ACTA ARITHMETICA
LXXXV.3 (1998)

Generators and equations for modular function fields of principal congruence subgroups

by

Nobuhiko Ishida (Osaka)

1. Introduction. For a positive integer N, let $\Gamma(N)$ denote the principal congruence subgroup of level N of $SL_2(\mathbb{Z})$, namely,

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

Let $\mathcal{H}$ be the upper complex half plane, and let

$$\mathcal{H}^* = \mathcal{H} \cup \mathbb{P}^1(\mathbb{Q}) = \mathcal{H} \cup \mathbb{Q} \cup \{\infty\}.$$

Then the modular curve $X(N)$ associated with the Riemann surface $\Gamma(N)\backslash\mathcal{H}^*$ is defined over the cyclotomic field $k_N = \mathbb{Q}(\zeta_N)$, where $\zeta_N = e^{2\pi i/N}$ is a primitive Nth root of unity (cf. Chap. 6 of Shimura [6]). Therefore if the genus g_N of the curve $X(N)$ is not 0, equivalently $N \geq 6$, then the function field $\mathbb{C}(X(N))$ of $X(N)$ over the complex number field $\mathbb{C}$ has two generators s and t such that

$$\mathbb{C}(X(N)) = \mathbb{C}(s,t), \qquad F_N(s,t) = 0, \qquad F_N(X,Y) \in \mathbb{Z}[\zeta_N][X,Y],$$

where $F_N(X,Y)$ is a polynomial of two variables X and Y such that $F_N(s,Y) = 0$ is an irreducible equation of t over $k_N(s)$. Note that $\mathbb{C}(X(N))$ can be identified with the field $A(N)$ of all the modular functions with respect to $\Gamma(N)$. Further, the function field $k_N(X(N))$ of $X(N)$ rational over k_N is identified with the field $\mathfrak{F}_N$ of all the modular functions of $A(N)$ with k_N-rational Fourier coefficients at the cusp $i\infty$. (See §6.2 of Shimura [6].) Thus such generators s and t may be taken from the field $\mathfrak{F}_N$.

The problem considered here is to give such two generators explicitly using Klein forms. Moreover, we would like to know the properties of the polynomial $F_N(X,Y)$. For N prime, this problem was solved by Ishii [2] and by the author and Ishii [1]. In [2], Ishii defined a family of modular functions

1991 *Mathematics Subject Classification*: Primary 14H05; Secondary 11F03, 11G30.

$X_r(\tau)$ $(r \in \mathbb{Z},\ r \not\equiv 0 \pmod N)$ by

$$X_r(\tau) = X_r(\tau, N) = \mathbf{e}\left(-\frac{(r-1)(N-1)}{4N}\right) \prod_{s=0}^{N-1} \frac{K_{r,s}(\tau)}{K_{1,s}(\tau)}, \tag{1.1}$$

where $K_{u,v}(\tau)$ are Klein forms of level N (the functions $K_{u,v}(\tau)$ are modular forms with respect to $\Gamma(2N^2)$ of weight -1) and $\mathbf{e}(\xi) = e^{2\pi\sqrt{-1}\xi}$. See Kubert and Lang [4] or Lang [5] for Klein forms. Then we know that $X_r(\tau) \in \mathfrak{F}_N$ (resp. $X_r(\tau)^{\varepsilon_N} \in \mathfrak{F}_N$) if r is odd (resp. if r is even), where ε_N is 1 or 2 according to whether N is odd or even. In fact, we see that the Fourier expansion of the functions at the cusp $i\infty$ has integral coefficients and its leading coefficient is ± 1. He showed that for every prime $N = p > 6$, two modular functions $X_2(\tau), X_3(\tau)$ generate $\mathfrak{F}_p$ over k_p (which implies that $X_2(\tau), X_3(\tau)$ generate $A(p)$ over $\mathbb{C}$) and he also showed that for $p = 7, 11$, $X_3(\tau)$ is integral over $\mathbb{Z}[X_2(\tau)]$ by constructing an equation satisfied with $X_2(\tau)$ and $X_3(\tau)$. Afterward, in [1], the author and Ishii proved that for every prime $N = p > 6$, $X_3(\tau)$ is integral over $\mathbb{Z}[X_2(\tau)]$ and determined the irreducible monic polynomial $F_p(X, Y) \in \mathbb{Z}[X, Y]$ of $X_3(\tau)$ over $\mathbb{Z}[X_2(\tau)]$. For a given prime $p > 6$, we can compute the polynomial $F_p(X, Y)$ using an effective algorithm given in [1]. For example:

$$\begin{aligned}
F_7(X,Y) &= Y^3 - X^3Y + X \quad (g_7 = 3),\\
F_{11}(X,Y) &= Y^{12} - X^7Y^8 + 2X^6Y^7 - 4X^5Y^6 + 5X^4Y^5 - 2X^3Y^4\\
&\quad + (X^{13} + X^2)Y^3 - (3X^{12} + X)Y^2\\
&\quad + 3X^{11}Y - X^{10} \quad (g_{11} = 26),\\
F_{13}(X,Y) &= Y^{20} + XY^{18} - X^2Y^{16} - X^9Y^{15} + 2X^3Y^{14} + 2X^{10}Y^{13}\\
&\quad - 5X^4Y^{12} - 7X^{11}Y^{11} - X^5Y^{10} + 14X^{12}Y^9\\
&\quad + (X^{19} + 6X^6)Y^8 - 10X^{13}Y^7 - (3X^{20} + 7X^7)Y^6\\
&\quad + (4X^{14} - X)Y^5 + (3X^{21} + 5X^8)Y^4\\
&\quad - 4X^{15}Y^3 - X^{22}Y^2 + 2X^{16}Y - X^{10} \quad (g_{13} = 50).
\end{aligned}$$

Note that all these examples have very small integral coefficients! (Compare with the modular equation for the modular curve $X_0(p)$ satisfied by the elliptic modular functions $j(\tau)$ and $j(p\tau)$.)

The purpose of this paper is to extend the above results to all integer $N \geq 6$ except for the integral property of the function $X_3(\tau)$ over $\mathbb{Z}[X_2(\tau)]$. Our results are as follows:

THEOREM 1. *Let N be an integer ≥ 6. Then*

$$A(N) = \mathbb{C}(X_2(\tau)^{\varepsilon_N}, X_3(\tau)), \tag{1.2}$$

where ε_N is 1 or 2 according to whether N is odd or even. Further, the function $X_3(\tau)$ is integral over $\mathbb{Q}[X_2(\tau)^{\varepsilon_N}]$.

We shall prove this theorem in Sections 3 and 4.

By this theorem, we know the existence of a polynomial $F_N(X,Y) \in \mathbb{Q}[X,Y]$ such that $F_N(X_2(\tau)^{\varepsilon_N}, Y)$ is the irreducible monic polynomial of $X_3(\tau)$ over $\mathbb{Q}[X_2(\tau)^{\varepsilon_N}]$. Since we can apply the method given in [1] to the general case also, we can compute the polynomial $F_N(X,Y)$. Here are some examples:

$$
\begin{aligned}
F_6(X,Y) &= Y^3 - X^2 + 1 \quad (g_6 = 1),\\
F_8(X,Y) &= Y^7 + 2Y^5 + Y^3 - X^4Y^2 + X^4 \quad (g_8 = 5),\\
F_9(X,Y) &= Y^6 - (X^5 - X^2)Y^3 + X^7 - 2X^4 + X \quad (g_9 = 10),\\
F_{10}(X,Y) &= Y^{14} + 4X^2Y^{10} + 2Y^9 - X^6Y^7 - 2X^4Y^6\\
&\quad + 3X^2Y^5 + Y^4 + X^8Y^3\\
&\quad - 3X^6Y^2 + 3X^4Y - X^2 \quad (g_{10} = 13),\\
F_{12}(X,Y) &= Y^{21} - 2Y^{18} + (6X^4 + 1)Y^{15} - (X^8 - 14X^4)Y^{12}\\
&\quad - (7X^8 + X^4)Y^9 + (X^{12} + 6X^8 + 9X^4)Y^6\\
&\quad - (2X^{12} - 4X^8 + 2X^4)Y^3 + X^{12} - 2X^8 + X^4 \quad (g_{12} = 25),\\
F_{14}(X,Y) &= Y^{38} - 10X^2Y^{33} + 3Y^{31} + 8X^6Y^{30} - 7X^4Y^{28} - X^{10}Y^{27}\\
&\quad - 17X^2Y^{26} + 26X^8Y^{25} + 3Y^{24} + 106X^6Y^{23} - 10X^{12}Y^{22}\\
&\quad + 27X^4Y^{21} - 104X^{10}Y^{20} + (X^{16} - 5X^2)Y^{19} - 130X^8Y^{18}\\
&\quad + (31X^{14} + 1)Y^{17} + 13X^6Y^{16} + 98X^{12}Y^{15}\\
&\quad - (3X^{18} - 26X^4)Y^{14} + 15X^{10}Y^{13} - (26X^{16} - X^2)Y^{12}\\
&\quad - 53X^8Y^{11} - 26X^{14}Y^{10} + (3X^{20} - 36X^6)Y^9\\
&\quad + 34X^{12}Y^8 + (4X^{18} - 8X^4)Y^7 + 13X^{10}Y^6\\
&\quad - (X^{16} + X^2)Y^5 - (X^{22} - 5X^8)Y^4 - 10X^{14}Y^3\\
&\quad + 2X^{20}Y^2 - X^{18} \quad (g_{14} = 49),\\
F_{15}(X,Y) &= Y^{27} + 3X^3Y^{24} - (X^{11} + X)Y^{21} + (X^{14} + 13X^9 + 11X^4)Y^{18}\\
&\quad - (9X^{17} + 22X^{12} - 7X^7 + X^2)Y^{15} + (X^{25} + 15X^{20} - 9X^{15}\\
&\quad + 14X^{10} + 4X^5)Y^{12} - (2X^{28} + 4X^{23} - 6X^{18} + 19X^{13}\\
&\quad - 21X^8 + 2X^3)Y^9 + (X^{31} + X^{21} - 4X^{16} + X^{11} + X)Y^6\\
&\quad - (2X^{29} - 6X^{24} + 4X^{19} + 4X^{14} - 6X^9 + 2X^4)Y^3\\
&\quad + X^{27} - 4X^{22} + 6X^{17} - 4X^{12} + X^7 \quad (g_{15} = 73).
\end{aligned}
$$

Note that $F_6(X,Y) = 0$ and $F_7(X,Y) = 0$ are the same equations as Klein has obtained from a different point of view (cf. Chap. 5 and 6 of III in Klein–Fricke [3]). In view of these examples and the result in the case N is prime, we think it is likely that $X_3(\tau)$ is integral over $\mathbb{Z}[X_2(\tau)^{\varepsilon_N}]$ for all

integer $N \geq 6$. However, we are currently unable to prove this conjecture. It seems impossible to prove it similar to the proof for primes in [1].

Acknowledgements. The author would like to express his hearty gratitude to Professor N. Ishii for encouraging him to consider this problem and for the useful advice.

2. The properties of the functions $X_r(\tau)$. For an integer $N \geq 6$ and an integer $r \not\equiv 0 \pmod N$, let $X_r(\tau)$ be the function defined by (1.1). As mentioned in the introduction, by the fundamental properties K1–K4 of Klein forms in §1 of Kubert and Lang [4], we know that $X_r(\tau) \in A(N)$ (resp. $X_r(\tau)^{\varepsilon_N} \in A(N)$) if r is odd (resp. if r is even). Further, we deduce the following properties of $X_r(\tau)$.

PROPOSITION 1. (1) *$X_{r+kN}(\tau) = (-1)^k X_r(\tau)$ for $k \in \mathbb{Z}$.*

(2) *$X_{-r}(\tau) = -X_r(\tau)$.*

(3) *For $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$, $c \equiv 0 \pmod N$,*

$$X_r(A(\tau)) = \mathbf{e}\left(\frac{(r^2-1)ab}{2N}\right)(-1)^{(r-1)b}\frac{X_{ra}(\tau)}{X_a(\tau)}.$$

(4) *In a neighborhood of the cusp $i\infty$ of $\Gamma(2N^2)$, the function $X_r(\tau)$ has an infinite product expansion*:

$$X_r(\tau) = q^{(r-1)(r+1-N)/(2N)}\frac{1-q^r}{1-q}\prod_{n=1}^{\infty}\frac{(1-q^{pn-r})(1-q^{pn+r})}{(1-q^{pn-1})(1-q^{pn+1})},$$

where $q = \mathbf{e}(\tau) = e^{2\pi\sqrt{-1}\tau}$.

(5) *$X_r(\tau)$ has neither poles nor zeros on $\mathcal{H}$.*

P r o o f. The statements (1)–(4) are obtained from K1–K4 in §1 of Kubert and Lang [4] by elementary computation. The statement (5) is deduced from the fact that Klein forms $K_{r,s}(\tau)$ have neither poles nor zeros on $\mathcal{H}$. ∎

In particular, the function $X_r(\tau)$ (or $X_r(\tau)^{\varepsilon_N}$) $\in A(N)$ has an x-expansion at the cusp $i\infty$ with integral coefficients and leading coefficient ± 1, where $x = \mathbf{e}(\tau/N)$ is a local parameter at the cusp $i\infty$.

Now, for a fixed N and r, let us denote by $X(\tau)$ the function $X_r(\tau)$ or $X_r(\tau)^{\varepsilon_N}$ according to whether r is odd or even. In the following, we shall compute the order of $X(\tau)$ at the cusps of $\Gamma(N)$.

LEMMA 1. *Let N be an integer ≥ 3. If N is odd, then put*

$$\mathfrak{S} = \{(u,v) \mid 1 \leq u \leq (N-1)/2,\ 1 \leq v \leq N,\ (u,v,N) = 1\}$$
$$\cup \{(N,v) \mid 1 \leq v \leq (N-1)/2,\ (v,N) = 1\}.$$

If N is even, then put

$$\begin{aligned}\mathfrak{S} = &\{(u,v) \mid 1 \le u \le N/2-1,\ 1 \le v \le N,\ (u,v,N)=1\}\\ &\cup \{(N/2,v) \mid 1 \le v \le N/2,\ (v,N/2)=1\}\\ &\cup \{(N,v) \mid 1 \le v \le N/2,\ (v,N)=1\}.\end{aligned}$$

For each $(u,v) \in \mathfrak{S}$, *take a matrix* $B(u,v) \in SL_2(\mathbb{Z})$ *so that*

$$B(u,v) \equiv \begin{pmatrix} u & * \\ v & * \end{pmatrix} \pmod N.$$

Then the set $\{B(u,v)(i\infty) \mid (u,v) \in \mathfrak{S}\}$ *of rational numbers is a system of representatives of inequivalent cusps of* $\Gamma(N)$.

Proof. See Lemma 1.42 of Shimura [6]. ∎

For each $(u,v) \in \mathfrak{S}$, let $P(u,v)$ denote the cusp of $\Gamma(N)$ represented by a rational number $B(u,v)(i\infty)$. Then the order $\nu_{u,v}(X(\tau))$ of the function $X(\tau)$ at the cusp $P(u,v)$ is defined to be the order of the x-expansion of $X(B(u,v)(\tau))$ at the cusp $i\infty$. To state the order of the function $X(\tau)$ at the cusp $P(u,v)$, let us define a function $\alpha_m(w)$ $(w,m \in \mathbb{Z})$ by $\alpha_m(w) = \langle w\rangle_m(\langle w\rangle_m - m)$, where $\langle w\rangle_m$ denotes the smallest non-negative integer congruent to w modulo m. Note that $\alpha_m(w)$ is determined by w mod m, and $\alpha_m(w) = \alpha_m(-w)$.

Proposition 2. *For any* $(u,v) \in \mathfrak{S}$, *let* $m = m_v = \mathrm{GCD}(v,N)$. *Then*

$$\nu_{u,v}(X(\tau)) = \begin{cases} \frac{1}{2}(\alpha_m(ru) - \alpha_m(u)) & \text{if } r \text{ is odd},\\ (\varepsilon_N/2)(\alpha_m(ru) - \alpha_m(u)) & \text{if } r \text{ is even}. \end{cases}$$

Proof. Let r be odd. By K1 and K4 of Kubert and Lang [4], we have

$$X(B(u,v)(\tau)) = c^* \prod_{s=0}^{N-1} K_{ru+sv,ru'+sv'}(\tau)/K_{u+sv,u'+sv'}(\tau),$$

where c^* is a non-zero constant. Therefore

$$\nu_{u,v}(X(\tau)) = \frac{1}{2N}\sum_{s=0}^{N-1}(\alpha_N(ru+sv) - \alpha_N(u+sv)).$$

If $\mathrm{GCD}(v,N) = 1$, then it is easy to see that

$$\sum_{s=0}^{N-1}\alpha_N(ru+sv) = \sum_{s=0}^{N-1}\alpha_N(u+sv) = -\frac{N(N^2-1)}{6}.$$

Thus,

$$\nu_{u,v}(X(\tau)) = 0 = \frac{1}{2}(\alpha_1(ru) - \alpha_1(u))$$

in this case. Next consider the case $m = \mathrm{GCD}(v,N) \ne 1$. Let $v = km$, $\mathrm{GCD}(k,N) = 1$. Then

$$\begin{aligned}
\nu_{u,v}(X(\tau)) &= \frac{1}{2N}\sum_{s=0}^{N-1}(\alpha_N(ru+sv)-\alpha_N(u+sv))\\
&= \frac{1}{2N}\sum_{s=0}^{N-1}(\alpha_N(ru+sm)-\alpha_N(u+sm))\\
&= \frac{m}{2N}\sum_{s=0}^{N/m-1}(\alpha_N(ru+sm)-\alpha_N(u+sm))\\
&= \frac{m}{2N}\sum_{s=0}^{N/m-1}\{\langle ru+sm\rangle_N(\langle ru+sm\rangle_N-N)\\
&\qquad -\langle u+sm\rangle_N(\langle u+sm\rangle_N-N)\}
\end{aligned}$$

since $\sum_{s=0}^{N/m-1}\langle w+sm\rangle_N=\sum_{t=0}^{N/m-1}(\langle w\rangle_m+tm)$ for any w

$$\begin{aligned}
&= \frac{m}{2N}\sum_{s=0}^{N/m-1}\{(\langle ru\rangle_m+sm)(\langle ru\rangle_m+sm-N)\\
&\qquad -(\langle u\rangle_m+sm)(\langle u\rangle_m+sm-N)\}\\
&= \frac{m}{2N}\sum_{s=0}^{N/m-1}(\alpha_m(ru)-\alpha_m(u))\\
&\quad + m^2(\langle ru\rangle_m-\langle u\rangle_m)\sum_{s=0}^{N/m-1}(2s+1-N/m)\\
&= \frac{1}{2}(\alpha_m(ru)-\alpha_m(u)).
\end{aligned}$$

In a similar way, we also obtain the desired formula for r even. ∎

Corollary 1. *Let $(u,v)\in\mathfrak{S}$. The functions $X(\tau)$ have poles only at the cusps $P(u,v)$ of $\Gamma(N)$ such that*

$$m=\mathrm{GCD}(v,N)>3,\quad \mathrm{GCD}(u,m)=1\quad \textit{and}\quad 0<u<N/2.$$

Further, the order of the functions $X_2(\tau)^{\varepsilon_N}$ and $X_3(\tau)$ at the cusps $P(u,v)$ are given by

$$\nu_{u,v}(X_2(\tau)^{\varepsilon_N})=\nu_{\overline{u},v}(X_2(\tau)^{\varepsilon_N})=\frac{\varepsilon_N}{2}(3\overline{u}^2-m\overline{u}),$$

$$\nu_{u,v}(X_3(\tau))=\nu_{\overline{u},v}(X_3(\tau))=\begin{cases}4\overline{u}^2-m\overline{u} & \textit{if } \overline{u}<m/3,\\ (2\overline{u}-m)^2 & \textit{if } \overline{u}\ge m/3,\end{cases}$$

where $\overline{w}$ is defined by

$$\overline{w}=\begin{cases}\langle w\rangle_m & \textit{if } \langle w\rangle_m<m/2,\\ m-\langle w\rangle_m & \textit{otherwise.}\end{cases}$$

Proof. By the property of α_m and straightforward calculation. ∎

COROLLARY 2. (1) *$X_3(\tau)$ has poles only at the points where $X_2(\tau)^{\varepsilon_N}$ has poles.*

(2) *If N is odd, then $X_3(\tau)$ has a zero at each point where $X_2(\tau)^{\varepsilon_N}$ has a zero.*

(3) *If $3 \nmid N$, then $X_2(\tau)^{\varepsilon_N}$ has a pole or a zero at each point where $X_3(\tau)$ has a zero.*

3. The generators of $A(N)$. In this section, we prove (1.2). In the following, for a modular function $f(\tau)$, we write simply f instead of $f(\tau)$ if there is no danger of confusion. Let N be an integer ≥ 6. Since $A(N)$ is an algebraic function field of dimension one over $\mathbb{C}$, if $f \in A(N)$ is a non-constant function, then $A(N)$ is finite over the subfield $\mathbb{C}(f)$ of $A(N)$. In this case, we denote by $d(f)$ the degree of $A(N)$ over $\mathbb{C}(f)$. Our proof is based on the next lemma.

LEMMA 2. *Let L be a subfield of $A(N)$ over $\mathbb{C}$ such that $[A(N) : L] < \infty$. Let $f_1, \ldots, f_n$ be non-constant functions of L. If $\mathrm{GCD}(d(f_1), \ldots, d(f_n)) = 1$, then $L = A(N)$.*

Proof. The degree $[A(N) : L]$ is a divisor of $d(f_i) = [A(N) : \mathbb{C}(f_i)]$ for each i. Hence, $\mathrm{GCD}(d(f_1), \ldots, d(f_n)) = 1$ implies $[A(N) : L] = 1$. ∎

First, we assume N is odd. So $\varepsilon_N = 1$ in this case. Let L be the subfield of $A(N)$ generated over $\mathbb{C}$ by $X_2(\tau)$ and $X_3(\tau)$. By Lemma 2, to prove $L = A(N)$, it suffices to show that there exist two pairs of positive integers (i_1, j_1) and (i_2, j_2) such that

$$\mathrm{GCD}(d(X_2), d(X_2^{i_1} + X_3^{j_1}), d(X_2^{i_2} + X_3^{j_2})) = 1.$$

It is well known that if $f \in A(N)$ is a non-constant function, then

$$d(f) = \deg(f)_\infty = (\text{the total degree of poles of } f).$$

(See for example Proposition 2.11 of Shimura [6].) Therefore, from the property of $\alpha_m(w)$ and Corollary 1 of Proposition 2, we have

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

where $\varphi(n)$ is Euler's function.

Let us compute $d(X_2^i + X_3^j)$ for a pair of positive integers i and j. We consider $(u, v) \in \mathfrak{S}$ such that the function $X_2^i + X_3^j$ has a pole at the cusp $P(u, v)$. By Corollary 1 of Proposition 2, the function $X_2^i + X_3^j$ has poles only at the cusps $P(u, v)$, $(u, v) \in \mathfrak{S}$, such that $m_v = \mathrm{GCD}(v, N) > 3$ and $0 < \overline{u} < m_v/3$. Let

$$\mathfrak{S}' = \{(u, v) \in \mathfrak{S} \mid m_v > 3,\ 0 < u < m_v/3,\ (u, m_v) = 1\}.$$

For $(u,v) \in \mathfrak{S}'$, we have by Corollary 1 of Proposition 2,

$$\nu_{u,v}(X_2) = \frac{3u^2 - m_v u}{2}, \quad \nu_{u,v}(X_3) = 4u^2 - m_v u.$$

Now we assume that i and j satisfy

$$i < 2j, \quad \frac{(2j-i)N}{8j-3i} \notin \mathbb{Z} \quad \text{and} \quad \left[\frac{(2j-i)N}{8j-3i}\right] = 1, \tag{3.1}$$

where $[x]$ denotes the greatest integer $\le x$. (In fact, there exist i and j satisfying the assumptions (3.1) for all $N \ge 7$.) Then, for a fixed v of $(u,v) \in \mathfrak{S}'$, we know the following:

(i) If $m_v < N$ (i.e., $v \ne N$), then

$$\nu_{u,v}(X_2^i) < \nu_{u,v}(X_3^j) \Leftrightarrow 0 < u < m_v/3,\ (u, m_v) = 1.$$

(ii) If $m_v = N$ (i.e., $v = N$), then

$$\nu_{u,v}(X_2^i) < \nu_{u,v}(X_3^j) \Leftrightarrow 1 < u < m_v/3,\ (u, m_v) = 1,$$
$$\nu_{u,v}(X_2^i) > \nu_{u,v}(X_3^j) \Leftrightarrow u = 1.$$

Further, we see that $\nu_{u,v}(X_2^i) < 0$ and $\nu_{u,v}(X_2^i) \ne \nu_{u,v}(X_3^j)$ for any $(u,v) \in \mathfrak{S}'$. Thus we get

$$\begin{aligned} d(X_2^i + X_3^j) &= -\sum_{\substack{m|N \\ m>3}} \varphi\left(\frac{N}{m}\right)\frac{N}{m} \sum_{\substack{0<u<m/3 \\ (u,m)=1}} \min\left\{\frac{3u^2 - mu}{2} i, (4u^2 - mu)j\right\} \\ &= -\sum_{\substack{m|N \\ m>3}} \varphi\left(\frac{N}{m}\right)\frac{N}{m} \sum_{\substack{0<u<m/3 \\ (u,m)=1}} \frac{3u^2 - mu}{2} i + \frac{3-N}{2} i - (4-N)j \\ &= id(X_2) + \frac{1}{2}\{2(N-4)j - (N-3)i\}. \end{aligned}$$

Now, for each $N \ge 7$, we take two pairs (i,j) of positive integers so that

$$(i_1, j_1) = \left(N-3, \frac{N-1}{2}\right) \quad \text{and} \quad (i_2, j_2) = \left(N-5, \frac{N-3}{2}\right).$$

They satisfy the above assumptions (3.1). In fact, take (i_1, j_1) for instance. Then we easily see that $i_1 < 2j_1$,

$$\frac{(2j_1 - i_1)N}{8j_1 - 3i_1} = \frac{2N}{N+5} = 1 + \frac{N-5}{N+5} \notin \mathbb{Z},$$

and so $\left[\frac{(2j_1-i_1)N}{8j_1-3i_1}\right] = 1$. Therefore we obtain

$$d(X_2^{i_1} + X_3^{j_1}) = i_1 d(X_2) + (N-5)/2,$$
$$d(X_2^{i_2} + X_3^{j_2}) = i_2 d(X_2) + (N-3)/2.$$

Consequently, we have

$$\mathrm{GCD}(d(X_2), d(X_2^{i_1} + X_3^{j_1}), d(X_2^{i_2} + X_3^{j_2})) \\ = (d(X_2), (N-5)/2, (N-3)/2) = 1.$$

This shows (1.2) for odd integer N.

Next we assume N is even and ≥ 6. We shall prove

$$A(N) = \mathbb{C}(X_2(\tau)^2, X_3(\tau)^2)$$

instead of proving (1.2). In this case also, it suffices to show that there exist two pairs of positive integers (i_1, j_1) and (i_2, j_2) such that

$$\mathrm{GCD}(d(X_2^2), d(X_2^{2i_1} + X_3^{2j_1}), d(X_2^{2i_2} + X_3^{2j_2})) = 1. \tag{3.2}$$

By a similar argument, if i and j satisfy the assumptions (3.1), we deduce

$$d(X_2^{2i} + X_3^{2j}) = id(X_2^2) + 2(N-4)j - (N-3)i.$$

Now take (i, j) so that

$$(i_1, j_1) = \left(\frac{N-2}{2}, \frac{N}{4}\right), \quad (i_2, j_2) = \left(N-4, \frac{N-2}{2}\right) \quad \text{if } N \equiv 0 \pmod 4,$$

$$(i_1, j_1) = \left(\frac{N-4}{2}, \frac{N-2}{4}\right), \quad (i_2, j_2) = \left(N-2, \frac{N}{2}\right) \quad \text{if } N \equiv 2 \pmod 4.$$

For those (i, j), it is easy to show (3.2). This completes the proof of (1.2).

4. The equations for $A(N)$. In this section we prove the last part of Theorem 1. Put $d_2 = d(X_2^{\varepsilon_N})$, $d_3 = d(X_3)$. Since the degree $A(N) = \mathbb{C}(X_2^{\varepsilon_N}, X_3)$ over $\mathbb{C}(X_2^{\varepsilon_N})$ is d_2, the function X_3 has an irreducible equation $\Psi_N(Y) = 0$ of degree d_2 over $\mathbb{C}(X_2^{\varepsilon_N})$. Let $\mathfrak{F}_N$ be the subfield of $A(N)$ generated by all modular functions of $A(N)$ with k_N-rational Fourier coefficients at the cusp $i\infty$. Since $\mathfrak{F}_N$ and $\mathbb{C}$ are linearly disjoint over k_N and $A(N) = \mathbb{C}\mathfrak{F}_N$ (cf. §6.2 of Shimura [6]), the result $A(N) = \mathbb{C}(X_2^{\varepsilon_N}, X_3)$ shows that $\mathfrak{F}_N$ is generated over k_N by $X_2^{\varepsilon_N}$ and X_3. In particular, we can take a polynomial $\Psi_N(Y)$ in $k_N(X_2^{\varepsilon_N})[Y]$. After multiplying a suitable element of $k_N[X_2^{\varepsilon_N}]$, we can write

$$\Psi_N(Y) = F_N(X_2^{\varepsilon_N}, Y),$$

where

$$F_N(X, Y) = \Phi_{d_2}(X)Y^{d_2} + \Phi_{d_2-1}(X)Y^{d_2-1} + \ldots + \Phi_1(X)Y + \Phi_0(X) \\ \in k_N[X, Y],$$

$\Phi_j(X) \in k_N[X]$ for all j, $\Phi_{d_2}(X)$ is monic, and $\Phi_{d_2}(X), \ldots, \Phi_1(X)$ and $\Phi_0(X)$ have no common factors. We also write

$$F_N(X, Y) = \sum_{i,j} C_{i,j} X^i Y^j, \quad C_{i,j} \in k_N.$$

In §3 of [1], we studied various properties of $\Phi_k(X)$ and $C_{i,j}$ for the case N is prime. In that paper, Lemmas 2–5 were deduced from the behavior of the functions $X_2(\tau)$ and $X_3(\tau)$ at the cusps (e.g. Proposition 2 of [1]). Thus a similar argument can be applied to the general cases. By Corollary 2 and Proposition 1(3) of this paper, we deduce the following:

LEMMA 3. (1) $\Phi_{d_2}(X) = 1$.
(2) $\max_{0\le k\le d_2} \deg \Phi_k(X) = d_3$.
(3) *If* $3 \nmid N$, *then* $\Phi_0(X)$ *is monomial.*
(4) *If* N *is odd, then* $\Phi_k(X)$ *is divisible by* X *for all* $k < d_2$.
(5) *If* N *is odd, then* $3i + 8j \not\equiv 8d_2 \pmod N$ *implies that* $C_{i,j} = 0$.
(6) *If* N *is even, then* $3i + 4j \not\equiv 4d_2 \pmod N$ *implies that* $C_{i,j} = 0$.

By using Lemma 3(1), we can prove a result corresponding to Lemma 1 of [1].

LEMMA 4. *Let* N *be an integer* ≥ 6. *Then* $F_N(X, Y) \in \mathbb{Q}[X, Y]$.

Proof. From Lemma 3(1), $F_N(X, Y) \in k_N[X, Y]$ is the minimal polynomial of X_3 over $\mathbb{C}(X_2^{\varepsilon_N})$. Consider the constant function $F_N(X_2^{\varepsilon_N}, X_3) \equiv 0$. We use the Galois theory of $\mathfrak{F}_N/\mathbb{Q}(j)$ (cf. §6.2 of Shimura [6]). Let $f(\tau) \in \mathfrak{F}_N$ and $f = \sum c_n x^n$ be its Fourier expansion. Then any element $\sigma \in \mathrm{Gal}(k_N/\mathbb{Q})$ can be extended to an element of $\mathrm{Gal}(\mathfrak{F}_N/\mathbb{Q}(j))$ by the action $f^\sigma = \sum c_n^\sigma x^n$. Since the Fourier expansions of $X_2^{\varepsilon_N}$ and X_3 at the cusp $i\infty$ have integral coefficients, we have

$$0 = F_N(X_2^{\varepsilon_N}, X_3)^\sigma = X_3^{d_2} + \sum C_{i,j}^\sigma (X_2^{\varepsilon_N})^i X_3^j.$$

Because the polynomial $Y^{d_2} + \sum C_{i,j}^\sigma X^i Y^j$ is again the minimal polynomial of X_3 over $\mathbb{C}(X_2^{\varepsilon_N})$, we have $C_{i,j}^\sigma = C_{i,j}$ for all $\sigma \in \mathrm{Gal}(k_N/\mathbb{Q})$. It follows that $C_{i,j} \in \mathbb{Q}$. ∎

This proves the last part of Theorem 1.

Finally, let us explain how to compute the coefficients $C_{i,j}$ effectively. Since a non-constant function of $A(N)$ necessarily has poles and since $F_N(X_2(\tau)^{\varepsilon_N}, X_3(\tau)) = 0$, we get a finite system of linear equations in $C_{i,j}$ by replacing $X_2(\tau)^{\varepsilon_N}$ and $X_3(\tau)$ with their x-expansions at the cusps where $X_2^{\varepsilon_N}$ or X_3 has poles and by letting the coefficients of non-positive powers of x be equal to 0. By solving these linear equations we will be able to determine all $C_{i,j}$ in principle. But, in general, the x-expansions are in $\mathbb{Z}[\zeta_N]((x))$. Therefore, to calculate the coefficients (especially when we use a computer) this method is not so effective. Let us consider the x-expansions at the cusps $P(u, N)$. At these cusps, by Proposition 1(3), the x-expansions are essentially in $\mathbb{Z}((x))$. Furthermore, by Lemma 3(5), (6), the elements of the coefficient matrix of the system of linear equations can be taken in $\mathbb{Z}$.

(See the proof of Lemma 7 in [1].) For some N, making sufficiently many linear equations obtained by equating the coefficients of powers of x, including positive powers, we are able to determine all the coefficients of $F_N(X, Y)$. See the examples given in Section 1. The calculations were performed by means of "Mathematica" on a Unix machine.

References

[1] N. Ishida and N. Ishii, *The equations for modular function fields of principal congruence subgroups of prime level*, Manuscripta Math. 90 (1996), 271–285.
[2] N. Ishii, *Construction of generators of modular function fields*, Math. Japon. 28 (1983), 655–681.
[3] F. Klein und R. Fricke, *Vorlesungen über die Theorie der elliptischen Modulfunctionen I*, Johnson reprint cooperation, New York, 1966.
[4] D. Kubert and S. Lang, *Units in the modular function fields*, Math. Ann. 218 (1975), 175–189.
[5] S. Lang, *Elliptic Functions*, Springer, New York, 1987.
[6] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Iwanami Shoten Publ. and Princeton Univ. Press, Tokyo, 1971.

Graduate School of Science
College of Integrated Arts and Sciences
Osaka Prefecture University
1-1 Gakuen-cho, Sakai-city, Osaka 599-8531, Japan
E-mail: ishida@an.email.ne.jp

Received on 5.5.1997 (3179)