 5$. Then $g_{\Delta_2}(25)=0$ and $g_{\Delta_5}(25)=4$. We know that $X_{\Delta_5}(\boldsymbol{Q})$ consists of the O-cusps [6]. Suppose that $X=X_{\Delta_5}$ has the hyperelliptic involution v. Then v fixes a O-cusp, hence v fixes all the O-cusps. Then the divisor class $cl((\mathrm{O}')-(\mathrm{O}''))$ are of order 2 for the O-cusps O' and O'', $\mathrm{O}'\neq\mathrm{O}''$. But we know that the Mordell-Weil group of the jacobian variety of X is isomorphic to

$\boldsymbol{Z}/71\boldsymbol{Z}$ [6]. □

§3. Automorphism groups of hyperelliptic curves $X_\Delta(N)$

In this section, we determined the automorphism groups of hyperelliptic modular curves of type $X_\Delta(N)$. For square free integers N, $\mathrm{Aut}\, X_\Delta(N)$ are determined [13], [19]. Hence it suffices to discuss for $X_1(16)$ and $X_1(18)$ cf. Theorem 2.1.

THEOREM 3.1. *The automorphisms of $X_1(16)$ and $X_1(18)$ are represented by 2×2 matricies.*

PROOF.

Case $N=18$: Let $\mathcal{X}$ be the minimal model of $X_1(18)$ $(/\boldsymbol{Z})$. The special fibre $\mathcal{X}\otimes\boldsymbol{F}_2$ has two irreducible components Z, Z' which are isomorphic to $\boldsymbol{P}^1$ and intersect transversally at three supersingular points S_1, S_2 and S_3 [2]. Let $v=w_2[7]$ be the hyperelliptic involution of $X_1(18)$. Since the jacobian variety $J_1(18)$ of $X_1(18)$ has stable reduction at the rational prime 2 [2], any endomorphism of $J_1(18)$ is defined over $\boldsymbol{Q}_2^{ur}$ [22] Lemma 1. Let G be the subgroup of $\mathrm{Aut}\, X_1(18)$ consisting of automorphisms g which fix the irreducible component Z. Then we see that the representation of G into the permutation group $\mathcal{S}_3$ of the set $\{S_1, S_2, S_3\}$ is faithfull. Thus we see that $G=\langle w_3, [7]\rangle$. Further w_2 exchanges Z by Z'. Thus $\mathrm{Aut}\, X_1(18)$ is generated by w_2, w_9 and [7].

Case $N=16$: The hyperelliptic involution $v=\gamma^2$ for $\gamma=[3]$. Put $X=X_1(16)$ and $Y=X/\langle v\rangle$. Let C_1, C_2 (resp. C_3, C_4) be the cusps on X lying over the cusp $\begin{pmatrix}1\\2\end{pmatrix}$ $\left(\text{resp. } \begin{pmatrix}1\\8\end{pmatrix}\right)$. Then C_i are the ramification points of the covering $X\to Y$. Let P_1, P_2 be the totally ramified cusps lying over $\begin{pmatrix}1\\4\end{pmatrix}$ and $\begin{pmatrix}-1\\4\end{pmatrix}$, respectively. Let S_v be the set of the Weierstrass points of X: $S_v=\{P_1, P_2, C_1, C_2, C_3, C_4\}$, and let $\mathcal{S}_6$ be the permutation group of the elements of S_v. Then $(\mathrm{Aut}\, X)/\langle v\rangle$ becomes a subgroup of $\mathcal{S}_6$.

LEMMA 3.2. $\{g\in\mathrm{Aut}\, X \mid g\gamma g^{-1}=\gamma^{\pm 1}\}=\langle\gamma, w_{16}\rangle$.

PROOF. We can take a local parameter x along the cusp ∞ of $X_0(16)$ such that the modular invariant $j=F(x)/G(x)$ for $F(x)=(x^8+2^4x^7+7\cdot 2^4x^6+7\cdot 2^6x^5+69\cdot 2^4x^4+13\cdot 2^7x^3+11\cdot 2^7x^2+2^{10}x+2^{13})^3$ and $G(x)=x(x+4)(x^2+4x+8)(x+2)^4$ [3] kapitel IV. Further the values $x=0$, -2, $-2+2\sqrt{-1}$, $-2-2\sqrt{-1}$ and -4

corresponds to the cusps ∞, $\binom{1}{2}$, $\binom{1}{4}$, $\binom{-1}{4}$ and $\binom{1}{8}$, respectively. If $g\gamma g^{-1}=\gamma^{\pm 1}$, then g induces an automorphism of h of $X_0(16)=\boldsymbol{P}^1(x)$, 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 δ be the automorphism of $\boldsymbol{P}^1(x)$ 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 $(\delta h\delta^{-1})^*(x)=\alpha x$ for some $\alpha\in C^\times$. If $\alpha\neq 1$, then $\alpha(1+\sqrt{-1})=1-\sqrt{-1}$, so that $\alpha=-\sqrt{-1}$. But then $1+\sqrt{-1}=(\delta h\delta^{-1})^*(1-\sqrt{-1})\neq(-\sqrt{-1})(1-\sqrt{-1})$. Therefore $\alpha=1$, i.e., $h=id$ and g belongs to $\langle\gamma\rangle$. □

At first, we show that any 2-sylow subgroup H of $G=\mathrm{Aut}\,X$ containg γ and w_{16} is equal to the subgroup $\langle w_{16}, \gamma\rangle$, which is a dihedral group with relation $w_{16}\gamma w_{16}^{-1}=\gamma^{-1}$. 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 $\boldsymbol{Q}(\zeta_{16})$. Let t be a local parameter along C. Then $g^*(t)=\zeta_5 t+a_2t^2+\cdots$ for a primitive 5-th root ζ_5 of unity, so that g is not defined over $\boldsymbol{Q}_5^{ur}$. But we know that any endomorphism of the jacobian variety of X is defined over $\boldsymbol{Q}_p^{ur}$ 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 $\{P_i\}$, $\{C_1, C_2\}$ and $\{C_3, C_4\}$, if necessary, we may assume that (1) $g(P_1)=P_2$ or (2) $g(P_1)=C_1$.

CLAIM. $g(P_1)\neq P_2$.

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

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

References

[1] A.O.L. Atkin and J. Lehner, Hecke operators on $\Gamma_0(m)$, Math. Ann. 185, 134-160 (1970).

[2] P. Deligne and M. Rapoport, Schémas de modules des courbes elliptiques, Vol. II of Proceedings of the International Summer School on Modular Functions, Antwerp 1972, Lecture Notes in Math. No. 349 (1973).

[3] N.D. Elkies, The automorphism group of the modular curve $X_0(63)$, Composito Matematica Vol. 74, No. 2 (1990).

[4] R. Fricke, Die Elliptischen Funktionen und ihre Anwendungen, Teubner, Verlag, Leipzig (1922).

[5] M.A. Kenku, Certain torsion points on elliptic curves defined over quadratic fields, J. London Math. Soc. 2, 19, 233-240 (1979).

[6] M.A. Kenku, On modular curves $X_0(125)$, $X_1(25)$ and $X_1(49)$, J. London Math. Soc. 2, 23, 415-427 (1981).

[7] M.A. Kenku and F. Momose, Torsion points on elliptic curves defined over quadratic fields, Nagoya Math. Soc. Vol. 109, 125-149 (1988).

[8] M.A. Kenku and F. Momose, Automorphism groups of the modular curves $X_0(N)$, Composito Math. **65**, 51-80 (1988).

[9] D. Kubert, Universal bounds on torsion points of elliptic curves, Proc. London Math. Soc. **3**, 33, 193-237 (1976).

[10] B. Mazur, Rational points on modular curves, Proceedings of the Conference on Modular Functions held in Bonn 1976, Lecture Notes in Math. **601** (1977).

[11] B. Mazur, Rational isogenies of prime degree, Inv. Math. **44**, 129-162 (1978).

[12] B. Mazur and H.P.F. Swinnerton-Dyer, Arithmetic of Weil curves, Inv. Math. **25**, 1-61 (1974).

[13] F. Momose, Automorphism groups of the modular curves $X_1(N)$, to appear.

[14] F. Momose, On the l-adic representations attached to modular forms, J. Facult. Sci. Univ. Tokyo, Vol. **28**, 89-109 (1981).

[15] F. Momose, Rational points on the modular curves $X_{split}(p)$, Comp. Math. **52**, 115-137 (1984).

[16] F. Momose, Rational points on the modular curves $X_0^+(p^r)$, J. Facult. Sci. Univ. Tokyo, Vol. 33, 441-466 (1986).

[17] F. Momose, Rational points on the modular curves $X_0^+(N)$, J. Math. Soc. Japan. Vol. 39, No. 2, 1987,

[18] A.P. Ogg, Hyperelliptic modular curves, Bull. Soc. Math. France, **102**, 449-462 (1974).

[19] A.P. Ogg, Uber die Automorphismengruppe von $X_0(N)$, Math. Ann. **228**, 279-292 (1977).

[20] K.A. Ribet, On l-adic representations attached to modular forms, Inv. Math. **28**, 245-275 (1975).

[21] K.A. Ribet, Twists of modular forms and endomorphisms of abelian varieties, Math. Ann. **253**, 245-275 (1975).

[22] K.A. Ribet, Endomorphisms of semi-stable abelian varieties over number fields, Ann. Math. **101**, 555-562 (1975).

[23] G. Shimura, On elliptic curves with complex multiplication as factors of the Jacobians of modular function fieilds, Nagoya Math. J. Vol. 43, 199-208 (1971).

[24] Modular functions of one variable VI, Lecture Notes in Math. **476** (1975).

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