ACTA ARITHMETICA
141.4 (2010)

# Function fields of certain arithmetic curves and application

by

Ja Kyung Koo and Dong Hwa Shin (Daejeon)

**1. Introduction.** It is well-known in the theory of modular forms and functions that the group $\mathrm{GL}_2^+(\mathbb{R})$ acts on the complex upper half-plane $\mathfrak{H}$ by linear fractional transformation. When we need to emphasize we think of an element $\gamma$ of $\mathrm{GL}_2^+(\mathbb{R})$ not only as a matrix but also as a transformation, we shall denote it by $\overline{\gamma}$. For a suitable discrete subgroup $\Gamma$ of $\mathrm{GL}_2^+(\mathbb{R})$ which is commensurable with $\mathrm{PSL}_2(\mathbb{Z})$ the orbit space $\overline{\Gamma}\backslash\mathfrak{H}$ can be given a Riemann surface structure, which can be compactified by adding the cusps to $\overline{\Gamma}\backslash\mathfrak{H}^*$ where $\mathfrak{H}^* = \mathfrak{H} \cup \mathbb{P}^1(\mathbb{Q})$ ([3] or [12]). We call this compact Riemann surface an *arithmetic curve*. A meromorphic function $f$ on $\mathfrak{H}$ invariant under the action of all $\gamma \in \Gamma$ is said to be *weakly modular* for $\Gamma$ (or $\overline{\Gamma}$). If a weakly modular function $f$ for $\Gamma$ is also meromorphic at all the cusps in the sense of [12], we say that $f$ is *modular* for $\Gamma$ (or $\overline{\Gamma}$).

For a positive integer $N$ we consider the following congruence subgroups:

$$\begin{aligned}
\Gamma_0(N) &= \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) : \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \equiv \left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right) \pmod N \right\},\\
\Gamma_1(N) &= \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) : \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \equiv \left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right) \pmod N \right\},\\
\Gamma(N) &= \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) : \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \equiv \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \pmod N \right\},
\end{aligned}$$

and let $\Phi_N$ be the Fricke involution $\left(\begin{smallmatrix} 0 & -1 \\ N & 0 \end{smallmatrix}\right)$. We are mainly concerned with the field of meromorphic functions on the compact Riemann surface $\langle\overline{\Gamma}, \overline{\Phi}_N\rangle\backslash\mathfrak{H}^*$ where $\Gamma$ is one of the above congruence subgroups. From now on, for convenience we let

$$\begin{aligned}
&\overline{\Gamma}_0^\dagger(N) = \langle\overline{\Gamma}_0(N), \overline{\Phi}_N\rangle, \quad \overline{\Gamma}_1^\dagger(N) = \langle\overline{\Gamma}_1(N), \overline{\Phi}_N\rangle, \quad \overline{\Gamma}^\dagger(N) = \langle\overline{\Gamma}(N), \overline{\Phi}_N\rangle,\\
&X_0(N) = \overline{\Gamma}_0(N)\backslash\mathfrak{H}^*, \qquad X_1(N) = \overline{\Gamma}_1(N)\backslash\mathfrak{H}^*, \qquad X(N) = \overline{\Gamma}(N)\backslash\mathfrak{H}^*,\\
&X_0^\dagger(N) = \overline{\Gamma}_0^\dagger(N)\backslash\mathfrak{H}^*, \qquad X_1^\dagger(N) = \overline{\Gamma}_1^\dagger(N)\backslash\mathfrak{H}^*, \qquad X^\dagger(N) = \overline{\Gamma}^\dagger(N)\backslash\mathfrak{H}^*,
\end{aligned}$$

2010 *Mathematics Subject Classification*: 11F03, 11G16, 11G30, 11R37, 14H55.
*Key words and phrases*: class fields, modular curves, modular units, Riemann surfaces, Siegel functions.

DOI: 10.4064/aa141-4-2  

and let $\mathcal{K}(R)$ be the field of meromorphic functions on any compact Riemann surface $R$ listed above. The function fields of our interest are classically described in terms of the modular invariant $j$ and the Fricke functions ([3] or [12]), which requires good understanding of the theory of elliptic curves. In general, the function field of a compact Riemann surface (viewed as an algebraic curve) can be generated by at most two functions ([10]). For instance, Ishida–Ishii constructed in [5] these two generators of $\mathcal{K}(X_1(N))$ by using certain products of Klein forms.

As preliminaries we review some arithmetic properties of Siegel functions developed by Kubert–Lang ([8]) and Koo–Shin ([7]). We then find generators of function fields in terms of $j$ and Siegel functions (Theorems 3.2 and 3.5) unlike in Ishida–Ishii's approach.

On the other hand, Kim–Koo ([6]) gave a genus formula for the arithmetic curve $X_1^\dagger(N)$. Using that formula they showed that $X_1^\dagger(N)$ has genus zero exactly when $1 \le N \le 12$ and $N = 14, 15$. Choi–Koo constructed in [1] primitive generators of genus zero curves $X_1^\dagger(N)$ by using elliptic functions and theta functions. However, their method seems to be too artificial and inconvenient for other similar situations. Therefore we revisit this subject and present a process of finding primitive generators in a more standard and systematic way (Theorem 4.2 and Table 1) by means of Siegel functions only. To this end we essentially follow the idea of Koo–Shin ([7]) who dealt with various modifications of Siegel functions.

Next, we know that a classical generator of the ring class field of the order of conductor $N$ ($\ge 2$) over an imaginary quadratic field $K$ is given by a singular value of $j$. Moreover, we recently showed that any power of a certain linear form of $j$ also becomes a generator of the ring class field over $K$ (Lemma 5.1). As an application of previous sections and this fact we shall further find a primitive generator of the ray class field modulo $N$ over $K$ ($\neq \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3})$) in terms of the singular values of $j$ and Siegel functions (Theorem 5.5) which is different from Ramachandra's ray class invariant ([11]) constructed from very complicated products of high powers of singular values of Klein forms and singular values of the discriminant $\Delta$. We also describe Galois groups between the two class fields mentioned above (Proposition 5.3) by adopting the idea of Gee ([4]).

**2. Preliminaries.** In this section we introduce Siegel functions and briefly review their transformation formulas and criterions for determining modularity which are developed in [8] and [7].

Let $\mathbf{B}_2(X) = X^2 - X + 1/6$ be the second Bernoulli polynomial. For any $r = (r_1, r_2) \in \mathbb{Q}^2 \setminus \mathbb{Z}^2$ we define the *Siegel function* $g_r(\tau)$ for $\tau \in \mathfrak{H}$ by the following $q_\tau$-product formula:

$$g_r(\tau) = -q_\tau^{\frac{1}{2}\mathbf{B}_2(r_1)} e^{\pi i r_2(r_1-1)}(1-q_z)\prod_{n=1}^{\infty}(1-q_\tau^n q_z)(1-q_\tau^n q_z^{-1}) \tag{2.1}$$

where $q_\tau = e^{2\pi i\tau}$ and $q_z = e^{2\pi iz}$ with $z = r_1\tau + r_2$. From the definition we can deduce the simple order formula

$$\operatorname{ord}_{q_\tau} g_r = \frac{1}{2}\mathbf{B}_2(\langle r_1\rangle) \tag{2.2}$$

where $\langle r_1\rangle$ is the fractional part of $r_1$ so that $0 \le \langle r_1\rangle < 1$. Here we remark that this function is holomorphic and never vanishes on $\mathfrak{H}$. In the following proposition we present basic transformation formulas for Siegel functions.

PROPOSITION 2.1 (see [7, Proposition 2.4]). *Let $r = (r_1, r_2) \in \mathbb{Q}^2 \setminus \mathbb{Z}^2$. Then:*

(i) $g_{-r} = -g_r$.

(ii) *For $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ and $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ we have*

$$g_r \circ S = \zeta_{12}^9 g_{rS} = \zeta_{12}^9 g_{(r_2,-r_1)}, \qquad g_r \circ T = \zeta_{12} g_{rT} = \zeta_{12} g_{(r_1,r_1+r_2)},$$

*where $\zeta_{12} = e^{2\pi i/12}$. Hence for $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, $g_r \circ \gamma = \varepsilon g_{r\gamma}$ with $\varepsilon$ a 12th root of unity.*

(iii) *For $s = (s_1, s_2) \in \mathbb{Z}^2$ we have*

$$g_{r+s} = \varepsilon(r,s) g_r \quad \text{where} \quad \varepsilon(r,s) = (-1)^{s_1 s_2 + s_1 + s_2} e^{-\pi i(s_1 r_2 - s_2 r_1)}.$$

REMARK 2.2. We see from Proposition 2.1(ii) and the order formula (2.2) that any product of Siegel functions is meromorphic at the cusps. Hence it is not necessary to check the meromorphy of Siegel functions at the cusps in what follows.

For a positive integer $N$ we denote by $\mathcal{F}_N$ the field of all modular functions $h$ for the principal congruence subgroup $\Gamma(N)$ for which the Fourier coefficients of $h \circ \gamma$ with respect to $q_\tau^{1/N}$ for any $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ belong to $\mathbb{Q}(\zeta_N)$ with $\zeta_N = e^{2\pi i/N}$. Then $\mathcal{F}_N$ is a Galois extension of $\mathcal{F}_1$ $(= \mathbb{Q}(j(\tau)))$ with $\mathrm{Gal}(\mathcal{F}_N/\mathcal{F}_1) \cong \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\pm\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ ([9] or [12]).

Kubert–Lang provided a condition for a product of Siegel functions to belong to $\mathcal{F}_N$. For $N \ge 2$ we say that a family of integers $\{m(r)\}_{r=(r_1,r_2)\in\frac{1}{N}\mathbb{Z}^2\setminus\mathbb{Z}^2}$ with $m(r) = 0$ except finitely many $r$ satisfies the *quadratic relation* modulo $N$ if

$$\sum_r m(r)(Nr_1)^2 \equiv \sum_r m(r)(Nr_2)^2 \equiv 0 \pmod{\gcd(2,N)\cdot N},$$
$$\sum_r m(r)(Nr_1)(Nr_2) \equiv 0 \pmod{N}.$$

PROPOSITION 2.3 (see [8, Chapter 3, Theorems 5.2 and 5.3]). *Let $N \geq 2$. A product of Siegel functions*

$$\prod_{r \in \frac{1}{N}\mathbb{Z}^2 \setminus \mathbb{Z}^2} g_r^{m(r)}(\tau)$$

*belongs to $\mathcal{F}_N$ if $\{m(r)\}_r$ satisfies the quadratic relation modulo $N$ and $\gcd(12, N) \cdot \sum_r m(r) \equiv 0 \pmod{12}$. In particular, $g_r^{12N}$ lies in $\mathcal{F}_N$ for $r \in \frac{1}{N}\mathbb{Z}^2 \setminus \mathbb{Z}^2$.*

We further examine a condition for a product of Siegel functions to be modular for $\Gamma_1(N)$. Note that for $t \in \mathbb{Z} \setminus N\mathbb{Z}$ we have the relation

$$\prod_{n=0}^{N-1} g_{(t/N,n/N)}(\tau) = e^{\pi i \frac{N-1}{2}(\frac{t}{N}+1)} g_{(t/N,0)}(N\tau) \tag{2.3}$$

from the identity $1 - X^N = (1 - X)(1 - \zeta_N X) \cdots (1 - \zeta_N^{N-1} X)$.

PROPOSITION 2.4 (see [7, Theorem 6.2]). *Let $N \geq 2$. A product*

$$g = \prod_{t=1}^{N-1} g_{(t/N,0)}^{m(t)}(N\tau)$$

*is modular for $\Gamma_1(N)$ if the family of integers $\{m(t)\}_{t=1}^{N-1}$ satisfies*

$$\sum_t m(t) \equiv 0 \pmod{12}, \qquad \sum_t m(t)t^2 \equiv 0 \pmod{\gcd(2, N) \cdot N}. \tag{2.4}$$

*In particular, $g_{(t/N,0)}^{12N}(N\tau)$ is modular for $\Gamma_1(N)$ for $t \in \mathbb{Z} \setminus N\mathbb{Z}$. Furthermore, for $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ we get*

$$\mathrm{ord}_{q_\tau}(g \circ \gamma) = \frac{\gcd(c, N)^2}{2N} \sum_{t=1}^{N-1} m(t) \mathbf{B}_2\left(\left\langle \frac{at}{\gcd(c, N)} \right\rangle\right). \tag{2.5}$$

Now we investigate the action of $\mathrm{Gal}(\mathcal{F}_N/\mathcal{F}_1)$ on certain Siegel functions for later use.

PROPOSITION 2.5. *Let $N \geq 2$, $s \in \mathbb{Z} \setminus N\mathbb{Z}$ and $t \in \mathbb{Z}$ with $\gcd(t, N) = 1$. Then the action of the element $\left(\begin{smallmatrix} t & 0 \\ 0 & t \end{smallmatrix}\right)$ of $\mathrm{Gal}(\mathcal{F}_N/\mathcal{F}_1)$ is given by*

$$g_{(0,s/N)}^{12N}(\tau)^{\left(\begin{smallmatrix} t & 0 \\ 0 & t \end{smallmatrix}\right)} = g_{(0,\langle st/N \rangle)}^{12N}(\tau), \qquad g_{(s/N,0)}^{12N}(N\tau)^{\left(\begin{smallmatrix} t & 0 \\ 0 & t \end{smallmatrix}\right)} = g_{(\langle st/N \rangle,0)}^{12N}(N\tau),$$

*where $\langle X \rangle$ is the fractional part of a real number $X$ with $0 \leq \langle X \rangle < 1$.*

*Proof.* See [8, p. 36, Proposition 2.1(iii)] and the relation (2.3). ∎

**3. Function fields of $X_1^\dagger(N)$.** In this section we first describe the function field $\mathcal{K}(X_1(N))$ in terms of $j$ and a product of Siegel functions. We can then naturally extend it to $\mathcal{K}(X_1^\dagger(N))$. Here we do not intend to reduce the

number of generators to be 2 as Ishida–Ishii did in [5]. From now on, unless otherwise specified, $N$ is always a positive integer $\geq 2$.

LEMMA 3.1. *For $N \geq 6$ let $g = g^{12N}_{(0,1/N)}(\tau) g^{12N}_{(1/N,0)}(N\tau)$. Then:*

(i) *$g$ is modular for $\Gamma_1(N)$.*

(ii) *If $g$ is invariant under the action of $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$, then $\gamma \equiv \pm\left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right) \pmod N$.*

*Proof.* (i) By Proposition 2.3 the function $g^{12N}_{(0,1/N)}(\tau)$ is modular for $\Gamma(N)$. It is also invariant under the action of $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ by Proposition 2.1(ii). Since $\Gamma_1(N) = \langle \Gamma(N), T \rangle$, $g^{12N}_{(0,1/N)}(\tau)$ is modular for $\Gamma_1(N)$. Furthermore, $g^{12N}_{(1/N,0)}(N\tau)$ is also modular for $\Gamma_1(N)$ by Proposition 2.4, which implies that $g = g^{12N}_{(0,1/N)}(\tau) g^{12N}_{(1/N,0)}(N\tau)$ is modular for $\Gamma_1(N)$.

(ii) Now we assume that $g \circ \gamma = g$ for some $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$. Then obviously $\mathrm{ord}_{q_\tau}(g \circ \gamma) = \mathrm{ord}_{q_\tau} g$. By (2.2) and (2.5),

$$\mathrm{ord}_{q_\tau}(g \circ \gamma) = 6N\mathbf{B}_2\left(\left\langle \frac{c}{N} \right\rangle\right) + 6\gcd(c,N)^2 \mathbf{B}_2\left(\left\langle \frac{a}{\gcd(c,N)} \right\rangle\right), \tag{3.1}$$

$$\mathrm{ord}_{q_\tau} g = 6N\mathbf{B}_2(0) + 6N^2\mathbf{B}_2\left(\frac{1}{N}\right) = N^2 - 5N + 6. \tag{3.2}$$

Suppose $\gcd(c,N) \neq N$. The shape of the graph of $Y = \mathbf{B}_2(X)$ over the interval $0 \leq X \leq 1$ indicates that the maximum value of $\mathbf{B}_2(X)$ is $1/6$ at $X = 0, 1$. So

$$\mathrm{ord}_{q_\tau}(g \circ \gamma) \leq 6N\mathbf{B}_2(1/N) + 6(N/2)^2\mathbf{B}_2(0) = 6/N - 6 + N + N^2/4.$$

On the other hand, for $N \geq 6$ we can easily check that

$$6/N - 6 + N + N^2/4 < N^2 - 5N + 6,$$

which contradicts $\mathrm{ord}_{q_\tau}(g \circ \gamma) = \mathrm{ord}_{q_\tau}(g)$. Thus $\gcd(c,N) = N$, which yields $\mathbf{B}_2(\langle a/N \rangle) = \mathbf{B}_2(1/N)$ from (3.1), (3.2) and the fact that $\mathrm{ord}_{q_\tau}(g \circ \gamma) = \mathrm{ord}_{q_\tau}(g)$. Therefore $a \equiv \pm 1 \pmod N$ from the shape of the graph $Y = \mathbf{B}_2(X)$. Now as $\det(\alpha) = 1$, we have $a \equiv d \equiv \pm 1 \pmod N$, which proves $\gamma \equiv \pm\left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right) \pmod N$ as desired. ∎

THEOREM 3.2. *Let $N \geq 6$. Then*

$$\mathcal{K}(X_0(N)) = \mathbb{C}(j(\tau), j(N\tau)),$$
$$\mathcal{K}(X_1(N)) = \mathbb{C}(j(\tau), g^{12N}_{(0,1/N)}(\tau) g^{12N}_{(1/N,0)}(N\tau)),$$
$$\mathcal{K}(X(N)) = \mathbb{C}(j(\tau), g^{12N}_{(0,1/N)}(\tau) g^{12N}_{(1/N,0)}(N\tau), g^{12N}_{(1/N,0)}(\tau)).$$

*Proof.* For $\mathcal{K}(X_0(N))$ we refer to [3]. Here we concentrate on $\mathcal{K}(X_1(N))$ and $\mathcal{K}(X(N))$. We see from [3] that

$$\mathrm{Gal}(\mathcal{K}(X(N))/\mathcal{K}(X_1(N))) \cong \left\{ \pm\left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\pm\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) : b \in \mathbb{Z}/N\mathbb{Z} \right\}$$

as a subgroup of

$$\mathrm{Gal}(\mathcal{K}(X(N))/\mathcal{K}(X(1))) \cong \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\pm\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right),$$

whose action is given by composition. Assume that $g^{12N}_{(0,1/N)}(\tau)g^{12N}_{(1/N,0)}(N\tau)$, which belongs to $\mathcal{K}(X_1(N))$ by Lemma 3.1, is fixed by the action of some $\gamma \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\pm\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$. Then by Lemma 3.1 we get $\gamma \equiv \pm\left(\begin{smallmatrix}1&*\\0&1\end{smallmatrix}\right) \pmod N$. Since $\mathcal{K}(X(1)) = \mathbb{C}(j(\tau))$ ([9] or [12]), we conclude by Galois theory that

$$\begin{aligned}\mathcal{K}(X_1(N)) &= \mathcal{K}(X(1))(g^{12N}_{(0,1/N)}(\tau)g^{12N}_{(1/N,0)}(N\tau))\\ &= \mathbb{C}(j(\tau), g^{12N}_{(0,1/N)}(\tau)g^{12N}_{(1/N,0)}(N\tau)).\end{aligned}$$

Next, we assume that $g^{12N}_{(1/N,0)}(\tau)$ is fixed by the action of $\pm\left(\begin{smallmatrix}1&b\\0&1\end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\pm\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$. Then $g^{12N}_{(1/N,0)}(\tau) \circ \left(\begin{smallmatrix}1&b\\0&1\end{smallmatrix}\right) = g^{12N}_{(1/N,b/N)}(\tau) = g^{12N}_{(1/N,0)}(\tau)$ by Proposition 2.1(ii). It follows from the action of the element $\left(\begin{smallmatrix}0&-1\\1&0\end{smallmatrix}\right)$ on both sides of $g^{12N}_{(1/N,b/N)}(\tau) = g^{12N}_{(1/N,0)}(\tau)$ that $g^{12N}_{(b/N,-1/N)}(\tau) = g^{12N}_{(0,-1/N)}(\tau)$. Now we compare the orders via the formula (2.2) to obtain $6N\mathbf{B}_2(\langle b/N\rangle) = 6N\mathbf{B}_2(0)$; hence $b \equiv 0 \pmod N$ by the shape of the graph $Y = \mathbf{B}_2(X)$. Therefore

$$\begin{aligned}\mathcal{K}(X(N)) &= \mathcal{K}(X_1(N))(g^{12N}_{(1/N,0)}(\tau))\\ &= \mathbb{C}(j(\tau), g^{12N}_{(0,1/N)}(\tau)g^{12N}_{(1/N,0)}(N\tau), g^{12N}_{(1/N,0)}(\tau)).\ \blacksquare\end{aligned}$$

We will extend the above results to the function fields $\mathcal{K}(X_0^\dagger(N))$, $\mathcal{K}(X_1^\dagger(N))$ and $\mathcal{K}(X^\dagger(N))$. Since $\Phi_N\left(\begin{smallmatrix}1&0\\-N&1\end{smallmatrix}\right)\Phi_N = -N\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$ and $\Gamma_1(N) = \left\langle \Gamma(N), \left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)\right\rangle$, we have $\overline{\Gamma}^\dagger(N) = \overline{\Gamma}_1^\dagger(N)$, and so $X^\dagger(N) = X_1^\dagger(N)$. Thus we are reduced to considering the first two cases.

LEMMA 3.3. *Let $\Gamma$ be $\Gamma_0(N)$ or $\Gamma_1(N)$. If a function $f$ on $\mathfrak{H}$ is weakly modular for $\Gamma$, then both $f + f\circ\Phi_N$ and $f\cdot f\circ\Phi_N$ are weakly modular for $\langle\overline{\Gamma}, \overline{\Phi}_N\rangle$.*

*Proof.* For any $\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right) \in \Gamma$ we deduce

$$\Phi_N\begin{pmatrix}a&b\\c&d\end{pmatrix} = \begin{pmatrix}d&-c/N\\-Nb&a\end{pmatrix}\Phi_N, \tag{3.3}$$

which implies $\Phi_N\Gamma = \Gamma\Phi_N$. Thus $f\circ\Phi_N$ is weakly modular for $\Gamma$.

On the other hand, since

$$\Phi_N \circ \Phi_N = -N\begin{pmatrix}1&0\\0&1\end{pmatrix} \tag{3.4}$$

which is the identity as a transformation, it follows that $(f + f\circ\Phi_N)\circ\Phi_N = f\circ\Phi_N + f$ and $(f\cdot f\circ\Phi_N)\circ\Phi_N = f\circ\Phi_N\cdot f$. This proves the lemma. ∎

LEMMA 3.4. *For $t \in \mathbb{Z} \setminus N\mathbb{Z}$ we have*

$$g_{(t/N,0)}(N\tau) \circ \Phi_N = -\zeta_{12}^9 g_{(0,t/N)}(\tau).$$

*Proof.* Observe by Proposition 2.1 that

$$\begin{aligned} g_{(t/N,0)}(N\tau) \circ \Phi_N &= g_{(t/N,0)} \circ \left(\begin{smallmatrix} N & 0 \\ 0 & 1 \end{smallmatrix}\right) \circ \left(\begin{smallmatrix} 0 & -1 \\ N & 0 \end{smallmatrix}\right)(\tau) = g_{(t/N,0)} \circ \left(\begin{smallmatrix} 0 & -N \\ N & 0 \end{smallmatrix}\right)(\tau) \\ &= g_{(t/N,0)} \circ \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)(\tau) = \zeta_{12}^9 g_{(0,-t/N)}(\tau) = -\zeta_{12}^9 g_{(0,t/N)}(\tau). \end{aligned}$$

∎

THEOREM 3.5. *For $N \geq 6$ we have*

$$\mathcal{K}(X_0^\dagger(N)) = \mathbb{C}(j(\tau) + j(N\tau), j(\tau)j(N\tau)),$$
$$\mathcal{K}(X_1^\dagger(N)) = \mathbb{C}(j(\tau) + j(N\tau), j(\tau)j(N\tau), g_{(0,1/N)}^{12N}(\tau) g_{(1/N,0)}^{12N}(N\tau)).$$

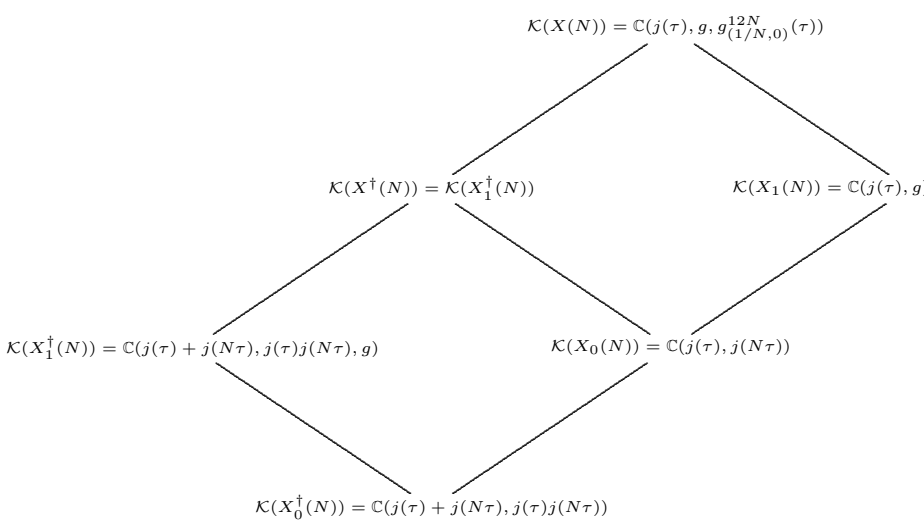
*Proof.* By Proposition 2.4 the function $g = g_{(1/N,0)}^{12N}(N\tau)$ is modular for $\Gamma_1(N)$. Moreover, by Lemma 3.4 we have $g \circ \Phi_N = g_{(0,1/N)}^{12N}(\tau)$. Hence the function $g_{(0,1/N)}^{12N}(\tau) g_{(1/N,0)}^{12N}(N\tau) = (g \circ \Phi_N) \cdot g$ lies in $\mathcal{K}(X_1^\dagger(N))$ by Lemma 3.3.

Let $\Gamma$ be $\Gamma_0(N)$ or $\Gamma_1(N)$. Note that $j(\tau)$ is not invariant under the action of $\Phi_N$ because $j(\tau) \circ \Phi_N = j \circ \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) \circ \left(\begin{smallmatrix} N & 0 \\ 0 & 1 \end{smallmatrix}\right)(\tau) = j(N\tau)$, and observe that $j(\tau)$ is a root of the quadratic equation

$$X^2 - (j(\tau) + j(N\tau))X + j(\tau)j(N\tau) = 0.$$

Now since $[\langle \overline{\Gamma}, \overline{\Phi}_N \rangle : \overline{\Gamma}] = 2$ by (3.3) and (3.4), we deduce the assertions from Theorem 3.2. ∎

We summarize all the results in the following diagram of a tower of function fields, with $g = g_{(0,1/N)}^{12N}(\tau) g_{(1/N,0)}^{12N}(N\tau)$:



**4. Primitive generators of $\mathcal{K}(X_1^\dagger(N))$ of genus zero.** Kim–Koo ([6]) showed that the curves $X_1^\dagger(N)$ have genus zero for $1 \le N \le 12$ and $N = 14, 15$, and for such curves Choi–Koo ([1]) found primitive generators of the function fields by using elliptic functions and theta functions. However, their method seems to be artificial and inconvenient for other similar situations. Therefore we propose a more systematic and standard way to find primitive generators in terms of Siegel functions only. First we develop an analogue of Proposition 2.4 motivated by Lemma 3.3.

PROPOSITION 4.1. *Let $N \ge 2$. Assume that a family of integers $\{m(t)\}_{t=1}^{N}$ satisfies the condition* (2.4). *Then the product*

$$g^\dagger = \prod_{t=1}^{N-1} (g_{(0,t/N)}(\tau) g_{(t/N,0)}(N\tau))^{m(t)}$$

*is an element of $\mathcal{K}(X_1^\dagger(N))$. Furthermore, for $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ we have*

$$\begin{aligned} (4.1)\quad & \mathrm{ord}_{q_\tau}(g^\dagger \circ \gamma) \\ &= \frac{1}{2} \sum_{t=1}^{N-1} m(t) \left\{ \mathbf{B}_2\left( \left\langle \frac{ct}{N} \right\rangle \right) + \frac{\gcd(c,N)^2}{N} \mathbf{B}_2\left( \left\langle \frac{at}{\gcd(c,N)} \right\rangle \right) \right\}. \end{aligned}$$

*Proof.* Let

$$g = \prod_{t=1}^{N-1} g_{(t/N,0)}^{m(t)}(N\tau) \quad \text{and} \quad g' = \prod_{t=1}^{N-1} g_{(0,t/N)}^{m(t)}(\tau).$$

Then we see from Proposition 2.4 that $g$ is modular for $\Gamma_1(N)$, and we further establish

$$g \circ \Phi_N = \prod_{t=1}^{N-1} (-\zeta_{12}^9 g_{(0,t/N)}(\tau))^{m(t)} = (-\zeta_{12}^9)^{\sum_t m(t)} \prod_{t=1}^{N-1} g_{(0,t/N)}^{m(t)}(\tau) = g'$$

by Lemma 3.4 and the condition $\sum_t m(t) \equiv 0 \pmod{12}$. Hence $g^\dagger = g' \cdot g = (g \circ \Phi_N) \cdot g$, which implies that $g^\dagger$ lies in $\mathcal{K}(X_1^\dagger(N))$ by Lemma 3.3.

Finally, for $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ we deduce the order formula

$$\begin{aligned} &\mathrm{ord}_{q_\tau}(g^\dagger \circ \gamma) = \mathrm{ord}_{q_\tau}(g' \circ \gamma) + \mathrm{ord}_{q_\tau}(g \circ \gamma) \\ &= \sum_{t=1}^{N} m(t) \frac{1}{2} \mathbf{B}_2\left( \left\langle \frac{ct}{N} \right\rangle \right) + \mathrm{ord}_{q_\tau}(g \circ \gamma) \quad \text{by Proposition 2.1(ii) and (2.2)} \\ &= \frac{1}{2} \sum_{t=1}^{N-1} m(t) \left\{ \mathbf{B}_2\left( \left\langle \frac{ct}{N} \right\rangle \right) + \frac{\gcd(c,N)^2}{N} \mathbf{B}_2\left( \left\langle \frac{at}{\gcd(c,N)} \right\rangle \right) \right\} \quad \text{by (2.5).} \end{aligned}$$

∎

The following theorem gives us a criterion for determining whether a given product of Siegel functions is a primitive generator or not. This is similar to those for the modular curves $X_1(N)$ shown in [7] or [13].

THEOREM 4.2. *Suppose that $X_1^\dagger(N)$ has genus zero and a product*

$$g^\dagger = \prod_{t=1}^{N-1} (g_{(0,t/N)}(\tau) g_{(t/N,0)}(N\tau))^{m(t)}$$

*lies in $\mathcal{K}(X_1^\dagger(N))$. For each cusp $s = a/c \in \mathbb{Q}$ with $\gcd(a,c) = 1$ which is inequivalent to $\infty$, if*

$$\frac{1}{2}\sum_{t=1}^{N-1} m(t)\left(\frac{1}{6} + N\mathbf{B}_2\left(\frac{t}{N}\right)\right) = -1, \tag{4.2}$$

$$\frac{1}{2}\sum_{t=1}^{N-1} m(t)\left\{\mathbf{B}_2\left(\left\langle\frac{ct}{N}\right\rangle\right) + \frac{\gcd(c,N)^2}{N}\mathbf{B}_2\left(\left\langle\frac{at}{\gcd(c,N)}\right\rangle\right)\right\} \geq 0, \tag{4.3}$$

*then $g^\dagger$ is a generator of $\mathcal{K}(X_1^\dagger(N))$.*

*Proof.* The width of $\infty$ on $X_1^\dagger(N)$ is 1 ([1]). From the order formula (4.1) in Proposition 4.1 and the hypothesis in the theorem it follows that $g^\dagger$ has a simple pole at $\infty$ and is holomorphic elsewhere. Therefore $X_1^\dagger(N)$ is isomorphic to the projective line $\mathbb{P}^1(\mathbb{C})$ through the map $\tau \mapsto [1 : g^\dagger(\tau)]$, and hence $\mathcal{K}(X_1^\dagger(N)) = \mathbb{C}(g^\dagger)$. ∎

**Table 1.** Primitive generators of $\mathcal{K}(X_1^\dagger(N))$

| $N$ | Inequivalent cusps of $X_1^\dagger(N)$ | Primitive generators of $\mathcal{K}(X_1^\dagger(N))$ |
|---|---|---|
| 2 | $\infty$ | · |
| 3 | $\infty$ | · |
| 4 | $\infty,\ \frac{1}{2}$ | $(\frac{1}{4})^{-8}(\frac{2}{4})^8$ |
| 5 | $\infty,\ \frac{1}{2}$ | $(\frac{1}{5})^{-5}(\frac{2}{5})^5$ |
| 6 | $\infty,\ \frac{1}{2}$ | $(\frac{1}{6})^{-3}(\frac{3}{6})^3$ |
| 7 | $\infty,\ \frac{1}{2},\ \frac{1}{3}$ | $(\frac{1}{7})^{-3}(\frac{2}{7})^2(\frac{3}{7})^1$ |
| 8 | $\infty,\ \frac{1}{2},\ \frac{1}{3}$ | $(\frac{1}{8})^{-2}(\frac{3}{8})^2$ |
| 9 | $\infty,\ \frac{1}{2},\ \frac{1}{3},\ \frac{1}{4}$ | $(\frac{1}{9})^{-2}(\frac{2}{9})^1(\frac{4}{9})^1$ |
| 10 | $\infty,\ \frac{1}{2},\ \frac{1}{3},\ \frac{1}{4}$ | $(\frac{1}{10})^{-1}(\frac{2}{10})^{-1}(\frac{3}{10})^1(\frac{4}{10})^1$ |
| 11 | $\infty,\ \frac{1}{2},\ \frac{1}{3},\ \frac{1}{4},\ \frac{1}{5}$ | $(\frac{1}{11})^{-3}(\frac{2}{11})^{-3}(\frac{3}{11})^{-3}(\frac{4}{11})^{-2}(\frac{5}{11})^{-1}$ |
| 12 | $\infty,\ \frac{1}{2},\ \frac{1}{3},\ \frac{1}{4},\ \frac{1}{5}$ | $(\frac{1}{12})^{-1}(\frac{5}{12})^1$ |
| 14 | $\infty,\ \frac{1}{2},\ \frac{1}{3},\ \frac{1}{4},\ \frac{1}{5},\frac{1}{6}$ | $(\frac{1}{14})^1(\frac{2}{14})^{-2}(\frac{4}{14})^{-2}(\frac{5}{14})^1(\frac{7}{14})^2$ |
| 15 | $\infty,\ \frac{1}{2},\ \frac{1}{3},\ \frac{1}{4},\ \frac{1}{5},\frac{1}{6},\ \frac{1}{7},\ \frac{1}{9}$ | $(\frac{1}{15})^{-1}(\frac{3}{15})^1(\frac{5}{15})^{-2}(\frac{6}{15})^2$ |

From [7, Theorem 6.4] we can readily determine the inequivalent cusps of $X_1(N)$, from which we get the inequivalent cusps of $X_1^\dagger(N)$ (Table 1). Furthermore, [1, Lemmas 3.2 and 3.3] enable us to estimate the widths of the cusps. However, these values are not necessary to apply Theorem 4.2. So we only provide the table for all the inequivalent cusps of $X_1^\dagger(N)$ without

finding their widths for $2 \le N \le 12$ and $N = 14, 15$. Then we can find families of integers $\{m(t)\}_{t=1}^{N-1}$ satisfying (2.4), (4.2) and (4.3) to accomplish our goal. In the table we use the notation

$$\prod_{t=1}^{N-1} \left(\frac{t}{N}\right)^{m(t)} = \prod_{t=1}^{N-1} (g_{(0,t/N)}(\tau) g_{(t/N,0)}(N\tau))^{m(t)}.$$

Observe that for $N = 2, 3$ the curve $X_1^\dagger(N)$ has only one cusp. Since our Siegel functions are supported on the cusps, it is not possible to find primitive generators of $\mathcal{K}(X_1^\dagger(N))$ in these two cases.

**5. Application to class fields.** As an application we shall construct a primitive generator of the ray class field modulo $N$ ($\ge 2$) over any imaginary quadratic field other than $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-3})$. To this end we shall utilize the singular values of $j$ and Siegel functions which are modular for $\Gamma_1^\dagger(N)$.

Let $K$ ($\ne \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3})$) be any imaginary quadratic field with discriminant $d_K$ ($\le -7$). Define

$$\theta = \begin{cases} \sqrt{d_K}/2 & \text{if } d_K \equiv 0 \pmod 4, \\ (-1+\sqrt{d_K})/2 & \text{if } d_K \equiv 1 \pmod 4, \end{cases}$$

which is a generator of the ring of integers $\mathcal{O}_K$ of $K$ and let $\min(\theta, \mathbb{Q}) = X^2 + B_\theta X + C_\theta \in \mathbb{Z}[X]$. We denote by $H$ and $K_{(N)}$ the Hilbert class field and the ray class field modulo $N$ ($\ge 2$) of $K$, respectively. It is then well-known that

$$K_{(N)} = K(h(\theta) : h \in \mathcal{F}_N \text{ is defined and finite at } \theta) \tag{5.1}$$

by the main theorem of complex multiplication ([9] or [12]). Furthermore, by Shimura's reciprocity law we have an isomorphism

$$\begin{aligned} W_{N,\theta}/\pm\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right) &\xrightarrow{\sim} \mathrm{Gal}(K_{(N)}/H), \\ \gamma &\mapsto (h(\theta) \mapsto h^\gamma(\theta)), \end{aligned} \tag{5.2}$$

where $h \in \mathcal{F}_N$ is defined and finite at $\theta$, and

$$W_{N,\theta} = \left\{ \begin{pmatrix} t - B_\theta s & -C_\theta s \\ s & t \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) : t, s \in \mathbb{Z}/N\mathbb{Z} \right\}$$

([12] or [4]). Now, let $H_\mathcal{O}$ be the ring class field of the order $\mathcal{O}$ of conductor $N$ ($\ge 2$) in $K$. Then we get

$$H_\mathcal{O} = K(j(N\theta)) \tag{5.3}$$

([9] or [12]). Moreover, we have

LEMMA 5.1 (see [7, Lemma 9.9]). *For any nonzero integer $m$, the value $(3j(N\theta)+1)^m$ generates $H_{\mathcal{O}}$ over $K$.*

LEMMA 5.2 (see proof of [7, Theorem 9.8]). *Let $N \geq 2$. Then each element $\left(\begin{smallmatrix} t & 0 \\ 0 & t \end{smallmatrix}\right)$ of $W_{N,\theta}/\pm\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ fixes the value $j(N\theta)$.*

PROPOSITION 5.3. *For $N \geq 2$, $\mathrm{Gal}(K_{(N)}/H_{\mathcal{O}})$ is isomorphic to the subgroup $\left\{\left(\begin{smallmatrix} t & 0 \\ 0 & t \end{smallmatrix}\right) : t \in (\mathbb{Z}/N\mathbb{Z})^*\right\}/\pm\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ of $W_{N,\theta}/\pm\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$.*

*Proof.* First, we have the degree formula

$$[K_{(N)} : H] = \frac{\varphi(N\mathcal{O}_K)w(N\mathcal{O}_K)}{w_K} \tag{5.4}$$

where $\varphi$ is the Euler function for ideals,

$$\varphi(\mathfrak{p}^n) = (\mathbf{N}_{K/\mathbb{Q}}\mathfrak{p} - 1)\mathbf{N}_{K/\mathbb{Q}}\mathfrak{p}^{n-1}$$

for a power of prime ideal $\mathfrak{p}$, $w(N\mathcal{O}_K)$ is the number of roots of unity in $K$ which are $\equiv 1 \pmod{N\mathcal{O}_K}$, and $w_K$ is the number of roots of unity in $K$ ([8]). We also have the formula

$$[H_{\mathcal{O}} : H] = \frac{N}{[\mathcal{O}_K^* : \mathcal{O}^*]} \prod_{p|N} \left(1 - \left(\frac{d_K}{p}\right)\frac{1}{p}\right)$$

where $\left(\frac{d_K}{p}\right)$ is the Legendre symbol for an odd prime $p$ and $\left(\frac{d_K}{2}\right)$ is the Kronecker symbol ([2]). Thus one can readily check that

$$[K_{(N)} : H_{\mathcal{O}}] = \frac{[K_{(N)} : H]}{[H_{\mathcal{O}} : H]} = \left|\left\{\left(\begin{smallmatrix} t & 0 \\ 0 & t \end{smallmatrix}\right) : t \in (\mathbb{Z}/N\mathbb{Z})^*\right\}/\pm\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)\right|.$$

Therefore by Lemma 5.2 the assertion follows by Galois theory. ∎

LEMMA 5.4. *If $N \geq 4$ and $1 < t \leq [N/2]$, then:*

(i) $\left|\dfrac{1-\zeta_N}{1-\zeta_N^t}\right| \leq \dfrac{1}{\sqrt{2}}$.

(ii) $\dfrac{1}{1-e^{-\pi\sqrt{-d_K}X}} < 1 + e^{-\frac{\pi\sqrt{-d_K}}{1.03}X}$ *for all* $X \geq 1$.

(iii) $1 + X < e^X$ *for all* $X > 0$.

(iv) $|g_{(1/N,0)}(N\theta)| < |g_{(t/N,0)}(N\theta)|$.

(v) $|g_{(0,1/N)}(\theta)| < |g_{(0,t/N)}(\theta)|$.

*Proof.* (i)–(iii) are almost trivial and (iv) is proved in [7, Lemma 9.3].

Hence we only prove (v). Putting

$$A = |e^{2\pi i\theta}| = e^{-\pi\sqrt{-d_K}}$$

we get

$$\begin{aligned}
\left|\frac{g_{(0,1/N)}(\theta)}{g_{(0,t/N)}(\theta)}\right| &\le \left|\frac{1-\zeta_N}{1-\zeta_N^t}\right| \prod_{n=1}^{\infty} \frac{(1+A^n)^2}{(1-A^n)^2} \quad \text{by the definition (2.1)} \\
&\le \frac{1}{\sqrt{2}} \prod_{n=1}^{\infty} (1+A^n)^2(1+A^{n/1.03})^2 \quad \text{by (i) and (ii)} \\
&\le \frac{1}{\sqrt{2}} \prod_{n=1}^{\infty} e^{2A^n+2A^{n/1.03}} \quad \text{by (iii)} \\
&= \frac{1}{\sqrt{2}}\, e^{\frac{2A}{1-A}+\frac{2A^{1/1.03}}{1-A^{1/1.03}}} \le \frac{1}{\sqrt{2}}\, e^{\frac{2e^{-\sqrt{7}\pi}}{1-e^{-\sqrt{7}\pi}}+\frac{2e^{-\sqrt{7}\pi/1.03}}{1-e^{-\sqrt{7}\pi/1.03}}} < 1 \quad \text{since } d_K \le -7,
\end{aligned}$$

which proves (v). ∎

THEOREM 5.5. *For $N \ge 2$, define*

$$\begin{aligned}
G(\tau) = (3j(N\tau)+1)&(g_{(0,1/N)}(\tau)g_{(1/N,0)}(N\tau))^{12N\phi(N)} \\
&\times \prod_{\substack{1\le s\le N-1 \\ \gcd(s,N)=1}} (g_{(0,s/N)}(\tau)g_{(s/N,0)}(N\tau))^{-12N}
\end{aligned}$$

*where $\phi$ is the Euler $\phi$-function for positive integers. Then the singular value $G(\theta)$ generates $K_{(N)}$ over $K$.*

*Proof.* The above function without the factor $3j(N\tau)+1$ is in $\mathcal{F}_N \cap \mathcal{K}(X_1^{\dagger}(N))$ by Propositions 2.3, 2.4 and 4.1. So its singular value $G(\theta)$ belongs to $K_{(N)}$ by (5.1) and (5.3). As a subfield of $K_{(N)}$, the field $K(G(\theta))$ is an abelian extension of $K$. Hence $K(G(\theta))$ contains the element

$$\prod_{\substack{1\le t\le N-1 \\ \gcd(t,N)=1}} G(\theta)^{\left(\begin{smallmatrix} t & 0 \\ 0 & t \end{smallmatrix}\right)}.$$

It then follows from (5.2) that the action of each element $\left(\begin{smallmatrix} t & 0 \\ 0 & t \end{smallmatrix}\right)$ is given by

$$(3j(N\theta)+1)^{\left(\begin{smallmatrix} t & 0 \\ 0 & t \end{smallmatrix}\right)} = 3j(N\theta)+1 \quad \text{by Lemma 5.2,}$$

$$((g_{(0,1/N)}(\theta)g_{(1/N,0)}(N\theta))^{12N\phi(N)})^{\left(\begin{smallmatrix} t & 0 \\ 0 & t \end{smallmatrix}\right)} = (g_{(0,t/N)}(\theta)g_{(t/N,0)}(N\theta))^{12N\phi(N)}$$

by Proposition 2.5,

$$\Big(\prod_{\substack{1\le s\le N-1\\ \gcd(s,N)=1}} (g_{(0,s/N)}(\theta)g_{(s/N,0)}(N\theta))^{-12N}\Big)^{\left(\begin{smallmatrix} t & 0\\ 0 & t\end{smallmatrix}\right)}$$

$$= \prod_{\substack{1\le s\le N-1\\ \gcd(s,N)=1}} (g_{(0,\langle st/N\rangle)}(\theta)g_{(\langle st/N\rangle,0)}(N\theta))^{-12N} \quad \text{by Proposition 2.5,}$$

$$= \prod_{\substack{1\le s\le N-1\\ \gcd(s,N)=1}} (g_{(0,s/N)}(\theta)g_{(s/N,0)}(N\theta))^{-12N}.$$

Thus we derive

$$\prod_{\substack{1\le t\le N-1\\ \gcd(t,N)=1}} G(\theta)^{\left(\begin{smallmatrix} t & 0\\ 0 & t\end{smallmatrix}\right)} = (3j(N\theta)+1)^{\phi(N)}.$$

This implies that $K(G(\theta))$ contains $H_{\mathcal{O}}$ by Lemma 5.1. Now, by Proposition 5.3 and Galois theory, it suffices to prove that if the element $\left(\begin{smallmatrix} t & 0\\ 0 & t\end{smallmatrix}\right)$ for some $t \in \mathbb{Z}$ with $1 \le t \le [N/2]$ and $\gcd(t,N) = 1$ fixes $G(\theta)$, then $t = 1$. So assume that $\left(\begin{smallmatrix} t & 0\\ 0 & t\end{smallmatrix}\right)$ fixes $G(\theta)$. If $N = 2, 3$, then obviously $t = 1$. So, we may assume $N \ge 4$. Then by the above description of the action of $\left(\begin{smallmatrix} t & 0\\ 0 & t\end{smallmatrix}\right)$ we deduce that

$$1 = \left|\frac{G(\theta)}{G(\theta)^{\left(\begin{smallmatrix} t & 0\\ 0 & t\end{smallmatrix}\right)}}\right| = \left|\frac{g_{(0,1/N)}(\theta)g_{(1/N,0)}(N\theta)}{g_{(0,t/N)}(\theta)g_{(t/N,0)}(N\theta)}\right|^{12N\phi(N)}$$

$$= \left|\frac{g_{(0,1/N)}(\theta)}{g_{(0,t/N)}(\theta)}\right|^{12N\phi(N)} \left|\frac{g_{(1/N,0)}(N\theta)}{g_{(t/N,0)}(N\theta)}\right|^{12N\phi(N)}.$$

But this equality holds only when $t = 1$ by Lemma 5.4(iv), (v), which concludes the proof. ∎

**Acknowledgements.** This research was supported by Basic Science Research Program through the National Research Foundation of Korea funded by the Ministry of Education, Science and Technology (2009-0063182).

## References

[1] S. Y. Choi and J. K. Koo, *Estimation of genus of arithmetic curves and applications*, Ramanujan J. 15 (2008), 1–17.

[2] D. A. Cox, *Primes of the Form $x^2 + ny^2$: Fermat, Class Field, and Complex Multiplication*, Wiley, 1989.

[3] F. Diamond and J. Shurman, *A First Course in Modular Forms*, Springer, 2005.

[4] A. Gee, *Class invariants by Shimura's reciprocity law*, J. Théor. Nombres Bordeaux 11 (1999), 45–72.

[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] C. H. Kim and J. K. Koo, *Estimation of genus for certain arithmetic groups*, Comm. Algebra 32 (2004), 2479–2495.
[7] J. K. Koo and D. H. Shin, *On some arithmetic properties of Siegel functions*, Math. Z. 264 (2010), 137–177.
[8] D. Kubert and S. Lang, *Modular Units*, Grundlehren Math. Wiss. 244, Spinger, 1981.
[9] S. Lang, *Elliptic Functions*, 2nd ed., Springer, 1987.
[10] R. Miranda, *Algebraic Curves and Riemann Surfaces*, Amer. Math. Soc., Providence, RI, 1995.
[11] K. Ramachandra, *Some applications of Kronecker's limit formulas*, Ann. of Math. 80 (1964), 104–148.
[12] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Iwanami Shoten and Princeton Univ. Press, 1971.
[13] Y. Yang, *Transformation formulas for generalized Dedekind eta functions*, Bull. London Math. Soc. 36 (2004), 671–682.

Ja Kyung Koo, Dong Hwa Shin
Department of Mathematical Sciences, KAIST
Daejeon 373-1, Korea
E-mail: jkkoo@math.kaist.ac.kr
shakur01@kaist.ac.kr

*Received on 19.12.2008*
*and in revised form on 18.7.2009* (5895)