ACTA ARITHMETICA
LXXXII.3 (1997)

Modular equations of hyperelliptic $X_0(N)$ and an application

by

Takeshi Hibino (Tokyo) and Naoki Murabayashi (Yamagata)

1. Introduction. Let $N \geq 1$ be an integer and let $X_0(N)$ be the modular curve over $\mathbb{Q}$ which corresponds to the modular group $\Gamma_0(N)$. As a defining equation of $X_0(N)$ we have the so-called modular equation of level N. It has many good properties, e.g. it reflects the defining property of $X_0(N)$, it is the coarse moduli space of the isomorphism classes of the generalized elliptic curves with a cyclic subgroup of order N. But its degree and coefficients are too large to be applied to practical calculations on $X_0(N)$. While it is an important problem to determine the algebraic points on $X_0(N)$, we need a more manageable defining equation, which will also help to solve other related problems. In the case of a hyperelliptic modular curve, a kind of normal form of a defining equation is given by N. Murabayashi ([9]) and M. Shimura ([13]).

In this paper, we give a relation between the modular equation of level N and the normal form in the case of a hyperelliptic modular curve $X_0(N)$ except for $N = 40, 48$. First recall that the modular equation of level N is written in the following form:

$$F_N(j, j_N) = 0, \qquad F_N(S, T) \in \mathbb{Z}[S, T],$$

where j is the modular invariant, $j_N(z) = j(Nz)$, and z is the natural coordinate on $\mathcal{H}$. Since $X_0(N)$ is hyperelliptic, it can be written in the following normal form:

$$y^2 = f(x), \qquad f(T) \in \mathbb{Q}[T], \ \deg f = 2g + 2,$$

where x is a covering map of degree two from $X_0(N)$ to $\mathbb{P}^1$ and g is the genus of $X_0(N)$. In this case, we obtain the following relation:

$$j = (A(x) + B(x)y)/C(x), \qquad A(x), B(x), C(x)(\neq 0) \in \mathbb{Q}(x).$$

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

When the genus of $X_0(N)$ is 0, R. Fricke gave the expression for j (see [3]), and N. D. Elkies did the same when the curve $X_0(N)$ is elliptic or hyperelliptic where N is a prime number other than 37 ([2]). We are interested in $X_0(N)$ for the 19 particular values of N for which the modular curve $X_0(N)$ is hyperelliptic. We extend Elkies' work. We give the expression for j for 17 values of N; to be specific, the cases $N = 40, 48$ are excluded.

Our method cannot be applied to the cases $N = 37, 40$ and 48; it is vital for our method that the hyperelliptic involution is of Atkin–Lehner type, and it is not of that type for these three cases. However, in §2.3 we solve the special case $N = 37$. In §3.2, we prove that a certain quantity $n(37)$, the number of $\mathbb{Q}$-rational points on a certain modular curve, is 0. Momose proved that it is 0 or 1, and also gave a criterion which could be used to decide which value it really takes. We check the expression of j for $N = 37$ against Momose's criterion, and deduce that $n(37) = 0$.

To get our equations and relations, we use the Fourier expansions of certain cusp forms of weight 2 on $\Gamma_0(N)$. Their Fourier coefficients are given by the Brandt matrix ([4], [11]) and the trace formula ([5], [14]).

Acknowledgments. The authors would like to thank the following people for their help in various ways: N. Adachi, Y. Hasegawa, K. Hashimoto, Y. Sato and M. Shimura. We would also like to thank F. Momose who informed us of the problem of the rational points of $X_{\mathrm{split}}(37)$ (see §3.2). The computations were done with *Mathematica*.

NOTATION

- N: a positive integer (= the level of a modular curve).
- $\Gamma_0(N) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) (\in \mathrm{SL}_2(\mathbb{Z})) \;\middle|\; c \equiv 0 \pmod{N} \right\}$.
- $\mathcal{H} = \{z \in \mathbb{C} \mid \mathrm{Im}(z) > 0\}$.
- $\mathcal{H}^* = \mathcal{H} \cup \mathbb{P}^1(\mathbb{Q}) = \mathcal{H} \cup \mathbb{Q} \cup \{i\infty\}$.
- $X_0(N)$: the modular curve defined over $\mathbb{Q}$ which corresponds to $\Gamma_0(N)$, i.e., $X_0(N)(\mathbb{C}) \cong \Gamma_0(N)\backslash\mathcal{H}^*$.
- g: the genus of $X_0(N)$.
- $S_2(\Gamma_0(N))$: the $\mathbb{C}$-vector space of cusp forms of weight 2 on $\Gamma_0(N)$. Let $f_1, \ldots, f_g$ be a basis of $S_2(\Gamma_0(N))$, z the natural coordinate on $\mathcal{H}$, $q = e^{2\pi\sqrt{-1}z}$ and let the Fourier expansion of f_i be

$$f_i = a_{i,1}q + a_{i,2}q^2 + \ldots, \qquad a_{i,j} \in \mathbb{Z},\ 1 \le i \le g,\ j = 1, 2, \ldots$$

  These coefficients can be taken in $\mathbb{Z}$ (see [12]).

2. Computation. If $X_0(N)$ is a hyperelliptic curve, its normal form can be obtained by Murabayashi's method ([9]). The hyperelliptic modular curves $X_0(N)$ have been classified by A. Ogg ([10]).

THEOREM 2.1 (A. Ogg). *There are exactly nineteen values of level N for which $X_0(N)$ is hyperelliptic. They are (g is the genus of $X_0(N)$):*

$$\begin{cases} g=2\colon N=22,23,26,28,29,31,37,50,\\ g=3\colon N=30,33,35,39,40,41,48,\\ g=4\colon N=47,\\ g=5\colon N=46,59,\\ g=6\colon N=71. \end{cases}$$

2.1. *A defining equation for hyperelliptic $X_0(N)$.* Let $\overline{i\infty}$ denote the point of $X_0(N)$ which is represented by $i\infty$. If $\overline{i\infty}$ is not a Weierstrass point of $X_0(N)$, then $X_0(N)$ can be written in the following normal form:

$$y^2=f(x), \qquad f(T)\in\mathbb{Q}[T],\ \deg f=2g+2,$$

where x is a covering map of degree two from $X_0(N)$ to $\mathbb{P}^1$. Here, a normal form means a defining equation of the type $y^2=f(x)$, $f(T)\in\mathbb{C}[T]$. By using a linear combination of the basis $f_1,\dots,f_g$ of $S_2(\Gamma_0(N))$, we choose another basis $h_1,\dots,h_g$ with the following Fourier expansions with rational coefficients:

$$\begin{cases} h_1(z)=q^g+s_{1,g+1}q^{g+1}+\ldots+s_{1,g+i}q^{g+i}+\ldots,\\ h_2(z)=q^{g-1}+s_{2,g}q^g+\ldots+s_{2,g+i}q^{g+i}+\ldots,\\ \ldots\\ h_g(z)=q+s_{g,2}q^2+\ldots+s_{g,g+i}q^{g+i}+\ldots \end{cases}$$

LEMMA 2.1. *Put $x=h_2(z)/h_1(z)$. Then $x: X_0(N)\to\mathbb{P}^1$ is of degree two.*

This lemma is due to M. Shimura (see [13]). We put

$$y=\frac{q}{h_1}\frac{dx}{dq}.$$

(This construction of x,y is the same as in [9] and [13].) Thus the Fourier expansions of x and y^2 are

$$y^2=q^{-(2g+2)}+\ldots, \qquad x=q^{-1}+\ldots$$

We can determine recursively the coefficients $a_1,a_2,\dots,a_{2g+2}$ of a defining equation as follows:

$$\begin{cases} y^2-x^{2g+2}=a_1q^{-2g-1}+\ldots,\\ y^2-x^{2g+2}-a_1x^{2g+1}=a_2q^{-2g}+\ldots,\\ \ldots \end{cases}$$

Thus we have a defining equation of $X_0(N)$:

$$y^2=x^{2g+2}+a_1x^{2g+1}+\ldots+a_{2g+2}.$$

Remark 2.1. To get a normal form, we need only know $s_{1,g+1},\dots,s_{1,3g+3}$, $s_{2,g},\dots,s_{2,3g+2}$. We need a few more Fourier coefficients to represent j and j_N in terms of x and y.

2.2. *Hyperelliptic involutions of Atkin–Lehner type.* Let $N = N'N''$ with $(N', N'') = 1$. As Atkin and Lehner showed ([1]), the involution $w = \left(\begin{smallmatrix} 0 & -1 \\ N & 0 \end{smallmatrix}\right)$ of $X_0(N)$ is factored into $w = w'w''$ ($w' = w_{N'}$, $w'' = w_{N''}$); in terms of matrices, w' is defined by any integral matrix with determinant N' of the form

$$w' = \begin{pmatrix} 1 & 0 \\ 0 & N' \end{pmatrix} \begin{pmatrix} N'a & b \\ N''c & d \end{pmatrix} = \begin{pmatrix} a & b \\ N''c & N'd \end{pmatrix} \begin{pmatrix} N' & 0 \\ 0 & 1 \end{pmatrix}$$
$$\in \begin{pmatrix} 1 & 0 \\ 0 & N' \end{pmatrix} \Gamma_0(N'') \cap \Gamma_0(N'') \begin{pmatrix} N' & 0 \\ 0 & 1 \end{pmatrix}.$$

Let $\mathrm{Aut}(X_0(N))$ be the group of automorphisms of $X_0(N)$ over $\mathbb{C}$ (for curves of genus ≥ 2). Let $\Gamma_0^*(N)$ be the normalization of $\Gamma_0(N)/\{\pm 1\}$ in $\mathrm{PGL}_2^+(\mathbb{Q})$, and put $B_0(N) = \Gamma_0^*(N)/\Gamma_0(N)$ ($\subseteq \mathrm{Aut}(X_0(N))$), which is determined in [1], §4. When $N = 37$, $\mathrm{Aut}(X_0(N)) \supset B_0(N)$. The modular curve $X_0(37)$ has a hyperelliptic involution which sends the cusps to non-cuspidal $\mathbb{Q}$-rational points, and we see $\mathrm{Aut}(X_0(37)) \simeq (\mathbb{Z}/2\mathbb{Z})^2$ and $B_0(37) \simeq \mathbb{Z}/2\mathbb{Z}$ (cf. [6], [7]). For each level N for which $X_0(N)$ is hyperelliptic, A. Ogg checked whether its hyperelliptic involution is of Atkin–Lehner type or not ([10]).

Theorem 2.2 (A. Ogg). *There are exactly eighteen values of level N besides $N = 37$ for which $X_0(N)$ is hyperelliptic. For two of these values, namely $N = 40, 48$, the hyperelliptic involution v is not of Atkin–Lehner type. The remaining sixteen values are listed in the table below, together with their genera and hyperelliptic involutions.*

N	g	v	N	g	v
22	2	w_{11}	35	3	w_{35}
23	2	w_{23}	39	3	w_{39}
26	2	w_{26}	41	3	w_{41}
28	2	w_7	46	5	w_{23}
29	2	w_{29}	47	4	w_{47}
30	3	w_{15}	50	2	w_{50}
31	2	w_{31}	59	5	w_{59}
33	3	w_{11}	71	6	w_{71}

$N = 37$ is the only case where $X_0(N)$ is hyperelliptic with an exceptional hyperelliptic involution s.

Remark 2.2. $\left(\begin{smallmatrix} -10 & 1 \\ -120 & 10 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} -6 & 1 \\ -48 & 6 \end{smallmatrix}\right)$ define the hyperelliptic involutions of $X_0(40)$ and $X_0(48)$ respectively.

We assume that $X_0(N)$ is hyperelliptic and that N is not equal to 37, 40 or 48. Let w_M be the hyperelliptic involution. Then

$$w_M = \begin{pmatrix} a & b \\ Nc/M & Md \end{pmatrix} \begin{pmatrix} M & 0 \\ 0 & 1 \end{pmatrix},$$

$M \,\|\, N$ and $adM - bcN/M = 1$. Let w_M^* be the automorphism of $\mathbb{Q}(X_0(N))$ induced by w_M, where $\mathbb{Q}(X_0(N))$ is the field of meromorphic functions on $X_0(N)$ defined over $\mathbb{Q}$. Let x, y, j and j_M be the functions defined in §2.1. The action of w_M^* on these functions is as follows:

$$w_M^* x = x, \quad w_M^* y = -y, \quad w_M^* j = j_M, \quad w_M^* j_M = j.$$

It is easily checked that

$$j + j_M,\ \frac{j - j_M}{y} \in \mathbb{Q}(X_0(N))^{\langle w_M^* \rangle} = \mathbb{Q}(x),$$

where $\mathbb{Q}(X_0(N))^{\langle w_M^* \rangle} = \{f \in \mathbb{Q}(X_0(N)) \mid w_M^* f = f\}$. Therefore $F(x) = j + j_M$ and $G(x) = (j - j_M)/y$ are rational functions of x. The rational functions F, G are determined explicitly by observing the pole divisors and the values at the cusps of $x,\ y,\ j$ and j_M. Denote by C the set of cusps on $X_0(N)$. The pole divisors of $j,\ j_M$ are

$$(j)_\infty = \sum_{P \in C} e_P P, \qquad (j_M)_\infty = \sum_{P \in C} e_P w_M(P),$$

where e_P is the ramification index of the covering of $X_0(N)$ to $X_0(1) = \mathbb{P}^1(j)$; i.e., e_P is the positive integer defined as follows. Put $\Gamma_0(N)_P = \{\Gamma \in \Gamma_0(N) \mid \Gamma(P) = P\}$ and $\mathrm{SL}_2(\mathbb{Z})_P = \{\Gamma \in \mathrm{SL}_2(\mathbb{Z}) \mid \Gamma(P) = P\}$. Then $e_P = [\mathrm{SL}_2(\mathbb{Z})_P : \Gamma_0(N)_P]$. In fact, e_P can be calculated as follows. Let ϱ be an element of $\mathrm{SL}_2(\mathbb{Z})$ such that $\varrho(P) = i\infty$. Since $\varrho \mathrm{SL}_2(\mathbb{Z})_P \varrho^{-1} = \mathrm{SL}_2(\mathbb{Z})_\infty$,

$$\varrho \Gamma_0(N)_P \varrho^{-1} = \left\{ \pm \begin{pmatrix} 1 & e_P \\ 0 & 1 \end{pmatrix}^m \;\middle|\; m \in \mathbb{Z} \right\}.$$

In our case, it is easy to see that

$$(j \pm j_M)_\infty = \sum_{P \in C} \max\{e_P, e_{w_M(P)}\} P.$$

The pole divisors of x, y are

$$(x)_\infty = \overline{i\infty} + w_M(\overline{i\infty}), \qquad (y)_\infty = (g+1)\{\overline{i\infty} + w_M(\overline{i\infty})\}.$$

First assume that N is a square-free integer. For any $P \in C$, excluding $\overline{i\infty}$ and $w_M(\overline{i\infty})$, denote by w_P the involution of Atkin–Lehner type such that $P = w_P(\overline{i\infty})$. The zero divisor of $x - x(P)$ is $P + w_M P$ and the value of $x(P)$ is calculated by $x(P) = x(w_P(\overline{i\infty})) = w_P^* x(\overline{i\infty})$. The function $w_P^* x$ is obtained by the action of the Atkin–Lehner involution on $S_2(\Gamma_0(N))$. Thus,

we obtain the following:

$$F(T) = \frac{F_{\mathrm{num}}(T)}{\prod_{P\in C\setminus\{\overline{i\infty},w_M(\overline{i\infty})\}}(T-x(P))^{\max\{e_P,e_{w_M(P)}\}/2}},$$
$$G(T) = \frac{G_{\mathrm{num}}(T)}{\prod_{P\in C\setminus\{\overline{i\infty},w_M(\overline{i\infty})\}}(T-x(P))^{\max\{e_P,e_{w_M(P)}\}/2}},$$
$$\deg F_{\mathrm{num}} = \sum_{P\in C}\max\{e_P, e_{w_M(P)}\}/2,$$
$$\deg G_{\mathrm{num}} = \deg F_{\mathrm{num}} - (g+1), \qquad F_{\mathrm{num}}(T), G_{\mathrm{num}}(T) \in \mathbb{Q}[T].$$

We determine the coefficients of F_{num} and G_{num} by the Fourier expansions of x, y, j and j_M to get the following:

$$j = \frac{F(x)+G(x)y}{2}, \qquad j_M = \frac{F(x)-G(x)y}{2},$$
$$j_N = \frac{F(w_N^*x)+G(w_N^*x)w_N^*y}{2}.$$

Last, we discuss the case where N is not a square-free integer; i.e., $N = 28, 50$. In this case, since $\mathrm{Aut}(X_0(N))$ is generated by the set of Atkin–Lehner involutions and does not act transitively on the set of cusps, we cannot determine all values at the cusps of x.

In the case $N = 28$, the Atkin–Lehner involution w_4 has two fixed cuspidal points ([10]), which will be denoted by P and Q respectively. It is easy to see that $w_7(P) = Q$. Let x and y be the modular functions of $X_0(28)$ defined in §2.1. Since $w_4^*x = (x+3)/(x-1)$ and $w_4^*y = -8y/(x-1)^3$, we get the equations $x(P) = (x(P)+3)/(x(P)-1)$ and $y(P) = -8y(P)/(x(P)-1)^3$. Therefore it is easy to see that $x(P) = -1$. Since the involution w_7 is hyperelliptic, $x(Q) = x(P) = -1$. The values at the other cusps of x are determined in the same way as in the square-free case. Finally, using the Fourier expansions of x, y, j and j_7, we can determine the coefficients of F_{num} and G_{num}.

In the case $N = 50$, put $C' = \{w_d(\overline{i\infty}) \mid d \,\|\, 50\}$ and $C'' = C\setminus C'$. Since $\mathrm{Aut}(X_0(50))$ is generated by the Atkin–Lehner involutions (see [1] and [6]), the set C' is the orbit of $\overline{i\infty}$ by $\mathrm{Aut}(X_0(50))$. For a positive divisor d of N with $1 < d < N$ and for an integer i prime to N, let $(\frac{i}{d})$ denote the point of $X_0(N)$ which is represented by i/d. Then $(\frac{i}{d})$ is defined over $\mathbb{Q}(\zeta_n)$, where $n = \gcd(d, N/d)$ and ζ_n is a primitive nth root of 1. Reducing i modulo n, we have $\varphi(n)$ Galois-conjugate cusps associated with d. By this notation, it is easy to see that

$$C'' = \left\{\left(\frac{1}{5}\right), \left(\frac{3}{5}\right), \left(\frac{7}{5}\right), \left(\frac{9}{5}\right), \left(\frac{1}{10}\right), \left(\frac{3}{10}\right), \left(\frac{7}{10}\right), \left(\frac{9}{10}\right)\right\}.$$

The cusps in C'' are defined over $\mathbb{Q}(\zeta_5)$. Let x and y be the modular functions of $X_0(50)$ defined in §2.1. We cannot determine the value of x at the cusps in C''. However, we can obtain a few relations among the values as follows. Since w_{50} is a hyperelliptic involution, $x\big(\big(\frac{i}{5}\big)\big) = x\big(\big(\frac{10-i}{10}\big)\big)$, for $i = 1, 3, 7$ and 9. The values $x\big(\big(\frac{1}{5}\big)\big), x\big(\big(\frac{3}{5}\big)\big), x\big(\big(\frac{7}{5}\big)\big)$ and $x\big(\big(\frac{9}{5}\big)\big)$ in $\mathbb{Q}(\zeta_5)$ are conjugate over $\mathbb{Q}$. Therefore these values are the roots of a polynomial over $\mathbb{Q}$ of degree 4, which we write as $\sum_{i=0}^{4} c_i T^i$. We can determine the rational functions in the forms similar to the rational functions F and G. Finally, using the Fourier expansions of x, y, j and j_{50}, we can determine the coefficients of F_{num} and G_{num}, and c_i's.

R e m a r k 2.3. If N is a prime number, the expressions for j and j_N are polynomials in x and y with rational coefficients. If N is a composite number, however, they are not polynomials but rational functions.

2.3. *The special case $N = 37$.* The case $N = 37$ is the unique case where $X_0(N)$ is hyperelliptic with an exceptional hyperelliptic involution s. Let x, y, j and j_{37} be the functions defined in §2.1. The action of w_{37}^* on these functions is as follows:

$$w_{37}^* x = \frac{1}{x}, \qquad w_{37}^* y = \frac{y}{x^3}, \qquad w_{37}^* j = j_{37}, \qquad w_{37}^* j_{37} = j.$$

The action of s^* on x and y is as follows:

$$s^* x = x, \qquad s^* y = -y.$$

It is easy to see that

$$j + s^* j, \frac{j - s^* j}{y} \in \mathbb{Q}(X_0(37))^{\langle s^* \rangle} = \mathbb{Q}(x).$$

Denote by $\overline{0}$ and $\overline{i\infty}$ the points of $X_0(37)$ which are represented by 0 and $i\infty$, respectively. The pole divisors of j and $s^* j$ are

$$(j)_\infty = 37\,\overline{0} + \overline{i\infty}, \quad (s^* j)_\infty = 37 s(\overline{0}) + s(\overline{i\infty}).$$

Since the hyperelliptic involution s sends the cusps to non-cuspidal $\mathbb{Q}$-rational points, i.e., $\{\overline{0}, \overline{i\infty}\} \cap \{s(\overline{0}), s(\overline{i\infty})\} = \emptyset$, we have

$$(j \pm s^* j)_\infty = 37\{\overline{0} + s(\overline{0})\} + \{\overline{i\infty} + s(\overline{i\infty})\}.$$

On the other hand, the divisors of x, y are

$$(x)_0 = \overline{0} + s(\overline{0}), \qquad (x)_\infty = \overline{i\infty} + s(\overline{i\infty}), \qquad (y)_\infty = 3\{\overline{i\infty} + s(\overline{i\infty})\}.$$

Considering the divisors and the values at the cusps of x, y, j and $s^* j$, we see that the rational functions F, G defined in §2.2 take the following form:

$$j + s^*j = \frac{2F_{\mathrm{num}}(x)}{x^{37}}, \qquad \frac{j - s^*j}{y} = \frac{2G_{\mathrm{num}}(x)}{x^{37}},$$
$$F_{\mathrm{num}}(T) = \sum_{i=0}^{38} a_i T^i, \qquad G_{\mathrm{num}}(T) = \sum_{i=0}^{35} b_i T^i,$$
$$\deg F_{\mathrm{num}} = 38, \qquad \deg G_{\mathrm{num}} = 35.$$

Therefore,

$$j = \frac{F_{\mathrm{num}}(x) + G_{\mathrm{num}}(x)y}{x^{37}}.$$

From the action of w_{37}^*,

$$j_{37} = \frac{F_{37,\mathrm{num}}(x) + G_{37,\mathrm{num}}(x)y}{x},$$
$$F_{37,\mathrm{num}}(T) = \sum_{i=0}^{38} a_{38-i} T^i, \qquad G_{37,\mathrm{num}}(T) = \sum_{i=0}^{35} b_{35-i} T^i.$$

We do not know the Fourier expansion of s^*j. But we can determine the coefficients a_i of the polynomials F_{num} and $F_{37,\mathrm{num}}$ since the coefficients of F_{num} are the reciprocals of those of $F_{37,\mathrm{num}}$. The same holds for the coefficients b_i of the polynomials G_{num} and $G_{37,\mathrm{num}}$.

3. Applications. Now, we have the expressions for j and j_N in terms of x, y as above. Since the expressions for j and j_N reflect the properties of $X_0(N)$ (i.e., it is the coarse moduli space of the isomorphism classes of the generalized elliptic curves with a cyclic subgroup of order N), we can apply them to arithmetic problems.

3.1. *Computation of isogenous curves.* Let N be a positive integer and F a field of characteristic either 0 or p not dividing N. Let E be an elliptic curve over F with modular invariant ε. We show how to compute a defining equation of the curve E' with modular invariant ε' which is N-isogenous to E. Eliminating y from the equations for j, we obtain a polynomial equation in x and j. Substituting ε for j, we find the F-rational roots of the resulting polynomial. Each root corresponds to an F-rational N-isogeny of E; to recover the modular invariant ε' of the isogenous curve, we need only represent y as a rational function in x and substitute these roots into the expression for j_N.

Example 3.1 ($N = 23$). Let x, y be the modular functions on $X_0(23)$ given in §2.1, satisfying $y^2 = (1 - x + x^3)(-7 + 3x - 8x^2 + x^3)$. Then we find that j, j_{23} are $(A(x) \pm B(x)y)/2$ with

$$\begin{aligned}A(x) = {} & -6750 + 48600x - 83835x^2 - 170775x^3 + 1115109x^4 \\ & - 2492280x^5 + 2732814x^6 - 116403x^7 - 4877702x^8 \\ & + 8362616x^9 - 6612454x^{10} + 302266x^{11} + 5423124x^{12} \\ & - 6447728x^{13} + 3209696x^{14} + 336674x^{15} - 1470068x^{16} \\ & + 953856x^{17} - 336927x^{18} + 74221x^{19} - 10465x^{20} \\ & + 920x^{21} - 46x^{22} + x^{23},\end{aligned}$$

$$\begin{aligned}B(x) = {} & (-5+x)(-3+x)(-2+x)(-1+x)x(1+x)(3-8x+x^2) \\ & \times (-9-6x+x^2)(-5+3x-7x^2+x^3)(-3+7x-7x^2+x^3) \\ & \times (-1-4x^3+x^4).\end{aligned}$$

Eliminating y, we find

$$\begin{aligned}0 &= j^2 - A(x)j + \frac{A(x)^2 - B(x)^2y^2}{4} \\ &= j^2 - A(x)j + (225 - 1080x + 2268x^2 - 2280x^3 + 1894x^4 \\ &\quad - 968x^5 + 732x^6 + 232x^7 + x^8)^3;\end{aligned}$$

taking $j = -3375$, we obtain a polynomial of degree 24 in x, whose only rational solution is $x = 0$, which corresponds to $y = \pm\sqrt{-7}$. Substituting these x, y in the formula for j and j_{23}, we obtain $j = -3375$ and $j_{23} = -3375$. These curves have complex multiplication by $\mathbb{Q}(\sqrt{-4})$.

R e m a r k 3.1. Conversely, taking $x = -1, 1, 2, 3$ and 5, we obtain the elliptic curves with modular invariants corresponding to these points. It is easy to see that they are elliptic curves with complex multiplication.

3.2. *Rational points of $X_{\mathrm{split}}(37)$.* In case $N = 37$, we apply the relations for j to the proof of the existence of rational points on $X_{\mathrm{split}}(37)$.

For a prime number p, let $X_{\mathrm{split}}(p)$ be the modular curve defined over $\mathbb{Q}$ which corresponds to the modular subgroup

$$\Gamma_{\mathrm{split}}(p) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} (\in \mathrm{SL}_2(\mathbb{Z})) \;\middle|\; b \equiv c \equiv 0 \text{ or } a \equiv d \equiv 0 \pmod{p} \right\},$$

i.e., $X_{\mathrm{split}}(p)(\mathbb{C}) = \Gamma_{\mathrm{split}}(p)\backslash\mathcal{H}^*$. The affine open subspace $X_{\mathrm{split}}(p)\backslash\{\text{cusps}\}$ is the coarse moduli space over $\mathbb{Q}$ of the isomorphism classes of elliptic curves with an unordered pair of independent subgroups of order p ([7]).

We will need a theorem regarding this modular curve proved by F. Momose (see [8]). Let $J_0(p)$ be the Jacobian variety of $X_0(p)$. Let w_p be the Atkin–Lehner involution as above. Denote by w_p the automorphism of $J_0(p)$ which is induced by the involution w_p. Put $J_0^-(p) = J_0(p)/((1 + w_p)J_0(p))$.

Denote by $n(p)$ the number of $\mathbb{Q}$-rational points on $X_{\mathrm{split}}(p)$ which are neither cusps nor CM points.

THEOREM 3.1 (F. Momose). *Let $p = 11$ or $p \geq 17$ be a prime number such that the Mordell–Weil group of $J_0^-(p)$ is of finite order. Then $n(p) = 0$, provided $p \neq 37$.*

In the case $p = 37$, it was only shown that $n(37) \leq 1$. Further, he showed the following proposition (loc.cit., Proposition 5.1):

PROPOSITION 3.1 (F. Momose). *Let x, y be the modular functions on $X_0(37)$ satisfying $y^2 = 37 - 11x^2 - 9x^4 - x^6$, and let*

$$j(z) = \frac{g(x) + h(x)y}{(x-1)(x+1)^{37}} \qquad \text{with } g(x), h(x) \in \mathbb{Q}[x].$$

Then $n(37) = 1$ if and only if $h(T) = 0$ has a $\mathbb{Q}$-rational solution.

Though g, h were not determined in his paper, we now obtain the formula for j as follows. Let x, y be the modular functions on $X_0(37)$ given by our method satisfying

$$y^2 = 1 + 14x + 35x^2 + 48x^3 + 35x^4 + 14x^5 + x^6.$$

Then we get

$$j = \frac{g(x) - h(x)y}{x^{37}}$$

with

$$\begin{aligned} h(T) = {} & (1+T)(1+3T+T^2)(1+11T+T^2)(1+7T+9T^2+7T^3+T^4) \\ & \times (1+39T+623T^2+5332T^3+27007T^4+85293T^5+174954T^6 \\ & +241803T^7+227140T^8+141862T^9 \\ & +54236T^{10}+10029T^{11}+T^{12}) \\ & \times (1+43T+747T^2+6741T^3+34232T^4+102516T^5 \\ & +196228T^6+254142T^7+227826T^8+140552T^9+57320T^{10} \\ & +13993T^{11}+1561T^{12}+6T^{13}+T^{14}). \end{aligned}$$

In this model the $\mathbb{Q}$-rational solutions of $h(T) = 0$ correspond to the non-cuspidal $\mathbb{Q}$-rational points on $X_{\mathrm{split}}(37)$. The equation $h(T) = 0$ has the $\mathbb{Q}$-rational solution $T = -1$. This root corresponds to the elliptic curve with modular invariant $2^3 3^3 11^3$. This curve has complex multiplication by $\mathbb{Q}(\sqrt{-4})$. This implies that there is no $\mathbb{Q}$-rational point on $X_{\mathrm{split}}(37)$ which is neither a cusp nor a CM point. Thus the proof of the following result is complete.

THEOREM 3.2. $n(37) = 0$.

R e m a r k 3.2. Using a minimal model of $X_0(37)$ over $\mathbb{Z}[1/37]$, F. Momose proved that there is no $\mathbb{Q}$-rational point on $X_{\mathrm{split}}(37)$ which is neither a cusp nor a CM point. Our proof is independent of Momose's and it was obtained at about the same time.

4. Results. Since displaying all of our results requires so much space, we show here only a few of them. The remaining formulae will be available via E-mail, FTP, or a Web site. For hyperelliptic $X_0(N)$, using the normal form $y^2 = f(x)$, $f(T) \in \mathbb{Q}[T]$, $\deg f = 2g+2$, we obtain the following formula:

$$j = (A(x) + B(x)y)/C(x), \qquad A(x), B(x), C(x)(\neq 0) \in \mathbb{Q}(x).$$

If the level N is a prime number except for $N = 37$, the denominator $C(x)$ is a constant. In the following tables, we show the formula in case of $N = 28, 37$ and 50.

$X_0(28)$	$j = (A(x) + B(x)y)/(2(-1+x)^{28}(1+x)^7)$
$A(x)$	$(5+2x+x^2)^3(13008+42177x+57719x^2+52963x^3+44885x^4+28058x^5$ $+15574x^6+5654x^7+1898x^8+181x^9+35x^{10}-9x^{11}+x^{12})(169075845$ $+1098116910x+3278374860x^2+6248929986x^3+8968175830x^4$ $+10623599914x^5+10765189860x^6+9454160838x^7+7305468855x^8$ $+4990760364x^9+3017246072x^{10}+1607026868x^{11}+753490212x^{12}$ $+299600564x^{13}+104970696x^{14}+28125740x^{15}+6098083x^{16}+1027846x^{17}$ $+34172x^{18}+1706x^{19}+2342x^{20}-958x^{21}+148x^{22}-18x^{23}+x^{24})$
$B(x)$	$(3+x)(3+x^2)(-7-10x+x^2)(5+2x+x^2)^3(17+4x+6x^2+4x^3+x^4)$ $\times(41+52x+30x^2+4x^3+x^4)(101+222x+87x^2+20x^3+99x^4-18x^5+x^6)$ $\times(117+174x+119x^2+52x^3+51x^4-2x^5+x^6)$ $\times(801+2232x+2556x^2+1608x^3+806x^4+136x^5+60x^6-8x^7+x^8)$
	$y^2 = (7+x^2)(2-x+x^2)(2+x+x^2)$
	$w_4^*x = (x+3)/(x-1),\ w_4^*y = -8y/(x-1)^3,\ w_7^*x = x,\ w_7^*y = -y$

$X_0(37)$	$j = (A(x) + B(x)y)/(2x^{37})$
$A(x)$	$1+111x+5735x^2+183372x^3+4070518x^4+66731757x^5+839493407x^6$ $+8317265927x^7+66131419272x^8+428160735157x^9+2284094397370x^{10}$ $+10141854349015x^{11}+37817937455677x^{12}+119384337840577x^{13}$ $+321369497716872x^{14}+742413958994112x^{15}+1479993441620981x^{16}$ $+2557518837768352x^{17}+3844682647926228x^{18}+5040446568786745x^{19}$ $+5771102747209386x^{20}+5772348707995318x^{21}+5039052928059619x^{22}$ $+3830661226098476x^{23}+2526431885027090x^{24}+1437737230666334x^{25}$ $+700668498928018x^{26}+289466658760084x^{27}+100014973703245x^{28}$ $+28384018942515x^{29}+6457169560547x^{30}+1138631535508x^{31}$ $+148372738444x^{32}+13304984549x^{33}+730929635x^{34}$ $+19194157x^{35}-13542x^{36}-8570x^{37}+x^{38}$

$X_0(37)$	$j = (A(x) + B(x)y)/(2x^{37})$ (cont.)
$B(x)$	$-(1+x)(1+3x+x^2)(1+11x+x^2)(1+7x+9x^2+7x^3+x^4)$ $\times(1+39x+623x^2+5332x^3+27007x^4+85293x^5+174954x^6+241803x^7$ $+227140x^8+141862x^9+54236x^{10}+10029x^{11}+x^{12})$ $\times(1+43x+747x^2+6741x^3+34232x^4+102516x^5+196228x^6+254142x^7$ $+227826x^8+140552x^9+57320x^{10}+13993x^{11}+1561x^{12}+6x^{13}+x^{14})$
	$y^2 = 1+14x+35x^2+48x^3+35x^4+14x^5+x^6$
	$w_{37}^* x = 1/x,\ w_{37}^* y = y/x^3$

$X_0(50)$	$j = (A(x) + B(x)y)/(2x^{25}(1-x+x^2-x^3+x^4)^2)$
$A(x)$	$1-27x+328x^2-2404x^3+12130x^4-46009x^5+140463x^6-362742x^7$ $+816971x^8-1634775x^9+2947150x^{10}-4837750x^{11}+7283825x^{12}$ $-10113250x^{13}+13004525x^{14}-15533650x^{15}+17267375x^{16}-17884450x^{17}$ $+17267375x^{18}-15533650x^{19}+13004525x^{20}-10113250x^{21}+7283825x^{22}$ $-4837749x^{23}+2947146x^{24}-1633257x^{25}+809839x^{26}-255521x^{27}$ $-1106705x^{28}+9868787x^{29}-59388022x^{30}+287219154x^{31}-1171478936x^{32}$ $+4151783509x^{33}-13056854599x^{34}+37007235600x^{35}-95655444000x^{36}$ $+227567476300x^{37}-501969994000x^{38}+1032749964225x^{39}$ $-1991498401100x^{40}+3613985237750x^{41}-6192689172300x^{42}$ $+10048194355375x^{43}-15475599952600x^{44}+22668854106600x^{45}$ $-31634943149000x^{46}+42118449170175x^{47}-53561435925500x^{48}$ $+65120676960350x^{49}-75752874230492x^{50}+84360772459109x^{51}$ $-89973966294576x^{52}+91924432360268x^{53}-89973972454560x^{54}$ $+84360789755333x^{55}-75752913429356x^{56}+65120755428254x^{57}$ $-53561577388652x^{58}+42118681382175x^{59}-31635292772600x^{60}$ $+22669339542600x^{61}-15476224169800x^{62}+10048939970575x^{63}$ $-6193518006300x^{64}+3614843691350x^{65}-1992327235100x^{66}$ $+1033495579425x^{67}-502594211200x^{68}+228052912300x^{69}-96005067600x^{70}$ $+37239447600x^{71}-13198317800x^{72}+4230251200x^{73}-1210690800x^{74}$ $+304628566x^{75}-66136232x^{76}+12115548x^{77}-1823264x^{78}+218005x^{79}$ $-19804x^{80}+1278x^{81}-52x^{82}+x^{83}$
$B(x)$	$(-1+x)(1-3x+x^2)(-1-x^2+x^3)(1-6x+9x^2-6x^3+x^4)$ $\times(1-4x-x^2-4x^3+x^4)(1-3x-3x^3+x^4)(1-2x+x^2-2x^3+x^4)$ $\times(-1+x-x^2+2x^3-3x^4+x^5)(1+x-4x^5+x^6)(-1-x-x^2-3x^4-x^5$ $-3x^6+x^7)(1-5x+7x^2-12x^3+14x^4-12x^5+7x^6-5x^7+x^8)$ $\times(-1-x-3x^3-3x^6+3x^7-5x^8+x^9)(1-x+2x^2-4x^3+5x^4-7x^5$ $+9x^6-8x^7+5x^8-4x^9+x^{10})(-1+2x-4x^3+5x^4-x^5-5x^6$ $+11x^7-19x^8+22x^9-16x^{10}+10x^{11}-6x^{12}+x^{13})$
	$y^2 = 1-4x-10x^3-4x^5+x^6$
	$w_2^* x = 1/x,\ w_2^* y = -y/x^3,\ w_{50}^* x = x,\ w_{50}^* y = -y$

References

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

[2] N. D. Elkies, *Explicit isogenies*, preprint.

[3] R. Fricke, *Die Elliptischen Funktionen und ihre Anwendungen*, Teubner, Leipzig, 1922.

[4] K. Hashimoto, *On Brandt matrices of Eichler orders*, preprint.

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

[6] M. A. Kenku and F. Momose, *Automorphism groups of the modular curve $X_0(N)$*, Compositio Math. 65 (1988), 51–80.

[7] B. Mazur, *Rational points on modular curves*, in: Modular Functions of One Variable V (Bonn, 1976), Lecture Notes in Math. 601, Springer, Berlin, 1977, 107–148.

[8] F. Momose, *Rational points on the modular curves $X_{\mathrm{split}}(p)$*, Compositio Math. 52 (1984), 115–137.

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

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

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

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

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

[14] 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
School of Science and Engineering
Waseda University
3-4-1, Okubo, Shinjuku-ku
Tokyo, Japan
E-mail: 695m5077@mn.waseda.ac.jp

Department of Mathematical Sciences and Faculty of Science
Yamagata University
1-4-12, Koshirakawa-cho, Yamagata-shi
Yamagata 990, Japan
E-mail: murabaya@kszaoh3.kj.yamagata-u.ac.jp

Received on 9.10.1996
and in revised form on 26.3.1997 (3058)