ACTA ARITHMETICA
101.4 (2002)

Generators and defining equation of the modular function field of the group $\Gamma_1(N)$

by

NOBUHIKO ISHIDA and NOBURO ISHII (Osaka)

1. Introduction. Let N be a positive integer. Let $\Gamma(N)$ denote the principal congruence subgroup of level N and $\Gamma_1(N)$ a subgroup of $\mathrm{SL}_2(\mathbb{Z})$ defined by

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \,\middle|\, a \equiv d \equiv 1 \bmod N,\ c \equiv 0 \bmod N \right\}.$$

Let $A(N)$ and $A_1(N)$ be the modular function fields with respect to the groups $\Gamma(N)$ and $\Gamma_1(N)$ respectively. Further let $X_1(N)$ be the modular curve associated with the modular function field $A_1(N)$. The genus of $X_1(N)$ is ≥ 1 if and only if $N = 11$, $N \geq 13$. The purpose of this paper is to construct "good" generators of $A_1(N)$ such that we can obtain a "simple" equation of the field $A_1(N)$, which gives an affine, in general, singular model over $\mathbb{Q}$ of the curve $X_1(N)$.

The non-cuspidal, $\mathbb{C}$-rational points of $X_1(N)$ parametrize the isomorphism classes of pairs of the elliptic curve over $\mathbb{C}$ and a point of order N on it. From this property, Reichert [9] obtained the equations of $X_1(N)$ for $N = 11, 13, \ldots, 18$ from "raw forms" which were deduced from the equation satisfied by N-torsion points on the elliptic curve called the $E(b,c)$-form. Further he calculated tables of elliptic curves over quadratic fields with torsion groups of special types. Independently, Lecacheux [7], Washington [11] and Darmon [2] constructed generators of the field $A_1(N)$ explicitly and determined the equation of $X_1(N)$ for $N = 13, 16, 25$ respectively, for the purpose of obtaining a family of cyclic extensions over $\mathbb{Q}$. The authors [3]–[5] constructed generators of $A(N), A_1(N)$ for any $N \geq 6$ and showed that the equation of $A_1(N)$ can be deduced very easily from the equation of $A(N)$ deduced from the relation between them. However our equation given in [5] is not simple as compared with the "raw forms" of Reichert. In this paper, we construct new kind of generators of $A_1(N)$ for any integer greater than 10

2000 *Mathematics Subject Classification*: Primary 14H05; Secondary 11F03, 11G18.

from similar functions used by Lecacheux, Washington and Darmon. The equations obtained from these new generators are as simple as the "raw forms" of Reichert.

In Sections 2 and 3, we shall introduce modular functions W_3, W_4, W_5 of $\Gamma_1(N)$ which are modular units (for modular units, see Kubert and Lang [6]) and show that the pairs $(W_3, W_5), (W_3, W_4)$ generate $A_1(N)$ over $\mathbb{C}$, respectively. In Section 4, we shall study the properties of the equation of $A_1(N)$ obtained from the relation between W_3 and W_5. In the last part of Section 4, as examples, we shall give equations for $11 \le N \le 20$, $N \ne 12$. Let J be the modular invariant function. In Section 5, we shall also show that the pairs (J, W_3) and (J, W_5) of modular functions each generate $A_1(N)$ over $\mathbb{C}$.

Throughout this paper, we shall use the following notation. For finitely many elements $a_1, \ldots, a_m$ of a unique factorization domain, we denote by $\mathrm{GCD}(a_1, \ldots, a_m)$ the greatest common divisor of $a_1, \ldots, a_m$. For $x \in \mathbb{R}$, we denote by $[x]$ the greatest integer not exceeding x. For a function $f(\tau)$ on the complex upper half plane and $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$, we put

$$f\,|_2\,[A] = f(A(\tau))(c\tau + d)^{-2},$$

where $A(\tau) = (a\tau + b)/(c\tau + d)$.

2. The function $W_r(\tau)$**.** Let N be a positive integer greater than 10. For a complex number τ in the complex upper half plane, we denote by L_τ the lattice in $\mathbb{C}$ generated by 1 and τ and by $\wp(z; L_\tau)$ the Weierstrass $\wp$-function associated with L_τ. For a pair (r, s) of integers such that $(r, s) \not\equiv (0, 0) \bmod N$, consider the function

$$E(\tau; r, s, N) = \wp\left(\frac{r\tau + s}{N}; L_\tau\right)$$

on the complex upper half plane. Then it is easy to see that $E(\tau; r, s, N)$ has the following transformation formula:

$$E(\tau; r, s, N)\,|_2\,[A] = E(\tau; ar + cs, br + ds, N) \quad \text{for } A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}).$$

In particular, for an integer s not congruent to 0 mod N, we know that the function

$$\phi_s(\tau) = \frac{1}{(2\pi i)^2}\wp\left(\frac{s}{N}; L_\tau\right) = \frac{1}{(2\pi i)^2}E(\tau; 0, s, N)$$

is a modular form of weight 2 of the group $\Gamma_1(N)$. Further if r and s are integers such that $r \not\equiv \pm s \bmod N$, then $\phi_r(\tau) - \phi_s(\tau)$ has neither zeros nor poles on the complex upper half plane, because the function $\wp(z; L_\tau) - \wp(s/N; L_\tau)$ has zeros (resp. poles) only at the points $z \equiv \pm s/N$ (resp. 0) mod L_τ. For a positive integer r not congruent to $0, \pm 1, \pm 2$ mod N, we define a modular function $W_r(\tau)$ with respect to $\Gamma_1(N)$ by

$$W_r(\tau) = \frac{\phi_2(\tau) - \phi_1(\tau)}{\phi_r(\tau) - \phi_1(\tau)}. \tag{1}$$

The function $W_r(\tau)$ has neither zeros nor poles on the complex upper half plane. We shall determine the order of $W_r(\tau)$ at the cusps of $\Gamma_1(N)$. In Ogg [8], all inequivalent cusps of $\Gamma_1(N)$ are given by the pairs (u,t) of integers such that:

- $1 \le t < N/2,\ 1 \le u \le D,\ \mathrm{GCD}(u,D) = 1$, or
- $t = N/2, N,\ 1 \le u \le D/2,\ \mathrm{GCD}(u,D) = 1$,

where $D = \mathrm{GCD}(t,N)$. Let (u,t) be one of the above cusps. Then, since $\mathrm{GCD}(u,t,N) = 1$, we can take a matrix $B(u,t) \in \mathrm{SL}_2(\mathbb{Z})$ such that

$$B(u,t) = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} u & * \\ t & * \end{pmatrix} \bmod N. \tag{2}$$

In the following, let $q = \exp(2\pi i\tau/N)$ and $\zeta = \exp(2\pi i/N)$. We know that q^D is the local parameter at the cusp (u,t). Therefore the order of $W_r(\tau)$ at the cusp (u,t) is equal to the order of the q^D-expansion of $W_r(B(u,t)(\tau))$. To describe the order of $W_r(\tau)$ at (u,t), we need the following notation. For an integer s, we denote by $\{s\}$ and $\mu(s)$ the integers uniquely determined by the following conditions:

$$0 \le \{s\} \le N/2, \qquad \mu(s) = \pm 1, \qquad s \equiv \mu(s)\{s\} \bmod N,$$

and further if $\{s\} = 0$ or $N/2$, then $\mu(s) = 1$.

Lemma 1. *The function $\phi_s \,|_2\, [B(u,t)]$ has the following q-expansion:*

$$\phi_s \,|_2\, [B(u,t)] - \frac{1}{12} = \begin{cases} \dfrac{\zeta^{s^*}}{(1-\zeta^{s^*})^2} - \displaystyle\sum_{m=1}^{\infty}\sum_{n=1}^{\infty} n(1-\zeta^{s^*n})(1-\zeta^{-s^*n})q^{mnN} & \text{if } \{st\}=0, \\ \displaystyle\sum_{n=1}^{\infty} n\zeta^{s^*n}q^{\{st\}n} + \sum_{m=1}^{\infty}\sum_{n=1}^{\infty} n(\zeta^{s^*n}q^{\{st\}n} + \zeta^{-s^*n}q^{-\{st\}n} - 2)q^{mnN} & \text{otherwise}, \end{cases}$$

where $s^* = \mu(st)sd$.

Proof. Since $\wp(z; L_\tau)$ is an L_τ-invariant even function, we have

$$\phi_s \,|_2\, [B(u,t)] = \frac{1}{(2\pi i)^2}\wp\left(\frac{st\tau + sd}{N}; L_\tau\right) = \frac{1}{(2\pi i)^2}\wp\left(\frac{\{st\}\tau + s^*}{N}; L_\tau\right).$$

The assertion follows from the well known expansion formula for $\wp(z; L_\tau)$

(see Robert [10], II, 5):

$$\frac{1}{(2\pi i)^2}\wp(z;L_\tau)=\sum_{m=-\infty}^{\infty}\frac{e^{2\pi iz}q^{mN}}{(1-e^{2\pi iz}q^{mN})^2}+\frac{1}{12}-2\sum_{m=1}^{\infty}\frac{q^{mN}}{(1-q^{mN})^2}.$$

(Use the fact $x/(1-x)^2=\sum_{m=1}^{\infty}mx^m$.) ∎

Lemma 2. *Let s be an integer such that $s\not\equiv 0 \bmod N$. Further, for N odd (resp. even), assume $s\not\equiv\pm1 \bmod N$ (resp. $N/2$). Then the order of the q-expansion of $(\phi_s-\phi_1)\,|_2\,[B(u,t)]$ is* $\min(\{st\},\{t\})$.

Proof. By Lemma 1, we know that the q-expansion of $\phi_s\,|_2\,[B(u,t)]-1/12$ begins with the term:

$$\begin{cases}\dfrac{\zeta^{sd}}{(1-\zeta^{sd})^2} & \text{if } \{st\}=0,\\ (\zeta^{\mu(st)sd}+\zeta^{-\mu(st)sd})q^{N/2} & \text{if } N \text{ is even and } \{st\}=N/2,\\ \zeta^{\mu(st)sd}q^{\{st\}} & \text{otherwise.}\end{cases}$$

It is to be noted that the coefficient $(\zeta^{\mu(st)sd}+\zeta^{-\mu(st)sd})$ of $q^{N/2}$ in the second case can be zero and the coefficients in the other cases are not zero. If $\{st\}\neq\{t\}$, then we get easily our assertion. Assume $\{st\}=\{t\}$. We must show that the coefficient C of $q^{\{st\}}$ of the q-expansion of the function $(\phi_s-\phi_1)\,|_2\,[B(u,t)]$ is not zero.

First assume $\{st\}=\{t\}=0$. Then $t=N$ and the coefficient C is

$$\frac{\zeta^{sd}}{(1-\zeta^{sd})^2}-\frac{\zeta^{d}}{(1-\zeta^{d})^2}=-\frac{\zeta^d(\zeta^{(s-1)d}-1)(\zeta^{(s+1)d}-1)}{(1-\zeta^{sd})^2(1-\zeta^d)^2}.$$

Since $\mathrm{GCD}(d,N)=1$ and $s\not\equiv\pm1 \bmod N$, this is not zero.

Next assume $\{st\}=\{t\}=N/2$. Then we know s is odd, $t=N/2$, $\mu(st)=\mu(t)=1$ and the coefficient C is

$$\zeta^{sd}+\zeta^{-sd}-\zeta^{d}-\zeta^{-d}=\frac{(\zeta^{(s+1)d}-1)(\zeta^{(s-1)d}-1)}{\zeta^{sd}}.$$

If this is zero, then $(s\pm1)d\equiv 0 \bmod N$. Since $t=N/2$, we have $\mathrm{GCD}(d,N/2)=1$. Therefore, $s\equiv\pm1 \bmod N/2$. This contradicts our assumption.

Finally, assume $\{st\}=\{t\}\neq 0,N/2$. Then $C=\zeta^{\mu(st)sd}-\zeta^{\mu(t)d}$. If $C=0$, then $\mu(st)sd\equiv\mu(t)d \bmod N$. Furthermore, since $\{st\}=\{t\}$, we have $\mu(st)st\equiv\mu(t)t \bmod N$. Since $\mathrm{GCD}(N,t,d)=1$, these two congruences show $s\equiv\pm1 \bmod N$. This contradicts the assumption. ∎

Since the local parameter at the cusp (u,t) is q^D, by Lemma 2, we have immediately

Proposition 1. *Let r be a positive integer such that $r\not\equiv 0,\pm1,\pm2 \bmod N$. Further, for N even, assume that $r\not\equiv\pm1 \bmod N/2$. Then W_r has* *poles or zeros only at the cusps and the order of* W_r *at the cusp* (u,t) *is*

$$\frac{\min(\{2t\},\{t\}) - \min(\{rt\},\{t\})}{D},$$

where $D = \mathrm{GCD}(t,N)$. *Furthermore* W_r *takes the value* 1 *at the cusps* (u,t) *for* t *such that* $t < \{2t\},\{rt\}$. *Note that the order is determined only by* t *and is independent of* u.

3. Generators $(W_3,W_4),(W_3,W_5)$**.** Let $N \geq 11,\ N \neq 12$. In this section, we shall show that the pairs (W_3,W_4) and (W_3,W_5) of functions each generate $A_1(N)$ over $\mathbb{C}$. Let us consider the representatives (u,t) of inequivalent cusps of $\Gamma_1(N)$ given in Section 1. Since the order of W_r at the cusp (u,t) depends only on t, we denote it by $\nu_t(W_r)$. For a non-negative integer k, if $kN/2 \leq rt < (k+1)N/2$, then

$$\{rt\} = \begin{cases} rt - kN/2 & \text{if } k \text{ is even,} \\ (k+1)N/2 - rt & \text{if } k \text{ is odd.} \end{cases}$$

Let $D = \mathrm{GCD}(t,N)$. Then by Proposition 1 we obtain the following:

$$\nu_t(W_3) = \begin{cases} 0 & \text{if } t \leq N/4, \\ (4t-N)/D & \text{if } N/4 \leq t \leq N/3, \\ (2N-5t)/D & \text{if } N/3 \leq t \leq N/2, \\ -1 & \text{if } t = N/2, \\ 0 & \text{if } t = N; \end{cases} \tag{3}$$

$$\nu_t(W_4) = \begin{cases} 0 & \text{if } t \leq N/5, \\ (5t-N)/D & \text{if } N/5 \leq t \leq N/4, \\ (N-3t)/D & \text{if } N/4 \leq t \leq 2N/5, \\ (2t-N)/D & \text{if } 2N/5 \leq t \leq N/2, \\ 0 & \text{if } t = N/2, \\ 0 & \text{if } t = N; \end{cases} \tag{4}$$

$$\nu_t(W_5) = \begin{cases} 0 & \text{if } t \leq N/6, \\ (6t-N)/D & \text{if } N/6 \leq t \leq N/5, \\ (N-4t)/D & \text{if } N/5 \leq t \leq N/4, \\ 0 & \text{if } N/4 \leq t \leq N/3, \\ (3t-N)/D & \text{if } N/3 \leq t \leq 2N/5, \\ (3N-7t)/D & \text{if } 2N/5 \leq t \leq N/2, \\ -1 & \text{if } t = N/2, \\ 0 & \text{if } t = N. \end{cases} \tag{5}$$

We find easily that W_3 has poles only at the cusps (u,t) such that $2N/5 < t \leq N/2$, W_4 has poles only at the cusps such that $N/3 < t < N/2$, and W_5 has poles only at the cusps such that $3N/7 < t \leq N/2$. In particular,

(6) W_5 has poles only at the points where W_3 does.

We shall make use of this property in the following section.

THEOREM 1. *Let the notation be as above. Then*

$$A_1(N) = \mathbb{C}(W_3, W_4) = \mathbb{C}(W_3, W_5).$$

Proof. Since we can prove $A_1(N) = \mathbb{C}(W_3, W_4)$ and $A_1(N) = \mathbb{C}(W_3, W_5)$ in the same way, we shall prove $A_1(N) = \mathbb{C}(W_3, W_4)$ in detail, and for $A_1(N) = \mathbb{C}(W_3, W_5)$ we shall only sketch the proof. For a non-constant function f of $A_1(N)$, denote by $d(f)$ the total degree of the poles of f. Then $d(f) = [A_1(N) : \mathbb{C}(f)]$. Therefore if we can find finitely many functions $f_1, \dots, f_n$ in $\mathbb{C}(W_3, W_4)$ such that $\mathrm{GCD}(d(f_1), \dots, d(f_n)) = 1$, we will have $A_1(N) = \mathbb{C}(W_3, W_4)$.

Let us consider the function $W_3^i + W_4^j$ for some (i, j). First, we assume N is odd. In this case, we take two pairs of $(i, j) = (4, N-10), (4, N-9)$. Let $(i, j) = (4, N-10)$. Then for $2N/5 < t < N/2$,

$$\begin{aligned}
&\nu_t(W_4^{N-10}) - \nu_t(W_3^4) \\
&\qquad = (N-10)(2t-N)/D + 4(5t-2N)/D = 2N\left(t - \frac{N-2}{2}\right)\Big/ D \\
&\qquad \begin{cases} < 0 & \text{if } t < (N-1)/2, \\ = 0 & \text{if } t = (N-1)/2. \end{cases}
\end{aligned}$$

Therefore, by (3) and (4) we obtain

$$\begin{aligned}
&d(W_3^4 + W_4^{N-10}) \\
&\quad = (N-10)\left\{ \sum_{N/3<t\le 2N/5} \frac{3t-N}{D} \cdot \varphi(D) + \sum_{2N/5<t<N/2} \frac{N-2t}{D} \cdot \varphi(D) \right\} \\
&\qquad - (N-10)\left(N - 2 \cdot \frac{N-1}{2}\right) + 4\left(5 \cdot \frac{N-1}{2} - 2N\right) \\
&\quad = (N-10)d(W_4) + N.
\end{aligned}$$

It is noted that $D = (t, N) = 1$ for $t = (N-1)/2$. Let $(i, j) = (4, N-9)$. Then

$$4(5t-2N)/D - (N-9)(N-2t)/D = 2(N+1)\left(t - \frac{N(N-1)}{2(N+1)}\right)\Big/ D.$$

Since we see easily that

$$\frac{N-3}{2} < \frac{N(N-1)}{2(N+1)} < \frac{N-1}{2},$$

we deduce similarly

$$d(W_3^4 + W_4^{N-9}) = (N-9)d(W_4) + N - 1.$$

Consequently, for N odd we have

$$\mathrm{GCD}(d(W_4), d(W_3^4 + W_4^{N-10}), d(W_3^4 + W_4^{N-9})) = \mathrm{GCD}(d(W_4), N, N-1) = 1.$$

Next, we assume N is even, and $N \geq 16$ for the present. In this case, we take three pairs of $(i,j) = (1, N-2), (6, N-15), (3, (N-14)/2)$. Firstly, let $(i,j) = (1, N-2)$. Since

$$(5t-2N)/D - (N-2)(N-2t)/D = (2N+1)\left(t - \frac{N^2}{2N+1}\right)\Big/D$$

and

$$\frac{N-2}{2} < \frac{N^2}{2N+1} < \frac{N}{2},$$

we obtain

$$\begin{aligned} &d(W_3 + W_4^{N-2}) \\ &= (N-2)\left\{ \sum_{N/3<t\leq 2N/5} \frac{3t-N}{D} \cdot \varphi(D) + \sum_{2N/5<t<N/2} \frac{N-2t}{D} \cdot \varphi(D) \right\} + \frac{\varphi(N/2)}{2} \\ &= (N-2)d(W_4) + \frac{\varphi(N/2)}{2}. \end{aligned}$$

Let $(i,j) = (6, N-15)$. Since

$$6(5t-2N)/D - (N-15)(N-2t)/D = 2N\left(t - \frac{N-3}{2}\right)\Big/D$$

and $\delta = ((N-2)/2, N) = 1$ (resp. 2) if $N \equiv 0 \bmod 4$ (resp. $N \equiv 2 \bmod 4$), we obtain

$$\begin{aligned} &d(W_3^6 + W_4^{N-15}) \\ &= (N-15)d(W_4) \\ &\quad - (N-15)\left(N - 2\cdot\frac{N-2}{2}\right)\Big/\delta + 6\left(5\cdot\frac{N-2}{2} - 2N\right)\Big/\delta + 6\cdot\frac{\varphi(N/2)}{2} \\ &= (N-15)d(W_4) + \frac{N}{\delta} + 6\cdot\frac{\varphi(N/2)}{2}. \end{aligned}$$

Lastly, take $(i,j) = (3, (N-14)/2)$. Then

$$3(5t-2N)/D - \frac{N-14}{2}(N-2t)/D = (N+1)\left(t - \frac{N(N-2)}{2(N+1)}\right)\Big/D.$$

Since

$$\frac{N-4}{2} < \frac{N(N-2)}{2(N+1)} < \frac{N-2}{2},$$

we conclude similarly that

$$d(W_3^3 + W_4^{(N-14)/2}) = \frac{N-14}{2}d(W_4) + \frac{N-2}{2\delta} + 3\cdot\frac{\varphi(N/2)}{2}.$$

Consequently,

$$\mathrm{GCD}(d(W_4), d(W_3 + W_4^{N-2}), d(W_3^6 + W_4^{N-15}), d(W_3^3 + W_4^{(N-14)/2})) = \mathrm{GCD}\left(d(W_4), \frac{\varphi(N/2)}{2}, \frac{N}{\delta}, \frac{N-2}{2\delta}\right) = 1.$$

For the remaining case of $N = 14$, we have $\mathrm{GCD}(d(W_4), d(W_3 + W_4^{12})) = 1$. This completes the proof of $A_1(N) = \mathbb{C}(W_3, W_4)$.

To prove $A_1(N) = \mathbb{C}(W_3, W_5)$, we may take $(i, j) = (N-14, N-10)$ and $((N-13)/2, (N-9)/2)$ for N odd, and $(i, j) = (N-3, N-2)$, $(N-21, N-15)$ and $((N-20)/2, (N-14)/2)$ for N even. ■

4. The defining equation of $A_1(N)$. We shall study the minimal equation of W_5 over $\mathbb{C}(W_3)$, which is a defining equation of $A_1(N)$ and gives an affine model of the curve $X_1(N)$. To simplify the notation, we write d_r instead of $d(W_r)$. Since W_3, W_5 have q-expansions at the cusp $i\infty$ with $\mathbb{Q}(\zeta)$-coefficients and $[A_1(N) : \mathbb{C}(W_3)] = d_3$, the minimal equation $F_N(W_3, Y) = 0$ of W_5 over $\mathbb{C}(W_3)$ can be of the form

$$F_N(X, Y) = \Phi_{d_3}(X)Y^{d_3} + \Phi_{d_3-1}(X)Y^{d_3-1} + \ldots + \Phi_1(X)Y + \Phi_0(X),$$

where $\Phi_j(X) \in \mathbb{Q}(\zeta)[X]$ for all j, the leading coefficient of $\Phi_{d_3}(X)$ is equal to 1, and $\Phi_{d_3}(X), \ldots, \Phi_1(X)$ and $\Phi_0(X)$ have no common factors except non-zero constants. Because we shall use a similar argument to that in Section 3 of Ishida and Ishii [4], we shall be brief. For details see [4]. Assume F and G generate $A_1(N)$ over $\mathbb{C}$, that is, $A_1(N) = \mathbb{C}(F, G)$. Let $\Phi(X, Y) \in \mathbb{C}[X, Y]$ be the polynomial such that $\Phi(F, Y) = 0$ is the minimal equation of G over $\mathbb{C}$. It has degree $d = d(F)$ as a polynomial of Y. Let R_1 denote the Riemann surface associated with $A_1(N)$. Then the inclusion of $\mathbb{C}(F)$ into $A_1(N)$ induces a morphishm φ of R_1 onto the projective space $\mathbb{P}^1(\mathbb{C})$ of dimension 1 such that

$$\varphi(Q) = \begin{cases} [F(Q), 1] & \text{if } F(Q) \neq \infty, \\ [1, 0] & \text{otherwise.} \end{cases}$$

For every point $\alpha \in \mathbb{P}^1(\mathbb{C})$, its inverse image $\varphi^*(\alpha)$ under φ is a divisor on R_1 given by

$$\varphi^*(\alpha) = \sum_{i=1}^{M} e_i Q_i, \tag{7}$$

where Q_i are all the distinct points of R_1 such that $F(Q_i) = \alpha$ and e_i is the absolute value of the order of F at the point Q_i. Let T be an indeterminate and $\mathbb{C}[[T]]$ the ring of formal power series in T and $\mathbb{C}((T))$ its fractional field. Put $U = T + \alpha$ (resp. $1/T$) if $\alpha \neq \infty$ (resp. $\alpha = \infty$). We can write

$\Phi(U,Y) = h(T)\Psi(Y)$, where

$$h(T) \in \mathbb{C}((T)),$$
$$\Psi(Y) = T^m Y^d + \Psi_{d-1}(T)Y^{d-1} + \ldots + \Psi_1(T)Y + \Psi_0(T),$$

m is a non-negative integer and $\Psi_j(T) \in \mathbb{C}[[T]]$ for all j. Further if $m \geq 1$ then at least one of $\Psi_j(T)(0 \leq j \leq d-1)$ is not divisible by T. By (7), we know that $\Psi(Y)$ decomposes into a product of M irreducible polynomials $G_i(Y)$ of degree e_i with coefficients in $\mathbb{C}[[T]]$. Let $|\,|$ be a valuation on $\mathbb{C}((T))$ defined by $|T| = \lambda$ for a $\lambda \in \mathbb{R}$, $0 < \lambda < 1$. Let f_i be the order of G at the point Q_i. Then we know that $G_i(Y)$ is pure of type $(e_i, -(f_i/e_i)\log\lambda)$. Further if we put

$$G_i(Y) = g_{i,e_i}(T)Y^{e_i} + \ldots + g_{i,1}(T)Y + g_{i,0}(T),$$

where $g_{i,k}(T) \in \mathbb{C}[[T]]$ for all k and $\mathrm{GCD}(g_{i,e_i}(T), \ldots, g_{i,0}(T)) = 1$, then (2.6) of [4] gives

(8) G has a pole (resp. zero) at Q_i if and only if

$$|g_{i,e_i}(T)| \text{ (resp. } |g_{i,0}(T)|) < 1.$$

LEMMA 3. *Let the notation be as above. Assume that the coefficients of $\Phi(X,Y)$ as a polynomial of Y have no common factors. Let $P_1, \ldots, P_m$ be all the distinct points of R_1 where F has zeros. Let e_i be the order of the zero of F at P_i. Further assume that G takes the value $\infty, 0, 1$ at P_i for $1 \leq i \leq k$, $k+1 \leq i \leq l$, $l+1 \leq i \leq m$ respectively. Then*

$$\Phi(0,Y) = c^* Y^a (Y-1)^b,$$

where c^* is a non-zero constant and

$$a = \sum_{k+1 \leq i \leq l} e_i, \qquad b = \sum_{l+1 \leq i \leq m} e_i.$$

Proof. Write $\Phi(T,Y) = h(T)\Psi(Y)$ as above. Then by assumption $h(0) \neq 0$. Decompose $\Psi(Y)$ into irreducible factors $G_i(Y)$ which correspond to P_i. Put

$$G_i(Y) = g_{i,e_i}(T)Y^{e_i} + \ldots + g_{i,1}(T)Y + g_{i,0}(T).$$

By assumption and (8), we have:

- if $1 \leq i \leq k$, then
$$|g_{i,0}(T)| = 1, \quad |g_{i,j}(T)| < 1 \quad \text{for } j \neq 0,$$
- if $k+1 \leq i \leq l$, then
$$|g_{i,e_i}(T)| = 1, \quad |g_{i,j}(T)| < 1 \quad \text{for } j \neq e_i.$$

For $l+1 \leq i \leq m$, since G takes the value 1, $G_i(Y)$ is written as a polynomial of $Y-1$ in

$$G_i(Y) = g^*_{i,e_i}(T)(Y-1)^{e_i} + \ldots + g^*_{i,1}(T)(Y-1) + g^*_{i,0}(T),$$

where $|g^*_{i,e_i}(T)| = 1, |g^*_{i,j}(T)| < 1$ for $j \neq e_i$. Since, for any power series $\omega(T) \in \mathbb{C}[[T]]$,

$$|\omega(T)| < 1 \quad \text{if and only if} \quad \omega(0) = 0,$$

we have

$$\begin{aligned}\Phi(0,Y) &= h(0) \prod_{1 \le i \le k} g_{i,0}(0) \prod_{k+1 \le i \le l} g_{i,e_i}(0) Y^{e_i} \prod_{l+1 \le i \le m} g^*_{i,e_i}(0)(Y-1)^{e_i} \\ &= c^* Y^a (Y-1)^b. \blacksquare\end{aligned}$$

In the following, to simplify the notation, we write $g_{i,k}$ instead of $g_{i,k}(T)$ if it is unnecessary to say explicitly that $g_{i,k}(T)$ is a power series of T.

THEOREM 2. *Let the assumption and the notation be as above, and let* $N \ge 11, \neq 12$. *Then*:

(i) $\Phi_{d_3}(X) = 1$.

(ii) $\max_{0 \le j \le d_3} \deg \Phi_j(X) = d_5$. *Furthermore, if* $7 \nmid N$, *then*

$$\deg \Phi_j(X) < \deg \Phi_a(X) = d_5 \quad \text{for all } j \neq a,$$

where

$$a = \sum_{2N/5 < t < 3N/7} \frac{5t - 2N}{D} \cdot \varphi(D) \quad \text{and} \quad D = \mathrm{GCD}(t, N).$$

(iii) *If* N *is odd, then*

$$\deg \Phi_j(X) \le \min\left(d_5, \frac{(N-7)(d_3 - j)}{N-5}\right).$$

If N *is even, then*

$$\deg \Phi_j(X) \le \min(d_5, d_3 - j).$$

(iv) $\Phi_j(X) \in \mathbb{Q}[X]$ *for all* j.

Proof. Let $(F, G) = (W_3, W_5)$ in the above explanation. By (6), W_5 has poles only at the points where W_3 does. Therefore the same argument as in Lemma 2 of [4] shows (i).

Next we prove (ii). By applying the latter part of Lemma 3 of [4] to the functions W_3, W_5 and the polynomial $F_N(X,Y)$, we obtain, by (i), $\max_j \deg \Phi_j(X) = d_5$. Let $\alpha = \infty$ and consider the decomposition

$$\Psi(Y) = T^{d_5} F_N(1/T, Y) = \prod_t G_{(u,t)}(Y).$$

Here $G_{(u,t)}(Y)$ are the irreducible factors corresponding to the cusps (u,t) where W_3 has poles, thus, the product runs through all the cusps (u,t) such that

(9) $2N/5 < t \le N/2$, and if $t < N/2$ (resp. $t = N/2$), then $1 \le u \le D$ (resp. $1 \le u \le D/2$), $\mathrm{GCD}(u, D) = 1$.

Since the degree of $G_{(u,t)}$ and the order of W_5 at the cusp (u,t) depend only on t by Proposition 1, we denote them by e_t and f_t respectively. Now let $7 \nmid N$. Since W_5 has zeros (resp. poles) at the cusp (u,t) for $2N/5 < t < 3N/7$ (resp. $3N/7 < t \leq N/2$), by (8) and (2.6) of [4], for the coefficients $g_{(u,t),j}$ of $G_{(u,t)}$, we have

$$\text{(10)} \qquad \begin{cases} |g_{(u,t),e_t}| = 1, & |g_{(u,t),j}| < 1, \quad j \neq e_t \quad \text{for } 2N/5 < t < 3N/7, \\ |g_{(u,t),0}| = 1, & |g_{(u,t),j}| < 1, \quad j \neq 0 \quad \text{for } 3N/7 < t \leq N/2. \end{cases}$$

Therefore

$$T^{d_5} F_N(1/T, Y) = \Big(\prod_{2N/5 < t < 3N/7} \prod_u g_{(u,t),e_t} \prod_{3N/7 < t \leq N/2} \prod_u g_{(u,t),0} \Big) Y^a + TH(Y),$$

where $H(Y)$ is an element of $\mathbb{C}[[T]](Y)$ and for each t, the u-product runs over all integers u such that the pair (u,t) satisfies (9). This shows (ii).

To prove (iii), let $\alpha = \infty$ again. By (5), $G_{(u,t)}(Y)$ is pure of type (e_t, γ_t), where

$$e_t = 5t - 2N, \qquad \gamma_t = -\frac{f_t}{e_t} \log \lambda = \frac{7t - 3N}{5t - 2N} \log \lambda.$$

Since $\gamma_t < \gamma_{t'}$ for $t > t'$, $\gamma_{(N-1)/2}$ (resp. $\gamma_{N/2}$) is the smallest slope among γ_t's if N is odd (resp. even). Put

$$c = \begin{cases} \exp(-\gamma_{(N-1)/2}) & \text{if } N \text{ is odd}, \\ \exp(-\gamma_{N/2}) & \text{if } N \text{ is even}. \end{cases}$$

Further extend the valuation $|\ |$ to the valuation $\|\ \|_c$ of $\mathbb{C}((T))(Y)$. See Cassels [1] for the definition of $\|\ \|_c$. Then, from the choice of c, we know that $\log(|g_{(u,t),e_t}| c^{e_t}) \geq \log(|g_{(u,t),j}| c^j)$ for all j. Thus, by (10), we have

$$\max_j \left(\left| \varPhi_j \left(\frac{1}{T} \right) T^{d_5} \right| c^j \right) = \|\varPsi(Y)\|_c = \prod \|G_{(u,t)}(Y)\|_c = \prod |g_{(u,t),e_t}| c^{e_t} = \lambda^{d_5} c^{d_3}.$$

This shows

$$\lambda^{d_5 - \deg \varPhi_j(X)} c^j \leq \lambda^{d_5} c^{d_3}.$$

By taking log on both sides, we have (iii).

To prove (iv), we shall transform W_3 and W_5 by the Atkin–Lehner involution. Put $V_3(\tau) = W_3(-1/(N\tau))$ and $V_5(\tau) = W_5(-1/(N\tau))$. Note that $A_1(N) = \mathbb{C}(V_3, V_5)$ and $F_N(V_3, Y) = 0$ is the minimal equation of V_5 over $\mathbb{C}(V_3)$. By the definition of the form $\phi_s(\tau)$ and the transformation formula for $E(\tau; r, s, N)$, we have

$$\phi_s \left(\frac{-1}{N\tau} \right) (N\tau)^{-2} = \frac{1}{(2\pi i)^2} \wp(s\tau, L_{N\tau}).$$

Furthermore by the expansion formula for the $\wp$-function given in Lemma 1, $\frac{1}{(2\pi i)^2}\wp(s\tau, L_{N\tau})$ has a q-expansion with $\mathbb{Q}$-coefficients. Thus the q-expansion of V_r lies in $\mathbb{Q}((q))$. Let us extend any element $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ to an automorphism of $\mathbb{Q}(\zeta)((q))$ by the mapping $\sum c_n q^n \mapsto \sum c_n^\sigma q^n$. Then, since $V_r^\sigma = V_r$ $(r = 3, 5)$, we have

$$F_N(V_3, V_5)^\sigma = F_N^\sigma(V_3^\sigma, V_5^\sigma) = F_N^\sigma(V_3, V_5) = 0.$$

This implies that $F_N^\sigma(V_3, Y) = 0$ is the minimal equation of V_5. Thus we have $F_N^\sigma(X, Y) = F_N(X, Y)$. Hence $\Phi_j(X) \in \mathbb{Q}[X]$ for all j. ∎

From Lemma 3 we obtain some properties of $F_N(X, Y)$.

THEOREM 3. *Let the notation be as above. Further assume N is prime. Then*:

(i) $F_N(0, Y) = F_N(1, Y) = Y^\alpha (Y - 1)^{d_3 - \alpha}$.
(ii) $F_N(X, 0) = c_1 X^\beta (X - 1)^{\gamma - \beta}$.
(iii) $F_N(X, 1) = c_2 X^\delta (X - 1)^{d_5 - \delta}$.
(iv) $F_N(X, X) = X^\varepsilon (X - 1)^{d_3 - \varepsilon}$.

Here c_1, c_2 are non-zero constants and

$$\alpha = \sum_{N/3<t<2N/5} (2N - 5t), \qquad \beta = \sum_{N/3<t<2N/5} (3t - N),$$

$$\gamma = \sum_{2N/5<t<N/2} (7t - 3N),$$

$$\delta = \sum_{N/4<t<2N/7} (4t - N) + \sum_{2N/7<t<N/3} (N - 3t),$$

$$\varepsilon = \sum_{N/3<t<3N/8} (3t - N) + \sum_{3N/8<t<2N/5} (2N - 5t).$$

Proof. The assertions for $F_N(0, Y), F_N(X, 0)$ are obtained from Proposition 1, (3) and (5) by applying Lemma 3 to the pairs $(F, G) = (W_3, W_5)$ and $(F, G) = (W_5, W_3)$ respectively.

Next we shall prove the assertion for $F_N(1, Y)$. Consider the function

$$V = W_3 - 1 = \frac{\phi_2 - \phi_3}{\phi_3 - \phi_1}.$$

Then all the points where V has zeros are the cusps $(1, t)$ for $t < N/4$. Further for $t < N/4$, W_5 takes the value 1 (resp. 0) for $t < N/6$ (resp. $N/6 < t < N/4$). Put $Z = X - 1$ and $\Psi(Z, Y) = F_N(Z + 1, Y)$. Then $\Psi(V, Y) = 0$ is the minimal equation of W_5 over $\mathbb{C}(V)$. Apply Lemma 3 to $(F, G) = (V, W_5)$. Because the order of V at $(1, t)$ is t for $t < N/6$ and

$d(V) = d_3$, we see that

$$F_N(1, Y) = \Psi(0, Y) = Y^{d_3 - h}(Y - 1)^h,$$

where $h = \sum_{t<N/6} t$. Furthermore it is easy to see that

$$h = \sum_{N/4<t<N/3} (4t - N) = d_3 - \alpha.$$

This completes the proof of (i). Applying Lemma 3 to $(F, G) = (W_5 - 1, W_3)$, similarly, we can show (iii).

Finally, we prove (iv). Let $V_1 = W_5 - W_3$. Since

$$V_1 = \frac{(\phi_2 - \phi_1)(\phi_3 - \phi_5)}{(\phi_5 - \phi_1)(\phi_3 - \phi_1)},$$

by (3) and (5) all points where V_1 has zeros (resp. poles) are the cusps $(1, t)$ for $t < N/6$, $N/3 < t < 2N/5$ (resp. $t > 2N/5$) and

$$\nu_t(V_1) = \begin{cases} 3t - N & \text{if } N/3 < t < 3N/8, \\ 2N - 5t & \text{if } t > 3N/8. \end{cases}$$

Since $A_1(N) = \mathbb{C}(V_1, W_3)$, $d(V_1) = d_3$ and $G(X, Z) = F(X, Z + X)$ is a polynomial of X of degree d_3, $G(X, V_1) = 0$ is the minimal equation of W_3 over $\mathbb{C}(V_1)$. The function W_3 takes the value 1 (resp. 0) at the cusps $(1, t)$ for $t < N/6$ (resp. $N/3 < t < 2N/5$). If we apply Lemma 3 to $(F, G) = (V_1, W_3)$, we have

$$F(X, X) = G(X, 0) = X^{\varepsilon}(X - 1)^{d_3 - \varepsilon}. \ \blacksquare$$

Let N be a prime. Since d_3 is also equal to the total degree of zeros of W_3, we have, by (3),

$$d_3 = \alpha + \sum_{N/4<t<N/3} (4t - N).$$

Thus $0 < \alpha < d_3$ and $F_N(0, 0) = F_N(1, 1) = F_N(1, 0) = F_N(0, 1) = 0$. From this, the polynomials $F_N(X, X), F_N(0, X), F_N(X, 0)$, and $F_N(X, 1)$ are each divisible by $X(X - 1)$. Put

$$R(X) = \frac{F_N(X, X) - F_N(0, X) - F_N(X, 0)}{X(X - 1)},$$

$$S(X) = \frac{F_N(X, 0) - F_N(X, 1)}{X - 1}.$$

Then Theorem 3 yields

PROPOSITION 2. *Let N be a prime. Then the polynomial $F_N(X, Y)$ can be written in the form*:

$$F_N(X,Y) = F_N(X,X) + F_N(0,Y) - F_N(0,X) \\ + (Y-X)\{(Y+X-1)R(X) + YS(X)\} \\ + X(X-1)Y(Y-1)(Y-X)U(X,Y),$$

where $U(X,Y) \in \mathbb{Q}[X,Y]$.

Proof. This is obtained by simple computation. We omit the proof. ∎

We can generalize the results of Theorem 3 to N composite as follows.

THEOREM 4. (i) *If* $3 \nmid N$, *then* $F_N(0,Y) = Y^{\alpha}(Y-1)^{d_3-\alpha}$.
(ii) *If* $6 \nmid N$, *then* $F_N(1,Y) = Y^{\alpha'}(Y-1)^{d_3-\alpha'}$.
(iii) *If* $5 \nmid N$, *then* $F_N(X,0) = c_1X^{\beta}(X-1)^{\gamma}$.
(iv) $F_N(X,1) = c_2X^{\delta}(X-1)^{d_5-\delta}$.
(v) $F_N(X,X) = c_3X^{\varepsilon}(X-1)^{d_3-\varepsilon}$.

Here c_1, c_2 *and* c_3 *are non-zero constants and*

$$\alpha = \sum_{N/3<t<2N/5} ((2N-5t)/D)\varphi(D),$$

$$\alpha' = \sum_{N/6<t\le N/5} (t/D)\varphi(D) + \sum_{N/5<t\le N/4} ((N-4t)/D)\varphi(D),$$

$$\beta = \sum_{N/3<t<2N/5} ((3t-N)/D)\varphi(D),$$

$$\gamma = \sum_{N/6<t\le N/5} ((6t-N)/D)\varphi(D) + \sum_{N/5<t<N/4} ((N-4t)/D)\varphi(D),$$

$$\delta = \sum_{N/4<t\le 2N/7} ((4t-N)/D)\varphi(D) + \sum_{2N/7<t<N/3} ((N-3t)/D)\varphi(D),$$

$$\varepsilon = \sum_{N/3<t\le 3N/8} ((3t-N)/D)\varphi(D) + \sum_{3N/8<t<2N/5} ((2N-5t)/D)\varphi(D).$$

Proof. The proof is the same as in the case of N prime so we omit it. ∎

Finally we give some examples.

EXAMPLE. (I) N prime:

$$F_{11}(X,Y) = Y^2(Y-1) - X(X-1).$$
$$F_{13}(X,Y) = Y(Y-1)^3 + X(X-1)Y + X^2(X-1).$$
$$F_{17}(X,Y) = Y^4(Y-1)^3 - 4X(X-1)Y^4 - X(X-1)(X-10)Y^3 \\ + 3(X^4 - X^3 - 3X^2 + 3X)Y^2 \\ - (X^5 - 5X^2 + 4X)Y + X(X-1)^2.$$

$$\begin{aligned}F_{19}(X,Y) = {} & Y^3(Y-1)^6 + 4X(X-1)Y^6 - 5X(X-1)(X-2)Y^5 \\ & - 3X(X-1)(X^2-5X-3)Y^4 \\ & + X(X-1)(4X^3+X^2-16X-3)Y^3 \\ & - X^2(X-1)(X^3+2X^2+3X-9)Y^2 \\ & + 3X^2(X-1)^2Y + X^2(X-1)^3.\end{aligned}$$

(II) N composite:

$$F_{14}(X,Y) = Y^4 - (X+1)Y^3 - (2X^2-3X)Y^2 + (X^3-X)Y + X(X-1)^2.$$

$$\begin{aligned}F_{15}(X,Y) = {} & Y^5 - 3Y^4 - 3(X-2)Y^3 + (6X-7)Y^2 \\ & + (X-1)(2X^2-X-4)Y - (X-1)^2(X^2+X+1).\end{aligned}$$

$$\begin{aligned}F_{16}(X,Y) = {} & Y^5 + (2X-4)Y^4 - (X^2+4X-6)Y^3 + (4X-4)Y^2 \\ & + (X^2-2X+1)Y + X(X-1)^2.\end{aligned}$$

$$\begin{aligned}F_{18}(X,Y) = {} & Y^5 - 3Y^4 - \left(X^2 - X - \tfrac{10}{3}\right)Y^3 + \left(\tfrac{1}{3}X^3 + X^2 - \tfrac{4}{3}X - \tfrac{5}{3}\right)Y^2 \\ & - \left(\tfrac{2}{3}X^3 - \tfrac{1}{3}X^2 - \tfrac{1}{3}X - \tfrac{1}{3}\right)Y + \tfrac{1}{3}X^3(X-1).\end{aligned}$$

$$\begin{aligned}F_{20}(X,Y) = {} & Y^7 - (3X+2)Y^6 + (X^2+8X+1)Y^5 - 10XY^4 \\ & - (5X^2-10X)Y^3 - (2X^3-10X^2+9X)Y^2 \\ & + (2X^4-2X^3-4X^2+4X)Y - X(X-1)^2(X^2+1).\end{aligned}$$

Comparing our result with Reichert's [9], our equations seem to correspond to "raw forms" of Reichert.

5. Generators $(J, W_3), (J, W_5)$**.** Let J be the modular invariant function. We shall show that the pairs (J, W_3) and (J, W_5) are generators of $A_1(N)$ over $\mathbb{C}$.

THEOREM 5. *Let $N = 11$ or be an integer ≥ 13. Then $A_1(N) = \mathbb{C}(J, W_3) = \mathbb{C}(J, W_5)$.*

Proof. Let $r = 3, 5$. We know that $A(N)$ is a Galois extension over $\mathbb{C}(J)$ with Galois group $\mathrm{SL}_2(\mathbb{Z})/\pm\Gamma(N)$ and $A_1(N)$ is the invariant field associated with the subgroup $\pm\Gamma_1(N)/\pm\Gamma(N)$. Therefore to prove $A_1(N) = \mathbb{C}(J, W_r)$, it is sufficient to show that for $A \in \mathrm{SL}_2(\mathbb{Z})$, $W_r(A(\tau)) = W_r(\tau)$ implies $A \in \Gamma_1(N)\{\pm 1\}$. Let $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ be such that $W_r(A(\tau)) = W_r(\tau)$.

First of all, we show that c is divisible by N. Assume that $c \not\equiv 0 \bmod N$. Without loss of generality, we can regard the matrix A as one of the matrices $B(u,t)$ given by (2) with $c \equiv t \bmod N$. Let C_r be the constant term of the q-extension of W_r. By Lemma 2,

$$C_r = \frac{(\zeta^r-1)^2(\zeta^3-1)(\zeta-1)}{(\zeta^{r+1}-1)(\zeta^{r-1}-1)(\zeta^2-1)^2} \neq 0. \tag{11}$$

Proposition 1 shows that the order of the q-extension of $W_r(A(\tau))$ is $\min(\{2c\},\{c\}) - \min(\{rc\},\{c\})$. Since $W_r(A(\tau)) = W_r(\tau)$, we see that

$$\min(\{2c\},\{c\}) = \min(\{rc\},\{c\})$$

and the coefficient L_r of the leading term of $W_r(A(\tau))$ is equal to C_r.

First consider the case $\{2c\} = \{c\}$. Then $3c \equiv 0 \bmod N$ and $3 \mid N$. Thus $\{c\} = \{2c\} = N/3$, $\mu(2c) = -\mu(c)$, $\{3c\} = 0$, $\{5c\} = N/3$, $\mu(5c) = -\mu(c)$. Therefore for $r = 3$ we have a contradiction. Let $r = 5$. Since, in Lemma 2, we know that the coefficient of the leading term of the function $(\phi_s - \phi_1)\,|_2\,[A]$ is $\zeta^{\mu(sc)sd} - \zeta^{\mu(c)d}$ in the case $\{c\} = \{sc\} \neq 0, N/2$ (line 19 in the proof of Lemma 2), we have

$$L_5 = \frac{\zeta^{\mu(2c)2d} - \zeta^{\mu(c)d}}{\zeta^{\mu(5c)5d} - \zeta^{\mu(c)d}} = \frac{1}{1 + \zeta^{-\mu(c)3d}}.$$

Since $L_5 = C_5$, we have $|1/C_5 - 1| = 1$. Replacing C_5 by the value given by (11) for $r = 5$, we get

$$\begin{aligned}
&|1/C_5 - 1|^2 \\
&= \frac{(\zeta^6+\zeta^5+\zeta^4+\zeta^3+\zeta^2+\zeta+1)(\zeta^{-6}+\zeta^{-5}+\zeta^{-4}+\zeta^{-3}+\zeta^{-2}+\zeta^{-1}+1)}{(\zeta^4+\zeta^3+\zeta^2+\zeta+1)^2(\zeta^{-4}+\zeta^{-3}+\zeta^{-2}+\zeta^{-1}+1)^2} \\
&= 1.
\end{aligned}$$

Since this equation is symmetric with respect to ζ and ζ^{-1}, after some elementary computation, we can obtain the following equation for $\xi = \zeta + \zeta^{-1}$:

$$\xi^8 + 4\xi^7 + \xi^6 - 10\xi^5 - 2\xi^4 + 14\xi^3 - 8\xi = 0.$$

However, since the irreducible equation of ξ over $\mathbb{Q}$ has degree $\varphi(N)/2$, we have a contradiction for N such that $\varphi(N)/2 > 7$. Further for N such that $\varphi(N)/2 \leq 7$, by direct computation, we can show ξ does not satisfy the above equation. Thus we also have a contradiction.

Next consider the case $\{2c\} > \{c\}$. Then $\{c\} = \min(\{rc\},\{c\})$, thus $\{rc\} \geq \{c\}$. If $\{rc\} > \{c\}$, then we have $C_r = 1$. From this, we have an equation for ζ, but we see immediately that ζ cannot satisfy it. Assume $\{rc\} = \{c\}$. If $\{c\} = N/2$, then $\{2c\} = 0 < \{c\}$. This contradicts the assumption. If $\{c\} < N/2$, then by Lemma 2,

$$L_r = \frac{-\zeta^{\mu(c)d}}{\zeta^{\mu(rc)rd} - \zeta^{\mu(c)d}}.$$

Thus $|1/C_r - 1| = 1$. Arguing as above, we get a contradiction.

Finally, consider the case $\{2c\} < \{c\}$. Then we must have $\{rc\} = \{2c\}$. If $\{2c\} = 0$, we have $\{c\} = 0$, because r is odd. If $\{2c\} = N/2$, then $\{2c\} \geq \{c\}$.

Therefore $\{rc\} = \{2c\} \neq 0$, $N/2$. By Lemma 2,

$$L_r = \frac{\zeta^{\mu(2c)2d}}{\zeta^{\mu(rc)rd}},$$

thus $|C_5| = 1$. However similarly we can show this equation is impossible. Hence at last we obtain $c \equiv 0 \bmod N$.

Now we show $d \equiv \pm 1 \bmod N$. By Proposition 1, W_3 (resp. W_5) has poles only at the cusps (u, t) such that $2N/5 \le t \le N/2$ (resp. $3N/7 \le t \le N/2$) and the order of the pole at (u, t), $t \neq N/2$, is $(5t - 2N)/D$ (resp. $(7t - 3N)/D$), while the order of the pole at $(u, N/2)$ is 1. Note that the order is determined only by t and is independent of u. Thus we denote by $\nu_r(W_r)$ the order of the pole of the function W_r at the cusp (u, t).

If N is odd (resp. $N \equiv 0 \bmod 4$), then we see at once that $\nu_r(t)$ has the maximal value only at the cusp $(1, t_0)$, where $t_0 = (N - 1)/2$ (resp. $N/2 - 1$). Since $c \equiv 0 \bmod N$, the matrix A transforms a cusp (u, t) to a cusp $(*, \{dt\})$. Therefore $dt_0 \equiv \pm t_0 \bmod N$. This shows that $d \equiv \pm 1 \bmod N$ and $A \in \{\pm 1\}\Gamma_1(N)$.

Let $N \equiv 2 \bmod 4$. Then $\nu_r(t)$ takes the maximal value at the cusp $(1, N/2-1)$ or $(1, N/2-2)$. We must compare $\nu_r(N/2-1)$ with $\nu_r(N/2-2)$. If $r = 3$ (resp. $r = 5$), then $\nu_r(N/2-2) > \nu_r(N/2-1)$ if and only if $N > 30$ (resp. $N > 42$). Thus $d(N/2 - 2) \equiv \pm(N/2 - 2) \bmod N$ if $N > 30$ (resp. $N > 42$), and $d(N/2 - 1) \equiv \pm(N/2 - 1) \bmod N$ if $N < 30$ (resp. $N < 42$). The former implies $d \equiv \pm 1 \bmod N$. The latter implies $d \equiv \pm 1 \bmod N/2$ but since d is odd, we know $d \equiv \pm 1 \bmod 2$, hence $d \equiv \pm 1 \bmod N$.

If $r = 3$, $N = 30$ or $r = 5$, $N = 42$, then $\nu_r(N/2 - 2) = \nu_r(N/2 - 1)$ and one of the following congruences holds true: $d(N/2-2) \equiv \pm(N/2-2) \bmod N$, $d(N/2 - 1) \equiv \pm(N/2 - 1) \bmod N$, $d(N/2 - 2) \equiv \pm(N/2 - 1) \bmod N$. The third congruence is impossible because $N, N/2 - 1$ are even and $d, N/2 - 2$ are odd. Hence also in this case $d \equiv \pm 1 \bmod N$. ■

Acknowledgements. The authors would like to express their hearty thanks to the referee for valuable suggestions and comments.

References

[1] J. W. S. Cassels, *Local Fields*, London Math. Soc. Stud. Texts 3, Cambridge Univ. Press, London, 1986.

[2] H. Darmon, *Notes on a polynomial of Emma Lehmer*, Math. Comp. 56 (1991), 795–800.

[3] N. Ishida, *Generators and equations for modular function fields of principal congruence subgroups*, Acta Arith. 85 (1998), 197–207.

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

[5] N. Ishida and N. Ishii, *The equation for the modular curve $X_1(N)$ derived from the equation for the modular curve $X(N)$*, Tokyo J. Math. 22 (1999), 167–175.
[6] D. Kubert and S. Lang, *Units in the modular function fields*, Math. Ann. 218 (1975), 175–189.
[7] O. Lecacheux, *Unité d'une famille de corps cycliques réels de degré* 6 *lié à la courbe modulaire* $X_1(13)$, J. Number Theory 31 (1989), 54–63.
[8] A. Ogg, *Rational points on certain elliptic modular curves*, in: Proc. Sympos. Pure Math. 24, Amer. Math. Soc., 1973, 221–231.
[9] M. A. Reichert, *Explicit determination of nontrivial torsion structures of elliptic curves over quadratic number fields*, Math. Comp. 46 (1986), 637–658.
[10] A. Robert, *Elliptic Curves*, Lecture Notes in Math. 326, Springer, 1973.
[11] L. C. Washington, *A family of cyclic quartic fields arising from modular curves*, Math. Comp. 196 (1991), 763–775.

Nobuhiko Ishida
Sanpo jyuutaku
2-4-9, Shinonome-higashi-machi
Sakai, Osaka 591-8041, Japan
E-mail: ishida@an.email.ne.jp

Noburo Ishii
Department of Mathematics and Information Sciences
College of Integrated Arts and Sciences
Osaka Prefecture University
1-1 Gakuen-cho
Sakai, Osaka 599-8531, Japan
E-mail: ishii@mi.cias.osakafu-u.ac.jp

Received on 10.4.2000
and in revised form on 25.4.2001 (3803)