Trends in Mathematics - New Series
Information Center for Mathematical Sciences
Volume 11, Number 2, 2009, pages 41–55

ASARC Workshop
Daecheon & Muju 2009


# FUNCTION FIELDS OF CERTAIN ARITHMETIC CURVES AND APPLICATION

JA KYUNG KOO AND DONG HWA SHIN

Abstract. Based on the classical theory of modular curves we describe the function fields of the arithmetic curves $X_1^\dagger(N) = \langle \overline{\Gamma}_1(N),\ \overline{\Phi}_N \rangle \backslash \mathfrak{H}^*$ where $\Phi_N = \left(\begin{smallmatrix} 0 & -1 \\ N & 0 \end{smallmatrix}\right)$ is the Fricke involution for $N \geq 2$. For the purpose we use the modular invariant $j$ and finite products of Siegel functions. And, we further construct primitive generators of the function fields of these curves $X_1^\dagger(N)$ with genus zero in a systematic way by means of Siegel functions only unlike Choi-Koo's method ([1]). As an application we find the ray class invariants over any imaginary quadratic fields other than $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-3})$ by utilizing the singular values of $j$ and Siegel functions which are different from the Ramachandra's invariants ([11]).

## 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. And, we think of an element $\gamma$ of $\mathrm{GL}_2^+(\mathbb{R})$ not only as a matrix but also as a transformation. When we need to emphasize 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*. And, a meromorphic function $f$ on $\mathfrak{H}$ invariant under the actions of all $\gamma \in \Gamma$ is said to be *weakly modular*

2000 *Mathematics Subject Classification.* 11F03, 11G16, 11G30, 11R37, 14H55.
*Key words and phrases.* class fields, modular curves, modular units, Riemann surfaces, Siegel functions.
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).

for $\Gamma$ (or $\overline{\Gamma}$). Moreover, 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 a field of meromorphic functions on the compact Riemann surface $\langle \overline{\Gamma},\ \overline{\Phi}_N \rangle \backslash \mathfrak{H}^*$ where $\Gamma$ is given by one of the above congruence subgroups. From now on, for convenience we let

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

and $\mathcal{K}(R)$ 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 theory of elliptic curves. And, in general the function field of a compact Riemann surface (as an algebraic curve) can be generated by at most two functions ([10]). For instance, Ishida-Ishii constructed in [5] these two generators of $\mathcal{K}\big(X_1(N)\big)$ 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]). After recalling those basic properties of Siegel functions we shall find generators of function fields in terms of $j$ and Siegel functions (Theorems 3.2 and 3.5) unlike Ishida-Ishii's approach.

On the other hand, Kim-Koo ([6]) made a genus formula of the arithmetic curve $X_1^\dagger(N)$. Using this formula they showed that $X_1^\dagger(N)$ has genus zero exactly when $1 \le N \le 12$ and $N = 14,\ 15$. And, Choi-Koo constructed in [1] primitive generators of such genus zero curves $X_1^\dagger(N)$ by using elliptic functions and theta functions. However, their method seems to be too artificial and inconvenient to be applied to other similar situations. Thus we shall revisit this subject in this paper to present a process of finding primitive generators in more a 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]) in which they dealt with various modifications of Siegel functions.

Next, we know that a classical generator of the ring class field of the order of conductor $N$ ($\geq 2$) over an imaginary quadratic field $K$ is given by a singular value of $j$. And we recently showed that any power of 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 would be different from the 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 $\Delta$. And, we also describe Galois groups between those 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 $\mathbf{B}_2(X) = X^2 - X + \frac{1}{6}$ 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* $g_r(\tau)$ on $\tau \in \mathfrak{H}$ by the following $q_\tau$-expansion 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

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

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

**Proposition 2.1.** *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 get*

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

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

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

$$g_{r+s} = \varepsilon(r,s) g_r$$

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

*Proof.* See [7] Proposition 2.4. □

*Remark* 2.2. Wee 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 meromorphicity 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 Fourier coefficients of $h \circ \gamma$ with respect to $q_\tau^{\frac{1}{N}}$ for any $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ belong to $\mathbb{Q}(\zeta_N)$ with $\zeta_N = e^{\frac{2\pi i}{N}}$. 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 determining whether a product of Siegel functions belongs to $\mathcal{F}_N$. For $N \geq 2$ we say that a family of integers $\{m(r)\}_{r \in \frac{1}{N}\mathbb{Z}^2 \setminus \mathbb{Z}^2}$ with $m(r) = 0$ except finitely many $r = (r_1,\ r_2)$ 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.** *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* $r \in \frac{1}{N}\mathbb{Z}^2 \setminus \mathbb{Z}^2$.

*Proof.* See [8] Chapter 3 Theorems 5.2 and 5.3. □

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

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

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

**Proposition 2.4.** *Let $N \geq 2$. A product*

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

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

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

*In particular, $g_{(\frac{t}{N},0)}^{12N}(N\tau)$ 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*

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

*Proof.* See [7] Theorem 6.2. □

Now we investigate some 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*

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

*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 $\mathcal{K}\big(X_1(N)\big)$ in terms of $j$ and a product of Siegel functions. We can then naturally extend it to $\mathcal{K}\big(X_1^\dagger(N)\big)$. Here we will 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 $g = g_{(0,\frac{1}{N})}^{12N}(\tau) g_{(\frac{1}{N},0)}^{12N}(N\tau)$. 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 we get $\gamma \equiv \pm \left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right) \pmod{N}$.*

*Proof.* (i) We see by Proposition 2.3 that the function $g_{(0,\frac{1}{N})}^{12N}(\tau)$ 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 $\Gamma_1(N) = \langle \Gamma(N),\ T \rangle$, $g_{(0,\frac{1}{N})}^{12N}(\tau)$ is modular for $\Gamma_1(N)$. Furthermore, the

function $g^{12N}_{(\frac{1}{N},0)}(N\tau)$ is modular for $\Gamma_1(N)$ by Proposition 2.4 from which we derive that $g = g^{12N}_{(0,\frac{1}{N})}(\tau)g^{12N}_{(\frac{1}{N},0)}(N\tau)$ 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 we obviously have $\mathrm{ord}_{q_\tau}(g\circ\gamma) = \mathrm{ord}_{q_\tau} g$. By (2.2) and (2.5) we achieve

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

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

Suppose $\gcd(c,N) \neq N$. The shape of the graph of $Y = \mathbf{B}_2(X)$ over the interval $0 \le X \le 1$ indicates that the maximum value of $\mathbf{B}_2(X)$ is $\frac{1}{6}$ at $X = 0,\ 1$. So $\mathrm{ord}_{q_\tau}(g\circ\gamma)$ is bounded by

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

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

$$\frac{6}{N} - 6 + N + \frac{N^2}{4} < N^2 - 5N + 6,$$

which contradicts the fact $\mathrm{ord}_{q_\tau}(g\circ\gamma) = \mathrm{ord}_{q_\tau}(g)$. Thus $\gcd(c,N) = N$, which induces $\mathbf{B}_2\big(\langle\frac{a}{N}\rangle\big) = \mathbf{B}_2\big(\frac{1}{N}\big)$ from (3.1), (3.2) and the fact $\mathrm{ord}_{q_\tau}(g\circ\gamma) = \mathrm{ord}_{q_\tau}(g)$. Therefore we derive $a \equiv \pm 1 \pmod N$ from the shape of the graph $Y = \mathbf{B}_2(X)$. Now that $\det(\alpha) = 1$, 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 $N \ge 6$. Then we obtain*

$$\begin{aligned} \mathcal{K}\big(X_0(N)\big) &= \mathbb{C}\big(j(\tau),\ j(N\tau)\big) \\ \mathcal{K}\big(X_1(N)\big) &= \mathbb{C}\big(j(\tau),\ g^{12N}_{(0,\frac{1}{N})}(\tau)g^{12N}_{(\frac{1}{N},0)}(N\tau)\big) \\ \mathcal{K}\big(X(N)\big) &= \mathbb{C}\big(j(\tau),\ g^{12N}_{(0,\frac{1}{N})}(\tau)g^{12N}_{(\frac{1}{N},0)}(N\tau),\ g^{12N}_{(\frac{1}{N},0)}(\tau)\big). \end{aligned}$$

*Proof.* As for the function field $\mathcal{K}\big(X_0(N)\big)$ we refer to [3]. Here we concentrate on the cases $\mathcal{K}\big(X_1(N)\big)$ and $\mathcal{K}\big(X(N)\big)$. We see from [3] that

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

as a subgroup of

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

whose action is given by composition. Assume that $g^{12N}_{(0,\frac{1}{N})}(\tau)g^{12N}_{(\frac{1}{N},0)}(N\tau)$, which belongs to $\mathcal{K}\big(X_1(N)\big)$ 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 $\mathcal{K}\big(X(1)\big) = \mathbb{C}\big(j(\tau)\big)$

([9] or [12]), we conclude by Galois theory that

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

Next, we assume that $g^{12N}_{(\frac{1}{N},0)}(\tau)$ 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 $g^{12N}_{(\frac{1}{N},0)}(\tau)\circ\left(\begin{smallmatrix}1 & b\\ 0 & 1\end{smallmatrix}\right) = g^{12N}_{(\frac{1}{N},\frac{b}{N})}(\tau) = g^{12N}_{(\frac{1}{N},0)}(\tau)$ 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 $g^{12N}_{(\frac{1}{N},\frac{b}{N})}(\tau) = g^{12N}_{(\frac{1}{N},0)}(\tau)$ that $g^{12N}_{(\frac{b}{N},-\frac{1}{N})}(\tau) = g^{12N}_{(0,-\frac{1}{N})}(\tau)$. Now we compare the orders via the formula (2.2) to obtain $6N\mathbf{B}_2\big(\big\langle\frac{b}{N}\big\rangle\big) = 6N\mathbf{B}_2(0)$; hence $b \equiv 0 \pmod N$ by the shape of the graph $Y = \mathbf{B}_2(X)$. Therefore we establish

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

□

From now on we extend the above results to the function fields $\mathcal{K}\big(X_0^\dagger(N)\big)$, $\mathcal{K}\big(X_1^\dagger(N)\big)$ and $\mathcal{K}\big(X^\dagger(N)\big)$. Since

$$\Phi_N\left(\begin{smallmatrix}1 & 0\\ -N & 1\end{smallmatrix}\right)\Phi_N = -N\left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right) \text{ and } \Gamma_1(N) = \big\langle\Gamma(N),\ \left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)\big\rangle,$$

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 consider 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 induce

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

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 achieve*

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

*Proof.* Observe by Proposition 2.1 that

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

□

**Theorem 3.5.** *For $N\geq 6$ we get*

$$\begin{aligned} \mathcal{K}\big(X_0^{\dagger}(N)\big) &= \mathbb{C}\big(j(\tau)+j(N\tau),\ j(\tau)j(N\tau)\big)\\ \mathcal{K}\big(X_1^{\dagger}(N)\big) &= \mathbb{C}\big(j(\tau)+j(N\tau),\ j(\tau)j(N\tau),\ g_{(0,\frac{1}{N})}^{12N}(\tau)g_{(\frac{1}{N},0)}^{12N}(N\tau)\big). \end{aligned}$$

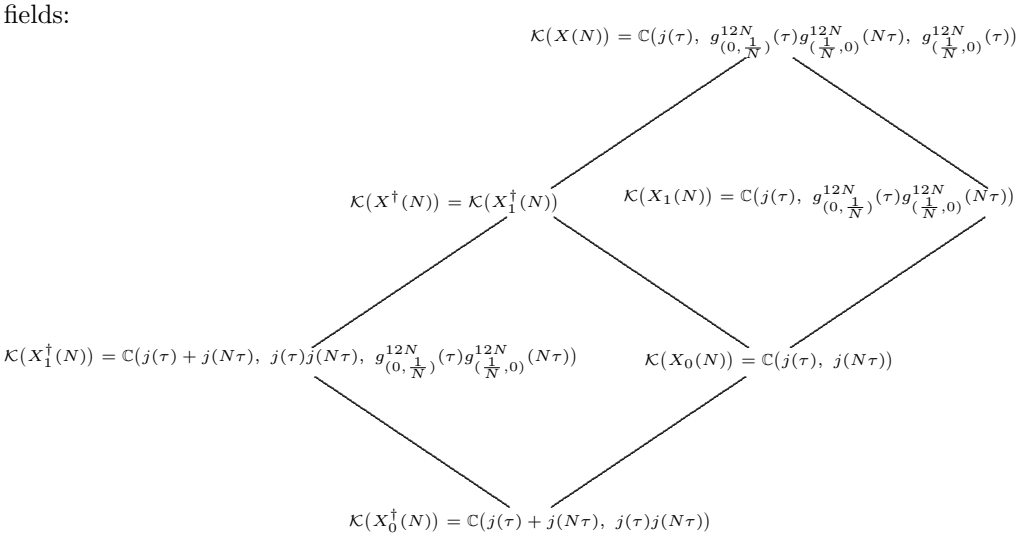
*Proof.* By Proposition 2.4 we know that the function $g=g_{(\frac{1}{N},0)}^{12N}(N\tau)$ is modular for $\Gamma_1(N)$. Moreover, by Lemma 3.4 we have $g\circ\Phi_N=g_{(0,\frac{1}{N})}^{12N}(\tau)$. Hence the function $g_{(0,\frac{1}{N})}^{12N}(\tau)g_{(\frac{1}{N},0)}^{12N}(N\tau)=(g\circ\Phi_N)\cdot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

Let $\Gamma$ be $\Gamma_0(N)$ or $\Gamma_1(N)$. Here we 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

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

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

We summarize all the results via the following diagram of a tower of function fields:



## 4. Primitive generators of $\mathcal{K}\big(X_1^\dagger(N)\big)$ 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 too artificial and inconvenient to be applied to other similar situations. Thus unlike their approach we would like to propose more systematic and standard way to find primitive generators in view 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 a product*

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

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

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

*Proof.* Let

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

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

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

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

And, 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*

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

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

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

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

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

*Proof.* The width of $\infty$ on $X_1^\dagger(N)$ is 1 ([1]). From the order formula (4.1) in Proposition 4.1 we know that the hypothesis in this theorem renders the fact 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 $\mathcal{K}\big(X_1^\dagger(N)\big) = \mathbb{C}(g^\dagger)$. □

By virtue of [7] Theorem 6.4 we can readily determine the inequivalent cusps of $X_1(N)$, from which we get the inequivalent cusps of $X_1^\dagger(N)$. Furthermore, the facts in [1] Lemmas 3.2 and 3.3 enable us to estimate the widths of cusps. However, it is unnecessary for us to know the values 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 $2 \leq N \leq 12$ 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 the goal. In the following table we use the convention $\prod_{t=1}^{N-1}\left(\frac{t}{N}\right)^{m(t)}$ to denote

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

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 $\mathcal{K}\big(X_1^\dagger(N)\big)$ in these two cases.

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

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

## 5. Application to class fields

As an application we shall construct a primitive generator of the ray class field modulo $N$ ($\geq 2$) 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 $K$ ($\neq \mathbb{Q}(\sqrt{-1}),\ \mathbb{Q}(\sqrt{-3})$) be any imaginary quadratic field with discriminant $d_K$ ($\leq -7$). Define

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

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 $N$ ($\geq 2$) of $K$, respectively. It is then well-known that

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

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

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

where $h \in \mathcal{F}_N$ is defined and finite at $\theta$, and $W_{N,\theta} = \Big\{ \left(\begin{smallmatrix} t-B_\theta s & -C_\theta s \\ s & t \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) : t, s \in \mathbb{Z}/N\mathbb{Z} \Big\}$ ([12] or [4]). Now, let $H_{\mathcal{O}}$ be the ring class field of the order $\mathcal{O}$ of

conductor $N$ ($\geq 2$) in $K$. Then we get

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

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

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

*Proof.* See [7] Lemma 9.9. □

**Lemma 5.2.** *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 $j(N\theta)$.*

*Proof.* See the proof of [7] Theorem 9.8. □

**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, namely

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

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]). And we also know 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 this fact and Lemma 5.2 we can prove the proposition by Galois theory. □

**Lemma 5.4.** *If $N \geq 4$ and $1 < t \leq [\frac{N}{2}]$, then we have the following inequalities:*

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

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

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

(iv) $\left|g_{(\frac{1}{N},0)}(N\theta)\right| < \left|g_{(\frac{t}{N},0)}(N\theta)\right|$.
(v) $\left|g_{(0,\frac{1}{N})}(\theta)\right| < \left|g_{(0,\frac{t}{N})}(\theta)\right|$.

*Proof.* (i)∼(iii) are almost trivial and (iv) is done in [7] Lemma 9.3. Hence we prove only (v). Putting $A = |e^{2\pi i\theta}| = e^{-\pi\sqrt{-d_K}}$ we get that

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

which proves (v). □

**Theorem 5.5.** *For $N \ge 2$, define a function*

$$G(\tau) = \big(3j(N\tau)+1\big)\big(g_{(0,\frac{1}{N})}(\tau)g_{(\frac{1}{N},0)}(N\tau)\big)^{12N\phi(N)} \prod_{\substack{1\le s\le N-1\\ \gcd(s,N)=1}} \big(g_{(0,\frac{s}{N})}(\tau)g_{(\frac{s}{N},0)}(N\tau)\big)^{-12N}$$

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

*Proof.* The function in the above without the factor $\big(3j(N\tau)+1\big)$ is in $\mathcal{F}_N \cap \mathcal{K}\big(X_1^{\dagger}(N)\big)$ 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 $K\big(G(\theta)\big)$ contains the following specific 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

$$\begin{aligned}
\big(3j(N\theta)+1\big)^{\left(\begin{smallmatrix} t & 0 \\ 0 & t \end{smallmatrix}\right)} &= 3j(N\theta)+1 \quad \text{by Lemma 5.2} \\
\Big(\big(g_{(0,\frac{1}{N})}(\theta)g_{(\frac{1}{N},0)}(N\theta)\big)^{12N\phi(N)}\Big)^{\left(\begin{smallmatrix} t & 0 \\ 0 & t \end{smallmatrix}\right)} &= \big(g_{(0,\frac{t}{N})}(\theta)g_{(\frac{t}{N},0)}(N\theta)\big)^{12N\phi(N)} \\
&\qquad \text{by Proposition 2.5} \\
\Big(\prod_{\substack{1\le s\le N-1\\ \gcd(s,N)=1}} \big(g_{(0,\frac{s}{N})}(\theta)g_{(\frac{s}{N},0)}(N\theta)\big)^{-12N}\Big)^{\left(\begin{smallmatrix} t & 0 \\ 0 & t \end{smallmatrix}\right)} &= \prod_{\substack{1\le s\le N-1\\ \gcd(s,N)=1}} \big(g_{(0,\langle\frac{st}{N}\rangle)}(\theta)g_{(\langle\frac{st}{N}\rangle,0)}(N\theta)\big)^{-12N} \\
&\qquad \text{by Proposition 2.5} \\
&= \prod_{\substack{1\le s\le N-1\\ \gcd(s,N)=1}} \big(g_{(0,\frac{s}{N})}(\theta)g_{(\frac{s}{N},0)}(N\theta)\big)^{-12N}.
\end{aligned}$$

Thus we derive

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

This implies that $K\big(G(\theta)\big)$ contains $H_{\mathcal{O}}$ by Lemma 5.1. Now 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 $1 \le t \le [\frac{N}{2}]$ and $\gcd(t,N)=1$ fixes $G(\theta)$, then $t=1$ by Proposition 5.3 and Galois theory. To this end we assume that $\left(\begin{smallmatrix} t & 0 \\ 0 & t \end{smallmatrix}\right)$ fixes $G(\theta)$. If $N=2,\ 3$, then we obviously have $t=1$. 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

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

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

## References


1. S. Y. Choi and J. K. Koo, *Estimation of genus of arithmetic curves and applications*, Ramanujan J. 15 (2008), no. 1, 1-17.
2. D. A. Cox, *Primes of the form $x^2+ny^2$: Fermat, Class Field, and Complex Multiplication*, John Wiley & Sons, Inc., 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. Theor. Nombres Bordeaux 11 (1999), no. 1, 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), no. 7, 2479-2495.
7. J. K. Koo and D. H. Shin, *On some arithmetic properties of Siegel functions*, Math. Zeit., 264 (2010) 137-177.
8. D. Kubert and S. Lang, *Modular Units*, Grundlehren der mathematischen Wissenschaften 244, Spinger-Verlag, 1981.
9. S. Lang, *Elliptic Functions, 2nd edition*, Spinger-Verlag, 1987.
10. R. Miranda, *Algebraic Curves and Riemann Surfaces*, Amer. Math. Soc., Providence, R.I., 1995.
11. K. Ramachandra, *Some applications of Kronecker's limit formulas*, Ann. Math. 80 (1964), 104-148.
12. G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Iwanami Shoten and Princeton University Press, 1971.
13. Y. Yang, *Transformation formulas for generalized Dedekind eta functions*, Bull. London Math. Soc. 36 (2004), no. 5, 671-682.

Department of Mathematical Sciences, KAIST
*Current address*: Daejeon 373-1, Korea
*E-mail address*: jkkoo@math.kaist.ac.kr

Department of Mathematical Sciences, KAIST
*Current address*: Daejeon 373-1, Korea
*E-mail address*: shakur01@kaist.ac.kr