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

The Equation for the Modular Curve $X_1(N)$ Derived from the Equation for the Modular Curve $X(N)$

Nobuhiko ISHIDA and Noburo ISHII

Osaka Prefecture University

(Communicated by K. Shinoda)

Dedicated to Professor Toyokazu Hiramatsu on his 60th birthday

Introduction.

Let N be a positive integer greater than 6. Let $\Gamma(N)$ denote the principal congruence subgroup of level N and $\Gamma_1(N)$ a subgroup of $SL_2(\mathbf{Z})$ defined by

$$\Gamma_1(N)=\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix}\in SL_2(\mathbf{Z}) \;\middle|\; a\equiv d\equiv 1 \bmod N,\ c\equiv 0 \bmod N\right\}.$$

Let $X(N)$ and $X_1(N)$ be the modular curves associated with the groups $\Gamma(N)$ and $\Gamma_1(N)$ respectively. Further let $A(N)$ and $A_1(N)$ be the modular function fields associated with the groups $\Gamma(N)$ and $\Gamma_1(N)$ respectively. Then the field $A(N)$ (resp. $A_1(N)$) is identified with the function field of $X(N)$ (resp. $X_1(N)$) rational over $\mathbf{C}$ and $A(N)$ is a Galois extension over $A_1(N)$ of degree N. In [3], the second author defined a family of modular functions $X_r(\tau)$ of level $2N^2$, for N and $r\in\mathbf{Z}$, $r\not\equiv 0 \bmod N$, by

$$X_r(\tau)=\exp\left(-\frac{\pi i(r-1)(N-1)}{2N}\right)\prod_{s=0}^{N-1}\frac{K_{r,s}(\tau)}{K_{1,s}(\tau)}, \tag{0.1}$$

where $K_{u,v}(\tau)$ are the Klein forms of level N. For the Klein forms we refer to Kubert and Lang [5]. Define an integer ε_N by

$$\varepsilon_N=\begin{cases} 1 & \text{if } N \text{ is odd}, \\ 2 & \text{if } N \text{ is even}. \end{cases}$$

Then we showed that $X_2(\tau)^{\varepsilon_N}$, $X_3(\tau)$ generate $A(N)$ over $\mathbf{C}$. This result was firstly proved by the second author [3] for the cases N are primes and was extended to arbitrary N greater than 6 by the first author [1]. Furthermore if N is a prime, then the authors [2] showed $X_3(\tau)$ is integral over the ring $\mathbf{Z}[X_2(\tau)]$. In general, in [1], it was shown

Received July 31, 1997

that $X_3(\tau)$ is integral over the ring $\mathbf{Q}[X_2(\tau)^{\varepsilon_N}]$. Let $F_N(X, Y)\in\mathbf{Q}[X, Y]$ be the polynomial such that $F_N(X_2^{\varepsilon_N}(\tau), Y)=0$ is the monic irreducible equation of $X_3(\tau)$ over $\mathbf{Q}[X_2^{\varepsilon_N}]$. In [1, 2], we determined the polynomial $F_N(X, Y)$ and gave an effective algorithm to calculate it. The equation $F_N(X, Y)=0$ gives an affine singular model of $X(N)$ over $\mathbf{Q}$.

The purpose of this paper is to show that an affine model over $\mathbf{Q}$ (over $\mathbf{Z}$ if N is prime) of the curve $X_1(N)$ can be obtained directly from the equation $F_N(X, Y)=0$. At first we shall prove in §1 that $A_1(N)$ is generated over $\mathbf{C}$ by $X_2(\tau)^{\varepsilon_N N}$ and $X_3(\tau)^N$. For a prime N, this was proved in [4]. From this we shall show that, for any two integers m_0 and n_0 such that $3m_0+8n_0=\varepsilon_N N$, $A_1(N)$ is generated over $\mathbf{C}$ by two functions $X_2(\tau)^{m_0}X_3(\tau)^{n_0}$ and $X_2(\tau)^8X_3(\tau)^{-3}$. By a slight deformation of $F_N(X, Y)$, in §2, we shall obtain an equation satisfied with functions $X_2(\tau)^{m_0}X_3(\tau)^{n_0}$ and $X_2(\tau)^8X_3(\tau)^{-3}$. Hence we can obtain at the same time affine models of $A(N)$ and $A_1(N)$ only by calculating $F_N(X, Y)$.

In [7], Reichert obtained the defining equation of $X_1(N)$ explicitly for $N=$ 11, 13, 14, 15, 16, 17 and 18. He used Kubert's $E(b, c)$ form to obtain one of equations for $X_1(N)$ called "raw form". In general, it seems to be very hard to transform "raw form" to the defining equation of $X_1(N)$. He writes that no general algorithm exists to find the transformation from "raw form" to the defining equation. In §3, we shall give some examples.

1. Generators of $A_1(N)$.

Fix a positive integer $N\geq 7$. Consider the functions $X_2(\tau)$, $X_3(\tau)$ defined by (0.1) for N and $r=2, 3$. We shall find out generators of $A_1(N)$ among functions of the form $X_2^mX_3^n$, for $m, n\in\mathbf{Z}$.

LEMMA 1. *Let m, n be integers. Then*

$$X_2^mX_3^n\in A_1(N) \iff 3m+8n\equiv 0 \mod \varepsilon_N N .$$

PROOF. By **K1**$\sim$**K4** in §1 of Kubert and Lang [5], we know

$$X_2^mX_3^n(\tau+1)=\exp\left(\frac{\pi i(3m+8n)}{N}\right)(-1)^mX_2^mX_3^n(\tau) .$$

Thus

$$X_2^mX_3^n\in A_1(N) \iff 3m+8n+Nm\equiv 0 \mod 2N .$$

It is easy to see that the above congruence is equivalent to a congruence $3m+8n\equiv 0$ $\mod \varepsilon_N N$. □

By Lemma 1, we have

PROPOSITION 1. *Let m_0, n_0 be integers such that $3m_0+8n_0=\varepsilon_N N$. Then*

$$X_2^{m_0}X_3^{n_0},\ X_2^8X_3^{-3},\ X_2^{\varepsilon_N N},\ X_3^N\in A_1(N) .$$

Let φ be the canonical map of $X(N)$ to $X_1(N)$. Then for a function $f \in A_1(N)$ the reciprocal image $\varphi^*((f))$ of the divisor (f) of the function f is the divisor of the function $f \circ \varphi$. (See II of Silverman [8].) Let P be a point on $X_1(N)$ and e_P the ramification index of φ at the point P. Since $X(N)$ is a Galois covering of $X_1(N)$ of degree N, the reciprocal image of a divisor (P) is given by

$$\varphi^*((P)) = e_P\left(\sum_{j=1}^{N/e_P} P_j\right),$$

where $P_1, \cdots, P_{N/e_P}$ are all points of $X(N)$ lying over P. Let $ord_P(f)$ be the order of a function f at a point P and $ord_{P_j}(f)$ the order of the function $f \circ \varphi$ at the point P_j. Then $ord_{P_j}(f)$ is independent of the choice of the point P_j and $ord_P(f) = ord_{P_j}(f)/e_P$. If $X_2^m X_3^n \in A_1(N)$, then we have

$$ord_P(X_2^m X_3^n) = \frac{1}{e_P}\left\{\frac{m}{\varepsilon_N} ord_{P_j}(X_2^{\varepsilon_N}) + n\, ord_{P_j}(X_3)\right\}.$$

By definition, a function $X_2^m X_3^n$ has zeros and poles only at cusps of $\Gamma_1(N)$. Let us calculate the order of the function $X_2^m X_3^n$ at cusps. In Ogg [6], all inequivalent cusps of $\Gamma_1(N)$ are given by pairs of integers $\begin{pmatrix} u \\ v \end{pmatrix}$, where $1 \leq v \leq N$ and if we write $GCD(v, N) = d$, then u runs all over integers such that $1 \leq u \leq d/2$, $GCD(u, d) = 1$. Further we know the ramification index of φ at the cusp $\begin{pmatrix} u \\ v \end{pmatrix}$ is d. Therefore from Proposition 2 of [1], we easily deduce

LEMMA 2. *Let $X_2^m X_3^n \in A_1(N)$. Then the function $X_2^m X_3^n$ has zeros and poles only at cusps of $\Gamma_1(N)$ and its order $v_{u,v}(X_2^m X_3^n)$ at a cusp $\begin{pmatrix} u \\ v \end{pmatrix}$ is given by*

$$v_{u,v}(X_2^m X_3^n) = \begin{cases} \dfrac{(3m+8n)u^2 - (m+2n)du}{2d} & \text{if } u < \dfrac{d}{3}, \\ \dfrac{(3m+8n)u^2 - (m+8n)du + 2d^2 n}{2d} & \text{if } u \geq \dfrac{d}{3}, \end{cases}$$

where $d = GCD(v, N)$.

This Lemma shows the order $v_{u,v}(X_2^m X_3^n)$ depends only on u and GCD of v and N.

THEOREM 1. *The functions $X_2^{\varepsilon_N N}$ and X_3^N generate $A_1(N)$ over* **C**.

PROOF. The argument used in [1, 3] to prove that $A(N)$ is generated by $X_2^{\varepsilon_N}$, X_3 over **C** can be applied to the present case also. We shall give a sketch of the proof. (See [1] for details.) For a non-constant function f of $A_1(N)$, denote by $d(f)$ the degree of $A_1(N)$ over $\mathbf{C}(f)$. We know $d(f)$ is equal to the total degree of poles of the function

f. (See for example Proposition 2.11 of Shimura [9].) Let L be the subfield of $A_1(N)$ generated by $X_2^{\varepsilon_N N}$ and X_3^N over $\mathbf{C}$. We shall prove that there exist a finite number of functions $f_1, \cdots, f_s$ of L such that $GCD(d(f_1), \cdots, d(f_s))=1$. Then, since the degree of $A_1(N)$ over L is a common divisor of those $d(f_i)$, we have $L=A_1(N)$. At first let N be odd. By Lemma 2, we have

$$d(X_2^N)=-\sum_{\substack{d\mid N\\ d>3}}\varphi\left(\frac{N}{d}\right)\frac{N}{d}\sum_{\substack{0<u<d/3\\ GCD(u,d)=1}}\frac{3u^2-du}{2},$$

where $\varphi(*)$ is Euler's function. We shall consider the functions of the form $X_2^{Ni}+X_3^{Nj}$ for positive integers i, j and calculate $d(X_2^{Ni}+X_3^{Nj})$. By Lemma 2, the function $X_2^{Ni}+X_3^{Nj}$ has poles only at the cusps $\begin{pmatrix}u\\ v\end{pmatrix}$, where $1\leq v\leq N$ and $d_v=GCD(v, N)>3$, $0<u<d_v/3$, $GCD(u, d_v)=1$. By the same lemma, we have

$$v_{u,v}(X_2^N)=\left(\frac{3u^2-d_vu}{2}\right)\frac{N}{d_v},\qquad v_{u,v}(X_3^N)=(4u^2-d_vu)\frac{N}{d_v}.$$

Take i, j such that $i<2j$. Then we have

$$v_{u,v}(X_2^{Ni})-v_{u,v}(X_3^{Nj})<0 \iff u>\frac{(2j-i)d_v}{8j-3i}.$$

Therefore further if we take i, j such that $1<(2j-i)N/(8j-3i)<2$, then we have $v_{u,v}(X_2^{Ni})-v_{u,v}(X_3^{Nj})<0$ for all cusps $\begin{pmatrix}u\\ v\end{pmatrix}$ except the cusp $\begin{pmatrix}1\\ N\end{pmatrix}$. Thus we have

$$d(X_2^{Ni}+X_3^{Nj})=-\sum_{\substack{d\mid N\\ d>3}}\varphi\left(\frac{N}{d}\right)\frac{N}{d}\sum_{\substack{0<u<d/3\\ GCD(u,d)=1}}\min\left\{\frac{3u^2-du}{2}i, (4u^2-du)j\right\}$$

$$=id(X_2^N)+\frac{2(N-4)j-(N-3)i}{2}.$$

Take $(i_1, j_1)=(N-3, (N-1)/2)$, $(i_2, j_2)=(N-5, (N-3)/2)$. These pairs satisfy the properties required above and we have

$$d(X_2^{Ni_1}+X_3^{Nj_1})=i_1d(X_2^N)+\frac{N-5}{2},\quad d(X_2^{Ni_2}+X_3^{Nj_2})=i_2d(X_2^N)+\frac{N-3}{2}.$$

Hence, we see

$$GCD(d(X_2^N), d(X_2^{Ni_1}+X_3^{Nj_1}), d(X_2^{Ni_2}+X_3^{Nj_2}))=1.$$

Therefore we have $A_1(N)=L$. In the case N is even, a similar argument can be applied. (Cf. [1].) □

THEOREM 2. *Let m_0, n_0 be integers such that $3m_0+8n_0=\varepsilon_N N$. Then $X_2^{m_0}X_3^{n_0}$, $X_2^8X_3^{-3}$ generate $A_1(N)$ over* **C**.

PROOF. By Proposition 1, we know $X_2^{m_0}X_3^{n_0}$, $X_2^8X_3^{-3}\in A_1(N)$. Since

$$X_2^{\varepsilon_N N}=(X_2^{m_0}X_3^{n_0})^3(X_2^8X_3^{-3})^{n_0}\,,\qquad X_3^N=(X_2^{m_0}X_3^{n_0})^{8/\varepsilon_N}(X_2^8X_3^{-3})^{-m_0/\varepsilon_N}\,,$$

Theorem 1 shows the assertion. □

2. An equation for $A_1(N)$.

Let $F_N(X, Y)\in\mathbf{Q}[X, Y]$ be the polynomial such that $F_N(X_2^{\varepsilon_N}, Y)=0$ is a monic irreducible equation of X_3 over $\mathbf{Q}[X_2^{\varepsilon_N}]$. In [1, 2], we showed that it has of the form:

$$F_N(X, Y)=Y^{d_2}+\Phi_{d_2-1}(X)Y^{d_2-1}+\cdots+\Phi_1(X)Y+\Phi_0(X)\,.$$

Here d_2 is the degree of $A(N)$ over $\mathbf{C}(X_2^{\varepsilon_N})$ and $\Phi_j(X)\in\mathbf{Q}[X]$ for all j and further the degree of $F_N(X, Y)$ as a polynomial of X is d_3 which is equal to the degree of $A(N)$ over $\mathbf{C}(X_3)$. Write $\Phi_j(X^{\varepsilon_N})=\sum_{i=0}^{\varepsilon_N d_3}C_{i,j}X^i$. Then

$$F_N(X^{\varepsilon_N}, Y)=Y^{d_2}+\sum_{i,j}C_{i,j}X^iY^j\,,$$

where i, j of the sum run over integers such that $0\leq i\leq\varepsilon_N d_3$, $0\leq j<d_2$. If N is prime, then we showed in [2] that all coefficients $C_{i,j}$ are integers. Let $\mathfrak{T}$ be the set of pairs of integers (i, j) such that $0\leq i\leq\varepsilon_N d_3$, $0\leq j<d_2$, $C_{i,j}\neq 0$. Then we have

LEMMA 3. *Let $(i, j)\in\mathfrak{T}$. Then*

(1) $3i+8j\equiv 8d_2 \bmod \varepsilon_N N$.

(2) $(N-3)i/2+(N-4)j\leq(N-4)d_2$.

PROOF. For (1), see [1, 2]. For (2), it was proved only for primes N in Lemma 6 of [2]. However the same argument is applied to the general cases. Thus we shall here explain the essential part of the proof. We shall use the notation and terminology in §3 of [2]. Let T be an indeterminate and $\mathbf{C}((T))$ be the field of formal power series in T. Let $|\ \ |$ be the valuation on $\mathbf{C}((T))$ defined by $|T|=\lambda$ for a $\lambda\in\mathbf{R}$, $0<\lambda<1$. Consider a decomposition of the function $T^{d_3}F_N(1/T, Y)$ into irreducible factors in $\mathbf{C}((T))[Y]$. Then by the argument in §3 of [2] we have

$$T^{d_3}F_N(1/T, Y)=\Psi(T)=\prod_{(u,v)}G_{u,v}(Y)\,,$$

where the indices (u, v) run all over the cusps $\begin{pmatrix}u\\ v\end{pmatrix}$ of $\Gamma(N)$ such that the function $X_2^{\varepsilon_N}$ has poles, thus,

$$GCD(v, N)=d_v>3\,,\quad GCD(u, d_v)=1\,,\quad 0<u<d_v/3$$

and $G_{u,v}(Y)$ is the irreducible factor corresponding to the cusp $\begin{pmatrix} u \\ v \end{pmatrix}$. Further we know that $G_{u,v}(Y)$ is pure of type $(e_{u,v}, \gamma_{u,v})$, where

$$e_{u,v}=\frac{2(d_v u-3u^2)}{\varepsilon_N}, \qquad \gamma_{u,v}=\frac{(d_v-4u)\varepsilon_N}{2(d_v-3u)}\log\lambda .$$

Since $\log\lambda<0$, we see easily that $\gamma_{u,v}>\gamma_{1,N}$ for all (u, v). Take a positive number c such that $\log c=-\gamma_{1,N}$. Let $\| \ \|_c$ be the valuation of $\mathbf{C}((T))(Y)$ which coincides with $|\ |$ on $\mathbf{C}((T))$. Then since $\gamma_{u,v}>\gamma_{1,N}$, we have $\|G_{u,v}(Y)\|_c=|g_{u,v}|c^{e_{u,v}}$, where $g_{u,v}$ is the leading coefficient of the polynomial $G_{u,v}(Y)$. Therefore

$$\|\Psi(Y)\|_c=\left(\prod_{(u,v)}|g_{u,v}|\right)c^{\sum e_{u,v}}=|T^{d_3}|c^{d_2}=\lambda^{d_2}c^{d_2} .$$

On the other hand, by definition, we have

$$\|\Psi(Y)\|_c=\max_j\{|\Phi_j(1/T)T^{d_3}c^j|\} .$$

Thus we have

$$\lambda^{d_3-\deg\Phi_j(X)}c^j\leq\lambda^{d_3}c^{d_2} .$$

By taking logarithm of both sides, we have the statement (2). □

Let m_0, n_0 be integers such that $3m_0+8n_0=\varepsilon_N N$. We can always take m_0, n_0 such that $m_0\geq 0$, $n_0\leq 0$. We shall deduce an equation of $X_2^{m_0}X_3^{n_0}$, $X_2^8X_3^{-3}$ from the polynomial $F_N(X, Y)$. To simplify the notation, put $\Lambda=X_2^{m_0}X_3^{n_0}$, $\Theta=X_2^8X_3^{-3}$. Choose $(i_0, j_0)\in\mathfrak{T}$ so that $3i_0+8j_0$ is the smallest value among $3i+8j$, $(i, j)\in\mathfrak{T}$. Then by (1) of Lemma 3, for $(i, j)\in\mathfrak{T}$, we have for a non-negative integer k, $3(i-i_0)+8(j-j_0)=\varepsilon_N Nk$. By the definition of m_0, n_0, we know there exists an integer l such that

$$i-i_0=km_0-8l, \qquad j-j_0=kn_0+3l .$$

Thus we have $X_2^iX_3^j=\Lambda^k\Theta^{-l}X_2^{i_0}X_3^{j_0}$. By (2) of Lemma 3,

$$\begin{aligned} 3i+8j&\leq\frac{6(N-4)}{N-3}(d_2-j)+8j \\ &=\frac{6(N-4)}{N-3}d_2+\left(8-\frac{6(N-4)}{N-3}\right)j . \end{aligned}$$

Since $8-6(N-4)/(N-3)\geq 0$, we have $3i+8j\leq 8d_2$ and the equality holds only for $(i, j)=(0, d_2)$. Further since $n_0\leq 0$ and $l=(j-j_0-n_0k)/3$, l takes the greatest value at $(i, j)=(0, d_2)$. Put

$$k_0=\frac{-3i_0+8(d_2-j_0)}{\varepsilon_N N}, \qquad l_0=\frac{d_2-j_0-n_0k_0}{3} . \tag{2.1}$$

For $(i, j)\in\mathfrak{T}$, let

$$k(i, j)=\frac{3(i-i_0)+8(j-j_0)}{\varepsilon_N N}, \qquad l(i,j)=\frac{j-j_0-n_0k(i, j)}{3}. \tag{2.2}$$

Then we have

$$F_N(X_2^{\varepsilon_N}, X_3)=X_2^{i_0}X_3^{j_0}\left(\Lambda^{k_0}\Theta^{-l_0}+\sum_{(i,j)\in\mathfrak{T}} C_{i,j}\Lambda^{k(i,j)}\Theta^{-l(i,j)}\right)=0.$$

Therefore we have

$$\Lambda^{k_0}+\sum_{(i,j)\in\mathfrak{T}} C_{i,j}\Lambda^{k(i,j)}\Theta^{l_0-l(i,j)}=0.$$

Put

$$G_N(X, Y)=Y^{k_0}+\sum_{(i,j)\in\mathfrak{T}} C_{i,j}X^{l_0-l(i,j)}Y^{k(i,j)}. \tag{2.3}$$

By the above argument we obtain

THEOREM 3. *Let m_0, n_0 be integers such that $3m_0+8n_0=\varepsilon_N N$, $m_0\geq 0$, $n_0\leq 0$. Then $X_2^{m_0}X_3^{n_0}$ is integral over $\mathbf{Q}[X_2^8X_3^{-3}]$. Further if N is prime, then $X_2^{m_0}X_3^{n_0}$ is integral over $\mathbf{Z}[X_2^8X_3^{-3}]$. Let $G_N(X, Y)$ be the polynomial defined by* (2.1)–(2.3). *Then $G_N(X_2^8X_3^{-3}, Y)=0$ is the monic irreducible equation of $X_2^{m_0}X_3^{n_0}$ over $\mathbf{Q}[X_2^8X_3^{-3}]$ and $G_N(X, Y)=0$ gives an affine model of $X_1(N)$. Further we have*

$$F_N(X^{\varepsilon_N}, Y)=X^{i_0-8l_0}Y^{j_0+3l_0}G_N(X^8Y^{-3}, X^{m_0}Y^{n_0}).$$

3. Examples.

Let $g_1(N)$ be the genus of $X_1(N)$. Since

$$g_1(N)=1+\frac{N^2}{24}\prod_{\substack{p\mid N\\ p:\text{prime}}}\left(1-\frac{1}{p^2}\right)-\frac{1}{4}\sum_{d\mid N}\varphi(d)\varphi(N/d),$$

we know $g_1(N)>0\Leftrightarrow N=11$, $N\geq 13$. Let us give examples of the polynomial $G_N(X, Y)$ for some $N\geq 7$, which are corresponding to "raw forms" of Reichert. By nature, they are not simpler than "raw form" of Reichert. Take m_0 and n_0 as given in §2. Put $\Lambda=X_2^{m_0}X_3^{n_0}$, $\Theta=X_2^8X_3^{-3}$.

(1) $N=7$ $(m_0=5, n_0=-1)$.

$$F_7(X, Y)=Y^3-X^3Y+X, \qquad G_7(X, Y)=Y^3-XY^2+X^2.$$

Since $G_7(\Theta, \Lambda)=0$, we have $\Theta=1/(\Omega^2-\Omega^3)$, where $\Omega=\Lambda/\Theta$. Therefore we know $A_1(7)=\mathbf{C}(\Omega)$.

(2) $N=8$ $(m_0=8, n_0=-1)$.

$$F_8(X^2, Y)=Y^7+2Y^5+Y^3-X^8Y^2+X^8,$$
$$G_8(X, Y)=Y^2+(2X-X^2)Y+X^2+X^3.$$

Since $G_8(\Theta, \Lambda)=0$, we have $\Theta=(\Omega+1)^2/(\Omega-1)$, where $\Omega=\Lambda/\Theta$. Therefore we know $A_1(8)=\mathbf{C}(\Omega)$.

(3) $N=9$ $(m_0=3, n_0=0)$.

$$F_9(X, Y)=Y^6-(X^5-X^2)Y^3+X^7-2X^4+X,$$
$$G_9(X, Y)=Y^5-XY^4+XY^3+X^2Y^2-2X^2Y+X^2.$$

Since $G_9(\Theta, \Lambda)=0$, we know $\Lambda=1/(\Omega-\Omega^2)$, where $\Omega=(\Lambda-1)\Theta/\Lambda^3$. Thus $A_1(9)=\mathbf{C}(\Omega)$.

(4) $N=10$ $(m_0=12, n_0=-2)$.

$$F_{10}(X^2, Y)=Y^{14}+4X^4Y^{10}+2Y^9-X^{12}Y^7-2X^8Y^6+3X^4Y^5+Y^4 \\ +X^{16}Y^3-3X^{12}Y^2+3X^4Y-X^2,$$
$$G_{10}(X, Y)=Y^5+(4X^2-X^3)Y^4+(X^5-2X^4+2X^3)Y^3+3(X^5-X^6)Y^2 \\ +(X^6+3X^7)Y-X^8.$$

(5) $N=11$ $(m_0=9, n_0=-2)$.

$$F_{11}(X, Y)=Y^{12}-X^7Y^8+2X^6Y^7-4X^5Y^6+5X^4Y^5-2X^3Y^4 \\ +(X^{13}+X^2)Y^3-(3X^{12}+X)Y^2+3X^{11}Y-X^{10},$$
$$G_{11}(X, Y)=Y^7-X^2Y^6+2X^3Y^5+(X^5-4X^4)Y^4-(3X^6-5X^5)Y^3 \\ +(3X^7-2X^6)Y^2-(X^8-X^7)Y-X^8.$$

Since $G(\Theta, \Lambda)=0$, by setting $U=\Lambda/\Theta^2$, $V=\Theta/\Lambda$, we deduce

$$U^2-(V-1)^2(V^4+V^3+3V^2+1)U-V(V-1)^3=0.$$

From this, by setting

$$T=\frac{1}{2}\left(\frac{2U-(V-1)^2(V^4+V^3+3V^2+1)}{(V-1)^3(V^3+V-1)}+1\right), \qquad S=\frac{1}{V-1}+1,$$

we have a Weierstrass equation:

$$T^2-T=S^3-S^2.$$

(6) $N=12$ $(m_0=8, n_0=0)$.

$$F_{12}(X^2, Y)=Y^{21}-2Y^{18}+(6X^4+1)Y^{15}-(X^8-14X^4)Y^{12} \\ -(7X^8+X^4)Y^9+(X^{12}+6X^8+9X^4)Y^6 \\ -(2X^{12}-4X^8+2X^4)Y^3+X^{12}-2X^8+X^4,$$

$$G_{12}(X, Y)= Y^6-(X^3-6X^2+2X)Y^5+(X^5-7X^4+14X^3+X^2)Y^4$$
$$-(2X^6-6X^5+X^4)Y^3+(X^7+4X^6+9X^5)Y^2$$
$$-(2X^7+2X^6)Y+X^7 .$$

(7) $N=13$ $(m_0=7, n_0=-1)$.

$$F_{13}(X, Y)= Y^{20}+XY^{18}-X^2Y^{16}-X^9Y^{15}+2X^3Y^{14}+2X^{10}Y^{13}$$
$$-5X^4Y^{12}-7X^{11}Y^{11}-X^5Y^{10}+14X^{12}Y^9+(X^{19}+6X^6)Y^8$$
$$-10X^{13}Y^7-(3X^{20}+7X^7)Y^6+(4X^{14}-X)Y^5+(3X^{21}+5X^8)Y^4$$
$$-4X^{15}Y^3-X^{22}Y^2+2X^{16}Y-X^{10} ,$$

$$G_{13}(X, Y)= Y^{10}-(X^2-X)Y^9+(2X^3-X^2)Y^8+(X^5-7X^4+2X^3)Y^7$$
$$-(3X^6-14X^5+5X^4)Y^6+(3X^7-10X^6-X^5)Y^5$$
$$-(X^8-4X^7-6X^6)Y^4-(4X^8+7X^7)Y^3+(2X^9+5X^8)Y^2$$
$$-X^8Y-X^{10} .$$

References

[1] N. ISHIDA, Generators and equations for modular function fields of principal congruence subgroups, Acta Arith. LXXXV. 3 (1998), 197–207.

[2] N. ISHIDA and N. ISHII, The equations for modular function fields of principal congruence subgroups of prime level, Manuscripta Math. **90** (1996), 271–285.

[3] N. ISHII, Construction of generators of modular function fields, Math. Japon. **28** (1983), 655–681.

[4] N. ISHII, Defining equations of modular function fields, Math. Japon. **38** (1993), 941–951.

[5] D. KUBERT and S. LANG, Units in the modular function fields, Math. Ann. **218** (1975), 175–189.

[6] A. OGG, Rational points on certain elliptic modular curves, Proc. Symp. Pure Math. **24** (1973), 221–231.

[7] M. A. REICHERT, Explicit determination of nontrivial torsion structures of elliptic curves over quadratic number fields, Math. Comp. **46** (1986), 637–658.

[8] J. H. SILVERMAN, The arithmetic of elliptic curves, Graduate Texts in Math. **106** (1986), Springer.

[9] G. SHIMURA, Introduction to the arithmetic theory of automorphic functions, Iwanami/Princeton Univ. Press (1971).

Present Addresses:
NOBUHIKO ISHIDA
113 KUROTUCHI-CHO, SAKAI-CITY, OSAKA, 591–8024 JAPAN.
e-mail: ishida@an.email.ne.jp

NOBURO ISHII
DEPARTMENT OF MATHEMATICS AND INFORMATION SCIENCE, OSAKA PREFECTURE UNIVERSITY,
GAKUEN-CHO, SAKAI-CITY, OSAKA, 599–8531 JAPAN.
e-mail: ishii@mi.cias.osakafu-u.ac.jp