Murabayashi, N.
Osaka J. Math.
29 (1992), 405–418

ON NORMAL FORMS OF MODULAR CURVES OF GENUS 2

NAOKI MURABAYASHI

(Received April 24, 1991)

0. Introduction

In this paper, we shall be interested in studying defining equations of algebraic curves X over $\bar{\boldsymbol{Q}}$, which are uniformized by arithmetic Fuchsian groups Γ.

It is well known that one can take the modular equation of level N, denoted by $\Phi_N(x, y)$, as a defining equation of the modular curve $X_0(N)$. This equation is very important, because it plays an essential role in complex multiplication theory over imaginary quadratic fields. Moreover it reflects a property of $X_0(N)$ as the coarse moduli space of generalized elliptic curves E with a cyclic subgroup of order N. However, in case of carrying out numerical calculations, it is difficult to treat the modular equation. The reason is that its degree and coefficients are fairly large. For example,

$$\begin{aligned}\Phi_2(x, y) = {} & x^3+y^3-x^2y^2+2^4\cdot 3\cdot 31xy(x+y)-2^4\cdot 3^4\cdot 5^3(x^2+y^2)+3^4\cdot 5^3\cdot 4027xy \\ & +2^8\cdot 3^7\cdot 5^6(x+y)-2^{12}\cdot 3^9\cdot 5^9\,, \\ \Phi_3(x, y) = {} & x^4+y^4-x^3y^3-2^2\cdot 3^3\cdot 9907xy(x^2+y^2)+2^3\cdot 3^2\cdot 31x^2y^2(x+y)+ \\ & 2^{15}\cdot 3^2\cdot 5^3(x^3+y^3)+2^{16}\cdot 3^5\cdot 5^3\cdot 17\cdot 263xy(x+y)+2\cdot 3^4\cdot 13\cdot 193\cdot \\ & 6367x^2y^2-2^{31}\cdot 5^6\cdot 22973xy+2^{20}\cdot 3^3\cdot 5^6(x^2+y^2)+2^{45}\cdot 3^3\cdot 5^9(x+y) \\ & \text{(cf. [8])}.\end{aligned}$$

Therefore it seems meaningful to give more convenient equations which can be treated easily and whose degrees and coefficients are as small as possible.

Suppose now that X is of genus two. Then the field $\bar{\boldsymbol{Q}}(X)$, consisting of rational functions on X defined over $\bar{\boldsymbol{Q}}$, is isomorphic to an algebraic function field $\bar{\boldsymbol{Q}}(x, y)$, where the relation between x and y is $y^2=f(x)$ and $f(T)\in\bar{\boldsymbol{Q}}[T]$ is a separable polynomial of degree 5 or 6. We call the equation $y^2=f(x)$ a normal form of X. In [2], Fricke determined normal forms of modular curves $X_0(23)$, $X_0(29)$, $X_0(31)$, which are sufficiently simple to treat easily from our viewpoint.

In this article, we will give the most efficient method for determining a normal form of the curve X of genus 2, using only Fourier coefficients of cusp forms of weight 2 with respect to the Fuchsian group Γ. In the case of $\Gamma=\Gamma_0(p)$ or $\Gamma^*(p)$ with p prime, we can calculate Fourier coefficients by using theta series derived from ideals of a maximal order of a quaternion algebra (cf.[4]). Therefore, for modular curves $X_0(p)$ or $X^*(p)$ of genus 2, we can explicitly determine their normal forms. Let $y^2=g(x)$ be a normal form of $X_0(p)$ or $X^*(p)$ which is obtained by our method. Then a remarkable fact is that the polynomial $g(T)$ always belongs to $\boldsymbol{Z}[T]$ and its discriminant is divisible only by 2 and p.

The content of this paper is as follows. In section 1 we give a table of normal forms of some modular curves of genus 2 which are derived from our algorithm. In section 2 we give an algorithm for calculating a normal form of certain curves of genus 2. More precisely, let X be a compact Riemann surface of genus 2 which is uniformized by a Fuchsian group of the first kind Γ with $i\infty$ as its cusp. Then we can determine a normal form of X only from Fourier coefficients obtained by expanding a basis of $S_2(\Gamma)$ around $i\infty$. In section 3 we review a work of Eichler [4] and give a table of Fourier coefficients calculated by Pizer's algorithm [11].

I wish to express my sincere thanks to Y. Sato who helped me to compute theta series, and Professor K. Hashimoto whose suggestions and encouragements were valuable.

1. Results for modular curves of genus 2 of prime level

In the following table, we give normal forms of modular curves of genus 2, which are obtained by our method (cf. section 2). The data necessary to obtain these results will be given in section 3.

Table 1.

	normal form $w^2=g(x)$.	discriminant of $g(T)$.
$X_0(23)$	$w^2=x^6-8x^5+2x^4+2x^3-11x^2+10x-7.$	$2^{12}\cdot 23^6.$
$X_0(29)$	$w^2=x^6-4x^5-12x^4+2x^3+8x^2+8x-7.$	$2^{12}\cdot 29^5.$
$X_0(31)$	$w^2=x^6-8x^5+6x^4+18x^3-11x^2-14x-3.$	$2^{12}\cdot 31^4.$
$X_0(37)$	$w^2=x^6+8x^5-20x^4+28x^3-24x^2+12x-4.$	$2^{12}\cdot 37^3.$

$X^*(67)$	$w^2=x^6-4x^5+6x^4-6x^3+9x^2-14x+9.$	$2^{12}\cdot 67^2.$
$X^*(73)$	$w^2=x^6-4x^5+6x^4+2x^3-15x^2+10x+1\cdot$	$2^{12}\cdot 73^2.$
$X^*(103)$	$w^2=x^6-10x^4+22x^3-19x^2+6x+1.$	$2^{12}\cdot 103^2.$
$X^*(107)$	$w^2=x^6-4x^5+10x^4-18x^3+17x^2-10x+1.$	$2^{12}\cdot 107^2.$
$X^*(167)$	$w^2=x^6-4x^5+2x^4-2x^3-3x^2+2x-3.$	$2^{12}\cdot 167^2.$
$X^*(191)$	$w^2=x^6+2x^4+2x^3+5x^2-6x+1.$	$2^{12}\cdot 191^2.$

REMARK 1.1. Our results for $X_0(23)$, $X_0(29)$, $X_0(31)$ coincide with those given in [5]. (In the case of $X_0(23)$ and $X_0(31)$, replace x by $x-1$).

REMARK 1.2. We can explain the exponent of each prime factor of the discriminant of $g(T)$ by a theory of T. Saito (cf. [12]). Roughly speaking, this number explains a gap between the model over $\boldsymbol{Z}$ defined by $w^2=g(x)$ and the minimal regular model.

2. An algorithm for determining a normal form

Let Γ be a Fuchsian group of the first kind such that $i\infty$ is included in the set of its cusps. Therefore there exists a unique positive real number h such that

$$\Gamma\cdot\{\pm 1\}\cap\left\{\pm\begin{pmatrix}1 & \boldsymbol{R}\\ 0 & 1\end{pmatrix}\right\}=\left\{\pm\begin{pmatrix}1 & mh\\ 0 & 1\end{pmatrix}\middle| m\in\boldsymbol{Z}\right\}.$$

Let X_Γ^{an} be a compact Riemann surface which is uniformized by Γ, and g the genus of X_Γ^{an}. We assume that $g\geq 2$.

Let $f_1=\sum_{j=1}^{\infty} a_j^{(1)}q_h^j, \cdots, f_g=\sum_{j=1}^{\infty} a_j^{(g)}q_h^j$ be a basis of $S_2(\Gamma)$, where $S_2(\Gamma)$ denotes the $\boldsymbol{C}$-vector space of cusp forms of weight 2 with respect to Γ, $q_h=\exp(2\pi i\frac{z}{h})$, and z is a parameter on the complex upper-half plane $\mathfrak{H}$. Put $k=\boldsymbol{Q}(a_j^{(1)}, \cdots, a_j^{(g)}\mid j\geq 1)$. The next lemma is well known.

Lemma 2.1. *Let Ω^1 be the sheaf of holomorphic 1-forms. Then the following map Ψ is an isomorphism from $S_2(\Gamma)$ to $H^0(X_\Gamma^{an}, \Omega^1)$:*

$$\begin{aligned}\Psi: S_2(\Gamma) &\longmapsto H^0(X_\Gamma^{an}, \Omega^1)\\ f &\longmapsto \frac{2\pi i}{h}f(z)dz\end{aligned}$$

Let F be the field of meromorphic modular functions with respect to Γ whose Fourier expansions with respect to q_h have coefficients in k. Then we have the following lemma.

Lemma 2.2.

(1) *F is an algebraic function field of one variable with a constant field k.*

(2) *The rational function field $\boldsymbol{C}(X_\Gamma^{an})$ of X_Γ^{an} is generated by F and $\boldsymbol{C}$. Therefore X_Γ^{an} has a model defined over k.*

REMARK 2.3. (1) is true for any subfield F' of $\boldsymbol{C}(X_\Gamma^{an})$ and any subfield k' of $\boldsymbol{C}$ such that:

(1) $k' \subsetneqq F'$.

(2) F' and $\boldsymbol{C}$ are linearly disjoint over k'.

Proof of Lemma 2.2.

(1) Note that F and $\boldsymbol{C}$ are linearly disjoint over k. Indeed, let $\mu_1, \cdots, \mu_m$ be elements of $\boldsymbol{C}$ whichr are linearly independent over k. Suppose $\sum_{i=1}^m \mu_i g_i = 0$ with g_i in F. Let $g_i = \sum_n c_{in} q_h^n$ with $c_{in} \in k$. Then $\sum_i \mu_i c_{in} = 0$ over for every n, so that $c_{in} = 0$ for all i and n, hence $g_1 = \cdots = g_m = 0$. We choose and fix an element u of $F \backslash k$ which is clearly transcendental over $\boldsymbol{C}$. Applying Proposition 28.9 in [7], we see that F and $\boldsymbol{C}(u)$ are linearly disjoint over $k(u)$. Hence,

$$[F: k(u)] \leq [\boldsymbol{C}(X_\Gamma^{an}): \boldsymbol{C}(u)] < \infty .$$

This completes the proof of (1).

(2) We will separate into two cases.

Case 1: X_Γ^{an} is not hyperelliptic.

In this case the canonical linear system $|K|$ of X_Γ^{an} is very ample. This implies that $\boldsymbol{C}(X_\Gamma^{an}) = \boldsymbol{C}(f_2/f_1, \cdots, f_g/f_1)$. Obviously we see that $f_j/f_1 \in F\,(2 \leq j \leq g)$. Therefore $\boldsymbol{C}(X_\Gamma^{an})$ is generated by F and $\boldsymbol{C}$.

Case 2: X_Γ^{an} is hyperelliptic.

In this case we see that $[\boldsymbol{C}(X_\Gamma^{an}): \boldsymbol{C}(f_2/f_1, \cdots, f_g/f_1)] = 2$ and the genus of $\boldsymbol{C}(f_2/f_1, \cdots, f_g/f_1)$ is zero. Therefore there exists an element v of $\boldsymbol{C}(f_2/f_1, \cdots, f_g/f_1)$ such that $\boldsymbol{C}(f_2/f_1, \cdots, f_g/f_1) = \boldsymbol{C}(v)$.

Obviously $v \in \langle F, \boldsymbol{C} \rangle$, where $\langle F, \boldsymbol{C} \rangle$ denotes the subfield of $\boldsymbol{C}(X_\Gamma^{an})$ generated by F and $\boldsymbol{C}$. Since $\boldsymbol{C}(X_\Gamma^{an})$ is a quadratic extension of $\boldsymbol{C}(v)$, there exists an element w of $\boldsymbol{C}(X_\Gamma^{an})$ satisfying conditions:

(1) $\boldsymbol{C}(X_\Gamma^{an}) = \boldsymbol{C}(v, w)$.

(2) the relation between v and w is $w^2 = f(v)$ and $f(T) \in \boldsymbol{C}[T]$ is a separable polynomial.

It follows that $\dfrac{dv}{w} \in H^0(X_\Gamma^{an}, \Omega^1)$. So there exists an element $(c_1, \cdots, c_g)$ of $\boldsymbol{C}^g$ such that

$$\frac{dv}{w} = c_1 \frac{2\pi i}{h} f_1(z)dz + \cdots + c_g \frac{2\pi i}{h} f_g(z)dz .$$

Since $dq_h=\dfrac{2\pi i}{h}q_h dz$, we obtain that

$$\frac{dv}{w}=c_1\frac{f_1(z)}{q_h}dq_h+\cdots+c_g\frac{f_g(z)}{q_h}dq_h\,.$$

Hence we have

$$w=\frac{1}{c_1\dfrac{q_h^{-1}f_1(z)dq_h}{dv}+\cdots+c_g\dfrac{q_h^{-1}f_g(z)dq_h}{dv}}\,.$$

Since $v\in\langle F, \boldsymbol{C}\rangle$, we easily see that

$$\frac{q_h^{-1}f_j(z)dq_h}{dv}\in\langle F, \boldsymbol{C}\rangle \text{ for } j=1, \cdots, g\,.$$

Therefore we have $w\in\langle F, \boldsymbol{C}\rangle$. Thus $\boldsymbol{C}(X_\Gamma^{an})$ is generated by F and $\boldsymbol{C}$.

Let X_Γ denote an irreducible non-singular projective curve defined over k which corresponds to the algebraic function field F. By lemma 2.2, X_Γ is a model of X_Γ^{an} defined over k.

Lemma 2.4. *Let $\overline{i\infty}$ denote the point of X_Γ^{an} which is represented by $i\infty$. Then $\overline{i\infty}\in X_\Gamma(k)$.*

Proof. We define the map $v\colon F\backslash\{0\}\longrightarrow \boldsymbol{Z}$ by

$$g=\sum_{n\geq n_0}^{\infty}a_nq_h^n(a_{n_0}\neq 0)\longmapsto n_0\,.$$

Then v is the valuation of F which corresponds to $\overline{i\infty}$ and its residue field is k. Therefore we see that $\overline{i\infty}$ is a k-rational point of X_Γ.

Lemma 2.5.

$$\Psi^{-1}(H^0(X_\Gamma, \Omega^1))=\left\{f\in S_2(\Gamma)\ \middle|\ \begin{array}{c}\text{coefficients of the}\\ q_h\text{-expansion of } f\\ \text{belong to } k\end{array}\right\}.$$

Proof. Put $S_2(\Gamma)_k=\{f\in S_2(\Gamma)\mid$ coefficients of the q_h-expansion of f belong to $k\}$. Since the degree of a canonical divisor of X_Γ^{an} is $2g$-2, an element of $H^0(X_\Gamma^{an}, \Omega^1)$ with a zero of order more than $2g$-2 at $\overline{i\infty}$ is zero. So $(a_1^{(1)}, \cdots, a_{2g-1}^{(1)}), \cdots, (a_1^{(g)}, \cdots, a_{2g-1}^{(g)})$, which are vectors of $k^{2g-1}\subseteqq \boldsymbol{C}^{2g-1}$, are linearly independent over $\boldsymbol{C}$. Therefore there exist $1\leq l_1<\cdots<l_g\leq 2g-1$ such that

$$\det\begin{bmatrix}a_{l_1}^{(1)} & \cdots\cdots\cdots & a_{l_1}^{(g)}\\ \vdots & & \vdots\\ a_{l_g}^{(1)} & \cdots\cdots\cdots & a_{l_g}^{(g)}\end{bmatrix}\neq 0\,.$$

For any element $h=\sum_{k=1}^{\infty}b_kq_h^k$ of $S_2(\Gamma)_k$, we have $h=\sum_{i=1}^{g}c_if_i$, where $c_i\in\boldsymbol{C}\,(1\leq i\leq g)$.

In particular, we have

$$\begin{bmatrix} a_{l_1}^{(1)} \cdots\cdots\cdots a_{l_1}^{(g)} \\ \vdots \qquad\qquad \vdots \\ a_{l_g}^{(1)} \cdots\cdots\cdots a_{l_g}^{(g)} \end{bmatrix} \begin{bmatrix} c_1 \\ \vdots \\ c_g \end{bmatrix} = \begin{bmatrix} b_{l_1} \\ \vdots \\ b_{l_g} \end{bmatrix} .$$

Therefore we have $c_i \in k$ $(1 \leq i \leq g)$, which implies that $\dim_C S_2(\Gamma) = \dim_k S_2(\Gamma)_k$. On the other hand, let $k(X_\Gamma)$ denote the rational function field of X_Γ. Then we have $k(X_\Gamma) = F$ by the definition of X_Γ. Any element $\omega \in H^0(X_\Gamma, \Omega^1)$ has an expression

$$\omega = x \cdot dy \; (x, y \in k(X_\Gamma)) .$$

By $k(X_\Gamma) = F$, we have $\omega = \sum_{j=0}^{\infty} d_j q_h^j \cdot dq_h (d_j \in k)$. Let f be an element of $S_2(\Gamma)$ such that $\Psi(f) = \omega$. Then clearly $f \in S_2(\Gamma)_k$. So we have $\Psi^{-1}(H^0(X_\Gamma, \Omega^1)) \subseteqq S_2(\Gamma)_k$. By comparing the dimensions over k, we have

$$\Psi^{-1}(H^0(X_\Gamma, \Omega^1)) = S_2(\Gamma)_k .$$

Until the end of this section, we assume that the genus of X_Γ is two. We can normalize f_1, f_2 in the following forms:

(1) if $\overline{i\infty}$ is a Weierstrass point of X_Γ, then

$$f_1 = \sum_{l=3}^{\infty} a_l q_h^l \; (a_3 \neq 0) , \quad f_2 = \sum_{l=1}^{\infty} b_l q_h^l \; (b_1 \neq 0)$$

(2) if $\overline{i\infty}$ is not a Weierstrass point of X_Γ, then

$$f_1 = \sum_{l=2}^{\infty} a_l q_h^l \; (a_2 \neq 0) , \quad f_2 = \sum_{l=1}^{\infty} b_l q_h^l \; (b_1 \neq 0) .$$

From now on, we assume that $f_i (i=1, 2)$ is a basis of $S_2(\Gamma)_k$ which is normalized as above. Here put $x = f_2/f_1$. Then $x \in k(X_\Gamma)$ and $k(X_\Gamma)$ is a quadratic extension over $k(x)$. So there exists an element y of $k(X_\Gamma)$ unique up to a constant multiple such that:

(2.6) $\begin{cases} (1) & k(X_\Gamma) = k(x, y). \\ (2) & \text{the relation between } x \text{ and } y \text{ is } y^2 = f(x) \text{ and } f(T) \in k[T] \text{ is a separable polynomial.} \end{cases}$

We see that the degree of $f(T)$ is equal to 5 or 6 by Hurwitz formula, because the genus of X_Γ is two By the definition, x has a pole of order 2 (resp. 1) at $\overline{i\infty}$ if $\overline{i\infty}$ is a Weierstrass point (resp. otherwise). Hence the degree of $f(T)$ is equal to 5 (resp.6) if $\overline{i\infty}$ is a Weierstrass point (resp. otherwise).

Main Theorem. *Let Γ be a Fuchsian group of the first kind which has $i\infty$ as its cusp. We assume that the compact Riemann surface X_Γ^{an} uniformized by Γ*

is of genus 2. Let $f_1=\sum_{l=e_1}^{\infty} a_l q_h^l (a_{e_1}\neq 0)$ *and* $f_2=\sum_{l=e_2}^{\infty} b_l q_h^l (b_{e_2}\neq 0)$ *be Fourier expansions of a basis of* $S_2(\Gamma)$ *at* $i\infty$, *where*

$$(e_1, e_2)=\begin{cases}(3, 1) \ (\textit{if } \overline{i\infty} \textit{ is a Weierstrass point})\\ (2, 1) \ (\textit{otherwise})\end{cases}$$

Put $k=\boldsymbol{Q}(a_j, b_j \mid j\geq 1)$. *Let* X_Γ *be the model of* X_Γ^{an} *defined over* k, *which is determined in Lemma 2.2.*

(1) *If* $\overline{i\infty}$ *is a Weierstrass point, then we can determine a normal form of* X_Γ *from* $\{a_3, a_4, \cdots, a_{13}, b_1, b_2, \cdots, b_{11}\}$.

(2) *If* $\overline{i\infty}$ *is not a Weierstrass point, then we can determine a normal form of* X_Γ *from* $\{a_2, a_3, \cdots, a_8, b_1, b_2, \cdots, b_7\}$.

REMARK 2.7. The proof of Main Theorem gives an algorithm for determining a normal form of X_Γ.

Proof of Main Theorem (An algorithm for determining a normal form). Let $x=f_2/f_1$ and y be as in (2.6). Then we have

$$x=q_h^{e_2-e_1}\frac{b_{e_2}+b_{e_2+1}q_h+b_{e_2+2}q_h^2+\cdots}{a_{e_1}+a_{e_1+1}q_h+a_{e_1+2}q_h^2+\cdots}.$$

We put $x=q_h^{e_2-e_1}\sum_{l=0}^{\infty} c_l q_h^l$. Then we get the following claim.

Claim 1. *For any integer* $l\geq 0$, c_l *can be determined by* $\{a_{e_1}, a_{e_1+1}, \cdots, a_{e_1+l}, b_{e_2}, b_{e_2+1}, \cdots, b_{e_2+l}\}$. *In particular,* $c_0=b_{e_2}a_{e_1}^{-1}\neq 0$.

For $1\leq k\leq 6$, we put $x^k=q_h^{(e_2-e_1)k}\cdot\sum_{l=0}^{\infty} c_l^{(k)} q_h^l$, where $c_l^{(1)}=c_l$. Then we see that $c_l^{(k)}$ can be determined by $\{c_0, \cdots, c_l\}$. Hence we get the following claim.

Claim 2: *For any integers* $l\geq 0$ *and* $1\leq k\leq 6$, $c_l^{(k)}$ *can be determined by* $\{a_{e_1}, a_{e_1+1}, \cdots, a_{e_1+l}, b_{e_2}, b_{e_2+1}, \cdots, b_{e_2+l}\}$. *In particular,* $c_0^{(k)}=c_0^k\neq 0$.

Since $(\frac{2\pi i}{h}f_1(z)dz, \frac{2\pi i}{h}f_2(z)dz)$ is a basis of $H^0(X_\Gamma, \Omega^1)$ and $\frac{dx}{y}(\neq 0)\in H^0(X_\Gamma, \Omega^1)$, there exists $(s, t)\ (\neq(0, 0))\in k^2$ such that

$$\frac{dx}{y}=s\frac{2\pi i}{h}f_1(z)dz+t\frac{2\pi i}{h}f_2(z)dz.$$

We see that $\frac{2\pi i}{h}f_1(z)dz$ has a zero at $\overline{i\infty}$, and $\frac{2\pi i}{h}f_2(z)dz$ does not have a zero at $\overline{i\infty}$. On the other hand, $\frac{dx}{y}$ has a zero at $\overline{i\infty}$. Therefore t must be zero, i.e.

$$\frac{dx}{y} = s\frac{2\pi i}{h}f_1(z)dz\,. \tag{2.8}$$

Put $w=sy$ and $g(T)=s^2f(T)$, where $f(T)$ is as in (2.6). Then obviously $k(X_\Gamma)=k(x, w)$ and $w^2=g(x)$. By (2.8), we have

$$\frac{dx}{w} = \frac{2\pi i}{h}f_1(x)dz\,.$$

Hence we obtain

$$\begin{aligned} w &= \frac{dx}{\frac{2\pi i}{h}f_1(z)dz} = \frac{d(c_0q_h^{e_2-e_1}+c_1q_h^{e_2-e_1+1}+c_2q_h^{e_2-e_1+2}+\cdots)}{(a_{e_1}q_h^{e_1-1}+a_{e_1+1}q_h^{e_1}+\cdots)dq_h} \\ &= \frac{\{c_0(e_2-e_1)q_h^{e_2-e_1-1}+c_1(e_2-e_1+1)q_h^{e_2-e_1}+\cdots\}dq_h}{(a_{e_1}q_h^{e_1-1}+a_{e_1+1}q_h^{e_1}+\cdots)dq_h} \\ &= q_h^{e_2-2e_1}\frac{c_0(e_2-e_1)+c_1(e_2-e_1+1)q_h+\cdots}{a_{e_1}+a_{e_1+1}q_h+a_{e_1+2}q_h^2+\cdots}\,. \end{aligned}$$

Put $w^2=q_h^{2(e_2-2e_1)}\sum_{l=0}^{\infty}d_lq_h^l$. Then it is easy to see that $d_l(\forall l\geq 0)$ are determined by $\{a_{e_1}, a_{e_1+1}, \cdots, a_{e_1+l}, c_0, c_1, \cdots, c_l\}$. Therefore we get the following claim.

Claim 3: *For any integer $l\geq 0$, d_l can be determined by $\{a_{e_1}, a_{e_1+1}, \cdots, a_{e_1+l}, b_{e_2}, b_{e_2+1}, \cdots, b_{e_2+l}\}$.*

Here we will separate into two cases.

Case 1: $\overline{i\infty}$ is a Weierstrass point of X_Γ.

In this case we have $(e_1, e_2)=(3, 1)$, so $e_2-e_1=-2$.

Put $g(T)=u_0T^5+u_1T^4+\cdots+u_5$. Now we calculate the Fourier expansion of $g(x)$ with respect to q_h.

$$\begin{aligned} g(x) &= u_0q_h^{-10}\sum_{l=0}^{\infty}c_l^{(5)}q_h^l+u_1q_h^{-8}\sum_{l=0}^{\infty}c_l^{(4)}q_h^l+u_2q_h^{-6}\sum_{l=0}^{\infty}c_l^{(3)}q_h^l \\ &\quad +u_3q_h^{-4}\sum_{l=0}^{\infty}c_l^{(2)}q_h^l+u_4q_h^{-2}\sum_{l=0}^{\infty}c_l^{(1)}q_h^l+u_5 \\ &= q_h^{-10}\{u_0c_0^{(5)}+\cdots+(u_0c_2^{(5)}+u_1c_0^{(4)})q_h^2+\cdots+(u_0c_4^{(5)} \\ &\quad +u_1c_2^{(4)}+u_2c_0^{(3)})q_h^4+\cdots+(u_0c_6^{(5)}+u_1c_4^{(4)}+u_2c_2^{(3)}+ \\ &\quad u_3c_0^{(2)})q_h^6+\cdots+(u_0c_8^{(5)}+u_1c_6^{(4)}+u_2c_4^{(3)}+u_3c_2^{(2)}+ \\ &\quad u_4c_0^{(1)})q_h^8+\cdots+(u_0c_{10}^{(5)}+u_1c_8^{(4)}+u_2c_6^{(3)}+u_3c_4^{(2)}+ \\ &\quad u_4c_2^{(1)}+u_5)q_h^{10}+\cdots\}\,. \end{aligned}$$

Comparing both sides of $w^2=g(x)$, we obtain following equations:

$$(2.9)\quad \begin{cases} u_0c_0^{(5)} = d_0\,, \\ u_0c_2^{(5)}+u_1c_0^{(4)} = d_2\,, \\ u_0c_4^{(5)}+u_1c_2^{(4)}+u_2c_0^{(3)} = d_4\,, \\ u_0c_6^{(5)}+u_1c_4^{(4)}+u_2c_2^{(3)}+u_3c_0^{(2)} = d_6\,, \\ u_0c_8^{(5)}+u_1c_6^{(4)}+u_2c_4^{(3)}+u_3c_2^{(2)}+u_4c_0^{(1)} = d_8\,, \\ u_0c_{10}^{(5)}+u_1c_8^{(4)}+u_2c_6^{(3)}+u_3c_4^{(2)}+u_4c_2^{(1)}+u_5 = d_{10}\,. \end{cases}$$

Thus by claim 2 and claim 3, it follows that $\{u_0, u_1, \cdots, u_5\}$ can be determined by $\{a_3, a_4, \cdots, a_{13}, b_1, b_2, \cdots, b_{11}\}$. Therefore we obtain a normal form $w^2=g(x)$.

Case 2: $\overline{i\infty}$ is not a Weierstrass point.
Put $g(T)=v_0T^6+v_1T^5+\cdots+v_6$. Then we have

$$\begin{aligned} g(x) = q_h^{-6}\{&v_0c_0^{(6)}+(v_0c_1^{(6)}+v_1c_0^{(5)})q_h^1+(v_0c_2^{(6)}+v_1c_1^{(5)}+ \\ &v_2c_0^{(4)})q_h^2+(v_0c_3^{(6)}+v_1c_2^{(5)}+v_2c_1^{(4)}+v_3c_0^{(3)})q_h^3+ \\ &(v_0c_4^{(6)}+v_1c_3^{(5)}+v_2c_2^{(4)}+v_3c_1^{(3)}+v_4c_0^{(2)})q_h^4+ \\ &(v_0c_5^{(6)}+v_1c_4^{(5)}+v_2c_3^{(4)}+v_3c_2^{(3)}+v_4c_1^{(2)}+v_5c_0^{(1)})q_h^5 \\ &+(v_0c_6^{(6)}+v_1c_5^{(5)}+v_2c_4^{(4)}+v_3c_3^{(3)}+v_4c_2^{(2)}+v_5c_1^{(1)} \\ &+v_6)q_h^6+\cdots\}\,. \end{aligned}$$

Hence we obtain following equations:

$$(2.10)\quad \begin{cases} v_0c_0^{(6)} = d_0\,, \\ v_0c_1^{(6)}+v_1c_0^{(5)} = d_1\,, \\ v_0c_2^{(6)}+v_1c_1^{(5)}+v_2c_0^{(4)} = d_2\,, \\ v_0c_3^{(6)}+v_1c_2^{(5)}+v_2c_1^{(4)}+v_3c_0^{(3)} = d_3\,, \\ v_0c_4^{(6)}+v_1c_3^{(5)}+v_2c_2^{(4)}+v_3c_1^{(3)}+v_4c_0^{(2)} = d_4\,, \\ v_0c_5^{(6)}+v_1c_4^{(5)}+v_2c_3^{(4)}+v_3c_2^{(3)}+v_4c_1^{(2)}+v_5c_0^{(1)}=d_5\,, \\ v_0c_6^{(6)}+v_1c_5^{(5)}+v_2c_4^{(4)}+v_3c_3^{(3)}+v_4c_2^{(2)}+v_5c_1^{(1)}+v_6 = d_6\,. \end{cases}$$

Thus by claim 2 and claim 3, it follows that $\{v_0, v_1, \cdots, v_6\}$ can be determined by $\{a_2, a_3, \cdots, a_8, b_1, b_2, \cdots, b_7\}$. Therefore we obtain a normal form $w^2=g(x)$.

3. The basis problem for modular forms

We want to apply the above algorithm to the case of modular curves of genus 2 with respect to the congruence subgroup of pıime level p. For this purpose, we review the special case of weight 2 in Eichler's work [4] in this section. Let $\mathfrak{A}$ be a definite quaternion algebra over $\boldsymbol{Q}$, and D the discriminant of $\mathfrak{A}$. We fix a square-free positive integer H prime to D.

DEFINITION 3.1. We say that $\mathcal{O}$ is an order of level H if the following properties are satisfied:

(1) $\mathcal{O}$ is an order of $\mathfrak{A}$.

(2) For all prime numbers p which divide D, $\mathcal{O}_p$ is a maximal order of $\mathfrak{A}_p$, where $\mathcal{O}_p=\mathcal{O}\otimes_{\boldsymbol{Z}}\boldsymbol{Z}_p$ and $\mathfrak{A}_p=\mathfrak{A}\otimes_{\boldsymbol{Q}}\boldsymbol{Q}_p$.

(3) For all $p|H$, $\mathcal{O}_p$ is isomorphic to $\{\begin{pmatrix} a & b \\ pc & d\end{pmatrix}|a,b,c,d\in\boldsymbol{Z}_p\}$.

(4) For all other p, $\mathcal{O}_p$ is isomorphic to $M_2(\boldsymbol{Z}_p)$, the ring of 2×2 matrices over $\boldsymbol{Z}_p$.

Let $\mathcal{O}$ be an order of level H in $\mathfrak{A}$, and $I_1,\cdots,I_h$ be a complete set of representatives of the distinct left $\mathcal{O}$-ideal classes. Put $\mathcal{O}_j=\{a\in\mathfrak{A}|I_ja\subseteq I_j\}$ $(1\leq j\leq h)$, which is called a right order of I_j, and let e_j denote the number of units of $\mathcal{O}_j$. Note that $u\in\mathcal{O}_j$ is a unit if and only if $N(u)=1$, where N denotes the reduced norm of $\mathfrak{A}$. Thus e_j is just the number of times the positive definite quadratic form $N(x)$, $x\in\mathcal{O}_j$, represents 1 and hence e_j is finite. For any positive integer n, put $b_{ij}(n)=\frac{1}{e_j}\times\#\{\alpha\in I_j^{-1}I_i|N(\alpha)=n\times\frac{N(I_i)}{N(I_j)}\}$, where $\#$ denotes the number of elements, and $N(I)$ denotes the norm of the ideal I. Moreover, put $b_{ij}(0)=\frac{1}{e_j}$.

DEFINITION 3.2. Let notations be as above. The Brandt matrices $B(n;D,H)$ for $n\geq 0$ are defined as $h\times h$ matrices $(b_{ij}(n))$.

Then the following proposition was proved by Eichler [4, Chap. 2, §6, Corollary 1].

Proposition 3.3. *The Brandt matrices* $\boldsymbol{B}(n;D,H)$ *can be simultaneously reduced to*

$$\begin{bmatrix} \boldsymbol{B}'(n;D,H) & \begin{matrix}0\\ \vdots\\ 0\end{matrix} \\ 0\cdots\cdots\cdots 0 & b(n)\end{bmatrix},$$

where $\boldsymbol{B}'(n;D,H)$ *is an* $(h-1)\times(h-1)$ *matrix, and* $b(n)$ *is the number of integral left* $\mathcal{O}$*-ideals of norm* n.

Put $\Theta(z;D,H)=\sum_{n=0}^{\infty}\boldsymbol{B}'(n;D,H)\exp(2\pi inz)$ and let its (i,j)-component be $\theta_{ij}(z)$, i.e. $\Theta(z;D,H)=(\theta_{ij}(z))$. Let $\theta(D,H)$ be the $\boldsymbol{C}$-vector space spanned by $\{\theta_{ij}(z)|1\leq i,j\leq h\}$. For any positive integer k, let $\theta(D,H)^k=\{\theta(kz)|\theta(z)\in\theta(D,H)\}$. Put

$$\Gamma_0(N)=\left\{\begin{pmatrix} a & b\\ c & d\end{pmatrix}\in SL_2(\boldsymbol{Z})|c\equiv 0 \pmod N\right\}.$$

Then the following theorem was proved by Eichler [4, Chap. 4, §1, Theorem].

Theorem 3.4. *Let N be a square-free positive integer and $N=p_1\cdots p_r$ a decomposition of N into a product of distinct primes p_i. Let $S_2(\Gamma_0(N))$ be the $\boldsymbol{C}$-vector space of cusp forms of weight 2 with respect to $\Gamma_0(N)$. Then we have*

$$S_2(\Gamma_0(N)) = \theta(p_1, p_2p_3\cdots p_r)\oplus\theta(p_2, p_3\cdots p_r)\oplus\theta(p_2, p_3\cdots p_r)^{p_1}$$
$$\oplus\cdots\oplus\sum_{k\mid p_1\cdots p_{r-1}}\theta(p_r, 1)^k\,.$$

Remark 3.5. In the above theorem, $\theta(p_2, p_3\cdots p_r)\oplus\theta(p_2, p_3\cdots p_r)^{p_1}\oplus\cdots\oplus\sum_{k\mid p_1\cdots p_{r-1}}\theta(p_r, 1)^k$ is the subspace spanned by old forms with respect to $\Gamma_0(N)$.

Under the assumption that we can find an order of level H, and in the case of $D=p$ with a prime number p, Pizer found an algorithm for calculating the Brandt matrices $\{\boldsymbol{B}(n; p, H)\}_{n\geq 0}$ in [11]. On the other hand, we can explicitly write a basis over $\boldsymbol{Z}$ of an order of level 1 (a maximal order). Therefore in the case of $N=p$, we can calculate coefficients of the q-expansion of some basis of $S_2(\Gamma_0(p))$. Let p be a prime number such that the genus of $X_0(p)$ is 2. Then by the genus formula of $X_0(p)$, we have $p=23, 29, 31, 37$. By using Pizer's algorithm in the case of $D=p$ ($p=23, 29, 31, 37$) and $H=1$, we obtain the table 2 which gives coefficients of the q-expansion of some basis f_1, f_2 of $S_2(\Gamma_0(p))$.

Table 2.

$S_2(\Gamma_0(23))$	$f_1 = q^2-2q^3-q^4+2q^5+q^6+2q^7-2q^8+\cdots.$ $f_2 = q-q^3-q^4-2q^6+2q^7+\cdots.$
$S_2(\Gamma_0(29))$	$f_1 = q^2-q^3-2q^4+2q^6+2q^7+q^8+\cdots.$ $f_2 = q-q^4-q^5-q^6+2q^7+\cdots.$
$S_2(\Gamma_0(31))$	$f_1 = q^2-2q^3+q^4-2q^6+2q^7-2q^8+\cdots.$ $f_2 = q-q^4+q^5-2q^6-3q^7+\cdots.$
$S_2(\Gamma_0(37))$	$f_1 = q^2+2q^3-2q^4+q^5-3q^6+\cdots.$ $f_2 = q+q^3-2q^4-q^7+\cdots.$

By our algorithm stated in section 2, we get a normal form of $X_0(p)$ ($p=23, 29, 31, 37$) only from the data of table 2. For a positive integer N, let $\Gamma^*(N)$ be the normalizer of $\Gamma_0(N)$ in $SL_2(\boldsymbol{R})$ and $X^*(N)$ the modular curve over $\boldsymbol{Q}$ which is uniformized by $\Gamma^*(N)$. Let p be a prime number such that the genus of $X^*(p)$ is 2. Then by [9, §5, Corollary 2.7], we have $p=67, 73, 103, 107, 167, 191$. Moreover we can calculate coefficients of the q-expansion of some basis f_1, f_2 of $S_2(\Gamma^*(p))$ ($p=67, 73, 103, 107, 167, 191$) because a element of $S_2(\Gamma^*(p))$ is a element of $S_2(\Gamma_0(p))$ which is fixed by the main involution w_p induced by the matrix $\begin{pmatrix} 0 & 1 \\ -p & 0 \end{pmatrix}$. More precisely, let $\theta_{ij} | [w_p]$ denote the action of w_p to θ_{ij}. Then by [11, §4, Theorem 9.1], we have

Table 3.

$S_2(\Gamma^*(67))$	$f_1= q^2-q^3-3q^4+3q^7+4q^8+\cdots.$ $f_2=q-3q^3-3q^4-3q^5+q^6+4q^7+\cdots.$
$S_2(\Gamma^*(73))$	$f_1= q^2-q^3+q^4-q^5+\cdots.$ $f_2=q+q^3+q^4-3q^6-q^7+\cdots.$
$S_2(\Gamma^*(103))$	$f_1= q^2-3q^4-q^5+4q^8+\cdots.$ $f_2=q-q^3-3q^4-3q^5-q^7+\cdots.$
$S_2(\Gamma^*(107))$	$f_1= q^2-q^3-q^4-q^5-q^6+2q^7-2q^8+\cdots.$ $f_2=q-2q^3-q^4-2q^5-q^6-q^7+\cdots.$
$S_2(\Gamma^*(167))$	$f_1= q^2-q^3-q^4+q^7-2q^8+\cdots.$ $f_2=q-q^3-q^4-q^5-q^6-2q^7+\cdots.$
$S_2(\Gamma^*(191))$	$f_1= q^2-q^4-q^5-q^6-q^7-2q^8+\cdots.$ $f_2=q-q^3-q^4-q^5-q^7-q^8+\cdots.$

$$(\theta_{ij}\,|\,[w_p]) = -\boldsymbol{B}'(p;p,1)\sum_{n=0}^{\infty}\boldsymbol{B}'(n;p,1)\exp(2\pi inz)\,.$$

Therefore if we put

$$(\theta'_{ij}) = (1_{h-1}-\boldsymbol{B}'(p;p,1))\sum_{n=0}^{\infty}\boldsymbol{B}'(n;p,1)\exp(2\pi inz)\,,$$

then $\theta'_{ij}\in S_2(\Gamma_0(p))$ and $\theta'_{ij}\,|\,[w_p]=\theta'_{ij}$. Thus we have an element of $S_2(\Gamma_0(p))$ which is fixed by w_p, and we can calculate coefficients of the q-expansion of it. Thus we get the table 3, from which we obtain normal forms of $X^*(p)$ as described in section 1.

References

[1] M. Eichler: Quadratische Formen und orthogonale Gruppen, Springer-Verlag, Berlin-Gottingen-Heidelberg, 1952.

[2] M. Eichler: *Uber die Darstellbarkeit von Thetafunktionen durch Thetareihen*, Journ. reine angew. Math. **195** (1956), 156–171.

[3] M. Eichler: *Quadratische Formen und Modulfunktionen*, Acta Arithmetica **4** (1958), 217–239.

[4] M. Eichler: *The basis problem for modular forms and the trace of the Hecke operators*, Lecture Notes in Mathematics No. 320, Springer-Verlag, Berlin-New York, 75–151.

[5] R. Fricke: Die Elliptischen Funktionen und ihre Anwendungen, Leipzig and Berlin, 1916.

[6] K. Hashimoto: *Base change of simple algebras and the symmetric maximal orders of quaternion algebras*, Memories of the school of science and engineering, Waseda Univ., No. **53** (1989), 21–45.

[7] A. Hattori: Gendaidaisuugaku (in Japanese), Asakurashoten 1968.

[8] O. Herrmann, *Uber die Berechnung der Fourierkoeffizienten der Funktion $j(\tau)$*, J. reine angew. Math. **274/275** (1974), 187–195.

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

[10] D. Mumford: Tata Lectures on Theta 2, Birkhauser.

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

[12] T. Saito: *The discriminants of curves of genus* 2, Comp. Math. **69** (1989), 229–240.

[13] G. Shimura: Introduction to the arithmetic theory of automorphic functions, Princeton University Press, 1971.

[14] H.P.F. Swinnerton-Dyer and B.J. Birch: *Elliptic curves and modular functions*, Lecture Notes in Mathematics No. 476, Springer-Verlag, Berlin/New York, 3–32.

[15] D. Zagier: *Modular points, modular curves, modular surfaces and modular forms*, Lecture Notes in Mathematics No. 1111, Springer-Verlag, Berlin-Heidelberg-New York, 225–248.

Department of Mathematics
School of Science and Engineering
Waseda University
3–4–1, Okubo Shinjuku-ku,
Tokyo, 169 Japan