TOKYO J. MATH.
VOL. 22, NO. 1, 1999

Hyperelliptic Quotients of Modular Curves $X_0(N)$

Masahiro FURUMOTO and Yuji HASEGAWA

Waseda University

(Communicated by T. Suzuki)

Introduction.

Let N be a positive integer, and let

$$\Gamma_0(N)=\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix}\in \mathrm{SL}_2(\mathbf{Z}) \;\middle|\; c\equiv 0 \pmod{N}\right\}.$$

Let $X_0(N)$ be the modular curve which corresponds to $\Gamma_0(N)$. For each positive divisor N' of N with $(N', N/N')=1$ (in which case we write $N'\|N$), $W_{N'}=W_{N'}^{(N)}$ denotes the corresponding Atkin–Lehner involution on $X_0(N)$. (W_1 is the identity.) It is known that the $W_{N'}$ generate an elementary 2-abelian group, which we denote by $W(N)$. The group $W(N)$ is of order $2^{\omega(N)}$, where $\omega(N)$ is the number of distinct prime divisors of N. Furthermore, these involutions are all defined over $\mathbf{Q}$: $W(N)\subseteq \mathrm{Aut}_{\mathbf{Q}}(X_0(N))$.

Let W' be a subgroup of $W(N)$. Then the hyperellipticity of the quotient curve $X_0(N)/W'$ has been determined for two extreme cases (i.e., for $W'=\{1\}$ or $W(N)$).

THEOREM 1 ([12]). *There are nineteen values of N for which $X_0(N)$ is hyperelliptic, i.e., $X_0(N)$ is hyperelliptic if and only if*

$$N=22,\ 23,\ 26,\ 28\text{–}31,\ 33,\ 35,\ 37,\ 39\text{–}41,\ 46\text{–}48,\ 50,\ 59,\ 71\,.$$

THEOREM 2 ([8] [6]). *Put $X_0^*(N)=X_0(N)/W(N)$. There are* 64 *values of N for which $X_0^*(N)$ is hyperelliptic.*

(i) *$X_0^*(N)$ is of genus two if and only if N is in the following list* (57 *values in total*):

67, 73, 85, 88, 93, 103, 104, 106, 107, 112,
115, 116, 117, 121, 122, 125, 129, 133, 134, 135,
146, 147, 153, 154, 158, 161, 165, 166, 167, 168,
170, 177, 180, 184, 186, 191, 198, 204, 205, 206,
209, 213, 215, 221, 230, 255, 266, 276, 284, 285,
286, 287, 299, 330, 357, 380, 390.

Received June 28, 1997
Revised November 20, 1997

The second author is partially supported by Waseda University Grant for Special Research Projects 97A-166.

(ii) *$X_0^*(N)$ is hyperelliptic with genus ≥ 3 if and only if*

$$N=136,\ 171,\ 176,\ 207,\ 252,\ 279,\ 315\ .$$

REMARK 1. Defining equations of hyperelliptic modular curves $X_0(N)$ are given in [4] [11] [15], and those of hyperelliptic modular curves $X_0^*(N)$ are given in [11] [5] [6].

Now the purpose of this article is to determine all hyperelliptic curves $X_0(N)/W'$ for proper subgroups W' of $W(N)$ for all N. As the results for genus two case are known [5], we restrict ourselves to the case where the genus is greater than two. Note that if there is a proper subgroup W' of $W(N)$ such that $X_0(N)/W'$ is a hyperelliptic curve of genus ≥ 3, then the integer N must satisfy the following conditions:

(i) N is not a power of a prime number;

(ii) $X_0(N)$ is of genus ≥ 5;

(iii) $X_0^*(N)$ is subhyperelliptic, by which we mean that it is either rational, elliptic or hyperelliptic. (Hence in particular $N \leq 390$.)

Moreover, since there is a model of $X_0(N)$, and hence of $X_0(N)/W'$, over **Q** having good reduction at all $p \nmid N$ ([10]), it follows from Ogg's observation [12] [13] that

PROPOSITION 1. *For a positive integer N, put $\psi(N) := N\prod_{q|N}(1+1/q)$, where the product is over prime divisors of N. Let p be a prime number such that $p \nmid N$. If one has*

$$\frac{1}{2^{\omega(N)-r}}\,\frac{p-1}{12}\,\psi(N)+2^r hs>2(p^2+1)\,,$$

then $X_0(N)/W'$ is non-hyperelliptic for any subgroup W' of $W(N)$ such that $[W(N): W']=2^r$. Here h is the largest divisor of 24 with $h^2|N$, and $s=s_2s_3$ is defined as follows. Write $h=h_2h_3$ with $h_2|8$ and $h_3|3$. Then

$$s_2=\begin{cases}3/4 & \text{if } 2|h_2{}^2\|N\,,\\ 1 & \text{otherwise}\,;\end{cases}$$

$$s_3=\begin{cases}2/3 & \text{if } h_3{}^2=9\|N\,,\\ 1 & \text{otherwise}\,.\end{cases}$$

As an application, we see by setting $p=2$ or 3 or 5 that $X_0(N)/W'$ is non-hyperelliptic for all proper subgroups W' of $W(N)$ for

$$\begin{aligned}N=\ &112,\ 117,\ 135,\ 136,\ 146,\ 147,\ 153,\ 158,\ 159,\ 166,\\ &171,\ 176,\ 177,\ 184,\ 188,\ 205,\ 206,\ 207,\ 209,\ 213,\\ &215,\ 220,\ 221,\ 252,\ 255,\ 266,\ 279,\ 284,\ 285,\ 286,\\ &287,\ 299,\ 315,\ 357,\ 380.\end{aligned}$$

Taking a glance at this, we have the following list of N for which the hyperellipticity of quotients of $X_0(N)$ must be tested.

TABLE 1

N									
42	46	51	52	55	56	57	58	60	62
63	65	66	68	69	70	72	74	75	76
77	78	80	82	84	85	86	87	88	90
91	92	93	94	95	96	98	99	100	102
104	105	106	108	110	111	114	115	116	118
119	120	122	123	124	126	129	130	132	133
134	138	140	141	142	143	145	150	154	155
156	161	165	168	170	174	180	182	186	190
195	198	204	210	222	230	231	238	276	330
390									

We will determine the hyperellipticity of $X_0(N)/W'$ for these N by using various methods which generalize those given in [8, App. C] and [6]. In particular, we will be able to determine the hyperellipticity of $X=X_0(N)/W'$ without calculating an equation related to X (cf. [8] [6]; especially [8, Prop. 2]).

1. The genus of the quotient $X_0(N)/W'$.

Let X be the quotient curve of $X_0(N)$ by a subgroup W' of $W(N)$:

$$X=X_0(N)/W'.$$

Since X corresponds to the Fuchsian group Γ' generated by $\Gamma_0(N)$ and the elements of W', the space of holomorphic 1-forms on X can be canonically identified with the space $S_2(\Gamma')$ of cuspforms of weight 2 on Γ'. Obviously, we have

$$S_2(\Gamma')=S_2(N)^{W'}=\{f\in S_2(N) \mid f|w=f \ (\forall w\in W')\},$$

where $S_2(N)=S_2(\Gamma_0(N))$. In particular, the genus of X is equal to the dimension of $S_2(N)^{W'}$. As one can find the data of the so-called W-splitting of $S_2(N)$ for $N\leq 300$ [2, Table 5], the dimension of $S_2(N)^{W'}$ is easily computed for $N\leq 300$. Similar data for larger N can be computed by using trace formulas of Hecke operators (or by Remark 2 below). Since for $N\geq 301$ only $N=330$ and 390 remain to be tested, it is sufficient for our purpose to give the data for these two values of N (Table 2). (*Remark.* The third column of Table 2 gives the dimensions of direct summands $S_2(N)^{(\pm,\cdots,\pm)}$ of $S_2(N)$, ordered lexicographically; see [2, Table 5].)

TABLE 2. The W-splitting of $S_2(N)$

N	$p\mid N$	the W-splitting of $S_2(N)$
330	2, 3, 5, 11	2, 6, 4, 4, 4, 5, 4, 4, 5, 4, 3, 5, 3, 4, 2, 6
390	2, 3, 5, 13	2, 8, 5, 5, 6, 4, 4, 5, 4, 6, 5, 4, 6, 3, 7, 3

EXAMPLE 1. Let $N=42$. From [2, Table 5], we see that the genera of the $X_0(42)/W'$ are as follows.

W'	genus	W'	genus
$\{1\}$	5	$\langle W_2, W_3\rangle$	1
$\langle W_2\rangle$	3	$\langle W_2, W_7\rangle$	1
$\langle W_3\rangle$	2	$\langle W_3, W_7\rangle$	1
$\langle W_7\rangle$	3	$\langle W_2, W_{21}\rangle$	1
$\langle W_6\rangle$	2	$\langle W_3, W_{14}\rangle$	0
$\langle W_{14}\rangle$	1	$\langle W_7, W_6\rangle$	1
$\langle W_{21}\rangle$	2	$\langle W_6, W_{14}\rangle$	0
$\langle W_{42}\rangle$	2	$W(42)$	0

REMARK 2. There is a formula for the number $\nu(N')=\nu(N'; N)$ of fixed points of $W_{N'}$ on $X_0(N)$. It is given by

$$\begin{aligned}\nu(N') = {} & \Big(\prod_{p\mid N/N'} c_1(p)\Big)h(-4N') \\ & + \begin{cases} \Big(\prod_{p\mid N/N'} c_2(p)\Big)h(-N') & \text{if } 4\leq N'\equiv 3 \pmod 4\,, \\ 0 & \text{otherwise} \end{cases} \\ & + \begin{cases} \prod_{p\mid N/2}\Big(1+\Big(\frac{-4}{p}\Big)\Big) & \text{if } N'=2\,, \\ 0 & \text{otherwise} \end{cases} \\ & + \begin{cases} \prod_{p\mid N/3}\Big(1+\Big(\frac{-3}{p}\Big)\Big) & \text{if } N'=3\,, \\ 0 & \text{otherwise} \end{cases} \\ & + \begin{cases} \prod_{p^\nu\parallel N/4}\big(p^{[\frac{\nu}{2}]}+p^{[\frac{\nu-1}{2}]}\big) & \text{if } N'=4\,, \\ 0 & \text{otherwise}\,, \end{cases}\end{aligned}$$

where $h(-d)$ is the class number of primitive quadratic forms of discriminant $-d$, $\Big(\frac{*}{*}\Big)$ is the Kronecker symbol and the functions $c_i(p)$ are defined as follows:

$$c_i(p)=\begin{cases} 1+\left(\dfrac{-N'}{p}\right) & \text{if } p\neq 2 \text{ and } N'\equiv 3 \pmod 4\,, \\[2ex] 1+\left(\dfrac{-4N'}{p}\right) & \text{if } p\neq 2 \text{ and } N'\not\equiv 3 \pmod 4\,, \end{cases}$$

$$c_1(2)=\begin{cases} 1 & \text{if } N'\equiv 1 \pmod 4 \text{ and } 2\| N\,, \\ 0 & \text{if } N'\equiv 1 \pmod 4 \text{ and } 4| N\,, \\ 2 & \text{if } N'\equiv 3 \pmod 4 \text{ and } 2\| N\,, \\ 3+\left(\dfrac{-N'}{2}\right) & \text{if } N'\equiv 3 \pmod 4 \text{ and } 4\| N\,, \\ 3\left(1+\left(\dfrac{-N'}{2}\right)\right) & \text{if } N'\equiv 3 \pmod 4 \text{ and } 8| N\,, \end{cases}$$

$$c_2(2)=1+\left(\frac{-N'}{2}\right) \qquad \text{if } N'\equiv 3 \pmod 4\,.$$

One can use this formula to compute the genus of $X_0(N)/W'$.

Let $X=X_0(N)/W'$ be the quotient curve of $X_0(N)$ by a proper subgroup W' of $W(N)$. Then each non-trivial element w of $W(N)/W'$ induces an involution on X:

$$\begin{tikzcd} X_0(N) \arrow[r, dash] & X \arrow[r, dash, "\text{degree 2}"] & X/\langle w\rangle \arrow[r, dash] & X_0^*(N)\,. \end{tikzcd}$$

First we determine all (X, w) such that $X/\langle w\rangle$ are of genus zero, i.e., all hyperelliptic curves X whose hyperelliptic involution is of Atkin–Lehner type. If the genus of $X/\langle w\rangle$ is zero, then so is that of $X_0^*(N)$. Since $N=119$ is the largest value of N for which $X_0^*(N)$ is of genus 0, we see from [2, Table 5] that there are 32 hyperelliptic curves X such that their hyperelliptic involutions are of Atkin–Lehner type.

THEOREM 3. *There are* 32 *pairs of* (N, W') *for which* $X_0(N)/W'$ *is a hyperelliptic curve of genus* $g\geq 3$ *such that the hyperelliptic involution* $v=v(N, W')$ *comes from an Atkin–Lehner involution. More precisely,* $X_0(N)/W'$ *is a hyperelliptic curve of* $g\geq 3$ *having an Atkin–Lehner involution as its hyperelliptic involution if and only if* (N, W') *is in the following list.*

$N=\prod p^{\nu}$	W'	g	v
$46=2\cdot 23$	$\langle W_2\rangle$	3	W_{23}
$51=3\cdot 17$	$\langle W_3\rangle$	3	W_{17}
$55=5\cdot 11$	$\langle W_5\rangle$	3	W_{11}
$56=2^3\cdot 7$	$\langle W_8\rangle$	3	W_7
$60=2^2\cdot 3\cdot 5$	$\langle W_4\rangle$	3	W_{15}
$60=2^2\cdot 3\cdot 5$	$\langle W_{12}\rangle$	4	W_{20}
$60=2^2\cdot 3\cdot 5$	$\langle W_{60}\rangle$	3	W_4
$62=2\cdot 31$	$\langle W_2\rangle$	4	W_{31}
$66=2\cdot 3\cdot 11$	$\langle W_6\rangle$	4	W_{11}
$66=2\cdot 3\cdot 11$	$\langle W_{66}\rangle$	3	W_6
$69=3\cdot 23$	$\langle W_3\rangle$	4	W_{23}
$70=2\cdot 5\cdot 7$	$\langle W_{10}\rangle$	4	W_{14}
$70=2\cdot 5\cdot 7$	$\langle W_{14}\rangle$	3	W_{10}
$78=2\cdot 3\cdot 13$	$\langle W_6\rangle$	6	W_{26}
$78=2\cdot 3\cdot 13$	$\langle W_{26}\rangle$	3	W_6
$78=2\cdot 3\cdot 13$	$\langle W_2, W_3\rangle$	3	W_{13}
$78=2\cdot 3\cdot 13$	$\langle W_{13}, W_6\rangle$	3	W_3
$87=3\cdot 29$	$\langle W_3\rangle$	5	W_{29}
$92=2^2\cdot 23$	$\langle W_4\rangle$	5	W_{23}
$92=2^2\cdot 23$	$\langle W_{92}\rangle$	4	W_4
$94=2\cdot 47$	$\langle W_2\rangle$	6	W_{47}
$94=2\cdot 47$	$\langle W_{94}\rangle$	4	W_2
$95=5\cdot 19$	$\langle W_5\rangle$	5	W_{19}
$95=5\cdot 19$	$\langle W_{19}\rangle$	3	W_5
$105=3\cdot 5\cdot 7$	$\langle W_3, W_5\rangle$	3	W_7
$105=3\cdot 5\cdot 7$	$\langle W_3, W_7\rangle$	3	W_5
$105=3\cdot 5\cdot 7$	$\langle W_7, W_{15}\rangle$	3	W_3
$110=2\cdot 5\cdot 11$	$\langle W_2, W_5\rangle$	4	W_{11}
$110=2\cdot 5\cdot 11$	$\langle W_2, W_{11}\rangle$	3	W_5
$110=2\cdot 5\cdot 11$	$\langle W_5, W_{22}\rangle$	3	W_2
$119=7\cdot 17$	$\langle W_7\rangle$	6	W_{17}
$119=7\cdot 17$	$\langle W_{17}\rangle$	4	W_7

Next assume that the genus of $X_0^*(N)$ is non-zero (i.e., $X_0^*(N)$ is either elliptic or hyperelliptic). Then any of Atkin–Lehner involutions on $X=X_0(N)/W'$ is non-hyperelliptic, hence has at most four fixed points whenever X is hyperelliptic ([12, Prop. 1]). Therefore if $W_{N'}$ induces a non-trivial action on X and has more than four fixed points, then X is non-hyperelliptic. We omit the list of (N, W') for which the curve $X_0(N)/W'$ turns out to be non-hyperelliptic in this way, since it would be of fairly large size. The reader may recover the list immediately from [2, Table 5] and Table 2 above. Note also that one may save the time by observing that if there is a covering $X\rightarrow Y$ between algebraic curves X and Y, and if Y is non-subhyperelliptic, then so is X. On the other hand, if there is a covering $X\rightarrow Y$ and if the genus of X (resp. Y) is three (resp. two), then X is necessarily hyperelliptic ([7, Prop. 2]). Thus we see that the five curves $X_0(85)/\langle W_{85}\rangle$, $X_0(165)/\langle W_{11}, W_{15}\rangle$, $X_0(114)/\langle W_2, W_{19}\rangle$, $X_0(130)/\langle W_2, W_{13}\rangle$ and $X_0(195)/\langle W_5, W_{39}\rangle$ are hyperelliptic (see [7]).

REMARK 3. We have determined the hyperellipticity of $X_0(N)/W'$ for

$$N=46,\ 51,\ 55,\ 56,\ 60,\ 62,\ 66,\ 69,\ 70,\ 74,\ 78,\ 87,\ 92,$$
$$94,\ 95,\ 108,\ 110,\ 111,\ 119,\ 142,\ 143,\ 145,\ 155$$

in this section.

2. Modular involutions.

In this section we always assume that $4|N$ or $9\|N$. Then $X_0(N)$ has modular involutions of non-Atkin–Lehner type; i.e., those involutions which are not Atkin–Lehner involutions but come from linear fractional transformations on the complex upper half plane. In this section, we discuss their action on $S_2(N)$. As a consequence, we will be able to determine the hyperellipticity of $X_0(N)/W'$ for some (N, W').

Put $S_\mu=\begin{pmatrix} \mu & 1 \\ 0 & \mu \end{pmatrix}$. Then S_2 is in the normalizer of $\Gamma_0(N)$ when N is divisible by 4, and S_3 is in the normalizer of $\Gamma_0(N)$ when N is divisible by 9.

Lemma 1. (i) *Let $2^\alpha\|N$ with $\alpha\geq 2$. Then as automorphisms of $X_0(N)$ we have*

$$S_2{}^2=1\,;\qquad S_2W_{p^\nu}=W_{p^\nu}S_2 \text{ if } p\neq 2\,.$$

(ii) *Let $2^\alpha\|N$ with $\alpha\geq 3$ and put $V_2=S_2W_{2^\alpha}S_2$. Then as automorphisms of $X_0(N)$ we have*

$$V_2{}^2=1\,;\qquad V_2W_{p^\nu}=W_{p^\nu}V_2\,.$$

(iii) *Let $9\|N$ and put $V_3=S_3W_9S_3{}^2$. Then as automorphisms of $X_0(N)$ we have*

$$V_3{}^2=1\,;\qquad V_3W_{p^\nu}=W_9{}^\varepsilon W_{p^\nu}V_3\,,$$

where

$$\varepsilon=\begin{cases} 0 & \text{if } p^\nu\equiv 0,\ 1 \pmod 3\,, \\ 1 & \text{otherwise}\,. \end{cases}$$

Proof. This follows from a direct calculation. □

The following two propositons generalize Propositions 2 and 3 of [6]. Proofs are similar to those in [6].

Proposition 2. *Let N be a positive integer such that $8|N$. Let N' be a positive divisor of N and let d be a positive divisor of N/N'. Define integers α, β and γ by*

$$2^\alpha\|N\,,\quad 2^{\alpha-\beta}\|N'\,,\quad 2^\gamma\|d\,,$$

so that $N=2^\alpha M$ and $N'=2^{\alpha-\beta}M'$ for some positive odd integers M, M' with $M'|M$. Let $f=\sum a_nq^n$ be a newform of weight 2 on $\Gamma_0(N')$ such that $f|W^{(N')}_{2^{\alpha-\beta}}=\lambda f$, and put

$$g_\pm{}^{(d)}=f^{(d)}\pm f^{(d)}|W^{(N)}_{2^\alpha}=f^{(d)}\pm 2^{\beta-2\gamma}\lambda f^{(d')}$$

with $d'=2^{\beta-2\gamma}d$, where we write $f^{(d)}(\tau)=f(d\tau)$, etc. Then the second column in the following table gives the common eigenforms for V_2 and W_{2^α}, with eigenvalues $\lambda(V_2)$ and $\lambda(W_{2^\alpha})$.

α, β, γ	common eigenform	$\lambda(V_2)$	$\lambda(W_{2^\alpha})$
$\alpha-2\geq\beta>\gamma=0$	$g_+{}^{(d)}$	$-$	$+$
	$g_-{}^{(d)}$	$+$	$-$
$\alpha-1=\beta>\gamma=0$	$g_+{}^{(d)}+\lambda g_+{}^{(2d)}$	$-$	$+$
	$g_-{}^{(d)}+\lambda g_-{}^{(2d)}$	$+$	$-$
$\alpha\geq 5, \alpha=\beta>\gamma=0$	$g_+{}^{(d)}-a_2g_+{}^{(2d)}+2g_+{}^{(4d)}$	$-$	$+$
	$g_-{}^{(d)}-a_2g_-{}^{(2d)}+2g_-{}^{(4d)}$	$+$	$-$
$\alpha=\beta=4>\gamma=0$	$g_+{}^{(d)}-a_2g_+{}^{(2d)}+4f^{(4d)}$	$-$	$+$
	$g_-{}^{(d)}-a_2g_-{}^{(2d)}$	$+$	$-$
$\alpha=\beta=3>\gamma=0$	$g_+{}^{(d)}+(1-a_2)g_+{}^{(2d)}$	$-$	$+$
	$g_-{}^{(d)}-(1+a_2)g_-{}^{(2d)}$	$+$	$-$
$\beta-\gamma>\gamma>0$	$g_+{}^{(d)}$	$+$	$+$
	$g_-{}^{(d)}$	$-$	$-$
$\beta=2\gamma$	$f^{(d)}$	λ	λ

PROPOSITION 3. *Let N be a positive integer such that $9\|N$, N' a positive divisor of N. Write $N=3^2M$, $N'=3^{2-\beta}M'$ with $M'|M$. Let $f=\sum a_nq^n$ be a newform of weight* 2 on $\Gamma_0(N')$ *such that $f|W^{(N')}_{3^{2-\beta}}=\lambda f$, and put $f_\chi=\sum a_n\chi(n)q^n$, where $\chi=\left(\frac{-3}{\cdot}\right)$. If $\beta=0$, then we further assume that $\lambda=+1$. Finally let d be a positive divisor of M/M'. Then the second column in the following table gives the common eigenforms for V_3 and W_9, with eigenvalues $\lambda(V_3)$ and $\lambda(W_9)$.*

β	common eigenform	$\lambda(V_3)$	$\lambda(W_9)$
0	$f^{(d)}$	$+$	$+$
1	$f^{(d)}-3\lambda f^{(3d)}-\chi(d)\sqrt{-3}f_\chi{}^{(d)}$	$-$	$-$
	$f^{(d)}-3\lambda f^{(3d)}+\chi(d)\sqrt{-3}f_\chi{}^{(d)}$	$+$	$-$
	$f^{(d)}+3\lambda f^{(3d)}$	$-$	$+$
2	$f^{(d)}-9f^{(9d)}-\chi(d)\sqrt{-3}f_\chi{}^{(d)}$	$-$	$-$
	$f^{(d)}+9f^{(9d)}-\dfrac{3a_3}{2}f^{(3d)}$	$-$	$+$
	$f^{(d)}-9f^{(9d)}+\chi(d)\sqrt{-3}f_\chi{}^{(d)}$	$+$	$-$
	$f^{(3d)}$	$+$	$+$

Here we write $f^{(d)}(\tau)=f(d\tau)$, etc.

REMARK 4. Let the symbols be as in Proposition 3, so in particular f is a newform of weight 2 on $\Gamma_0(N')$. Suppose $\beta=0$, so that $9\|N'$. Then $\lambda=+1$ if and only if f_χ is also a newform of weight 2 on $\Gamma_0(N')$.

Using the above two propositions, we find that

THEOREM 4. *The quotient curve $X_0(N)/W'$ is a hyperelliptic curve of genus $g\geq 3$ with hyperelliptic involution v coming from a non-Atkin–Lehner modular involution, if and only if the pair (N, W') is in the following list. (As usual, W' is assumed to be proper.)*

$N=\prod p^{\nu}$	W'	g	v
$63=3^2\cdot 7$	$\langle W_9\rangle$	3	V_3W_7
$72=2^3\cdot 3^2$	$\langle W_9\rangle$	3	$V_2V_3W_8$
$104=2^3\cdot 13$	$\langle W_{104}\rangle$	3	V_2W_8
$120=2^3\cdot 3\cdot 5$	$\langle W_5, W_{24}\rangle$	3	V_2W_8
$126=2\cdot 3^2\cdot 7$	$\langle W_9, W_7\rangle$	3	V_3
$126=2\cdot 3^2\cdot 7$	$\langle W_9, W_{14}\rangle$	3	V_3W_2
$168=2^3\cdot 3\cdot 7$	$\langle W_{24}, W_{56}\rangle$	4	V_2W_8

Applying [12, Prop. 1], we also find that the curve $X_0(N)/W'$ is non-hyperelliptic for the following (N, W'):

$N=\prod p^{\nu}$	W'	w	g	$\bar{g}$
$88=2^3\cdot 11$	$\langle W_{11}\rangle$	S_2	5	1
$90=2\cdot 3^2\cdot 5$	$\langle W_{90}\rangle$	V_3	4	1
$168=2^3\cdot 3\cdot 7$	$\langle W_8, W_7\rangle$	W_3V_2	5	1
$168=2^3\cdot 3\cdot 7$	$\langle W_3, W_{56}\rangle$	V_2	4	1
$168=2^3\cdot 3\cdot 7$	$\langle W_7, W_{24}\rangle$	V_2	5	1

Here g is the genus of $X=X_0(N)/W'$ and $\bar{g}$ is the genus of $X/\langle w\rangle$.

REMARK 5. We have determined the hyperellipticity of $X_0(N)/W'$ for

$$N=72,\ 104,\ 126,\ 168$$

in this section. (The curve $X_0(126)/\langle W_{63}\rangle$ is not hyperelliptic by Propositon 1.)

3. Some isomorphisms.

In this section we give some isomorphisms between certain quotient curves of $X_0(N)$.

PROPOSITION 4. *Assume that* $4\|N$ *and write* $N=4M$. *Let* W' *be a subgroup of* $W(N)$ *generated by* $W_4, W_{M_1}, \cdots, W_{M_s}$ $(M_i\|M)$. *Then we have the following isomorphism*:

$$X_0(N)/W' \cong X_0(2M)/\langle\{W_{M_i}\}_i\rangle .$$

PROOF. See [6, Prop. 7]. □

From this we have

$$X_0(68)/\langle W_4\rangle \cong X_0(34), \qquad X_0(82)/\langle W_{41}\rangle \cong X_0^*(164),$$
$$X_0(84)/\langle W_4, W_7\rangle \cong X_0(42)/\langle W_7\rangle, \qquad X_0(98)/\langle W_{49}\rangle \cong X_0^*(196),$$
$$X_0(106)/\langle W_{53}\rangle \cong X_0^*(212), \qquad X_0(118)/\langle W_{59}\rangle \cong X_0^*(236),$$
$$X_0(154)/\langle W_7, W_{11}\rangle \cong X_0^*(308), \qquad X_0(174)/\langle W_3, W_{29}\rangle \cong X_0^*(348),$$
$$X_0(180)/\langle W_4, W_9\rangle \cong X_0(90)/\langle W_9\rangle, \qquad X_0(180)/\langle W_4, W_5\rangle \cong X_0(90)/\langle W_5\rangle,$$
$$X_0(180)/\langle W_4, W_{45}\rangle \cong X_0(90)/\langle W_{45}\rangle, \qquad X_0(198)/\langle W_9, W_{11}\rangle \cong X_0^*(396),$$
$$X_0(204)/\langle W_4, W_{51}\rangle \cong X_0(102)/\langle W_{51}\rangle, \qquad X_0(210)/\langle W_3, W_5, W_7\rangle \cong X_0^*(420),$$
$$X_0(238)/\langle W_7, W_{17}\rangle \cong X_0^*(476), \qquad X_0(276)/\langle W_4, W_{23}\rangle \cong X_0(138)/\langle W_{23}\rangle .$$

According to Lemma 1 (iii), we also have

PROPOSITION 5. *Assume that* $9\|N$. *Let* W' *be a subgroup of* $W(N)$ *generated by* $W_{N_1}, \cdots, W_{N_t}$ $(N_i\|N)$, *and let* $W''=\langle\{W_9^{\varepsilon(N_i)}W_{N_i}\}_i\rangle$, *where*

$$\varepsilon(M)=\begin{cases} 0 & \textit{if } M\equiv 1 \bmod 3 \textit{ or if } 9\|M \textit{ and } M/9\equiv 1 \bmod 3, \\ 1 & \textit{otherwise}. \end{cases}$$

Then we have the following isomorphism:

$$X_0(N)/W' \cong X_0(N)/W'' .$$

From this we have

$$X_0(90)/\langle W_{18}, W_{10}\rangle \cong X_0(90)/\langle W_2, W_5\rangle,$$
$$X_0(99)/\langle W_{99}\rangle \cong X_0(99)/\langle W_{11}\rangle,$$
$$X_0(180)/\langle W_{36}, W_{20}\rangle \cong X_0(180)/\langle W_5, W_{36}\rangle,$$
$$X_0(198)/\langle W_{11}, W_{18}\rangle \cong X_0(198)/\langle W_2, W_{99}\rangle .$$

REMARK 6. We have determined the hyperellipticity of $X_0(N)/W'$ for

$$N=68,\ 82,\ 98,\ 118$$

in this section.

4. Fixed points of Atkin–Lehner involutions.

In this section, we discuss the fixed points of Atkin–Lehner involutions. The important fact is that these involutions are defined over **Q**, so that we can make use of Ogg's observation (see [6, Prop. 6]).

PROPOSITION 6. *Let W' be a (proper) subgroup of $W(N)$ with $2^{\omega(N)-r}$ elements, so that $W(N)/W'$ is a subgroup of order 2^r of $\mathrm{Aut}_{\mathbf{Q}}X$, where $X=X_0(N)/W'$ is of genus ≥ 3. Take an element $W_{N'}$ of $W(N)\setminus W'$. Assume that there are elements $W_{N''}$ and $W_{N'''}$ of W' such that the numbers of fixed points of $W_{N_1}=W_{N'}W_{N''}$ and $W_{N_2}=W_{N'}W_{N'''}$ are given by*

$$\nu(N_1)=2^{\omega(N)-r}, \qquad \nu(N_2)=3\cdot 2^{\omega(N)-r}.$$

Assume further that
(i) $N_2\not\equiv 3 \pmod 4$ *or* (i′) $N_2\equiv 3 \pmod 8$ *and* $2|(N/N_2)$;
(ii) $3|h(-4N_2)$.
Then X is not hyperelliptic.

PROOF. By assumption (ii) on $h(-4N_2)$, we have $N_2\geq 5$. Therefore by Remark 2 we find that

$$\nu(N_2)=\begin{cases} c_1\cdot h(-4N_2)+c_2\cdot h(-N_2) & \text{if } N_2\equiv 3 \pmod 4 \\ c_1\cdot h(-4N_2) & \text{otherwise}. \end{cases}$$

But we assume (i′) if $N_2\equiv 3 \pmod 4$, hence the coefficient c_2 vanishes. This means that the set of fixed points of W_{N_2} consists of pairs (E, C) with E defined over a field of degree dividing $3\cdot 2^{\omega(N)-r}$ and divisible by 3. The group W', which is an elementary 2-group, acts fixed-point-freely on this set. Thus, this set contributes to three conjugate fixed points of W_{N_2} on X. Now apply [6, Prop. 6]. □

EXAMPLE 2. Let $N=58=2\cdot 29$ and $W'=\langle W_2\rangle$. The genus of $X=X_0(58)/W'$ is three, and W_{29} has four fixed points on X. The involution W_{58} (resp. W_{29}) has two (resp. six) fixed points on $X_0(58)$, contributing to one (resp. three) fixed points of W_{29} on X. Since $h(-4\cdot 29)=6$, we see from Proposition 6 that X is non-hyperelliptic.

The pairs (N, W') to which Proposition 6 applies are listed in Table 3.

REMARK 7. We have determined the hyperellipticity of $X_0(N)/W'$ for

$$N=58, 76, 86, 106, 122, 124, 132, 134,$$
$$140, 150, 174, 182, 190, 222$$

in this section.

TABLE 3. List of (N, W') to which Prop. 6 can be applied

$N=\prod p^\nu$	W'	N'	N''	N'''	$h(-4N_1)$	$h(-4N_2)$
$58=2\cdot 29$	$\langle W_2\rangle$	29	2	1	2	6
$58=2\cdot 29$	$\langle W_{58}\rangle$	29	58	1	1	6
$76=2^2\cdot 19$	$\langle W_{19}\rangle$	4	1	19	*	6
$76=2^2\cdot 19$	$\langle W_{76}\rangle$	4	1	76	*	3
$86=2\cdot 43$	$\langle W_{86}\rangle$	2	1	86	1	3
$102=2\cdot 3\cdot 17$	$\langle W_2, W_{17}\rangle$	3	34	17	4	6
$102=2\cdot 3\cdot 17$	$\langle W_{17}, W_6\rangle$	3	6	17	1	6
$106=2\cdot 53$	$\langle W_{106}\rangle$	2	1	106	1	6
$114=2\cdot 3\cdot 19$	$\langle W_2, W_{57}\rangle$	3	1	114	1	6
$122=2\cdot 61$	$\langle W_{122}\rangle$	2	1	122	1	6
$124=2^2\cdot 31$	$\langle W_{31}\rangle$	4	1	31	*	6
$130=2\cdot 5\cdot 13$	$\langle W_2, W_{65}\rangle$	13	130	2	2	6
$132=2^2\cdot 3\cdot 11$	$\langle W_3, W_{44}\rangle$	4	1	44	*	3
$132=2^2\cdot 3\cdot 11$	$\langle W_{11}, W_{12}\rangle$	4	1	11	*	6
$134=2\cdot 67$	$\langle W_{134}\rangle$	2	1	134	1	3
$140=2^2\cdot 5\cdot 7$	$\langle W_7, W_{20}\rangle$	4	1	140	*	6
$140=2^2\cdot 5\cdot 7$	$\langle W_{20}, W_{28}\rangle$	4	1	35	*	12
$150=2\cdot 3\cdot 5^2$	$\langle W_2, W_{75}\rangle$	6	1	75	2	6
$150=2\cdot 3\cdot 5^2$	$\langle W_3, W_{50}\rangle$	2	3	150	1	6
$170=2\cdot 5\cdot 17$	$\langle W_2, W_{17}\rangle$	5	17	34	4	12
$170=2\cdot 5\cdot 17$	$\langle W_{10}, W_{34}\rangle$	2	1	85	1	12
$174=2\cdot 3\cdot 29$	$\langle W_2, W_{87}\rangle$	3	2	87	2	6
$182=2\cdot 7\cdot 13$	$\langle W_{14}, W_{26}\rangle$	2	26	91	2	12
$186=2\cdot 3\cdot 31$	$\langle W_6, W_{62}\rangle$	2	6	93	1	12
$190=2\cdot 5\cdot 19$	$\langle W_2, W_{95}\rangle$	5	2	95	2	3
$190=2\cdot 5\cdot 19$	$\langle W_{10}, W_{38}\rangle$	5	38	95	4	3
$198=2\cdot 3^2\cdot 11$	$\langle W_2, W_{99}\rangle$	9	2	99	2	3
$204=2^2\cdot 3\cdot 17$	$\langle W_3, W_{68}\rangle$	4	1	204	*	6
$204=2^2\cdot 3\cdot 17$	$\langle W_{12}, W_{68}\rangle$	4	1	51	*	12
$210=2\cdot 3\cdot 5\cdot 7$	$\langle W_5, W_6, W_{14}\rangle$	35	6	1	8	6
$222=2\cdot 3\cdot 37$	$\langle W_6, W_{74}\rangle$	2	6	111	1	12
$230=2\cdot 5\cdot 23$	$\langle W_5, W_{46}\rangle$	2	5	230	2	6
$330=2\cdot 3\cdot 5\cdot 11$	$\langle W_5, W_{11}, W_6\rangle$	110	6	1	8	12
$390=2\cdot 3\cdot 5\cdot 13$	$\langle W_6, W_{10}, W_{26}\rangle$	30	1	26	4	12

(If the fixed points of W_{N_1} consist of cusps, then we marked "*" in the sixth column.)

5. Reduction modulo $p$.

Let $p$ be a prime number and $N$ a positive integer such that $N=pM$, $p\nmid M$. The reduction modulo $p$ of $X_0(pM)$ consists of two copies Z, Z' of $X_0(M)$ in characteristic $p$, intersecting transversally at the supersingular points ([3]; see Figure 1). For the actions of Atkin–Lehner involutions on $X_0(N)$ mod$p$, see e.g., [6, §5]. Let W' be a subgroup of $W(N)$. If W' is generated by some of $W_{N'}$ with $p\nmid N'$, then $X_0(N)/W'$ mod$p$ is again of the shape in Figure 1 with $Z=Z'=X_0(M)/W'$. If W' contains some $W_{N'}$ with $p|N'$, then $X_0(N)/W'$ mod$p$ becomes as in Figure 2:

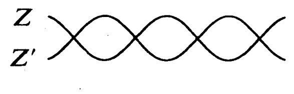

FIGURE 1. $X_0(pM) \bmod p$

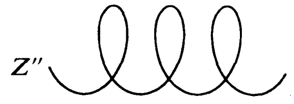

FIGURE 2

where the normalization of Z'' is isomorphic to $X_0(M)/W''$ with W'' consisting of all $W_{N'} \in W'$ such that $p \nmid N'$. Now assume that $X = X_0(N)/W'$ is hyperelliptic. Assume further for simplicity that the special fibre $\mathscr{X} \otimes \mathbf{F}_p$ of the minimal model $\mathscr{X}$ of X at p is as in Figure 1 or 2. (It is easy to generalize the following argument to the case in which one needs to blow up the singularities to reach the minimal model; see also Example 3.)

Case 1. Assume that $\mathscr{X} \otimes \mathbf{F}_p$ is as in Figure 1 and that $|Z \cap Z'| \geq 3$. Then the hyperelliptic involution u of X acts on $\mathscr{X} \otimes \mathbf{F}_p$ in such a way that it exchanges Z for Z' and maps $\alpha \in Z$ to $\alpha \in Z'$ if α is a supersingular point (to see this, consider the graph of $\mathscr{X} \otimes \mathbf{F}_p$). Therefore $v = W_p u$ fixes each component of $\mathscr{X} \otimes \mathbf{F}_p$; it fixes each $\mathbf{F}_p$-rational supersingular point and exchanges properly $\mathbf{F}_{p^2}$-rational supersingular point α for its conjugate $\bar{\alpha}$.

Case 2. Assume that $\mathscr{X} \otimes \mathbf{F}_p$ is as in Figure 2. Then the hyperelliptic involution u of X acts on the normalization of $\mathscr{X} \otimes \mathbf{F}_p$, so there exists an element u of order 2 of $\mathrm{Aut}_{\mathbf{F}_p}(X_0(M)/W'')$ such that

$$u\alpha = \alpha' := W_{N''}\alpha \tag{1}$$

for all properly $\mathbf{F}_{p^2}$-rational supersingular points α on Z'', where $W_{N''}$ is a representative of W'/W'' (note that $W'/W'' \cong \mathbf{Z}/2\mathbf{Z}$).

All the supersingular points of $X_0(N) \bmod p$ can be calculated by using the covering map $X_0(N) \to \mathbf{P}_j^1$ over $\mathbf{F}_p$. In fact, Fricke [4] gave an explicit equation of the covering map $X_0(N) \to \mathbf{P}_j^1$ over $\mathbf{Q}$ for all $X_0(N)$ with genus $g \leq 1$ and for some hyperelliptic $X_0(N)$. We list these coverings in Tables 4 and 5.

EXAMPLE 3. Let $N = 42 = 2 \cdot 3 \cdot 7$. We must check the hyperellipticity of $X_0(42)/W'$ for $W' = \langle W_2 \rangle$ and $\langle W_7 \rangle$ (see Example 1). Take $p = 7$. Then $X_0(42) \bmod 7$ is as in Figure 1 with $Z = Z' = X_0(6)$. The modular curve $X_0(6)$ is of genus zero, and its defining equation is given by

$$j = 256 \frac{(x+3)^3(x^3+9x^2+21x+3)^3}{x(x+4)^3(2x+9)^2}. \tag{2}$$

The only supersingular j-invariant in characteristic $p = 7$ is $j = 12^3$, and the supersingular points on $X_0(6)$ are obtained by solving the equation (2):

$$(x^2+x+4)(x^2+4x+5)(x^2+6x+6) = 0, \tag{3}$$

namely,

TABLE 4. The j-invariant $j=F_M(P)$ of $P\in X_0(M)$ $(X_0(M)\cong \mathbf{P}^1)$

$M=\prod p^\nu$	$P=x,\ F_M(P)=F_M(x)$	W-actions
2	$64(x+4)^3/x^2$	$x\|W_2=1/x$
3	$27(x+1)(9x+1)^3/x$	$x\|W_3=1/x$
$4=2^2$	$64(x^2+8x+4)^3/(x^4(2x+1))$	$x\|W_4=1/(4x)$
5	$(x^2+10x+5)^3/x$	$x\|W_5=125/x$
$6=2\cdot 3$	$F_3\circ f(x),\ f(X)=X(2X+9)^2/(27(X+4))$	$x\|W_2=-2(2x+9)/(x+4)$ $x\|W_3=-9(x+4)/(2x+9)$
7	$(x^2+13x+49)(x^2+5x+1)^3/x$	$x\|W_7=49/x$
$8=2^3$	$256(x^4+8x^3+20x^2+16x+1)^3/(x(x+4)(x+2)^2)$	$x\|W_8=8/x$
$9=3^2$	$27(9x^4+36x^3+54x^2+28x+1)^3/(x(x^2+3x+3))$	$x\|W_9=3/x$
$10=2\cdot 5$	$F_5\circ f(x),\ f(X)=X(2X+5)^2/(X+2)$	$x\|W_2=-(2x+5)/(x+2)$ $x\|W_5=-5(x+2)/(2x+5)$
$12=2^2\cdot 3$	$F_6\circ f(x),\ f(X)=\frac{1}{2}X(X+6)$	$x\|W_4=-4(x+3)/(x+4)$ $x\|W_3=-3(x+4)/(x+3)$
13	$(x^2+5x+13)(x^4+7x^3+20x^2+19x+1)^3/x$	$x\|W_{13}=13/x$
$16=2^4$	$F_8\circ f(x),\ f(X)=\frac{1}{2}X(X+4)$	$x\|W_{16}=8/x$
$18=2\cdot 3^2$	$F_6\circ f(x),\ f(X)=\frac{1}{2}X(X^2+6X+12)$	$x\|W_2=-2(x+3)/(x+2)$ $x\|W_9=-3(x+2)/(x+3)$
$25=5^2$	$F_5\circ f(x),\ f(X)=X(X^4+5X^3+15X^2+25X+25)$	$x\|W_{25}=5/x$

$$\alpha_1=3-3\sqrt{-1}\,,\quad \alpha_2=-2+\sqrt{-1}\,,\quad \alpha_3=-3+2\sqrt{-1}$$

and their conjugates. Let (E, C) be a pair representing any one of α_i or $\bar{\alpha}_i$ $(i=1, 2, 3)$. It is easy to check that $|\mathrm{Aut}(E, C)|=2$, so Figure 1 itself is the special fibre at $p=7$ of the minimal model of $X_0(42)$ (over $\mathbf{Z}$).

(i) $W'=\langle W_2\rangle$. Put $X=X_0(42)/\langle W_2\rangle$ and consider X modulo $p=7$, which is of the shape in Figure 1 with $Z=Z'=X_0(6)/\langle W_2\rangle$. Since $W_2\alpha_1=\alpha_1$ and $W_2\alpha_i=\bar{\alpha}_i$ $(i=2, 3)$, we see that the special fibre $\mathscr{X}\otimes\mathbf{F}_7$ at $p=7$ of the minimal model $\mathscr{X}$ of X is as follows:

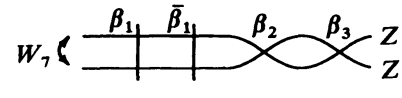

FIGURE 3

TABLE 5. The j-invariant $j=F_M(P)$ of $P\in X_0(M)$ $(X_0(M)\ncong\mathbf{P}^1)$

$M=\prod p^\nu$	$P=(x,y)$, $F_M(P)=F_M(x,y)$	W-actions
$14=2\cdot 7$	$X_0(14)$: $y^2=x^4-14x^3+19x^2-14x+1$, $x_7=((x+1)(x^2-9x+1)-y(x-1))/(2x)$	$(x,y)\mid W_2=(1/x,\ -y/x^2)$ $(x,y)\mid W_7=(1/x,\ y/x^2)$
$15=3\cdot 5$	$X_0(15)$: $y^2=x^4-10x^3-13x^2+10x+1$, $x_5=(x^4-9x^3-9x-1-y(x^2-4x-1))/(2x)$	$(x,y)\mid W_3=(-1/x,\ y/x^2)$ $(x,y)\mid W_5=(-1/x,\ -y/x^2)$
$24=2^3\cdot 3$	$X_0(24)$: $y^2=x^3+11x^2+36x+36$, $x_{12}=x$	$P\mid W_{24}=-P+(0,6)$ $P\mid W_3=P+(-3,0)$
$30=2\cdot 3\cdot 5$	$X_0(30)$: $y^2=x^8+6x^7+9x^6+6x^5-4x^4$ $-6x^3+9x^2-6x+1$, $x_{15}=(x+2)^2(x+1)/x^2$, $y_{15}=-(x^2-2x-4)y/x^4$	$(x,y)\mid W_2=((x+1)/(x-1),$ $-4y/(x-1)^4)$ $(x,y)\mid W_3=(-1/x,\ -y/x^4)$ $(x,y)\mid W_5=(-1/x,\ y/x^4)$
$32=2^5$	$X_0(32)$: $y^2=x^3+6x^2+16x+16$, $x_{16}=x$	$P\mid W_{32}=-P\pm(0,4)$
$35=5\cdot 7$	$X_0(35)$: $y^2=x^8-4x^7-6x^6-4x^5-9x^4$ $+4x^3-6x^2+4x+1$, $x_7=(x^6-5x^5+5x^3-5x-1-y(x^2-3x-1))/(2x)$	$(x,y)\mid W_5=(-1/x,\ y/x^4)$ $(x,y)\mid W_7=(-1/x,\ -y/x^4)$
$36=2^2\cdot 3^2$	$X_0(36)$: $y^2=x^3+6x^2+12x+9$, $x_{18}=x$	$P\mid W_{36}=-P+(0,3)$ $P\mid W_9=P+(-3,0)$

Here β_i is the image of α_i under the map $X_0(6)\rightarrow X_0(6)/\langle W_2\rangle$. The curve $X_0(6)/\langle W_2\rangle$ is parametrized by

$$x'=x+x\,|\,W_2=\frac{x^2-18}{x+4},$$

so we have

$$\beta_1=-1+\sqrt{-1}\,,\quad \beta_2=3\,,\quad \beta_3=1\,.$$

Now assume that X is hyperelliptic, with hyperelliptic involution u. Then u acts on $\mathscr{X}\otimes\mathbf{F}_7$ and $v=W_7u$ must fix Z and Z' with $v\beta_1=\bar{\beta}_1$, $v\beta_i=\beta_i$ $(i=2,3)$. But no elements of $\mathrm{PGL}_2(\mathbf{F}_7)$ satisfy this property. Hence X is not hyperelliptic.

(ii) $W'=\langle W_7\rangle$. Put $X=X_0(42)/\langle W_7\rangle$. Then the special fibre $\mathscr{X}\otimes\mathbf{F}_7$ at $p=7$ of the minimal model $\mathscr{X}$ of X is as in Figure 2, with $Z''=X_0(6)$. There are three conjugate pairs of properly $\mathbf{F}_{7^2}$-rational supersingular points, that is, the roots of the equation (3). It can easily be checked that there does not exist an element of order 2 of $\mathrm{PGL}_2(\mathbf{F}_7)$ with the property (1), so we conclude that X is non-hyperelliptic.

Proceeding as in Example 3, we see that the curve $X_0(N)/W'$ is non-hyperelliptic for (N, W') given in Tables 6 and 7.

REMARK 8. The meaning of symbols given in Table 4 would be clear. Let us exaplain those given in Table 5. The second column gives the defining equations of $X_0(M)$ and the covering map $X_0(M) \to X_0(m)$:

$$X_0(M) \in (x, y) \mapsto \begin{cases} x_m \in X_0(m) & \text{if } X_0(m) \cong \mathbf{P}^1\,; \\ (x_{15}, y_{15}) \in X_0(15) & \text{if } m = 15\,, \end{cases}$$

where x_m, y_m are generators of the function field $\mathbf{Q}(X_0(m))$ of $X_0(m)$ given in Tables 4 and 5.

TABLE 6

$N=\prod p^{\nu}$	W'	p	M	Fig.
$42=2\cdot3\cdot7$	$\langle W_2\rangle$	7	6	1
$42=2\cdot3\cdot7$	$\langle W_7\rangle$	7	6	2
$52=2^2\cdot13$	$\langle W_{13}\rangle$	13	4	2
$57=3\cdot19$	$\langle W_{19}\rangle$	19	3	2
$63=3^2\cdot7$	$\langle W_7\rangle$	7	9	2
$65=5\cdot13$	$\langle W_5\rangle$	5	13	2
$65=5\cdot13$	$\langle W_{13}\rangle$	13	5	2
$75=3\cdot5^2$	$\langle W_3\rangle$	3	25	2
$77=7\cdot11$	$\langle W_7\rangle$	11	7	1
$80=2^4\cdot5$	$\langle W_{16}\rangle$	5	16	1
$84=2^2\cdot3\cdot7$	$\langle W_{84}\rangle$	7	12	2
$84=2^2\cdot3\cdot7$	$\langle W_3, W_7\rangle$	7	12	2
$84=2^2\cdot3\cdot7$	$\langle W_{12}, W_{28}\rangle$	7	12	2
$85=5\cdot17$	$\langle W_5\rangle$	17	5	1
$85=5\cdot17$	$\langle W_{17}\rangle$	17	5	2
$88=2^3\cdot11$	$\langle W_8\rangle$	11	8	1
$88=2^3\cdot11$	$\langle W_{88}\rangle$	11	8	2
$90=2\cdot3^2\cdot5$	$\langle W_2, W_9\rangle$	5	18	1
$90=2\cdot3^2\cdot5$	$\langle W_2, W_5\rangle$	5	18	2
$91=7\cdot13$	$\langle W_{13}\rangle$	13	7	2
$93=3\cdot31$	$\langle W_3\rangle$	31	3	1
$93=3\cdot31$	$\langle W_{31}\rangle$	31	3	2
$93=3\cdot31$	$\langle W_{93}\rangle$	31	3	2
$99=3^2\cdot11$	$\langle W_{11}\rangle$	11	9	2
$102=2\cdot3\cdot17$	$\langle W_6, W_{34}\rangle$	17	6	2
$114=2\cdot3\cdot19$	$\langle W_6, W_{38}\rangle$	19	6	2
$115=5\cdot23$	$\langle W_5\rangle$	23	5	1
$115=5\cdot23$	$\langle W_{115}\rangle$	23	5	2
$116=2^2\cdot29$	$\langle W_{116}\rangle$	29	4	2
$123=3\cdot41$	$\langle W_{41}\rangle$	41	3	2
$129=3\cdot43$	$\langle W_{129}\rangle$	43	3	2
$130=2\cdot5\cdot13$	$\langle W_5, W_{26}\rangle$	13	10	2
$133=7\cdot19$	$\langle W_{19}\rangle$	19	7	2
$133=7\cdot19$	$\langle W_{133}\rangle$	19	7	2
$138=2\cdot3\cdot23$	$\langle W_2, W_{23}\rangle$	23	6	2
$141=3\cdot47$	$\langle W_{47}\rangle$	47	3	2
$156=2^2\cdot3\cdot13$	$\langle W_3, W_{13}\rangle$	13	12	2
$156=2^2\cdot3\cdot13$	$\langle W_{12}, W_{52}\rangle$	13	12	2
$161=7\cdot23$	$\langle W_{161}\rangle$	23	7	2
$170=2\cdot5\cdot17$	$\langle W_2, W_{85}\rangle$	17	10	2
$170=2\cdot5\cdot17$	$\langle W_5, W_{34}\rangle$	17	10	2
$170=2\cdot5\cdot17$	$\langle W_{17}, W_{10}\rangle$	17	10	2
$186=2\cdot3\cdot31$	$\langle W_3, W_{62}\rangle$	31	6	2
$230=2\cdot5\cdot23$	$\langle W_2, W_{115}\rangle$	23	10	2
$276=2^2\cdot3\cdot23$	$\langle W_{23}, W_{12}\rangle$	23	12	2

TABLE 7

$N=\prod p^{\nu}$	W'	p	M	Fig.
$96=2^5\cdot3$	$\langle W_{32}\rangle$	3	32	1
$96=2^5\cdot3$	$\langle W_{96}\rangle$	3	32	2
$105=3\cdot5\cdot7$	$\langle W_{35}\rangle$	3	35	1
$120=2^3\cdot3\cdot5$	$\langle W_3, W_5\rangle$	5	24	2
$154=2\cdot7\cdot11$	$\langle W_{11}, W_{14}\rangle$	11	14	2
$154=2\cdot7\cdot11$	$\langle W_7, W_{22}\rangle$	11	14	2
$165=3\cdot5\cdot11$	$\langle W_5, W_{11}\rangle$	11	15	2
$180=2^2\cdot3^2\cdot5$	$\langle W_9, W_{20}\rangle$	5	36	2
$210=2\cdot3\cdot5\cdot7$	$\langle W_2, W_5, W_7\rangle$	7	30	2
$210=2\cdot3\cdot5\cdot7$	$\langle W_2, W_3, W_{35}\rangle$	7	30	2
$330=2\cdot3\cdot5\cdot11$	$\langle W_3, W_{11}, W_{10}\rangle$	11	30	2

(The last column of Tables 6 and 7 indicates the figure of $X_0(N)/W'$ mod$p$.)

For $M=24$, 32 and 36, the actions of Atkin–Lehner involutions are given by the group law on $X_0(M)$; explicit action will be written down by using the addition formula. For example, let $M=24$. Then

$$\begin{cases}(x, y)|W_{24}=(12(3x+6+y)/x^2, 6(x+4)(x^2+18x+36+6y)/x^3), \\ (x, y)|W_3 \ =(-3(x+4)/(x+3), 3y/(x+3)^2).\end{cases}$$

The action of W_{32} on $X_0(32)$ described in Table 5 includes an ambiguity; but this would not affect our arguments.

The data for $M=30$ are not given in [4]; these can be obtained by calculating the relations among modular forms (i.e., in the same manner as in [4]).

REMARK 9. We have determined the hyperellipticity of $X_0(N)/W'$ for

$N=$ 42, 52, 57, 63, 65, 77, 80, 84, 85, 88, 90, 91,
93, 96, 99, 102, 105, 114, 115, 116, 120, 123, 129, 130,
133, 138, 141, 156, 161, 170, 186, 198, 204, 230, 276.

6. Methods using the trace formulas of Hecke operators.

In this section we use the trace formulas of Hecke oprators to conclude that none of the remaining cases is hyperelliptic. We refer to [9] [16] for explicit trace formulas. Except for very few cases, the method explained in Section 5 would apply to the remaining cases. This method, however, would become complicated when N grows (especially when divisible by three or more distinct primes); sometimes direct use of the trace formulas would be helpful.

6.1. Rational points over finite fields. Let X be the quotient curve of $X_0(N)$ by a subgroup W' of $W(N)$. Then X is defined over $\mathbf{Q}$, and there is a model of $X/\mathbf{Q}$ which has good reduction outside N ([10]). Let p be a prime number with $p\nmid N$. Then X has good reduction at p and the number of rational points of $\tilde{X}=X \bmod p$ over $\mathbf{F}_{p^\alpha}$ can be computed by using the trace formula of Hecke operators:

$$|\tilde{X}(\mathbf{F}_{p^\alpha})|=1+p^\alpha-\operatorname{tr}T(p^\alpha)|S_2(N)^{W'} \\ +\begin{cases}p\cdot\operatorname{tr}T(p^{\alpha-2})|S_2(N)^{W'} & \text{if } \alpha\geq 2\,, \\ 0 & \text{otherwise}\,.\end{cases}$$

This is a direct deduction from the so-called Eichler–Shimura congruence relation. If X is hyperelliptic, then we must have

$$|\tilde{X}(\mathbf{F}_q)|\leq 2(1+q)\,,$$

since $\tilde{X}$ is a double covering of $\mathbf{P}^1$ over $\mathbf{F}_p$. It follows from this observation that X is non-hyperelliptic for the following (N, W'), as indicated in the third column:

$N=\prod p^{\nu}$	W'	$(q, \lvert\tilde{X}(\mathbf{F}_q)\rvert)$
$75=3\cdot 5^2$	$\langle W_{25}\rangle$	(4, 11)
$100=2^2\cdot 5^2$	$\langle W_{100}\rangle$	(9, 22)
$154=2\cdot 7\cdot 11$	$\langle W_2, W_7\rangle$	(9, 22)
$154=2\cdot 7\cdot 11$	$\langle W_2, W_{77}\rangle$	(3, 10)
$154=2\cdot 7\cdot 11$	$\langle W_{14}, W_{22}\rangle$	(3, 10)
$165=3\cdot 5\cdot 11$	$\langle W_3, W_{11}\rangle$	(4, 13)
$165=3\cdot 5\cdot 11$	$\langle W_3, W_{55}\rangle$	(2, 7)
$165=3\cdot 5\cdot 11$	$\langle W_5, W_{33}\rangle$	(7, 18)
$195=3\cdot 5\cdot 13$	$\langle W_3, W_{65}\rangle$	(4, 14)
$195=3\cdot 5\cdot 13$	$\langle W_{15}, W_{39}\rangle$	(4, 11)
$231=3\cdot 7\cdot 11$	$\langle W_3, W_{77}\rangle$	(4, 12)
$238=2\cdot 7\cdot 17$	$(W_2, W_{119}\rangle$	(9, 24)
$238=2\cdot 7\cdot 17$	$\langle W_{14}, W_{34}\rangle$	(9, 28)

6.2. Gap sequences. Let X be an algebraic curve over $\mathbf{C}$ of genus g. The Weierstrass gap sequence G_P at a point P of X is defined by

$$G_P=\{n\in\mathbf{Z}\mid n>0 \text{ and } (f)_{\infty}\neq n(P) \text{ for all } f\in\mathbf{C}(X)\}\,,$$

where $\mathbf{C}(X)$ is the function field of X over $\mathbf{C}$ and $(f)_{\infty}$ is the polar divisor of f. A point P on X is called a Weierstrass point if $G_P\neq\{1, 2, \cdots, g\}$. If X is hyperelliptic and P is a Weierstrass point of X, then $G_P=\{1, 3, 5, \cdots, 2g-1\}$. Now recall that the gap sequence at $P=\overline{i\infty}\in X_0(N)/W'$ can easily be computed by the following formula

$$G_P=\{n\in Z\mid \exists f\in S_2(N)^{W'} \text{ such that } f=q^n+\cdots\}\,.$$

(A basis of $S_2(N)^{W'}$ is obtained by using trace formulas of Hecke operators.) Thus we see that $X_0(N)/W'$ is non-hyperelliptic for the following (N, W'), since the point $P=\overline{i\infty}$ is a Weierstrass point with gap sequence $G_P\neq\{1, 3, \cdots, 2g-1\}$.

$N=\prod p^{\nu}$	W'	G_P
$180=2^2\cdot 3^2\cdot 5$	$\langle W_5, W_{36}\rangle$	$\{1, 2, 3, 4, 7\}$
$210=2\cdot 3\cdot 5\cdot 7$	$\langle W_5, W_7, W_6\rangle$	$\{1, 2, 5\}$
$210=2\cdot 3\cdot 5\cdot 7$	$\langle W_3, W_{10}, W_{14}\rangle$	$\{1, 2, 5\}$
$210=2\cdot 3\cdot 5\cdot 7$	$\langle W_5, W_6, W_{14}\rangle$	$\{1, 2, 4\}$
$330=2\cdot 3\cdot 5\cdot 11$	$\langle W_{11}, W_6, W_{10}\rangle$	$\{1, 2, 3, 5\}$
$390=2\cdot 3\cdot 5\cdot 13$	$\langle W_5, W_6, W_{26}\rangle$	$\{1, 2, 3, 4, 7\}$

7. Defining equations of hyperelliptic curves $X_0(N)/W'$ with $g\geq 3$.

In this section, we present the defining equations of all the hyperelliptic curves $X_0(N)/W'$ $(W'\neq\{1\}, W(N))$ with $g\geq 3$. One finds in [11] [15] an algorithm for computing the equations of (hyperelliptic) modular curves (see also [8]).

$N=\prod p^{\nu}$	W'	$f(z)$	$\mathrm{disc}(f(z))$
$46=2\cdot 23$	$\langle W_2\rangle$	$(z^2-4z-4)(z^3-z^2+1)(z^3-z^2-4z+5)$	$2^{17}23^8$
$51=3\cdot 17$	$\langle W_3\rangle$	$(z+1)(z^3-5z^2+3z-3)(z^4-2z^3+3z^2-6z+5)$	$-2^{16}3^3 17^{10}$
$55=5\cdot 11$	$\langle W_5\rangle$	$z(z^2+z-1)(z^2-7z+11)(z^3-4z-4)$	$-2^{16}5^2 11^7$
$56=2^3 7$	$\langle W_8\rangle$	$(z-1)(z-2)(z^2+z+2)(z^4-4z^3-8z+4)$	$2^{34}7^6$
$60=2^2 3\cdot 5$	$\langle W_4\rangle$	$(z^2-z-1)(z^2-4z-1)(z^4-z^3+2z^2+z+1)$	$2^{28}3^6 5^4$
	$\langle W_{12}\rangle$	$(z^2+z+1)(z^4+3z^3+8z^2+3z+1)(z^4+4z^3+10z^2+4z+1)$	$-2^{34}3^3 5^7$
	$\langle W_{60}\rangle$	$(z-1)(z-3)(z^2-5z+5)(z^4-9z^3+32z^2-51z+31)$	$2^{20}3^2 5^3$
$62=2\cdot 31$	$\langle W_2\rangle$	$(z^3+z^2+1)(z^3-3z^2+4z-3)(z^4-6z^3+9z^2-8z+8)$	$-2^{24}31^9$
$66=2\cdot 3\cdot 11$	$\langle W_6\rangle$	$(z^4-7z^3+11z^2-8z+4)(z^6-9z^5+32z^4-57z^3+56z^2-33z+11)$	$2^{21}3^2 11^5$
	$\langle W_{66}\rangle$	$(z^2-3z+3)(z^6-9z^5+32z^4-57z^3+56z^2-33z+11)$	$2^{16}3\cdot 11^3$
$69=3\cdot 23$	$\langle W_3\rangle$	$(z^3+z^2+2z+1)(z^3-3z^2+2z+1)(z^4-6z^3+7z^2+6z-11)$	$-2^{20}3^2 23^{11}$
$70=2\cdot 5\cdot 7$	$\langle W_{10}\rangle$	$(z^4+5z^3+13z^2+16z+8)$ $\times(z^6+11z^5+50z^4+127z^3+186z^2+147z+49)$	$2^{21}5^3 7^6$
	$\langle W_{14}\rangle$	$(z^2+z-1)(z^6-z^5+7z^3-16z^2+15z-5)$	$2^{16}5^4 7^4$
$78=2\cdot 3\cdot 13$	$\langle W_6)$	$(z^4+7z^3+20z^2+26z+13)(z^4+7z^3+16z^2+18z+9)$ $\times(z^6+10z^5+43z^4+98z^3+129z^2+96z+32)$	$2^{33}3^5 13^9$
	$\langle W_{26}\rangle$	$(z^4+3z^3+z^2+3z+1)(z^4+3z^3+5z^2+3z+1)$	$-2^{16}3^5 13^3$
	$\langle W_2, W_3\rangle$	$(z-3)(z^2+z+1)(z^2+z-3)(z^3+z^2-4)$	$2^{23}3^5 13^6$
	$\langle W_{13}, W_6\rangle$	$(z-1)(z^2-3z-1)(z^2-3z+3)(z^3-5z^2+8z-8)$	$2^{17}3^3 13^4$
$87=3\cdot 29$	$\langle W_3\rangle$	$(z^3-z^2+2z+1)(z^3-5z^2+6z-3)$ $\times(z^6-4z^5+12z^4-22z^3+32z^2-28z+17)$	$-2^{24}3^4 29^{12}$
$92=2^2 23$	$\langle W_4\rangle$	$(z^3-z^2+2z-1)(z^3-4z^2+4z-8)$ $\times(z^6-5z^5+14z^4-25z^3+28z^2-20z+8)$	$-2^{54}23^7$
	$\langle W_{92}\rangle$	$(z-1)(z^3-4z^2+7z-5)$ $\times(z^6-11z^5+54z^4-151z^3+252z^2-238z+101)$	$2^{24}23^4$
$94=2\cdot 47$	$\langle W_2\rangle$	$(z^4-6z^3+9z^2-8)(z^5-z^4-3z^3+3z^2+4z+1)$ $\times(z^5-5z^4+9z^3-5z^2-4z+5)$	$-2^{30}47^{11}$
	$\langle W_{94}\rangle$	$(z^5-10z^4+39z^3-72z^2+58z-11)(z^5-6z^4+11z^3-4z^2-2z+1)$	$2^{20}47^4$

$N=\prod p^{\nu}$	W'	$f(z)$	$\operatorname{disc}(f(z))$
$95=5\cdot 19$	$\langle W_5\rangle$	$(z-2)(z^3-2z^2+4)(z^4-3z^3-3z^2+z-1)(z^4-3z^3+z^2+5z-5)$	$-2^{24}5^6 19^9$
	$\langle W_{19}\rangle$	$(z^4-3z^3-3z^2+z-1)(z^4-3z^3+z^2+5z-5)$	$2^{16}5^6 19^4$
$105=3\cdot 5\cdot 7$	$\langle W_3, W_5\rangle$	$(z-2)(z^2+z+1)(z^2-3z-3)(z^3-2z^2-4)$	$2^{16}3^2 5^9 7^6$
	$\langle W_3, W_7\rangle$	$z(z^2+z-1)(z^2+z-5)(z^3+4z^2+4z-4)$	$-2^{16}3\cdot 5^{10}7^2$
	$\langle W_7, W_{15}\rangle$	$(z-2)(z^2+z+1)(z^2-3z+1)(z^3-2z^2-4)$	$2^{16}3\cdot 5^2 7^5$
$110=2\cdot 5\cdot 11$	$\langle W_2, W_5\rangle$	$(z^2-z-1)(z^2-z+3)(z^3-4z^2+5z-10)(z^3-2z^2+4z-4)$	$-2^{21}5^4 11^9$
	$\langle W_2, W_{11}\rangle$	$(z-1)(z^2+z-1)(z^2+z+3)(z^3-z^2-8)$	$2^{19}5^6 11^6$
	$\langle W_5, W_{22}\rangle$	$(z-2)(z^2-z-1)(z^2-z+3)(z^3-2z^2+4z-4)$	$2^{16}5^3 11^4$
$119=7\cdot 17$	$\langle W_7\rangle$	$(z^4-2z^3+3z^2+2z+1)(z^5-3z^4+5z^3-z^2-2z+1)$ $\times(z^5-7z^4+21z^3-37z^2+34z-19)$	$2^{28}7^6 17^{11}$
	$\langle W_{17}\rangle$	$(z^5-2z^4+3z^3-6z^2-7)(z^5+2z^4+3z^3+6z^2+4z+1)$	$2^{20}7^6 17^6$

$N=\prod p^{\nu}$	W'	$f(z)$	$\operatorname{disc}(f(z))$
$63=3^2 7$	$\langle W_9\rangle$	$(z^4+z^3+3z^2+z+1)(z^4+5z^3+15z^2+5z+1)$	$2^{16}3^{12}7^6$
$72=2^3 3^2$	$\langle W_9\rangle$	$z^8-8z^6+30z^4-8z^2+1$	$2^{40}3^6$
$104=2^3 13$	$\langle W_{104}\rangle$	$z(z-2)(z^6-4z^5+3z^4+8z^3-15z^2+10z-4)$	$2^{22}13^3$
$120=2^3 3\cdot 5$	$\langle W_5, W_{24}\rangle$	$(z^2-z-1)(z^2-3z+3)(z^2-3z+1)(z^2-5z+5)$	$-2^{24}3\cdot 5^3$
$126=2\cdot 3^2 7$	$\langle W_9, W_7\rangle$	$(z^2+3)(z^2+z+1)(z^4+5z^3+8z^2+7z+7)$	$2^{28}3^4 7^4$
	$\langle W_9, W_{14}\rangle$	$(z^4-5z^3+9z^2-5z+1)(z^4-z^3-3z^2-z+1)$	$-2^{16}3^6 7^3$
$168=2^3 3\cdot 7$	$\langle W_{24}, W_{56}\rangle$	$(z^2+z+1)(z^4+3z^3+7z^2+8z+4)(z^4+4z^3+11z^2+14z+7)$	$-2^{29}3^3 7^4$

$N=\prod p^{\nu}$	W'	$f(z)$	$\operatorname{disc}(f(z))$
$85=5\cdot 17$	$\langle W_{85}\rangle$	$z^8-6z^7+13z^6-16z^5+26z^4-42z^3+32z^2-8z+1$	$2^{16}5^2 17^3$
$114=2\cdot 3\cdot 19$	$\langle W_2, W_{19}\rangle$	$(z^2+z+1)(z^6-z^5+6z^4+7z^3+6z^2-z+1)$	$2^{16}3^7 19^3$
$130=2\cdot 5\cdot 13$	$\langle W_2, W_{13}\rangle$	$z^8+6z^7+25z^6+72z^5+146z^4+202z^3+184z^2+100z+25$	$2^{16}5^5 13^3$
$165=3\cdot 5\cdot 11$	$\langle W_{11}, W_{15}\rangle$	$(z^4-3z^3+3z^2-3z+1)(z^4-3z^3+7z^2-3z+1)$	$-2^{16}3^2 5^3 11^3$
$195=3\cdot 5\cdot 13$	$\langle W_5, W_{39}\rangle$	$z^8-6z^7+17z^6-28z^5+22z^4+2z^3-12z^2+5$	$2^{16}5^3 13^3$

References

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

[2] A. O. L. Atkin and D. J. Tingley, Numerical tables on elliptic curves, *Modular Functions of One Variable IV* (B. Birch and W. Kuyk, eds.), Lecture Notes in Math. **476** (1975), Springer, 74–144.

[3] P. Deligne and M. Rapoport, Les schémas de modules de courbes elliptiques, *Modular Functions of One Variable II* (P. Deligne and W. Kuyk, eds.), Lecture Notes in Math. **349** (1973), Springer, 143–316.

[4] R. Fricke, *Die Elliptischen Funktionen und ihre Anwendungen*, Teubner (1916).

[5] Y. Hasegawa, Table of quotient curves of modular curves $X_0(N)$ with genus 2, Proc. Japan Acad. Ser. A **71** (1995), 235–239.

[6] ———, Hyperelliptic modular curves $X_0^*(N)$, Acta Arith. **81** (1997), 369–385.

[7] ———, Modular abelian surfaces and hyperelliptic curves of genus two, preprint.

[8] Y. Hasegawa and K. Hashimoto, Hyperelliptic modular curves $X_0^*(N)$ with square-free levels, Acta Arith. **77** (1996), 179–193.

[9] H. Hijikata, Explicit formula of the traces of Hecke operators for $\Gamma_0(N)$, J. Math. Soc. Japan **26** (1974), 56–82.

[10] J. Igusa, Kroneckerian model of fields of elliptic modular functions, Amer. J. Math. **81** (1959), 561–577.

[11] N. Murabayashi, On normal forms of modular curves of genus 2, Osaka J. Math. **29** (1992), 405–418.

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

[13] ———, Modular functions, *The Santa Cruz Conference on Finite Groups* (B. Cooperstein and G. Mason, eds.), Proc. Sympos. Pure Math. **37** (1980), Amer. Math. Soc., 521–532.

[14] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Iwanami/Princeton Univ. Press (1971).

[15] M. Shimura, Defining equations of modular curves $X_0(N)$, Tokyo J. Math. **18** (1995), 443–456.

[16] M. Yamauchi, On the traces of Hecke operators for a normalizer of $\Gamma_0(N)$, J. Math. Kyoto Univ. **13** (1973), 403–411.

Present Address:
Yuji Hasegawa (author for correspondence)
Department of Mathematics, Waseda University,
3–4–1, Okubo, Shinjuku-ku, Tokyo, 169–8555 Japan.
e-mail: hasegawa@gm.math.waseda.ac.jp