ACTA ARITHMETICA
LXXVII.2 (1996)

Hyperelliptic modular curves $X_0^*(N)$ with square-free levels

by

Yuji Hasegawa and Ki-ichiro Hashimoto (Tokyo)

Introduction. Let N be a positive integer, and let

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

For each positive divisor N' of N with $(N',\ N/N') = 1$ (we write $N' \parallel N$), $W_{N'} = W_{N'}^{(N)}$ denotes the corresponding Atkin–Lehner involution defined for $\Gamma_0(N)$. (If $N' = 1$, W_1 means the identity operator.) Then we define the modular group $\Gamma_0^*(N)$ to be

$$\Gamma_0^*(N) = \langle \Gamma_0(N) \cup \{W_{N'}\}_{N' \parallel N} \rangle,$$

i.e., $\Gamma_0^*(N)$ is generated by $\Gamma_0(N)$ and $\{W_{N'}\}_{N' \parallel N}$. Then $\Gamma_0^*(N)$ is a normalizer of $\Gamma_0(N)$ in $\mathrm{GL}_2^+(\mathbb{Q}) = \{A \in M_2(\mathbb{Q}) \mid \det A > 0\}$. The factor group $\Gamma_0^*(N)/\Gamma_0(N)$ is abelian of type $(2, \ldots, 2)$ and of order $2^{\omega(N)}$, where $\omega(N)$ denotes the number of distinct prime divisors of N. Moreover, it is known that $\Gamma_0^*(N)$ is the *full* normalizer of $\Gamma_0(N)$ if N is divisible neither by 4 nor by 9. In the case N is divisible by 4 or 9, the full normalizer of $\Gamma_0(N)$ is strictly bigger than $\Gamma_0^*(N)$, and the factor group is no longer abelian. See [1] and [11] for this topic.

Let $X_0^*(N)$ be the modular curve which corresponds to $\Gamma_0^*(N)$, namely,

$$X_0^*(N) = X_0(N)/\langle \{W_{N'}\}_{N' \parallel N} \rangle.$$

In [13], Ogg determined all hyperelliptic $X_0(N)$ in order to investigate the rational points of $Y_0(N) = \Gamma_0(N)\backslash\mathfrak{H}$, where $\mathfrak{H}$ is the complex upper half plane. There are nineteen values of N for which $X_0(N)$ is hyperelliptic.

After the work of Ogg, Mazur asked Kluit whether it is possible to determine all of hyperelliptic curves of type $X_0^*(N)$. Since $\mathrm{Aut}\, X_0^*(N)$ is very small, and the Fuchsian group $\Gamma_0^*(N)$ is maximal if N is square-free, Ogg's

1991 *Mathematics Subject Classification*: Primary 14H45; Secondary 14G05, 14H25, 11F11, 11G30.

methods do not seem to work well in this case. So, to check the hyperellipticity of $X_0^*(N)$ (for given N), Kluit [10] directly computed the numbers of rational points of $X_0^*(N)$ over finite fields using traces of Hecke operators (see Section 1). Note that this procedure only gives a necessary condition for $X_0^*(N)$ being hyperelliptic. The following table lists the *square-free* N for which Kluit failed to determine whether $X_0^*(N)$ is hyperelliptic or not:

127	183	185	194	217	246
258	282	290	310	318	322
345	370	462	510	546	570
690	714	2310			

He ended his work by conjecturing that none of these are hyperelliptic. In this article, we shall prove this conjecture.

Notation. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ denote respectively the ring of rational integers, the field of rational nambers and the field of complex numbers. $\mathbb{F}_{p^\nu}$ denotes the finite field with p^ν elements. $\mathbb{P}^n$ is the n-dimensional projective space (over a field which may be indicated in each context).

1. Rational points over finite fields. Let X be a curve defined over $\mathbb{Q}$. Then X is called *sub-hyperelliptic* if X is rational (genus $= 0$), elliptic (genus $= 1$), or hyperelliptic. Then X is sub-hyperelliptic if and only if there exists a double covering $X \to \mathbb{P}^1$ defined over $\mathbb{Q}$. If X is sub-hyperelliptic and has good reduction at a prime p, there exists a double covering $\widetilde{X} \to \mathbb{P}^1$ over $\mathbb{F}_p$, where $\widetilde{X}$ is the reduction of X at p. Thus, if X is sub-hyperelliptic and has good reduction modulo p, we have

$$\sharp\widetilde{X}(\mathbb{F}_{p^\nu}) \le 2(1+p^\nu), \tag{1}$$

since $\sharp\mathbb{P}^1(\mathbb{F}_{p^\nu}) = 1 + p^\nu$.

It is well known that each $W_{N'}$ is defined over $\mathbb{Q}$, so that $X_0^*(N)$ is defined over $\mathbb{Q}$. Moreover, there exists a model of $X_0^*(N)$ over $\mathbb{Z}$ which has good reduction at each prime p with $p\nmid N$ (cf. [9]). Hence if $X = X_0^*(N)$ is sub-hyperelliptic, (1) holds for all $p\nmid N$. On the other hand, Ogg [13] (see also [14]) found the inequality

$$\sharp\widetilde{X}_0(N)(\mathbb{F}_{p^2}) \ge \frac{p-1}{12} N \prod_{\substack{q\mid N\\ q\ \text{prime}}} \left(1+\frac{1}{q}\right) + 2^{\omega(N)} \tag{2}$$

for $p\nmid N$, the first term of the right hand side being the contribution of supersingular points, and the second being that of cusps. From this, we have

$$\sharp\widetilde{X}_0^*(N)(\mathbb{F}_{p^2}) \ge \frac{1}{2^{\omega(N)}} \cdot \frac{p-1}{12} N \prod_{q\mid N} \left(1+\frac{1}{q}\right) + 1 \tag{3}$$

for $p \nmid N$, since the covering map $X_0(N) \to X_0^*(N)$ is of degree $2^{\omega(N)}$. Therefore, if

$$2(1+p^2) < \frac{1}{2^{\omega(N)}} \cdot \frac{p-1}{12} N \prod_{q|N} \left(1+\frac{1}{q}\right) + 1 \tag{4}$$

for some $p \nmid N$, then $X_0^*(N)$ is not sub-hyperelliptic.

Theorem (Kluit). *$X_0^*(N)$ is sub-hyperelliptic for only finitely many N.*

Proof. We can find an upper bound for N for which $X_0^*(N)$ may be sub-hyperelliptic. In fact, if $N \ge 10848$, there exists a prime p such that $p \nmid N$ and satisfies the inequality (4). This can be shown as follows.

Put

$$f(N) := \frac{1}{2^{\omega(N)}} N \prod_{q|N} \left(1+\frac{1}{q}\right) \quad \text{and} \quad g(p) := 12\frac{1+2p^2}{p-1}.$$

Then $f(N)$ is multiplicative and $g(p)$ is increasing for $p \ge 2$. Suppose all prime numbers are ordered in a natural way: $p_1 = 2, p_2 = 3, \ldots$ Then

Lemma. *If $r \ge 6$, then*

$$f(p_1 \ldots p_r) > g(p_{r+1}).$$

Proof. For $r = 6, f(2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13) = 1512 > g(17) = 434.25$. For $r > 6$, we use induction on r; it is sufficient to show that

$$\frac{f(p_1 \ldots p_r)}{f(p_1 \ldots p_{r-1})} > \frac{g(p_{r+1})}{g(p_r)}.$$

But

$$\frac{f(p_1 \ldots p_r)}{f(p_1 \ldots p_{r-1})} = f(p_r) = \frac{1}{2}(p_r+1) > 4$$

and

$$\frac{g(p_{r+1})}{g(p_r)} = \frac{1+2p_{r+1}^2}{1+2p_r^2} \cdot \frac{p_r - 1}{p_{r+1}-1} < \frac{1+2p_{r+1}^2}{1+2p_r^2} \le \frac{1+8p_r^2}{1+2p_r^2} < 4.$$

This proves the lemma. (Note that $p_{r+1} < 2p_r$ by Chebyshev's theorem.) ■

Now return to the proof of the Theorem. Write $r = \omega(N)$ and let $N = p_{i_1}^{\alpha_1} \ldots p_{i_r}^{\alpha_r}$ with $i_1 < \ldots < i_r$. Then $i_k \ge k$, so $p_{i_k} \ge p_k$ and $f(N) \ge f(p_1 \ldots p_r)$. Let p be the smallest prime not dividing N. Then $p \le p_{r+1}$ and so $g(p) \le g(p_{r+1})$. Hence, by the previous lemma, we obtain

$$f(N) \ge f(p_1 \ldots p_r) > g(p_{r+1}) \ge g(p) \quad \text{if } r \ge 6,$$

i.e., inequality (4) holds if $r \ge 6$. Next we assume $r < 6$ and $N \ge 10848$. Then $p \le p_6 = 13$, so $g(p) \le g(13) = 339$. On the other hand, we have $f(N) > N/2^5 \ge 339 \ge g(p)$, hence again (4) holds. ■

In the proof of the Theorem, we have an explicit but rather rough estimate $N < 10848$. Checking the inequality (4) for each $N = 1, \ldots, 10847$ with p the first prime not dividing N, and excluding N for which (4) holds, we get the collection of N for which we do not know whether $X_0^*(N)$ is hyperelliptic or not (Table 1).

Table 1

Genus	N									
3	97	109	113	127	128	136	139	144	149	151
	152	162	164	169	171	175	178	179	183	185
	187	189	194	196	203	207	217	234	236	240
	245	246	248	249	252	258	270	282	290	294
	295	303	310	312	315	318	329	348	420	429
	430	455	462	476	510					
4	137	148	160	172	173	176	199	200	201	202
	214	219	224	225	228	242	247	254	259	260
	261	262	264	267	273	275	280	300	305	306
	308	319	321	322	335	341	342	345	350	354
	355	366	370	374	385	399	426	434	483	546
	570									
5	157	181	192	208	212	216	218	226	235	237
	250	253	278	279	302	323	364	371	377	378
	391	396	402	406	410	414	418	435	438	440
	442	444	465	494	495	595	630	714	770	798
6	163	197	211	244	265	272	274	291	297	301
	325	336	340	470	506	561	564	690	780	858
7	193	232	268	288	296	298	309	360	372	450
	456	460	474	492	498	504	518	558	582	660
	870	924								
8	292	408	468	480	534	540	552	606	930	966
	990	1020								
9	516	522	528	1110	1140					
10	600	840	1050	1230	1290					
12	2310									
13	1260									
14	2730									
15	1470									
19	1680									

Next we calculate $\sharp\widetilde{X}_0^*(N)(\mathbb{F}_{p^\nu})$ exactly for all N given in Table 1, using the traces of Hecke operators. Trace formulas of Hecke operators are given in [8] and [17]. If the inequality (1) breaks down, then $X_0^*(N)$ is not hyperelliptic. However, the following holds:

Let X be a non-singular curve defined over $\mathbb{F}_p$ with genus g. Let ν be a natural number such that $p^\nu \geq 4g^2$. Then

$$\sharp X(\mathbb{F}_{p^\nu}) \leq 2(1 + p^\nu).$$

Proof. Let α_i be the eigenvalues of Frobenius map. Then $|\alpha_i| = \sqrt{p}$ by Weil's theorem, so $|\sum_{i=1}^{2g} \alpha_i^\nu| \le 2g \cdot \sqrt{p}^\nu \le p^\nu$. Hence

$$\sharp X(\mathbb{F}_{p^\nu}) = 1 + p^\nu - \sum_{i=1}^{2g} \alpha_i^\nu \le 1 + 2p^\nu < 2(1 + p^\nu),$$

as desired. ■

So testing the inequality $\sharp\widetilde{X}_0^*(N)(\mathbb{F}_{p^\nu}) > 2(1+p^\nu)$ makes sense for $p^\nu < 4g^2$. Calculation of $\sharp\widetilde{X}_0^*(N)(\mathbb{F}_{p^\nu})$ for square-free N was done in [10], in which Kluit listed up 21 values of square-free integer N for which he could not determine whether $X_0^*(N)$ is hyperelliptic or not. He also conjectured that none of these are in fact hyperelliptic; this is equivalent to saying that, under the assumption that N is square-free, $X_0^*(N)$ is hyperelliptic if and only if it is of genus two. Here we re-calculate $\sharp\widetilde{X}_0^*(N)(\mathbb{F}_{p^\nu})$ for *all* N given in Table 1. We will give the list of N's removed from Table 1 in Appendix A. The remainder of Table 1 is given in Table 2. (Of course, all N listed in the introduction are contained in Table 2.)

Table 2

Genus	N									
3	127	136	144	152	162	164	171	175	183	185
	194	196	207	217	234	240	246	252	258	270
	282	290	294	310	312	315	318	348	420	462
	476	510								
4	160	176	264	280	300	306	322	342	345	370
	546	570								
5	216	279	396	630	714					
6	336	690								
7	360	450								
10	840									
12	2310									
19	1680									

2. Determination of hyperelliptic $X_0^*(N)$. Let $S_2^*(N)$ be the space of cuspforms of weight two with respect to $\Gamma_0^*(N)$. If $X_0^*(N)$ is of genus g, then $\dim_{\mathbb{C}} S_2^*(N) = g$. In this section, we assume $g \ge 3$. Let $\langle f_1, \ldots, f_g\rangle$ be a basis of $S_2^*(N)$. Since $S_2^*(N)$ can be identified with the space of holomorphic 1-forms, we have a canonical morphism (see, e.g., [5], Chap. IV, §5)

$$(f_1 : \ldots : f_g) : X = X_0^*(N) \to X' \subseteq \mathbb{P}^{g-1}. \tag{5}$$

This gives the canonical embedding if X is not hyperelliptic. Let p be a prime number with $(p, N) = 1$ and put $f_j'(\tau) = f_j(\tau) + pf_j(p\tau)$ for $j = 1, \ldots, g$. Then $\langle f_1', \ldots, f_g'\rangle_{\mathbb{C}} \subseteq S_2^*(pN)$.

PROPOSITION 1. *Let p and N be as above. Assume that $X_0^*(N)$ and $X_0^*(pN)$ are of the same genus and that $X_0^*(N)$ is not hyperelliptic. Then $X_0^*(pN)$ is not hyperelliptic either.*

Proof. Since $f_j' \equiv f_j$ modulo p, $X_0^*(pN)$ is isomorphic to $X_0^*(N)$ in characteristic p. ∎

Applying this to the case $N = 97$ and $N = 273$ with $p = 2$, we can drop two values $N = 194$ and 546 from Table 2.

Now return to (5). Then X is hyperelliptic if and only if X' is of genus zero, and in this case, X' is the $(g-1)$-uple embedding of $\mathbb{P}^1$ in $\mathbb{P}^{g-1}$. So, if X is hyperelliptic, we may assume that $f_1, \ldots, f_g$ are of the form

$$(6) \qquad \begin{cases} f_1 = q + a_2^{(1)} q^2 + a_3^{(1)} q^3 + \ldots, \\ f_2 = q^2 + a_3^{(2)} q^3 + \ldots, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ f_g = q^g + a_{g+1}^{(g)} q^{g+1} + \ldots \end{cases}$$

or

$$(7) \qquad \begin{cases} f_1 = q + a_2^{(1)} q^2 + a_3^{(1)} q^3 + \ldots, \\ f_2 = q^3 + a_4^{(2)} q^4 + \ldots, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ f_g = q^{2g-1} + a_{2g}^{(g)} q^{2g} + \ldots \end{cases}$$

according as $\overline{i\infty}$ is an ordinary point or a Weierstrass point, where $q = \exp(2\pi i\tau), \tau \in \mathfrak{H}$. So our interest reduces to the case that $S_2^*(N)$ has a basis of the form (6) or (7). In what follows, we assume that $S_2^*(N)$ has a basis $\langle f_1, \ldots, f_g \rangle$ of the form (6), because we did not encounter the case that $S_2^*(N)$ has a basis of the form (7).

EXAMPLE. Let $N = 282$. We have obtained a basis of $S_2^*(282)$ which is neither of the form (6) nor (7) (see Appendix B). Thus $X_0^*(282)$ is not hyperelliptic.

If X has $g = 3$, then X' is a plane curve, so X' is of genus zero if and only if f_1, f_2, f_3 satisfy a quadratic relation. For the case $g \geq 4$, X' is no longer a plane curve, so it seems to be difficult to determine the genus of X'. Instead, we will make use of the following method. (Of course, this can be applied to the case $g = 3$.) Put

$$z = \frac{f_{g-1}}{f_g}, \qquad w = \frac{dz}{2\pi i f_g \, d\tau} = \left(\frac{f_g}{q}\right)^{-1} \frac{dz}{dq}$$

and define

$$G(T) = T^{2g+2} + v_{2g+1}T^{2g+1} + \ldots + v_0 \in \mathbb{Q}[T]$$

by the condition $\mathrm{ord}_q(w^2 - G(z)) \geq 1$, i.e., the Laurent series $w^2 - G(z)$ consists only of positive q-power terms. Put

$$w^2 - G(z) = \sum_{j\geq 1} d_j q^j. \tag{8}$$

Then

PROPOSITION 2. $X = X_0^*(N)$ *is hyperelliptic if and only if the following two conditions hold*:

(i) $G(T)$ *is separable*,
(ii) $d_1 = \ldots = d_h = 0$, *where* $h = 4g^2 + 8g - 20$.

Proof. Suppose X is hyperelliptic. Then

$$[\mathbb{C}(X) : \mathbb{C}(f_1/f_g, \ldots, f_{g-1}/f_g)] = 2$$

and the genus of $\mathbb{C}(f_1/f_g, \ldots, f_{g-1}/f_g)$ is zero, that is,

$$\mathbb{C}(f_1/f_g, \ldots, f_{g-1}/f_g) = \mathbb{C}(x)$$

for some x in $\mathbb{C}(f_1/f_g, \ldots, f_{g-1}/f_g)$. Since the image X' of X (see (5)) is the $(g-1)$-uple embedding of $\mathbb{P}^1$ in $\mathbb{P}^{g-1}$ and the order of the pole of f_j/f_g at $\overline{i\infty}$ is $g-j$, we can take $z = f_{g-1}/f_g$ as x. On the other hand, there exists an element $y \in \mathbb{C}(X)$ such that (i) $\mathbb{C}(X) = \mathbb{C}(z, y)$ and (ii) $y^2 = F(z)$ with some separable polynomial $F(T) \in \mathbb{C}[T]$, for $\mathbb{C}(X)$ is a quadratic extension of $\mathbb{C}(z)$. Then dz/y is a holomorphic 1-form on X, so there exists a linear relation

$$\frac{dz}{y} = c_1 2\pi i f_1(\tau)\, d\tau + c_2 2\pi i f_2(\tau)\, d\tau + \ldots + c_g 2\pi i f_g(\tau)\, d\tau.$$

Comparing the orders of zero at $\overline{i\infty}$ on both sides, we see that

$$\frac{dz}{y} = c_g 2\pi i f_g(\tau) d\tau.$$

Put $w = c_g y$ and $G(T) = c_g^2 F(T)$. Then $w^2 = G(z)$ with G separable.

Conversely, suppose $G(T)$ is separable and $d_i = 0$ for $i = 1, \ldots, h$. Let $\nu_P(\varphi)$ denote the order of zero of $\varphi \in \mathbb{C}(X)$ at $P \in X$, and $n_\infty(\varphi)$ the sum of the orders of the poles of φ. Then

$$\nu_P(z) = \nu_P(f_{g-1}) - \nu_P(f_g) = \nu_P(f_{g-1} d\tau) - \nu_P(f_g d\tau),$$

so $n_\infty(z) \leq 2g - 2$. Similarly,

$$n_\infty(w) = n_\infty\left(\frac{dz}{2\pi i f_g d\tau}\right) \leq 6g - 6.$$

This shows that $n_\infty(w^2 - G(z)) \le 4g^2 + 8g - 20 = h$. Hence we conclude that $w^2 - G(z)$ is identically zero. Since the equation $w^2 = G(z)$ defines a curve of genus exactly g, this must be the defining equation for X. ∎

A basis of $S_2^*(N)$ is computed by using Brandt matrices and trace formulas of Hecke operators ([4], [7], [8], [15], [17]).

Example. (See also Appendix C.) From Table 2, $X_0^*(127)$ is of genus three and we do not know whether it is hyperelliptic or not. A basis of $S_2^*(127)$ is given by

$$\begin{aligned}
f_1 &= q - 2q^4 - 4q^5 - 3q^6 - 3q^7 + 3q^8 + 3q^{10} + q^{11} + 3q^{12} + 4q^{13} + 3q^{14} + \ldots,\\
f_2 &= q^2 - 2q^4 - q^5 - 2q^6 - q^7 + 2q^8 + q^9 + 2q^{11} + 3q^{12} + 2q^{13} + q^{14} + \ldots,\\
f_3 &= q^3 - q^4 - q^5 - q^6 - q^7 + 3q^8 - q^9 + 2q^{10} - q^{11} + q^{12} + 3q^{13} + 2q^{14} + \ldots
\end{aligned}$$

and they satisfy no quadratic equation. In fact, they satisfy a quartic equation

$$\begin{aligned}
f_1^3 f_3 - f_1^2 f_2^2 - 3f_1^2 f_3^2 + f_1 f_2^3 - f_1 f_2 f_3^2 &\\
+ 4f_1 f_3^3 + 2f_2^3 f_3 - 3f_2^2 f_3^2 + 3f_2 f_3^3 - 2f_3^4 &= 0,
\end{aligned}$$

which gives the defining equation for $X_0^*(127)$. Thus, $X_0^*(127)$ is not hyperelliptic. We can use Proposition 2 instead of the argument above. z and w are given by

$$\begin{aligned}
z &= q^{-1} + 1 + q^2 + q^3 - q^4 + q^5 + 2q^6 - q^7 + q^8 + \ldots,\\
w &= -q^{-4} - q^{-3} - 2q^{-2} - 2q^{-1} - 3 - 9q - 9q^2 - 4q^3 - 27q^4 - 30q^5 + \ldots
\end{aligned}$$

Then we have

$$G(T) = T^8 - 6T^7 + 19T^6 - 44T^5 + 67T^4 - 58T^3 + 25T^2 + 4T - 2$$

and

$$w^2 - G(z) = -18q + \ldots$$

This gives another proof that $X_0^*(127)$ is not hyperelliptic.

Since all other cases can be proved similarly, we only list in Appendix B the data of basis of $S_2^*(N)$ by giving their Fourier coefficients and d_1 appearing in (8); recall that if $X_0^*(N)$ is hyperelliptic, all d_j's must vanish, so in particular if $d_1 \ne 0$, then $X_0^*(N)$ is not hyperelliptic.

Proceeding in this way, we get finally

Theorem. *Assume that N is square-free. Then $X_0^*(N)$ is hyperelliptic if and only if $X_0^*(N)$ is of genus two.*

Remark. It is known that $X_0^*(N)$ is of genus two if and only if N is in the following list:

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			

Their defining equations are given in [6] (see also [12]).

Remark. There are 64 values of N ($\neq 1$) with largest 119 for which $X_0^*(N)$ is of genus zero. Also there are 65 values of N with largest 238 for which $X_0^*(N)$ is of genus one.

Appendix A. Table 3 is the list of N's removed from Table 1. The first column gives N, the second the genus of $X_0^*(N)$, and the third gives the pair $(p^\nu, \sharp\widetilde{X}_0^*(N)(\mathbb{F}_{p^\nu}))$ from which we know that $X_0^*(N)$ is not hyperelliptic.

Table 3

N	g		N	g		N	g		N	g	
97	3	$(2,7)$	173	4	$(4,14)$	350	4	$(9,23)$	377	5	$(4,14)$
109	3	$(4,11)$	199	4	$(4,12)$	354	4	$(7,17)$	378	5	$(25,62)$
113	3	$(4,11)$	200	4	$(9,25)$	355	4	$(4,13)$	391	5	$(4,13)$
128	3	$(9,24)$	201	4	$(2,7)$	366	4	$(25,54)$	402	5	$(5,14)$
139	3	$(4,11)$	202	4	$(3,9)$	374	4	$(9,23)$	406	5	$(3,10)$
149	3	$(4,12)$	214	4	$(9,22)$	385	4	$(3,9)$	410	5	$(3,10)$
151	3	$(4,11)$	219	4	$(2,7)$	399	4	$(2,7)$	414	5	$(25,60)$
169	3	$(4,11)$	224	4	$(9,22)$	426	4	$(25,55)$	418	5	$(9,22)$
178	3	$(9,21)$	225	4	$(4,15)$	434	4	$(9,25)$	435	5	$(2,7)$
179	3	$(4,12)$	228	4	$(5,14)$	483	4	$(4,15)$	438	5	$(5,14)$
187	3	$(5,13)$	242	4	$(9,24)$	157	5	$(2,8)$	440	5	$(9,25)$
189	3	$(4,11)$	247	4	$(9,21)$	181	5	$(4,14)$	442	5	$(3,9)$
203	3	$(13,29)$	254	4	$(9,25)$	192	5	$(25,56)$	444	5	$(11,26)$
236	3	$(9,22)$	259	4	$(4,12)$	208	5	$(3,10)$	465	5	$(4,12)$
245	3	$(4,13)$	260	4	$(3,9)$	212	5	$(3,12)$	494	5	$(9,26)$
248	3	$(9,24)$	261	4	$(4,15)$	218	5	$(3,12)$	495	5	$(4,12)$
249	3	$(4,14)$	262	4	$(9,26)$	226	5	$(3,9)$	595	5	$(4,13)$
295	3	$(4,12)$	267	4	$(4,14)$	235	5	$(2,7)$	770	5	$(3,9)$
303	3	$(4,13)$	273	4	$(2,7)$	237	5	$(2,7)$	798	5	$(25,57)$
329	3	$(4,12)$	275	4	$(4,12)$	250	5	$(3,9)$	163	6	$(2,8)$
429	3	$(4,11)$	305	4	$(4,14)$	253	5	$(2,7)$	197	6	$(4,15)$
430	3	$(9,24)$	308	4	$(3,10)$	278	5	$(9,30)$	211	6	$(4,15)$
455	3	$(4,11)$	319	4	$(4,11)$	302	5	$(9,29)$	244	6	$(3,11)$
137	4	$(4,12)$	321	4	$(4,15)$	323	5	$(4,12)$	265	6	$(2,8)$
148	4	$(3,11)$	335	4	$(9,23)$	364	5	$(5,15)$	272	6	$(7,18)$
172	4	$(5,17)$	341	4	$(4,15)$	371	5	$(4,15)$	274	6	$(3,9)$

Table 3 (cont.)

N	g		N	g		N	g	
291	6	$(2,9)$	456	7	$(5,14)$	606	8	$(5,16)$
297	6	$(7,17)$	460	7	$(13,31)$	930	8	$(7,18)$
301	6	$(4,13)$	474	7	$(25,64)$	966	8	$(5,13)$
325	6	$(3,9)$	492	7	$(5,13)$	990	8	$(49,106)$
340	6	$(3,13)$	498	7	$(25,62)$	1020	8	$(7,18)$
470	6	$(9,26)$	504	7	$(25,60)$	516	9	$(5,19)$
506	6	$(3,11)$	518	7	$(3,10)$	522	9	$(19,48)$
561	6	$(2,7)$	558	7	$(25,54)$	528	9	$(7,18)$
564	6	$(25,72)$	582	7	$(5,15)$	1110	9	$(49,110)$
780	6	$(7,17)$	660	7	$(7,17)$	1140	9	$(7,18)$
858	6	$(25,59)$	870	7	$(49,102)$	600	10	$(49,136)$
193	7	$(2,8)$	924	7	$(25,66)$	1050	10	$(11,25)$
232	7	$(3,12)$	292	8	$(3,10)$	1230	10	$(13,29)$
268	7	$(5,21)$	408	8	$(5,16)$	1290	10	$(49,123)$
288	7	$(25,68)$	468	8	$(25,64)$	1170	12	$(7,22)$
296	7	$(3,13)$	480	8	$(49,114)$	1260	13	$(13,30)$
298	7	$(3,13)$	534	8	$(5,16)$	2730	14	$(11,27)$
309	7	$(2,8)$	540	8	$(13,29)$	1470	15	$(13,34)$
372	7	$(5,13)$	552	8	$(11,28)$			

Appendix B. In this appendix, we give a basis of $S_2^*(N)$ for our cases, i.e., for nineteen values of N, $N \neq 194, 546$ from the table in introduction; the cases $N = 194$ and 546 are excluded by Proposition 1.

If $f_i(\tau) \in S_2^*(N)$ $(1 \le i \le g)$ has the Fourier expansion $f_i(\tau) = \sum_{n\ge1} a_n^{(i)} q^n$, we give its Fourier coefficients $(a_1^{(i)}, \ldots, a_r^{(i)})$ with $r = 3g+3$. For all $N \neq 282$, f_i's are of the form (6), and we calculate d_1 using this basis. (*Note*. In the argument in Section 2, we have assumed for simplicity that the Fourier expansion of f_i starts with the term q^i $(i = 1, \ldots, g)$; of course the argument can be easily modified when we use a basis with some f_i starting with the term $a_i q^i$, $a_i \neq 0, 1$.)

Table 4

N	A basis of $S_2^*(N)$	d_1
127	$(1,0,0,-2,-4,-3,-3,3,0,3,1,3)$	-18
	$(0,1,0,-2,-1,-2,-1,2,1,0,2,3)$	
	$(0,0,1,-1,-1,-1,-1,3,-1,2,-1,1)$	
183	$(1,0,0,-2,-2,-1,-1,1,-2,1,-4,1)$	-8
	$(0,1,0,-2,0,-1,-1,1,0,-1,-1,2)$	
	$(0,0,1,-1,-1,-1,1,3,-3,1,-2,0)$	
185	$(1,0,0,0,-2,-4,-4,-2,-2,2,3,4)$	-48
	$(0,1,0,-1,-1,-2,0,-1,-1,1,1,2)$	
	$(0,0,1,0,-1,-2,-1,0,-2,2,2,2)$	

Table 4 (cont.)

N	A basis of $S_2^*(N)$	d_1
217	$(1,0,0,1,-3,-3,-1,-6,-3,3,-2,3)$ $(0,1,0,-1,-1,-1,0,-1,-1,0,-1,0)$ $(0,0,1,1,-2,-2,0,-3,-2,3,1,1)$	-5832
246	$(1,0,0,0,-2,-1,-3,-2,-2,0,0,1)$ $(0,1,0,-1,0,-1,-2,-1,0,-2,3,1)$ $(0,0,1,0,0,-1,-3,0,-3,0,1,1)$	-298
258	$(1,0,0,-1,-2,0,-2,1,-2,-1,1,-1)$ $(0,1,0,-1,-1,-1,1,-1,0,-1,-2,1)$ $(0,0,1,-1,-2,0,2,3,-3,1,2,-1)$	4202
282	$(1,0,-1,0,0,0,-3,-2,1,-1,-4,0)$ $(0,1,0,-1,0,-1,-1,-1,0,-1,0,1)$ $(0,0,0,0,1,0,-2,0,0,-1,-1,0)$	—
290	$(1,0,0,-1,-1,0,-2,0,-3,0,-2,0)$ $(0,1,0,-2,0,0,0,1,0,-1,-4,0)$ $(0,0,1,0,-1,-1,0,0,-3,1,1,1)$	196
310	$(1,0,0,0,-1,-1,-2,-2,-2,0,-3,1)$ $(0,1,0,-1,0,-1,0,-1,-1,-1,-1,1)$ $(0,0,1,0,0,-1,-2,0,-2,0,-1,1)$	-58
318	$(1,0,0,-1,-1,0,-2,0,-2,1,-1,0)$ $(0,1,0,-2,1,0,-2,1,-1,-1,1,0)$ $(0,0,1,0,-1,-1,0,0,-2,1,-1,1)$	452
462	$(1,0,0,0,-1,0,-1,-2,-1,0,-1,0)$ $(0,1,0,-1,0,0,0,-1,-1,-1,0,0)$ $(0,0,1,0,-1,-1,0,0,-1,1,0,1)$	14
510	$(1,0,0,0,0,0,-2,-1,-1,-1,-2,-1)$ $(0,2,0,-1,-1,-1,1,-3,-1,-1,-1,1)$ $(0,0,2,-1,-1,-1,-1,3,-3,1,-3,-1)$	$1255/1024$
322	$(1,0,0,0,-2,-1,-1,-1,-1,0,0,1,-4,0,-2)$ $(0,1,0,0,-1,-1,0,-2,-1,-3,2,0,1,-1,2)$ $(0,0,1,0,-1,-1,0,0,-2,1,0,1,-2,0,0)$ $(0,0,0,1,-1,0,0,-2,1,-1,2,-1,1,0,0)$	192
345	$(1,0,0,0,-1,-1,-2,-1,-1,0,-3,0,0,-3,0)$ $(0,1,0,0,0,-1,-2,-2,0,-1,-1,0,-1,-1,0)$ $(0,0,1,0,0,-1,-1,-1,-2,0,1,0,-2,1,-1)$ $(0,0,0,1,0,-1,0,-2,0,0,-1,2,-1,-1,0)$	-1478
370	$(1,0,0,0,-1,-1,-2,0,-2,0,-1,-1,0,-1,0)$ $(0,2,0,0,-1,-3,-2,-2,0,-2,4,-3,-2,-3,3)$ $(0,0,1,0,-1,0,-1,0,-2,0,2,-2,0,0,2)$ $(0,0,0,2,-1,-1,2,-4,-2,0,-2,-1,2,-1,3)$	$5165/2048$

Table 4 (cont.)

N	A basis of $S_2^*(N)$	d_1
570	$(1,0,0,0,0,-1,-2,0,-1,0,-1,1,-1,-1,-1)$ $(0,1,0,0,0,-1,-1,-1,0,-1,1,0,-1,-1,0)$ $(0,0,1,0,0,-1,-1,0,-2,0,2,1,-1,1,-1)$ $(0,0,0,1,-1,0,2,-2,0,0,-2,-1,-1,-1,1)$	-150
714	$(1,0,0,0,0,-1,-1,0,0,-1,-2,1,-1,0,-2,0,-1,1)$ $(0,1,0,0,0,-1,-1,0,0,-2,1,0,0,0,0,-2,0,1)$ $(0,0,1,0,0,-1,-1,0,-1,0,0,1,1,1,-2,0,0,1)$ $(0,0,0,1,0,0,0,-1,0,-1,-1,-1,0,0,0,-1,0,0)$ $(0,0,0,0,1,0,-1,0,0,-1,-1,0,1,1,-1,0,0,0)$	-126
690	$(1,0,0,0,0,0,-1,0,-1,-1,-2,-1,-2,-1,-1,-1,0,0,-2,1,1)$ $(0,1,0,0,0,0,-1,-1,0,-1,-1,-1,1,-3,0,0,0,-1,3,0,-1)$ $(0,0,1,0,0,0,0,0,-2,0,-1,-1,-2,-1,-1,-1,1,0,1,0,0)$ $(0,0,0,1,0,0,-1,-1,0,0,1,-1,-1,-1,0,-1,2,0,1,-1,1)$ $(0,0,0,0,1,0,0,0,0,-1,-3,0,0,0,-1,0,0,0,1,1,0)$ $(0,0,0,0,0,1,-1,-1,0,0,2,-1,0,0,0,2,-1,-2,2,0,-1)$	-285030
2310	$(2,0,0,0,0,0,0,0,0,0,0,0,-4,-1,1,1,-1,-1,-2,0,-2,-2,0,-1,$ $-3,-2,-4,-2,-1,-1,-2,-3,-2,4,-2,-1,3,1,5)$ $(0,1,0,0,0,0,0,0,0,0,0,0,-1,-1,0,0,0,-1,0,-1,0,-1,-1,-1,0,$ $-2,0,0,0,0,0,-2,0,0,0,0,1,-1,-1)$ $(0,0,2,0,0,0,0,0,0,0,0,0,-2,-1,1,1,-3,-1,-2,0,-2,0,2,-1,$ $-3,-2,-8,0,1,-3,0,-5,-2,4,0,-3,7,5,1)$ $(0,0,0,2,0,0,0,0,0,0,0,0,-2,-1,1,-1,-1,-1,-2,-2,0,0,4,-3,$ $-1,-2,-2,-2,1,-1,0,-3,0,0,0,1,1,-1,1)$ $(0,0,0,0,2,0,0,0,0,0,0,0,-2,-1,-1,1,-1,-1,0,0,0,0,-2,-1,$ $-3,-2,0,0,-1,1,2,-1,0,4,-2,1,1,-3,1)$ $(0,0,0,0,0,2,0,0,0,0,0,0,-2,-1,-1,-1,1,-3,2,0,0,0,0,-1,1,$ $-2,0,0,-1,-1,0,-1,0,2,0,-1,-1,3,-1)$ $(0,0,0,0,0,0,1,0,0,0,0,0,0,0,0,-1,-1,0,-1,0,-1,0,-1,0,0,$ $1,0,-1,0,0,0,2,0,-1,-1,0,1,0,0)$ $(0,0,0,0,0,0,0,1,0,0,0,0,-1,-1,0,0,1,0,0,0,0,0,0,-1,0,-2,$ $0,0,-1,0,0,-2,0,2,0,0,1,0,1)$ $(0,0,0,0,0,0,0,0,2,0,0,0,-4,-1,1,3,-1,-1,0,0,0,0,4,-1,-1,$ $0,-6,0,1,-1,2,-7,0,4,0,-1,5,1,1)$ $(0,0,0,0,0,0,0,0,0,2,0,0,-2,-1,1,1,1,-1,-2,-2,0,0,2,-1,$ $-1,-2,0,0,3,-1,0,-1,0,2,0,1,1,-1,1)$ $(0,0,0,0,0,0,0,0,0,0,1,0,0,0,0,0,0,-1,0,0,0,0,-1,-2,0,0,0,0,$ $0,1,0,-1,0,-1,1,0,0,1,0,0)$ $(0,0,0,0,0,0,0,0,0,0,0,2,-2,-1,1,1,1,-1,0,0,0,0,2,-3,-1,$ $-2,-2,0,-1,-1,0,-3,0,4,0,-1,5,3,1)$	$\frac{609836825}{4096}$

Appendix C. For the special case, there is a less computational method, suggested by Professor F. Momose.

Let $M_0(p)$ be the coarse moduli space over $\mathbb{Z}$ of the isomorphism classes of the generalized elliptic curves with a finite locally free cyclic subgroup of rank p, and put $M_0^*(p) = M_0(p)/\langle W_p \rangle$. By [3], the special fibre $M_0(p) \otimes \mathbb{F}_p$ is reduced and consists of two irreducible components which are the images of the morphisms

$$\Phi_1 : M_0(1) \otimes \mathbb{F}_p \to M_0(p) \otimes \mathbb{F}_p, \qquad E \mapsto (E, \ker(\phi)),$$
$$\Phi_2 : M_0(1) \otimes \mathbb{F}_p \to M_0(p) \otimes \mathbb{F}_p, \qquad E \mapsto (E^{(p)}, \ker(\widehat{\phi})),$$

where E is an elliptic curve over $\overline{\mathbb{F}}_p$ and $E^{(p)}$ is obtained by twisting coefficients $a \mapsto a^p$ of the defining equation for E; ϕ denotes the Frobenius isogeny and $\widehat{\phi}$ its dual. For each supersingular point Q of $M_0(1) \otimes \mathbb{F}_p$, we have $\Phi_1(Q) = \Phi_2(Q^{(p)})$. The images of Φ_1 and Φ_2 intersect transversally at the supersingular points. Put $\overline{W}_p = W_p \otimes \mathbb{F}_p$. Then $\overline{W}_p$ acts on $M_0(p) \otimes \mathbb{F}_p$ by $(E, \ker(\phi)) \mapsto (E^{(p)}, \ker(\widehat{\phi}))$. So it exchanges each supersingular point which is properly $\mathbb{F}_{p^2}$-rational with its conjugate, while it fixes each $\mathbb{F}_p$-rational supersingular point. Since $C := M_0^*(p) \otimes \mathbb{F}_p = (M_0(p) \otimes \mathbb{F}_p)/\langle \overline{W}_p \rangle$, C becomes as in Fig. 1,

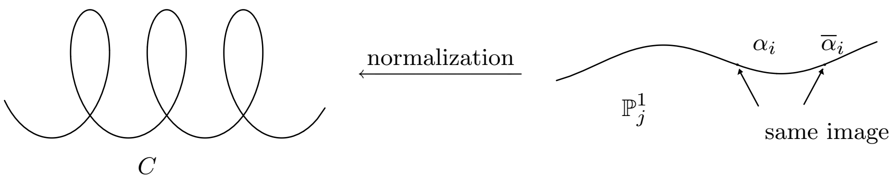

Fig. 1

where α_i, $\overline{\alpha}_i$ are properly $\mathbb{F}_{p^2}$-rational supersingular j-invariants. Now let $p = 127$ and assume that $X_0^*(127)$ is hyperelliptic. Then

$$\mathrm{Pic}^0_{C/\mathbb{F}_{127}} \cong H^1(\Gamma(C), \mathbb{Z}) \otimes \mathbb{G}_m$$

for the graph $\Gamma(C)$ associated with $C = M_0^*(127) \otimes \mathbb{F}_{127}$, and the hyperelliptic involution σ of $X_0^*(127)$ acts on $\mathrm{Pic}^0_{C/\mathbb{F}_{127}}$ by -1. Thus we have $\sigma(\gamma_i) = \gamma_i^{-1}$, where γ_i $(i = 1, 2, 3)$ are paths (see Fig. 2).

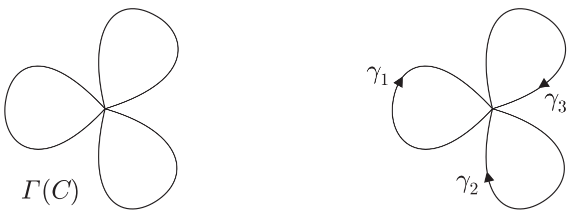

Fig. 2

From this, if $X_0^*(127)$ is hyperelliptic, there must exist an element A of

$\mathrm{PGL}_2(\mathbb{F}_{127})$ such that

$$A^2 = I_2, \quad A\alpha_i = \overline{\alpha}_i \quad (i = 1, 2, 3).$$

Numerical values for α_i can be found in [2]. An easy calculation shows that there does not exist such an element in $\mathrm{PGL}_2(\mathbb{F}_{127})$. Hence $X_0^*(127)$ is not hyperelliptic.

Acknowledgements. The authors wish to express their thanks to Professor F. Momose and Professor N. Murabayashi for valuable discussions.

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*, in: Modular Functions of One Variable IV, B. Birch and W. Kuyk (eds.), Lecture Notes in Math. 476, Springer, Berlin, 1975, 74–144.

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

[4] M. Eichler, *The basis problem for modular forms and the traces of the Hecke operators*, in: Modular Functions of One Variable I, W. Kuyk (ed.), Lecture Notes in Math. 320, Springer, Berlin, 1973, 75–151.

[5] R. Hartshorne, *Algebraic Geometry*, Grad. Texts in Math. 52, Springer, New York, 1977.

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

[7] K. Hashimoto, *On Brandt matrices of Eichler orders*, Mem. School Sci. Engrg. Waseda Univ. 59 (1995), 143–165.

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

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

[10] P. G. Kluit, *Hecke operators on $\Gamma^*(N)$ and their traces*, Dissertation of Vrije Universiteit, Amsterdam, 1979.

[11] J. Lehner and M. Newman, *Weierstrass points of $\Gamma_0(N)$*, Ann. of Math. 79 (1964), 360–368.

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

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

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

[15] A. Pizer, *An algorithm for computing modular forms on $\Gamma_0(N)$*, J. Algebra 64 (1980), 340–390.

[16] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Iwanami Shoten and Princeton Univ. Press, 1971.

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

Department of Mathematics
Waseda University
3-4-1, Okubo Shinjuku-ku
Tokyo 169, Japan
E-mail: hase@cfi.waseda.ac.jp
khasimot@cfi.waseda.ac.jp

Received on 19.7.1995 (2838)