Ray class fields generated by torsion points of certain elliptic curves

by

Ja Kyung Koo, Dong Hwa Shin and Dong Sung Yoon

BK21 Research Report

09 - 20

August 3, 2009

DEPARTMENT OF MATHEMATICAL SCIENCES

The second stage of BK21 Fostering A World Class Talent

KAIST 한국과학기술원 Korea Advanced Institute of Science and Technology

RAY CLASS FIELDS GENERATED BY TORSION POINTS OF CERTAIN ELLIPTIC CURVES

JA KYUNG KOO, DONG HWA SHIN, AND DONG SUNG YOON

Abstract. We first normalize the derivative Weierstrass $\wp'$-function appearing in the Weierstrass equations which give rise to analytic parametrizations of elliptic curves by the Dedekind η-function. And, by making use of this normalization of $\wp'$ we associate certain elliptic curve to a given imaginary quadratic field K and then generate an infinite family of ray class fields over K by adjoining to K torsion points of such elliptic curve(Theorem 5.3). We further construct some ray class invariants of imaginary quadratic fields by utilizing the singular values of the normalization of $\wp'$, as the y-coordinate in the Weierstrass equation of this elliptic curve(Theorem 6.2, Corollary 6.4), which would be a partial result for the Lang-Schertz conjecture of constructing ray class fields over K by means of the Siegel-Ramachandra invariant([10] p.292, [13] p.386).

1. Introduction

Let K be an imaginary quadratic field with discriminant $d_K \leq -7$ and $\mathcal{O}_K$ be its ring of integers. Let θ be an element in the complex upper half plane $\mathfrak{H}$ which generates $\mathcal{O}_K$, namely $\mathcal{O}_K = [\theta,\ 1]$. For an elliptic curve E (over $\mathbb{C}$) with invariant $j(\mathcal{O}_K) = j(\theta)$ where j is the elliptic modular function, there is an analytic parametrization

$$\varphi\ :\ \mathbb{C}/\mathcal{O}_K \xrightarrow{\sim} E \subset \mathbb{P}^2(\mathbb{C})\ :\ y^2 = 4x^3 - g_2(\mathcal{O}_K)x - g_3(\mathcal{O}_K) \tag{1.1}$$

where $g_2(\mathcal{O}_K) = 60\sum_{\omega\in\mathcal{O}_K\setminus\{0\}}\frac{1}{\omega^4}$ and $g_3(\mathcal{O}_K) = 140\sum_{\omega\in\mathcal{O}_K\setminus\{0\}}\frac{1}{\omega^6}$([15]). Let h be the Weber function on E defined by

$$h(x,\ y) = -2^7 3^5 \frac{g_2(\mathcal{O}_K)g_3(\mathcal{O}_K)}{\Delta(\mathcal{O}_K)}x$$

where $\Delta(\mathcal{O}_K) = g_2(\mathcal{O}_K)^3 - 27g_3(\mathcal{O}_K)^2$. If H and $K_{(N)}$ are the Hilbert class field and the ray class field modulo $N\mathcal{O}_K$ of K for each integer $N \geq 2$, respectively, we know from the main theorem of complex multiplication that

$$H = K\big(j(\mathcal{O}_K)\big) \quad \text{and} \quad K_{(N)} = K\left(j(\mathcal{O}_K),\ h\big(\varphi(\tfrac{1}{N})\big)\right)$$

([10] or [14]). Thus in order to describe a ray class field $K_{(N)}$ we are to use only the x-coordinates of the Weierstrass equation in (1.1). However, we want to improve in this paper the above result so that we are able to rewrite it as

$$K_{(N)} = K\big(\varphi(\tfrac{1}{N})\big) = K\left(x\big(\varphi(\tfrac{1}{N})\big),\ y\big(\varphi(\tfrac{1}{N})\big)\right)$$

by an appropriate modification of the curve in (1.1).

2000 *Mathematics Subject Classification.* 11F11, 11G15, 11R37.

Key words and phrases. elliptic curves, modular forms and functions, ray class fields, 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).

Ishida-Ishii showed in [4] that for $N \geq 7$ the function field $\mathbb{C}\big(X_1(N)\big)$ of the modular curve $X_1(N) = \Gamma_1(N)\backslash\mathfrak{H}^*$ can be generated by two functions $X_2^{\varepsilon_N N}$ and X_3^N where $\mathfrak{H}^* = \mathfrak{H} \cup \mathbb{P}^1(\mathbb{Q})$, $\Gamma_1(N) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) : \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \equiv \left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right) \pmod{N} \right\}$ and

$$\varepsilon_N = \begin{cases} 1 & \text{if } N \text{ is odd} \\ 2 & \text{if } N \text{ is even} \end{cases}, \quad X_2(\tau) = e^{(\frac{1}{N}-1)\frac{\pi i}{2}} \prod_{t=0}^{N-1} \frac{\mathfrak{k}_{(\frac{2}{N},\ \frac{t}{N})}(\tau)}{\mathfrak{k}_{(\frac{1}{N},\ \frac{t}{N})}(\tau)}, \quad X_3(\tau) = e^{(\frac{1}{N}-1)\pi i} \prod_{t=0}^{N-1} \frac{\mathfrak{k}_{(\frac{3}{N},\ \frac{t}{N})}(\tau)}{\mathfrak{k}_{(\frac{1}{N},\ \frac{t}{N})}(\tau)}$$

as finite products of the Klein forms(see Section 2). They further presented an algorithm to find a polynomial $F_N(X,\ Y) \in \mathbb{Z}[\zeta_N][X,\ Y]$ with $\zeta_N = e^{\frac{2\pi i}{N}}$ such that $F_N(X_2^{\varepsilon_N N},\ X_3^N) = 0$, which can be viewed as an affine singular model for the modular curve $X_1(N)$. And, for a fixed level N, Hong-Koo([3]) pointed out that if $P = \big(X_2(\theta)^{\varepsilon_N N},\ X_3(\theta)^N\big)$ is a nonsingular point on the curve defined by the equation $F_N(X,\ Y) = 0$, then the ray class field $K_{(N)}$ is generated by adjoining P to K. But it leaves us certain inconvenience of finding the polynomial $F_N(X,\ Y)$ explicitly.

In this paper we will develop this theme of [3] from a different point of view to overcome such inconvenience. First in Section 3 we shall normalize the derivative Weierstrass $\wp'$-function by the Dedekind η-function to be a modular function and then we associate certain elliptic curve to a given imaginary quadratic field K with $d_K \leq -39$. Next, we will find an infinite family of ray class fields $K_{(N)}$ generated by adjoining to K certain N-torsion points of such elliptic curve if $N \geq 8$ and $4 \mid N$(Theorem 5.3).

Furthermore, we shall show by adopting Schertz's argument([13]) that certain singular value of the normalization of $\wp'$, as the y-coordinate in the Weierstrass equation of the above elliptic curve, gives rise to a ray class invariant of $K_{(N)}$ over K for some N, for example $N = p^n$ where p is an odd prime which is inert or ramified in $K/\mathbb{Q}$(Corollary 6.4 and Remark 6.5). Here we note that Theorem 6.2, Corollary 6.4 and Remark 6.5 give us partial results of the Lang-Schertz conjecture concerning the Kronecker Jugendtraum over K. These ray class invariants are, in practical use, simpler than those of Ramachandra([12]) consisting of too complicated products of high powers of singular values of the Klein forms and singular values of the Δ-function.

2. Modular forms and functions

For a lattice L in $\mathbb{C}$ the *Weierstrass $\wp$-function* is defined by

$$\wp(z;\ L) = \frac{1}{z^2} + \sum_{\omega \in L\setminus\{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right) \qquad (z \in \mathbb{C}), \tag{2.1}$$

and the *Weierstrass σ-function* is defined by

$$\sigma(z;\ L) = z \prod_{\omega \in L\setminus\{0\}} \left(1 - \frac{z}{\omega}\right) e^{\frac{z}{\omega} + \frac{1}{2}(\frac{z}{\omega})^2} \qquad (z \in \mathbb{C}).$$

Taking the logarithmic derivative we come up with the *Weierstrass ζ-function*

$$\zeta(z;\ L) = \frac{\sigma'(z;\ L)}{\sigma(z;\ L)} = \frac{1}{z} + \sum_{\omega \in L\setminus\{0\}} \left(\frac{1}{z-\omega} + \frac{1}{\omega} + \frac{z}{\omega^2} \right) \qquad (z \in \mathbb{C}).$$

Then, differentiating the function $\zeta(z+\omega;\ L) - \zeta(z;\ L)$ for $\omega \in L$ results in 0, because $\zeta'(z;\ L) = -\wp(z;\ L)$ and the $\wp$-function is periodic with respect to L. Hence there is a constant $\eta(\omega;\ L)$ such that $\zeta(z+\omega;\ L) = \zeta(z;\ L) + \eta(\omega;\ L)$.

For a pair $(r_1,\ r_2) \in \mathbb{Q}^2 \setminus \mathbb{Z}^2$ we define the *Klein form* as

$$\mathfrak{k}_{(r_1,\ r_2)}(\tau) = e^{-\frac{1}{2}(r_1\eta_1 + r_2\eta_2)(r_1\tau + r_2)} \sigma(r_1\tau + r_2;\ [\tau,\ 1]) \qquad (\tau \in \mathbb{C})$$

where $\eta_1 = \eta(\tau;\ [\tau,\ 1])$ and $\eta_2 = \eta(1;\ [\tau,\ 1])$. And we define the *Siegel function* by

$$g_{(r_1,\ r_2)}(\tau) = \mathfrak{k}_{(r_1,\ r_2)}(\tau)\eta^2(\tau) \qquad (\tau \in \mathfrak{H})$$

where η is the *Dedekind η-function* satisfying

$$\eta(\tau) = \sqrt{2\pi}\zeta_8 q_\tau^{\frac{1}{24}} \prod_{n=1}^{\infty}(1-q_\tau^n) \qquad (q_\tau = e^{2\pi i\tau},\ \tau \in \mathfrak{H}). \tag{2.2}$$

If we let $\mathbf{B}_2(X) = X^2 - X + \frac{1}{6}$ be the second Bernoulli polynomial, then from the q_τ-product formula of the Weierstrass σ-function([10] Chapter 18 Theorem 4) and (2.2) we get the following Fourier expansion formula

$$g_{(r_1,\ r_2)}(\tau) = -q_\tau^{\frac{1}{2}\mathbf{B}_2(r_1)} e^{\pi i r_2(r_1-1)}(1-q_z)\prod_{n=1}^{\infty}(1-q_\tau^n q_z)(1-q_\tau^n q_z^{-1}) \tag{2.3}$$

where $q_z = e^{2\pi i z}$ with $z = r_1\tau + r_2$. Here we note that $\eta(\tau)$ and $g_{(r_1,\ r_2)}(\tau)$ have no zeros and poles on $\mathfrak{H}$ due to (2.2) and (2.3). And, we have the order formula

$$\mathrm{ord}_{q_\tau}\Big(g_{(r_1,\ r_2)}(\tau)\Big) = \frac{1}{2}\mathbf{B}_2\big(\langle r_1\rangle\big) \tag{2.4}$$

where $\langle X\rangle$ is the fractional part of $X \in \mathbb{R}$ with $0 \le \langle X\rangle < 1$([8] Chapter 2 Section 1).

Next, we further define

$$g_2(L) = 60\sum_{\omega\in L\setminus\{0\}}\frac{1}{w^4},\quad g_3(L) = 140\sum_{\omega\in L\setminus\{0\}}\frac{1}{w^6},\quad \Delta(L) = g_2(L)^3 - 27g_3(L)^2 \tag{2.5}$$

and the *elliptic modular function* by

$$j(L) = 2^6 3^3\frac{g_2(L)^3}{\Delta(L)}. \tag{2.6}$$

Proposition 2.1. (i) *For $\tau \in \mathfrak{H}$ we have the following Fourier expansion formulas*

$$g_2(\tau) = g_2([\tau,\ 1]) = (2\pi)^4\frac{1}{2^2 3}\Big(1 + 240\sum_{n=1}^{\infty}\sigma_3(n)q_\tau^n\Big)$$

$$g_3(\tau) = g_3([\tau,\ 1]) = (2\pi)^6\frac{1}{2^3 3^3}\Big(1 - 504\sum_{n=1}^{\infty}\sigma_5(n)q_\tau^n\Big)$$

$$\Delta(\tau) = \Delta([\tau,\ 1]) = (2\pi i)^{12}q_\tau\prod_{n=1}^{\infty}(1-q_\tau^n)^{24}$$

where

$$\sigma_k(n) = \sum_{d>0,\ d|n} d^k.$$

(ii) *On $\mathfrak{H}$, $g_2(\tau)$(respectively, $g_3(\tau)$) has zeros only at $\alpha(\zeta_3)$(respectively, $\alpha(\zeta_4)$) for $\alpha \in \mathrm{SL}_2(\mathbb{Z})$, and has no poles.*

Proof. See [10] Chapters 3, 4 and 18. □

Remark 2.2. (i) By definition (2.2) and Proposition 2.1(i) we see the relation

$$\eta(\tau)^{24} = \Delta(\tau). \tag{2.7}$$

(ii) It follows from definition (2.6) and Proposition 2.1(i) that $j(\tau)=j([\tau,\ 1])$ has the Fourier expansion with integer coefficients

$$j(\tau)=\frac{1}{q_\tau}+744+196884q_\tau+21493760q_\tau^2+864299970q_\tau^3+20245856256q_\tau^4+\cdots.$$

For each integer $N\geq 1$, let

$$\Gamma(N)=\left\{\begin{pmatrix}a&b\\c&d\end{pmatrix}\in\mathrm{SL}_2(\mathbb{Z})\ :\ \begin{pmatrix}a&b\\c&d\end{pmatrix}\equiv\begin{pmatrix}1&0\\0&1\end{pmatrix}\pmod N\right\}.$$

Proposition 2.3. *We have the following modularity:*

Functions / *Modularity*	$g_2(\tau)$	$g_3(\tau)$	$\eta(\tau)^2$	$\eta(\tau)^4$	$\eta(\tau)^6$	$\eta(\tau)^{12}$	$\eta(\tau)^{24}$	$j(\tau)$
with respect to	$\Gamma(1)$	$\Gamma(1)$	$\Gamma(12)$	$\Gamma(6)$	$\Gamma(3)$	$\Gamma(2)$	$\Gamma(1)$	$\Gamma(1)$
weight	4	6	1	2	3	6	12	0

Proof. See [10] Chapter 3 Section 2 and [8] Chapter 3 Lemma 5.1. □

For a pair $(r_1,\ r_2)\in\mathbb{Q}^2\setminus\mathbb{Z}^2$ we now define the *Fricke function*

$$f_{(r_1,\ r_2)}(\tau)=-2^7 3^5\frac{g_2(\tau)g_3(\tau)\wp(r_1\tau+r_2;\ [\tau,\ 1])}{\Delta(\tau)}\qquad(\tau\in\mathfrak{H}),\tag{2.8}$$

and for $N\geq 1$ we let

$$\mathcal{F}_N=\mathbb{Q}\Big(j(\tau),\ f_{(r_1,\ r_2)}(\tau)\ :\ (r_1,\ r_2)\in\frac{1}{N}\mathbb{Z}\setminus\mathbb{Z}^2\Big)\tag{2.9}$$

which we call the *modular function field of level* N *rational over* $\mathbb{Q}(\zeta_N)$.

Proposition 2.4. *Let* $N\geq 1$ *and* $X(N)$ *denote the modular curve* $\Gamma(N)\backslash\mathfrak{H}^*$ *where* $\mathfrak{H}^*=\mathfrak{H}\cup\mathbb{P}^1(\mathbb{Q})$. *(The points of* $\mathbb{P}^1(\mathbb{Q})=\mathbb{Q}\cup\{\infty\}$ *are called cusps.) Then*

(i) $\mathbb{C}\big(X(N)\big)=\mathbb{C}\mathcal{F}_N$.

(ii) $\mathcal{F}_N$ *coincides with the field of functions in* $\mathbb{C}\big(X(N)\big)$ *whose Fourier expansions with respect to* $q_\tau^{\frac{1}{N}}$ *have coefficients in* $\mathbb{Q}(\zeta_N)$.

Proof. See [14] Propositions 6.1 and 6.9(1). □

Proposition 2.5. $\mathcal{F}_N$ *is a Galois extension of* $\mathcal{F}_1=\mathbb{Q}\big(j(\tau)\big)$ *whose Galois group is isomorphic to* $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1_2\}$. *In order to describe the Galois action on* $\mathcal{F}_N$ *we consider the decomposition*

$$\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1_2\}=\left\{\begin{pmatrix}1&0\\0&d\end{pmatrix}\ :\ d\in(\mathbb{Z}/N\mathbb{Z})^*\right\}\cdot\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1_2\}.$$

Here, the matrix $\left(\begin{smallmatrix}1&0\\0&d\end{smallmatrix}\right)$ *acts on* $\sum_{n=-\infty}^{\infty}c_n q_\tau^{\frac{n}{N}}\in\mathcal{F}_N$ *by*

$$\sum_{n=-\infty}^{\infty}c_n q_\tau^{\frac{n}{N}}\mapsto\sum_{n=-\infty}^{\infty}c_n^{\sigma_d}q_\tau^{\frac{n}{N}}$$

where σ_d *is the automorphism of* $\mathbb{Q}(\zeta_N)$ *induced by* $\zeta_N\mapsto\zeta_N^d$. *And, for an element* $\gamma\in\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1_2\}$ *let* $\gamma'\in\mathrm{SL}_2(\mathbb{Z})$ *be a preimage of* γ *via the natural surjection* $\mathrm{SL}_2(\mathbb{Z})\to\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1_2\}$. *Then* γ *acts on* $h\in\mathcal{F}_N$ *by composition*

$$h\mapsto h\circ\gamma'$$

as linear fractional transformation.

Proof. See [10] Chapter 6 Theorem 3. □

Proposition 2.6. *Let $N \geq 2$. A finite product of Siegel functions*

$$\prod_{r=(r_1,\ r_2)\in\frac{1}{N}\mathbb{Z}^2\setminus\mathbb{Z}^2} g_r(\tau)^{m(r)}$$

belongs to $\mathcal{F}_N$ if

$$\begin{aligned}
&\sum_r m(r)(Nr_1)^2 \equiv \sum_r m(r)(Nr_2)^2 \equiv 0 \pmod{\gcd(2,\ N)\cdot N}\\
&\sum_r m(r)(Nr_1)(Nr_2) \equiv 0 \pmod{N}\\
&\sum_r m(r)\cdot\gcd(12,\ N) \equiv 0 \pmod{12}.
\end{aligned}$$

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

3. Normalization of $\wp'$ by Dedekind η-function and some geometry

Let L be a lattice in $\mathbb{C}$. An elliptic curve E (over $\mathbb{C}$) with invariant $j(L)$ has an analytic parametrization in the projective plane $\mathbb{P}^2(\mathbb{C})$ with homogeneous coordinates $[X : Y : Z]$ via

$$\begin{array}{rcl}\varphi\ :\ \mathbb{C}/L & \stackrel{\sim}{\longrightarrow} & E\ :\ Y^2Z = 4X^3 - g_2(L)XZ^2 - g_3(L)Z^3\\ z & \mapsto & [\wp(z;\ L) : \wp'(z;\ L) : 1]\end{array} \tag{3.1}$$

([15] Chapter VI Proposition 3.6(b)). And we have a relation

$$\wp'(z;\ L) = -\frac{\sigma(2z;\ L)}{\sigma(z;\ L)^4} \tag{3.2}$$

([15] p.166).

Let $N \geq 2$ and $L = [\tau,\ 1]$ with $\tau \in \mathfrak{H}$ as a variable. Furthermore, let $z = r_1\tau + r_2$ with $(r_1,\ r_2) \in \frac{1}{N}\mathbb{Z}^2 \setminus \mathbb{Z}^2$. By (3.1) and (3.2) the Weierstrass equation satisfies

$$\frac{\sigma(2r_1\tau + 2r_2;\ [\tau,\ 1])^2}{\sigma(r_1\tau + r_2;\ [\tau,\ 1])^8} = 4\wp(r_1\tau + r_2;\ [\tau,\ 1])^3 - g_2(\tau)\wp(r_1\tau + r_2;\ [\tau,\ 1]) - g_3(\tau). \tag{3.3}$$

Now we set

$$u(\tau) = \frac{g_2(\tau)^3}{\eta(\tau)^{24}},\ v(\tau) = \frac{g_3(\tau)}{\eta(\tau)^{12}},\ x_{(r_1,\ r_2)}(\tau) = -\frac{1}{2^7 3^5} f_{(r_1,\ r_2)}(\tau),\ y_{(r_1,\ r_2)}(\tau) = -\frac{g_{(2r_1,\ 2r_2)}(\tau)}{g_{(r_1,\ r_2)}(\tau)^4}. \tag{3.4}$$

Then one can readily check that the equation (3.3) becomes

$$u(\tau)v(\tau)^3 y_{(r_1,\ r_2)}(\tau)^2 = 4x_{(r_1,\ r_2)}(\tau)^3 - u(\tau)v(\tau)^2 x(\tau) - u(\tau)v(\tau)^4. \tag{3.5}$$

Moreover, by (2.5) and (2.7) we have an additional relation

$$u(\tau) - 27v(\tau)^2 = 1. \tag{3.6}$$

Combining (3.5) and (3.6) we further obtain some geometric fact. To this end we first need the following lemma.

Lemma 3.1. (i) *Let $\tau_1,\ \tau_2 \in \mathfrak{H}$. Then $j(\tau_1) = j(\tau_2)$ if and only if $\tau_2 = \gamma(\tau_1)$ for some $\gamma \in \mathrm{SL}_2(\mathbb{Z})$.*

(ii) *Let L be a lattice in $\mathbb{C}$ and $z_1,\ z_2 \in \mathbb{C}\setminus L$. Then $\wp(z_1;\ L) = \wp(z_2;\ L)$ if and only if $z_1 \equiv \pm z_2 \pmod{L}$.*

(iii) *For* $(r_1,\ r_2)\in\mathbb{Q}^2\setminus\mathbb{Z}^2$ *we have*

$$\begin{aligned} g_{(r_1,\ r_2)}(\tau)\circ\begin{pmatrix}0&-1\\1&0\end{pmatrix} &= \zeta_{12}^9 g_{(r_1,\ r_2)\left(\begin{smallmatrix}0&-1\\1&0\end{smallmatrix}\right)}(\tau) &= \zeta_{12}^9 g_{(r_2,\ -r_1)}(\tau)\\ g_{(r_1,\ r_2)}(\tau)\circ\begin{pmatrix}1&1\\0&1\end{pmatrix} &= \zeta_{12} g_{(r_1,\ r_2)\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)}(\tau) &= \zeta_{12} g_{(r_1,\ r_1+r_2)}(\tau).\end{aligned}$$

Proof. See [1] Theorem 10.9, Lemma 10.4 and [7] Proposition 2.4(2). □

Proposition 3.2. *Let* $\mathbb{P}^3(\mathbb{C})$ *be the projective space with homogeneous coordinates* $[V:X:Y:Z]$ *and* S *be a surface in* $\mathbb{P}^3(\mathbb{C})$ *given by the homogeneous equation*

$$(Z^2+27V^2)V^3Y^2 = 4X^3Z^4-(Z^2+27V^2)V^2XZ^2-(Z^2+27V^2)V^4Z.$$

Let $\Gamma_{1,\ 4}(N)$ *be the congruence subgroup* $\Gamma_1(N)\cap\Gamma(4)$ *where* $\Gamma_1(N)=\left\{\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)\in\mathrm{SL}_2(\mathbb{Z})\ :\ \left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)\equiv\left(\begin{smallmatrix}1&*\\0&1\end{smallmatrix}\right)\pmod N\right\}$ *and* $X_{1,\ 4}(N)$ *be its corresponding modular curve* $\Gamma_{1,\ 4}(N)\backslash\mathfrak{H}^*$. *If* $4\mid N$, *then we have a holomorphic map*

$$\begin{aligned}\iota\ :\ X_{1,\ 4}(N) &\longrightarrow S\\ \tau &\longmapsto [v(\tau):x_{(0,\ \frac{1}{N})}(\tau):y_{(0,\ \frac{1}{N})}(\tau):1].\end{aligned}$$

In particular, if M *is the image of* $\{cusps,\ \alpha(\zeta_3),\ \alpha(\zeta_4)\ :\ \alpha\in\mathrm{SL}_2(\mathbb{Z})\}$ *via the natural quotient map* $\mathfrak{H}^*\to X_{1,\ 4}(N)$, *then the restriction morphism* $\iota: X_{1,\ 4}(N)\setminus M\to S$ *gives an embedding into* $\mathbb{P}^3(\mathbb{C})$.

Proof. Let $4\mid N$. Since the functions $v(\tau),\ x_{(0,\ \frac{1}{N})}(\tau),\ y_{(0,\ \frac{1}{N})}(\tau),\ 1$ are not all identically zero, the map ι extends to a holomorphic map defined on all of the modular curve $X_{1,\ 4}(N)$([11] Chapter V Lemma 4.2) and its image is contained in S by (3.5) and (3.6) provided that it is well-defined.

Since $v(\tau)\in\mathbb{C}(X(2))$ by Proposition 2.3, $v(\tau)\in\mathbb{C}(X_{1,\ 4}(N))$. And, $x_{(0,\ \frac{1}{N})}(\tau)\in\mathcal{F}_N$ by definition (2.9) and $y_{(0,\ \frac{1}{N})}(\tau)\in\mathcal{F}_N$ by Proposition 2.6. Here we observe that $\Gamma_1(N)=\langle\Gamma(N),\ T=\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)\rangle$. We then obtain by definition (2.8) and Proposition 2.3 that

$$\begin{aligned} x_{(0,\ \frac{1}{N})}(\tau)\circ T &= \frac{g_2(T(\tau))g_3(T(\tau))\wp(\frac{1}{N};\ [T(\tau),\ 1])}{\Delta(T(\tau))}\\ &= \frac{g_2(\tau)g_3(\tau)\wp(\frac{1}{N};\ [\tau+1,\ 1])}{\Delta(\tau)}\\ &= \frac{g_2(\tau)g_3(\tau)\wp(\frac{1}{N};\ [\tau,\ 1])}{\Delta(\tau)} = x_{(0,\ \frac{1}{N})}(\tau),\end{aligned}$$

from which we get $x_{(0,\ \frac{1}{N})}(\tau)\in\mathbb{C}(X_1(N))\subseteq\mathbb{C}(X_{1,\ 4}(N))$. On the other hand, if $\gamma\in\Gamma_{1,\ 4}(N)(\subseteq\Gamma_1(N))$, then γ is of the form $(\gamma_1T^{e_1})\cdots(\gamma_nT^{e_n})$ for some $\gamma_1,\cdots,\gamma_n\in\Gamma(N)$ and $e_1,\cdots,e_n\in\mathbb{Z}$ such that $e_1+\cdots+e_n\equiv 0\pmod 4$. Thus we derive from the fact $y_{(0,\ \frac{1}{N})}(\tau)\in\mathcal{F}_N$ that

$$\begin{aligned} y_{(0,\ \frac{1}{N})}(\tau)\circ\gamma &= \left(\frac{g_{(0,\ \frac{2}{N})}(\tau)}{g_{(0,\ \frac{1}{N})}(\tau)^4}\right)\circ\gamma = \left(\frac{g_{(0,\ \frac{2}{N})}(\tau)}{g_{(0,\ \frac{1}{N})}(\tau)^4}\right)\circ(\gamma_1T^{e_1})\cdots(\gamma_nT^{e_n})\\ &= \zeta_{12}^{-3(e_1+\cdots+e_n)}\frac{g_{(0,\ \frac{2}{N})}(\tau)}{g_{(0,\ \frac{1}{N})}(\tau)^4}\quad\text{by Lemma 3.1}\\ &= \frac{g_{(0,\ \frac{2}{N})}(\tau)}{g_{(0,\ \frac{1}{N})}(\tau)^4} = y_{(0,\ \frac{1}{N})}(\tau)\quad\text{by the fact } e_1+\cdots+e_n\equiv 0\pmod 4,\end{aligned}$$

which yields $y_{(0,\ \frac{1}{N})}(\tau)\in\mathbb{C}\big(X_{1,\ 4}(N)\big)$. Hence the map ι is well-defined.

Now, assume $\iota(\tau_1)=\iota(\tau_2)$ for some points $\tau_1,\ \tau_2\in\mathfrak{H}^*\setminus\{\text{cusps},\ \alpha(\zeta_3),\ \alpha(\zeta_4):\alpha\in\mathrm{SL}_2(\mathbb{Z})\}$. Then we deduce by definitions (2.6) and (3.4) that

$$j(\tau_1)=j(\tau_2),\quad f_{(0,\ \frac{1}{N})}(\tau_1)=f_{(0,\ \frac{1}{N})}(\tau_2)\quad\text{and}\quad \frac{g_{(0,\ \frac{2}{N})}(\tau_1)}{g_{(0,\ \frac{1}{N})}(\tau_1)^4}=\frac{g_{(0,\ \frac{2}{N})}(\tau_2)}{g_{(0,\ \frac{1}{N})}(\tau_2)^4}.$$

(Note that all functions $v(\tau)$, $x_{(0,\ \frac{1}{N})}(\tau)$, $y_{(0,\ \frac{1}{N})}(\tau)$ do not have poles on $\mathfrak{H}$.) So we get $\tau_2=\gamma(\tau_1)$ for some $\gamma=\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)\in\mathrm{SL}_2(\mathbb{Z})$ by the fact $j(\tau_1)=j(\tau_2)$ and Lemma 3.1(i). Moreover, it follows from the fact $f_{(0,\ \frac{1}{N})}(\tau_1)=f_{(0,\ \frac{1}{N})}(\tau_2)$ and definition (2.8) that

$$\begin{aligned}&\frac{g_2(\tau_1)g_3(\tau_1)\wp(\frac{1}{N};\ [\tau_1,\ 1])}{\Delta(\tau_1)}=\frac{g_2(\tau_2)g_3(\tau_2)\wp(\frac{1}{N};\ [\tau_2,\ 1])}{\Delta(\tau_2)}\\ =\ &\frac{g_2\big(\gamma(\tau_1)\big)g_3\big(\gamma(\tau_1)\big)\wp(\frac{1}{N};\ [\gamma(\tau_1),\ 1])}{\Delta\big(\gamma(\tau_1)\big)}=\frac{g_2(\tau_1)g_3(\tau_1)\wp(\frac{1}{N}(c\tau_1+d);\ [\tau_1,\ 1])}{\Delta(\tau_1)}\end{aligned}$$

due to Proposition 2.3 and definition (2.1). And, we achieve by Proposition 2.1(ii) and Lemma 3.1(ii)

$$\frac{1}{N}\equiv\pm\frac{1}{N}(c\tau_1+d)\pmod{[\tau_1,\ 1]},$$

from which we have $c\equiv 0\pmod N$ and $d\equiv\pm1\pmod N$. Hence the relation $\det(\gamma)=ad-bc=1$ implies $a\equiv d\equiv\pm1\pmod N$. Thus we may assume that γ belongs to the congruence subgroup $\Gamma_1(N)$ because γ and $-\gamma$ give rise to the same linear fractional transformation. On the other hand, since $\Gamma_1(N)=\big\langle\Gamma(N),\ T=\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)\big\rangle$, γ is of the form $(\gamma_1T^{e_1})\cdots(\gamma_nT^{e_n})$ for some $\gamma_1,\cdots,\gamma_n\in\Gamma(N)$ and $e_1,\cdots,e_n\in\mathbb{Z}$ such that $e_1+\cdots+e_n\equiv b\pmod N$. Furthermore, from the fact that $\frac{g_{(0,\ \frac{2}{N})}(\tau_1)}{g_{(0,\ \frac{1}{N})}(\tau_1)^4}=\frac{g_{(0,\ \frac{2}{N})}(\tau_2)}{g_{(0,\ \frac{1}{N})}(\tau_2)^4}$ and $\frac{g_{(0,\ \frac{2}{N})}(\tau)}{g_{(0,\ \frac{1}{N})}(\tau)^4}\in\mathcal{F}_N$ we derive

$$\begin{aligned}&\frac{g_{(0,\ \frac{2}{N})}(\tau_1)}{g_{(0,\ \frac{1}{N})}(\tau_1)^4}=\frac{g_{(0,\ \frac{2}{N})}(\tau_2)}{g_{(0,\ \frac{1}{N})}(\tau_2)^4}=\frac{g_{(0,\ \frac{2}{N})}\big(\gamma(\tau_1)\big)}{g_{(0,\ \frac{1}{N})}\big(\gamma(\tau_1)\big)^4}=\left(\frac{g_{(0,\ \frac{2}{N})}(\tau)}{g_{(0,\ \frac{1}{N})}(\tau)^4}\right)\circ\gamma(\tau_1)\\ =\ &\left(\frac{g_{(0,\ \frac{2}{N})}(\tau)}{g_{(0,\ \frac{1}{N})}(\tau)^4}\right)\circ(\gamma_1T^{e_1})\cdots(\gamma_nT^{e_n})(\tau_1)=\zeta_{12}^{-3(e_1+\cdots+e_n)}\frac{g_{(0,\ \frac{2}{N})}(\tau_1)}{g_{(0,\ \frac{1}{N})}(\tau_1)^4}\quad\text{by Lemma 3.1(iii).}\end{aligned}$$

Therefore $e_1+\cdots+e_n\equiv 0\pmod 4$, and so $b\equiv 0\pmod 4$ because $e_1+\cdots+e_n\equiv b\pmod N$ and $4\mid N$. We then see that γ belongs to the congruence subgroup $\Gamma_{1,\ 4}(N)$, which implies that τ_1 and τ_2 represent the same point on $X_{1,\ 4}(N)\setminus M$. This proves that the restriction morphism is indeed an embedding as desired. □

Remark 3.3. (i) Unfortunately, however, the morphism $\iota: X_{1,\ 4}(N)\to S$ is not injective. For instance, one can check it with the cusps. Indeed, let s be a cusp of width w and $\alpha=\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)$ be an element of $\mathrm{SL}_2(\mathbb{Z})$ such that $\alpha(\infty)=s$. Then we get that

$$\begin{aligned}\mathrm{ord}_s\big(v(\tau)\big)&=w\times\mathrm{ord}_{q_\tau}\big(v(\tau)\circ\alpha\big)=w\times\tfrac{1}{2}\mathrm{ord}_{q_\tau}\big((u(\tau)-1)\circ\alpha\big)\quad\text{by the relation (3.6)}\\ &=w\times\tfrac{1}{2}\mathrm{ord}_{q_\tau}\big((\tfrac{1}{2^63^3}j(\tau)-1)\circ\alpha\big)\quad\text{by definitions (3.4) and (2.6)}\\ &=w\times\tfrac{1}{2}\mathrm{ord}_{q_\tau}\big(\tfrac{1}{2^63^3}j(\tau)-1\big)\quad\text{by Proposition 2.3}\\ &=w\times\big(-\tfrac{1}{2}\big)\quad\text{by Remark 2.2(ii).}\qquad(3.7)\end{aligned}$$

And, we further obtain that

$$\begin{aligned}
&\mathrm{ord}_s\Big(y_{(0,\ \frac{1}{N})}(\tau)\Big) = w\times\mathrm{ord}_{q_\tau}\left(\frac{g_{(0,\ \frac{2}{N})}(\tau)}{g_{(0,\ \frac{1}{N})}(\tau)^4}\circ\alpha\right)\\
=&\ w\times\mathrm{ord}_{q_\tau}\left(\frac{g_{(\frac{2c}{N},\ \frac{2d}{N})}(\tau)}{g_{(\frac{c}{N},\ \frac{d}{N})}(\tau)^4}\right)\quad\text{by Lemma 3.1 because }\mathrm{SL}_2(\mathbb{Z})=\left\langle\left(\begin{smallmatrix}0&-1\\1&0\end{smallmatrix}\right),\ \left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)\right\rangle\\
=&\ w\times\Big(\tfrac{1}{2}\mathbf{B}_2\big(\langle\tfrac{2c}{N}\rangle\big)-4\cdot\tfrac{1}{2}\mathbf{B}_2\big(\langle\tfrac{c}{N}\rangle\big)\Big)\quad\text{by the formula (2.4)}\\
=&\ \begin{cases} w\times\big(\langle\frac{c}{N}\rangle-\frac{1}{4}\big) & \text{if } 0\le\langle\frac{c}{N}\rangle<\frac{1}{2}\ (\text{, so }\langle\frac{2c}{N}\rangle=2\langle\frac{c}{N}\rangle)\\ w\times\big(-\langle\frac{c}{N}\rangle+\frac{3}{4}\big) & \text{if } \frac{1}{2}\le\langle\frac{c}{N}\rangle<1\ (\text{, so }\langle\frac{2c}{N}\rangle=2\langle\frac{c}{N}\rangle-1).\end{cases}
\end{aligned}$$

It then follows

$$w\times\big(-\tfrac{1}{4}\big)\le\mathrm{ord}_s\Big(y_{(0,\ \frac{1}{N})}(\tau)\Big)\le w\times\tfrac{1}{4},\tag{3.8}$$

whose first equality holds if and only if $\langle\frac{c}{N}\rangle=0$. On the other hand, we have by (3.5) and (3.6)

$$\big(1+27v(\tau)^2\big)v(\tau)^3y_{(0,\ \frac{1}{N})}(\tau)^2=4x_{(0,\ \frac{1}{N})}(\tau)^3-\big(1+27v(\tau)^2\big)v(\tau)^2x_{(0,\ \frac{1}{N})}(\tau)-\big(1+27v(\tau)^2\big)v(\tau)^4.\tag{3.9}$$

Let $t=\mathrm{ord}_s\big(x_{(0,\ \frac{1}{N})}(\tau)\big)$ and assume $\langle\frac{c}{N}\rangle\neq0$. Observe that there exist at least two such inequivalent cusps with respect to $\Gamma_{1,\ 4}(N)$, for example $s=1,\ -1$. Then we derive by (3.7) and (3.8)

$$w\times(-3)<\mathrm{ord}_s\big(\text{LHS of (3.9)}\big).\tag{3.10}$$

In this case, if $t\neq w\times(-1)$, then one can readily check that

$$\mathrm{ord}_s\big(\text{RHS of (3.9)}\big)=\begin{cases} w\times(-3) & \text{if } t>w\times(-1)\\ 3t & \text{if } t<w\times(-1),\end{cases}$$

because $\mathrm{ord}_s(\cdot)$ is a valuation on the function field $\mathbb{C}\big(X_{1,\ 4}(N)\big)$. Hence, this fact and (3.10) lead to a contradiction to the identity (3.9), and so $t=w\times(-1)$. Therefore we claim that

$$\iota(s)=\left[\left(\frac{v(\tau)\circ\alpha}{x_{(0,\ \frac{1}{N})}(\tau)\circ\alpha}\right)\Bigg|_{q_\tau=0}:1:\left(\frac{y_{(0,\ \frac{1}{N})}(\tau)\circ\alpha}{x_{(0,\ \frac{1}{N})}(\tau)\circ\alpha}\right)\Bigg|_{q_\tau=0}:\left(\frac{1}{x_{(0,\ \frac{1}{N})}(\tau)\circ\alpha}\right)\Bigg|_{q_\tau=0}\right]=[0:1:0:0]$$

([11] Chapter V Lemma 4.2), from which we conclude that the morphism is not injective.

(ii) As for the possible zeros of $x_{(0,\ \frac{1}{N})}(\tau)$ in $\mathfrak{H}$, it is probable that the restriction morphism $\iota:\Gamma_{1,\ 4}(N)\backslash\mathfrak{H}\to S$ is injective. For example, if $N=4$, then the image of $\{\alpha(\zeta_3),\ \alpha(\zeta_4):\alpha\in\mathrm{SL}_2(\mathbb{Z})\}$ via the natural quotient map $\mathfrak{H}^*\to X_{1,\ 4}(N)$ consists of 20 points, namely

$$\Big\{\zeta_3,\ \zeta_3+1,\ \zeta_3+2,\ \zeta_3+3,\ \tfrac{1}{-\zeta_3+1},\ \tfrac{1}{-\zeta_3+2},\ \tfrac{2\zeta_3-1}{3\zeta_3+2},\ \tfrac{\zeta_3-2}{\zeta_3-1},$$
$$\zeta_4,\ \zeta_4+1,\ \zeta_4+2,\ \zeta_4+3,\ \tfrac{1}{-\zeta_4+1},\ \tfrac{1}{-\zeta_4+2},\ \tfrac{1}{-\zeta_4+3},\ \tfrac{\zeta_4+1}{\zeta_4+2},\ \tfrac{\zeta_4-1}{-\zeta_4+2},\ \tfrac{\zeta_4-2}{\zeta_4-1},\ \tfrac{\zeta_4+2}{-\zeta_4-1},\ \tfrac{2\zeta_4+1}{3\zeta_4+2}\Big\}.$$

And, by numerical computation one can show that the value of $y_{(0,\ \frac{1}{N})}(\tau)$ at each point is distinct, which implies that the restriction morphism ι is injective.

(iii) It seems that in the above proposition there should be an additional hidden relation between $v(\tau)$ and $y_{(0,\ \frac{1}{N})}(\tau)$ because $y_{(0,\ \frac{1}{N})}(\tau)$ is a modular unit(see [8] or [7]). That is, $y_{(0,\ \frac{1}{N})}(\tau)$ satisfies a monic polynomial

$$f(Y) = \prod_{\gamma \in \mathrm{Gal}(\mathcal{F}_N/\mathcal{F}_1)} \left(Y - y_{(0,\ \frac{1}{N})}(\tau)^{\gamma}\right)$$

with coefficients in $\mathbb{Q}[v(\tau)]$. If we consider $f(Y)$ as a polynomial $f(V,\ Y)$ of Y and V, then the intersection of S and a hypersurface obtained from $f(V,\ Y)$ may be a (singular) curve in $\mathbb{P}^3(\mathbb{C})$.

4. Explicit description of Shimura's reciprocity law

We shall briefly review an algorithm of determining all conjugates of the singular value of a modular function, from which we can find the conjugates of the singular values of certain Siegel functions due to [2](or [16]) and [6].

Throughout this section by K we mean an imaginary quadratic field with discriminant d_K and define

$$\theta = \begin{cases} \frac{\sqrt{d_K}}{2} & \text{for } d_K \equiv 0 \pmod 4 \\ \frac{-1+\sqrt{d_K}}{2} & \text{for } d_K \equiv 1 \pmod 4, \end{cases} \tag{4.1}$$

from which we get $\mathcal{O}_K = [\theta,\ 1]$. And, we denote by H and $K_{(N)}$ the Hilbert class field and the ray class field modulo $N\mathcal{O}_K$ over K for an integer $N \geq 1$, respectively.

Proposition 4.1. *By the main theorem of complex multiplication we derive that*

(i) $H = K\big(j(\theta)\big)$.

(ii) $K_{(N)} = K\big(h(\theta)\ :\ h \in \mathcal{F}_N$ *is defined and finite at* $\theta\big)$.

(iii) *If* $d_K \leq -7$ *and* $N \geq 2$, *then* $K_{(N)} = H\big(f_{(0,\ \frac{1}{N})}(\theta)\big)$.

Proof. See [10] Chapter 10. □

Proposition 4.2. *Let* $\min(\theta,\ \mathbb{Q}) = X^2 + B_\theta X + C_\theta \in \mathbb{Z}[X]$. *For every integer* $N \geq 2$ *the matrix group*

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

gives rise to the surjection

$$\begin{array}{ccc} W_{N,\ \theta} & \longrightarrow & \mathrm{Gal}(K_{(N)}/H) \\ \alpha & \longmapsto & \Big(h(\theta) \mapsto h^{\alpha}(\theta)\Big) \end{array}$$

where $h \in \mathcal{F}_N$ *is defined and finite at* θ. *If* $d_K \leq -7$, *then the kernel is* $\{\pm 1_2\}$.

Proof. See [2] or [16]. □

Under the properly equivalent relation, primitive positive definite quadratic forms $aX^2 + bXY + cY^2$ of discriminant d_K determine a group $\mathrm{C}(d_K)$, called the *form class group of discriminant* d_K. We identify $\mathrm{C}(d_K)$ with the set of all *reduced quadratic forms*, which are characterized by the conditions

$$-a < b \leq a < c \quad \text{or} \quad 0 \leq b \leq a = c \tag{4.2}$$

together with the discriminant relation

$$b^2 - 4ac = d_K. \tag{4.3}$$

From the above two conditions for reduced quadratic forms we deduce

$$1 \leq a \leq \sqrt{\tfrac{-d_K}{3}}. \tag{4.4}$$

As is well-known([1]) $\mathrm{C}(d_K)$ is isomorphic to $\mathrm{Gal}(H/K)$. Now, for a reduced quadratic form $Q = aX^2 + bXY + cY^2$ of discriminant d_K we define a CM-point

$$\theta_Q = \frac{-b + \sqrt{d_K}}{2a}. \tag{4.5}$$

Furthermore, we define $\beta_Q = (\beta_p)_p \in \prod_{p\,:\,\mathrm{prime}} \mathrm{GL}_2(\mathbb{Z}_p)$ as

$$\beta_p = \begin{cases} \begin{pmatrix} a & \frac{b}{2} \\ 0 & 1 \end{pmatrix} & \text{if } p \nmid a \\ \begin{pmatrix} -\frac{b}{2} & -c \\ 1 & 0 \end{pmatrix} & \text{if } p \mid a \text{ and } p \nmid c \\ \begin{pmatrix} -\frac{b}{2} - a & -\frac{b}{2} - c \\ 1 & -1 \end{pmatrix} & \text{if } p \mid a \text{ and } p \mid c \end{cases} \quad \text{for } d_K \equiv 0 \pmod 4 \tag{4.6}$$

and

$$\beta_p = \begin{cases} \begin{pmatrix} a & \frac{b-1}{2} \\ 0 & 1 \end{pmatrix} & \text{if } p \nmid a \\ \begin{pmatrix} \frac{-b-1}{2} & -c \\ 1 & 0 \end{pmatrix} & \text{if } p \mid a \text{ and } p \nmid c \\ \begin{pmatrix} \frac{-b-1}{2} - a & \frac{1-b}{2} - c \\ 1 & -1 \end{pmatrix} & \text{if } p \mid a \text{ and } p \mid c \end{cases} \quad \text{for } d_K \equiv 1 \pmod 4. \tag{4.7}$$

Proposition 4.3. *Assume $d_K \leq -7$ and $N \geq 2$. Then we have a bijective map*

$$\begin{array}{ccc} W_{N,\,\theta}/\{\pm 1_2\} \times \mathrm{C}(d_K) & \longrightarrow & \mathrm{Gal}(K_{(N)}/K) \\ (\alpha,\ Q) & \longmapsto & \Big(h(\theta) \mapsto h^{\alpha\beta_Q}(\theta_Q)\Big). \end{array}$$

Here, $h \in \mathcal{F}_N$ is defined and finite at θ. The action of α on $\mathcal{F}_N$ is the action as an element of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1_2\} \cong \mathrm{Gal}(\mathcal{F}_N/\mathcal{F}_1)$. *And, as for β_Q we note that there exists $\beta \in \mathrm{GL}_2^+(\mathbb{Q}) \cap \mathrm{M}_2(\mathbb{Z})$ such that $\beta \equiv \beta_p \pmod{N\mathbb{Z}_p}$ for all primes p dividing N by the Chinese remainder theorem. Thus the action of β_Q on $\mathcal{F}_N$ is understood as that of β which is also an element of* $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1_2\}$.

Proof. See [6] Theorem 3.4. □

We need some transformation formulas of Siegel functions to apply the above proposition.

Proposition 4.4. *Let $N \geq 2$. For $(r_1,\ r_2) \in \frac{1}{N}\mathbb{Z}^2 \setminus \mathbb{Z}^2$ the function $g_{(r_1,\ r_2)}(\tau)^{12N}$ satisfies*

$$g_{(r_1,\ r_2)}(\tau)^{12N} = g_{(-r_1,\ -r_2)}(\tau)^{12N} = g_{(\langle r_1\rangle,\ \langle r_2\rangle)}(\tau)^{12N}.$$

And, it belongs to $\mathcal{F}_N$ and α in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1_2\} \cong \mathrm{Gal}(\mathcal{F}_N/\mathcal{F}_1)$ acts on the function by

$$\Big(g_{(r_1,\ r_2)}(\tau)^{12N}\Big)^{\alpha} = g_{(r_1,\ r_2)\alpha}(\tau)^{12N}.$$

Proof. See [7] Proposition 2.4 and Theorem 2.5. □

5. Generation of ray class fields by torsion points of elliptic curves

Let K be an imaginary quadratic field with discriminant d_K and θ as in (4.1). Here, we shall construct the ray class field $K_{(N)}$ by adjoining to K some N-torsion point of certain elliptic curve, if $d_K \leq -39$, $N \geq 8$ and $4 \mid N$.

For convenience we set

$$D = \sqrt{\tfrac{-d_K}{3}} \quad \text{and} \quad A = |e^{2\pi i\theta}| = e^{-\pi\sqrt{-d_K}}.$$

Lemma 5.1. *We have the following inequalities:*

(i) *If $d_K \leq -7$, then*

$$\frac{1}{1-A^{\frac{X}{a}}} < 1 + A^{\frac{X}{1.03a}} \tag{5.1}$$

for $1 \leq a \leq D$ and all $X \geq \frac{1}{2}$.

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

Proof. (i) The inequality (5.1) is equivalent to

$$A^{\frac{X}{a}\frac{3}{103}} + A^{\frac{X}{a}} < 1.$$

Since $A = e^{-\pi\sqrt{-d_K}} \leq e^{-\pi\sqrt{7}} < 1$, $1 \leq a \leq D$ and $X \geq \frac{1}{2}$, we obtain that

$$A^{\frac{X}{a}\frac{3}{103}} + A^{\frac{X}{a}} \leq A^{\frac{1}{2D}\frac{3}{103}} + A^{\frac{1}{2D}} = e^{-\frac{\pi\sqrt{3}}{2}\frac{3}{103}} + e^{\frac{-\pi\sqrt{3}}{2}} < 1$$

by the fact $A^{\frac{1}{D}} = e^{-\pi\sqrt{3}}$. This proves (i).

(ii) Immediate.

□

Lemma 5.2. *Assume that $d_K \leq -39$ and $N \geq 8$. Let $Q = aX^2 + bXY + cY^2$ be a reduced quadratic form of discriminant d_K. If $a \geq 2$, then the inequality*

$$\left|\frac{g_{(\frac{2s}{N},\ \frac{2t}{N})}(\theta_Q)}{g_{(\frac{s}{N},\ \frac{t}{N})}(\theta_Q)^4}\right| < \left|\frac{g_{(0,\ \frac{2}{N})}(\theta)}{g_{(0,\ \frac{1}{N})}(\theta)^4}\right|.$$

holds for $(s,\ t) \in \mathbb{Z}^2$ with $(2s,\ 2t) \notin N\mathbb{Z}^2$.

Proof. We may assume $0 \leq s \leq \frac{N}{2}$ by Proposition 4.4. And, observe that $2 \leq a \leq D$ by (4.4) and $A \leq e^{-\pi\sqrt{39}} < 1$. From the Fourier expansion formula (2.3) we establish that

$$\begin{aligned}
&\left|\left(\frac{g_{(0,\ \frac{2}{N})}(\theta)}{g_{(0,\ \frac{1}{N})}(\theta)^4}\right)^{-1}\left(\frac{g_{(\frac{2s}{N},\ \frac{2t}{N})}(\theta_Q)}{g_{(\frac{s}{N},\ \frac{t}{N})}(\theta_Q)^4}\right)\right| \\
\leq\ & A^{(\frac{1}{4}-\frac{1}{4a}+\frac{s}{aN})}T(N,\ s,\ t)\prod_{n=1}^{\infty}\frac{(1+A^n)^8(1+A^{\frac{1}{a}(n+\frac{2s}{N})})(1+A^{\frac{1}{a}(n-\frac{2s}{N})})}{(1-A^n)^2(1-A^{\frac{1}{a}(n+\frac{s}{N})})^4(1-A^{\frac{1}{a}(n-\frac{s}{N})})^4} \\
\leq\ & A^{(\frac{1}{4}-\frac{1}{4a})}T(N,\ s,\ t)\prod_{n=1}^{\infty}\frac{(1+A^n)^8(1+A^{\frac{n}{a}})(1+A^{\frac{1}{a}(n-1)})}{(1-A^n)^2(1-A^{\frac{n}{a}})^4(1-A^{\frac{1}{a}(n-\frac{1}{2})})^4} \quad \text{by the fact } 0 \leq s \leq \frac{N}{2} \\
\leq\ & A^{\frac{1}{8}}T(N,\ s,\ t)\prod_{n=1}^{\infty}\frac{(1+A^n)^8(1+A^{\frac{n}{D}})(1+A^{\frac{1}{D}(n-1)})}{(1-A^n)^2(1-A^{\frac{n}{D}})^4(1-A^{\frac{1}{D}(n-\frac{1}{2})})^4} \quad \text{by the fact } 2 \leq a \leq D
\end{aligned}$$

where

$$T(N,\ s,\ t)=\left|\frac{(1-\zeta_N)^4}{1-\zeta_N^2}\right|\left|\frac{1-e^{2\pi i(\frac{2s}{N}\theta_Q+\frac{2t}{N})}}{\left(1-e^{2\pi i(\frac{s}{N}\theta_Q+\frac{t}{N})}\right)^4}\right|=\left|\frac{(1-\zeta_N)^3}{1+\zeta_N}\right|\left|\frac{1+e^{2\pi i(\frac{s}{N}\theta_Q+\frac{t}{N})}}{\left(1-e^{2\pi i(\frac{s}{N}\theta_Q+\frac{t}{N})}\right)^3}\right|.$$

If $s=0$, then

$$T(N,\ s,\ t)=\left|\left(\frac{1-\zeta_N}{1-\zeta_N^t}\right)^3\right|\left|\frac{1+\zeta_N^t}{1+\zeta_N}\right|=\left|\left(\frac{\sin\frac{\pi}{N}}{\sin\frac{t\pi}{N}}\right)^3\right|\left|\frac{\cos\frac{t\pi}{N}}{\cos\frac{\pi}{N}}\right|\leq 1.$$

If $s\neq 0$, then

$$\begin{aligned} T(N,\ s,\ t) &\leq \left|\frac{(1-\zeta_N)^3}{1+\zeta_N}\right|\frac{1+A^{\frac{1}{Na}}}{(1-A^{\frac{1}{Na}})^3} \quad \text{by the fact } 1\leq s\leq\frac{N}{2}\\ &\leq \left|\frac{(1-\zeta_N)^3}{1+\zeta_N}\right|\frac{1+A^{\frac{1}{ND}}}{(1-A^{\frac{1}{ND}})^3} \quad \text{by the fact } 2\leq a\leq D\\ &= \frac{4\sin^3\frac{\pi}{N}}{\cos\frac{\pi}{N}}\frac{1+e^{-\frac{\pi\sqrt{3}}{N}}}{(1-e^{-\frac{\pi\sqrt{3}}{N}})^3} \quad \text{by the fact } A^{\frac{1}{D}}=e^{-\pi\sqrt{3}}\\ &< 3.05 \quad \text{from the graph on } N\geq 8. \end{aligned}$$

Therefore we achieve that

$$\begin{aligned} &\left|\left(\frac{g_{(0,\ \frac{2}{N})}(\theta)}{g_{(0,\ \frac{1}{N})}(\theta)^4}\right)^{-1}\left(\frac{g_{(\frac{2s}{N},\ \frac{2t}{N})}(\theta_Q)}{g_{(\frac{s}{N},\ \frac{t}{N})}(\theta_Q)^4}\right)\right|\\ <\ & 3.05A^{\frac{1}{8}}\prod_{n=1}^{\infty}\frac{(1+A^n)^8(1+A^{\frac{n}{D}})(1+A^{\frac{1}{D}(n-1)})}{(1+A^{\frac{n}{1.03}})^{-2}(1+A^{\frac{n}{1.03D}})^{-4}(1+A^{\frac{1}{1.03D}(n-\frac{1}{2})})^{-4}} \quad \text{by Lemma 5.1(i)}\\ <\ & 3.05A^{\frac{1}{8}}\prod_{n=1}^{\infty}e^{8A^n+A^{\frac{n}{D}}+A^{\frac{1}{D}(n-1)}+2A^{\frac{n}{1.03}}+4A^{\frac{n}{1.03D}}+4A^{\frac{1}{1.03D}(n-\frac{1}{2})}} \quad \text{by Lemma 5.1(ii)}\\ =\ & 3.05A^{\frac{1}{8}}e^{\frac{8A}{1-A}+\frac{A^{\frac{1}{D}}}{1-A^{\frac{1}{D}}}+\frac{1}{1-A^{\frac{1}{D}}}+\frac{2A^{\frac{1}{1.03}}}{1-A^{\frac{1}{1.03}}}+\frac{4A^{\frac{1}{1.03D}}}{1-A^{\frac{1}{1.03D}}}+\frac{4A^{\frac{1}{2.06D}}}{1-A^{\frac{1}{1.03D}}}}\\ <\ & 1 \quad \text{by the facts } A\leq e^{-\pi\sqrt{39}} \text{ and } A^{\frac{1}{D}}=e^{-\pi\sqrt{3}}. \end{aligned}$$

This proves the lemma. □

Now we are ready to prove our main theorem of generating ray class fields.

Theorem 5.3. *Let K be an imaginary quadratic field with $d_K\leq -39$ and $N\geq 8$. Then*

$$K_{(N)}=K\left(x_{(0,\ \frac{1}{N})}(\theta),\ y_{(0,\ \frac{1}{N})}(\theta)^{\frac{4}{\gcd(4,\ N)}}\right).$$

In particular, if $4\mid N$ then $K_{(N)}$ is generated by adjoining to K the N-torsion point

$$P=\left(x_{(0,\ \frac{1}{N})}(\theta),\ y_{(0,\ \frac{1}{N})}(\theta)\right) \tag{5.2}$$

of the elliptic curve

$$u(\theta)v(\theta)^3y^2=4x^3-u(\theta)v(\theta)^2x-u(\theta)v(\theta)^4. \tag{5.3}$$

Proof. Since $x_{(0,\ \frac{1}{N})}(\tau) \in \mathcal{F}_N$ by definition (2.9) and $y_{(0,\ \frac{1}{N})}(\tau)^{\frac{4}{\gcd(4,\ N)}} \in \mathcal{F}_N$ by Proposition 2.6, their singular values $x_{(0,\ \frac{1}{N})}(\theta)$ and $y_{(0,\ \frac{1}{N})}(\theta)^{\frac{4}{\gcd(4,\ N)}}$ lie in $K_{(N)}$ by Proposition 4.1(ii). Assume that any element $(\alpha,\ Q) \in W_{N,\ \theta}/\{\pm 1_2\} \times \mathrm{C}(d_K)$ fixes both $x_{(0,\ \frac{1}{N})}(\theta)$ and $y_{(0,\ \frac{1}{N})}(\theta)^{\frac{4}{\gcd(4,\ N)}}$. Then we derive by Propositions 4.3 and 4.4 that

$$y_{(0,\ \frac{1}{N})}(\theta)^{12N} = \left(y_{(0,\ \frac{1}{N})}(\theta)^{12N}\right)^{(\alpha,\ Q)} = \frac{g_{(0,\ \frac{2}{N})\alpha\beta_Q}(\theta_Q)^{12N}}{g_{(0,\ \frac{1}{N})\alpha\beta_Q}(\theta_Q)^{48N}} = \frac{g_{(\frac{2s}{N},\ \frac{2t}{N})}(\theta_Q)^{12N}}{g_{(\frac{s}{N},\ \frac{t}{N})}(\theta_Q)^{48N}}$$

for some $(s,\ t) \in \mathbb{Z}^2$ with $(2s,\ 2t) \notin N\mathbb{Z}^2$. This yields

$$\left|\frac{g_{(0,\ \frac{2}{N})}(\theta)}{g_{(0,\ \frac{1}{N})}(\theta)^4}\right| = \left|\frac{g_{(\frac{2s}{N},\ \frac{2t}{N})}(\theta_Q)}{g_{(\frac{s}{N},\ \frac{t}{N})}(\theta_Q)^4}\right|.$$

Then it follows from Lemma 5.2 and the conditions (4.2) and (4.3) for reduced quadratic forms that

$$Q = \begin{cases} X^2 - \frac{d_K}{4}Y^2 & \text{for } d_K \equiv 0 \pmod 4 \\ X^2 + XY + \frac{1-d_K}{4}Y^2 & \text{for } d_K \equiv 1 \pmod 4), \end{cases}$$

and hence $\beta_Q = 1_2$ by (4.6) and (4.7), and $\theta_Q = \theta$ by (4.5). We then obtain by Propositions 4.3 and 4.2 that

$$x_{(0,\ \frac{1}{N})}(\theta) = \left(x_{(0,\ \frac{1}{N})}(\theta)\right)^{(\alpha,\ Q)} = x_{(0,\ \frac{1}{N})}^{\alpha\beta_Q}(\theta_Q) = x_{(0,\ \frac{1}{N})}^{\alpha}(\theta) = \left(x_{(0,\ \frac{1}{N})}(\theta)\right)^{\alpha}.$$

Hence α should be the identity in $W_{N,\ \theta}/\{\pm 1_2\}$ because $x_{(0,\ \frac{1}{N})}(\theta)$ generates $K_{(N)}$ over H by Proposition 4.1(iii). Therefore $(\alpha,\ Q)$ represents the identity in $\mathrm{Gal}(K_{(N)}/K)$, which proves that the singular values $x_{(0,\ \frac{1}{N})}(\theta)$ and $y_{(0,\ \frac{1}{N})}(\theta)^{\frac{4}{\gcd(4,\ N)}}$ indeed generate $K_{(N)}$ over K.

On the other hand, Proposition 2.1(ii) implies that $u(\theta),\ v(\theta) \neq 0$, and hence the equation in (5.3) represents an elliptic curve. And, (3.5) shows that the point P in (5.2) lies on the elliptic curve as N-torsion point. The proof of the remaining part of the theorem (the case $4 \mid N$) is the same as that of the first part. □

6. Primitive generators of ray class fields

In this last section we shall show that some ray class invariants of imaginary quadratic fields can be constructed from the y-coordinate of the elliptic curve in (5.3) by utilizing the idea of Schertz([13]).

Let K be an imaginary quadratic field with discriminant d_K and θ as in (4.1). For a nonzero integral ideal $\mathfrak{f}$ of K we denote by $\mathrm{Cl}(\mathfrak{f})$ the ray class group of conductor $\mathfrak{f}$ and write C_0 for its unit class. By definition the ray class field $K_{\mathfrak{f}}$ modulo $\mathfrak{f}$ of K is a finite abelian extension of K whose Galois group is isomorphic to $\mathrm{Cl}(\mathfrak{f})$ via the (inverse of) Artin map. If $\mathfrak{f} \neq \mathcal{O}_K$ and $C \in \mathrm{Cl}(\mathfrak{f})$, then we take an integral ideal $\mathfrak{c}$ in C so that $\mathfrak{f}\mathfrak{c}^{-1} = [z_1,\ z_2]$ with $z = \frac{z_1}{z_2} \in \mathfrak{H}$. Now we define the *Siegel-Ramachandra invariant* by

$$g_{\mathfrak{f}}(C) = g_{(\frac{a}{N},\ \frac{b}{N})}(z)^{12N}$$

where N is the smallest positive integer in $\mathfrak{f}$ and $a,\ b \in \mathbb{Z}$ such that $1 = \frac{a}{N}z_1 + \frac{b}{N}z_2$. This value depends only on the class C and belongs to $K_{\mathfrak{f}}$. Furthermore, we have a well-known transformation formula

$$g_{\mathfrak{f}}(C_1)^{\sigma(C_2)} = g_{\mathfrak{f}}(C_1C_2) \tag{6.1}$$

for $C_1,\ C_2 \in \mathrm{Cl}(\mathfrak{f})$ where σ is the Artin map([8] Chapter 11 Section 1).

Let χ be a character of $\mathrm{Cl}(\mathfrak{f})$. We then denote by $\mathfrak{f}_\chi$ the conductor of χ and let χ_0 be the proper character of $\mathrm{Cl}(\mathfrak{f}_\chi)$ corresponding to χ. For a nontrivial character χ of $\mathrm{Cl}(\mathfrak{f})$ with $\mathfrak{f} \neq \mathcal{O}_K$ we define the Stickelberger element and the L-function as follows:

$$S_\mathfrak{f}(\chi,\ g_\mathfrak{f}) = \sum_{C \in \mathrm{Cl}(\mathfrak{f})} \chi(C) \log |g_\mathfrak{f}(C)| \quad \text{and} \quad L_\mathfrak{f}(s,\ \chi) = \sum_{\substack{\mathfrak{a} \neq 0\ :\ \text{integral ideals} \\ \gcd(\mathfrak{a},\ \mathfrak{f}) = \mathcal{O}_K}} \frac{\chi(\mathfrak{a})}{\mathbf{N}_{K/\mathbb{Q}}(\mathfrak{a})^s} \quad (s \in \mathbb{C}).$$

If $\mathfrak{f}_\chi \neq \mathcal{O}_K$, then we see from the second Kronecker limit formula that

$$L_{\mathfrak{f}_\chi}(1,\ \chi_0) = T_0 S_{\mathfrak{f}_\chi}(\overline{\chi}_0,\ g_{\mathfrak{f}_\chi})$$

where T_0 is certain nonzero constant depending on χ_0([10] Chapter 22 Theorem 2). Here we observe that the value $L_{\mathfrak{f}_\chi}(1,\ \chi_0)$ is nonzero([5] Chapter IV Proposition 5.7). Moreover, multiplying the above relation by the Euler factor we derive the identity

$$\prod_{\mathfrak{p} | \mathfrak{f},\ \mathfrak{p} \nmid \mathfrak{f}_\chi} \big(1 - \overline{\chi}_0(\mathfrak{p})\big) L_{\mathfrak{f}_\chi}(1,\ \chi_0) = T S_\mathfrak{f}(\overline{\chi},\ g_\mathfrak{f}) \tag{6.2}$$

where T is certain nonzero constant depending on $\mathfrak{f}$ and χ([8] Chapter 11 Section 2 LF 2).

Lemma 6.1. *Let $\mathfrak{f}$ be an integral ideal of K. Then we have the degree formula*

$$[K_\mathfrak{f} : K] = \frac{h_K \phi(\mathfrak{f}) w(\mathfrak{f})}{w_K}$$

where h_K is the class number, ϕ is the Euler function for ideals, namely

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

for a power of prime ideal $\mathfrak{p}$ (and we set $\phi(\mathcal{O}_K) = 1$), $w(\mathfrak{f})$ is the number of roots of unity in K which are $\equiv 1 \pmod{\mathfrak{f}}$ and w_K is the number of roots of unity in K.

Proof. See [9] Chapter VI Theorem 1. ☐

Theorem 6.2. *Let $\mathfrak{f} \neq \mathcal{O}_K$ be an integral ideal of K with prime ideal factorization*

$$\mathfrak{f} = \prod_{k=1}^{n} \mathfrak{p}_k^{e_k}.$$

Assume that

$$[K_\mathfrak{f} : K] > 2 \sum_{k=1}^{n} [K_{\mathfrak{f}\mathfrak{p}_k^{-e_k}} : K]. \tag{6.3}$$

Then the singular value

$$\varepsilon = \frac{g_\mathfrak{f}(C')}{g_\mathfrak{f}(C_0)^4} \quad \textit{for any class } C' \in \mathrm{Cl}(\mathfrak{f})$$

generates $K_\mathfrak{f}$ over K.

Proof. We identify $\mathrm{Cl}(\mathfrak{f})$ with $\mathrm{Gal}(K_\mathfrak{f}/K)$ via the Artin map. Setting $F = K(\varepsilon)$ we derive that

$$\begin{aligned} & \#\big\{\chi \text{ of } \mathrm{Gal}(K_\mathfrak{f}/K) :\ \chi|_{\mathrm{Gal}(K_\mathfrak{f}/F)} \neq 1\big\} \qquad (6.4) \\ = \ & \#\big\{\chi \text{ of } \mathrm{Gal}(K_\mathfrak{f}/K)\big\} - \#\big\{\chi \text{ of } \mathrm{Gal}(K_\mathfrak{f}/K)\ :\ \chi|_{\mathrm{Gal}(K_\mathfrak{f}/F)} = 1\big\} \\ = \ & \#\big\{\chi \text{ of } \mathrm{Gal}(K_\mathfrak{f}/K)\big\} - \#\big\{\chi \text{ of } \mathrm{Gal}(F/K)\big\} = [K_\mathfrak{f} : K] - [F : K]. \end{aligned}$$

Furthermore, we have

$$\begin{aligned} & \#\{\chi \text{ of } \mathrm{Gal}(K_{\mathfrak{f}}/K) \;:\; \mathfrak{p}_k \nmid \mathfrak{f}_\chi \text{ for some } k\} \\ = \;& \#\{\chi \text{ of } \mathrm{Gal}(K_{\mathfrak{f}}/K) \;:\; \mathfrak{f}_\chi \mid \mathfrak{f}\mathfrak{p}_k^{-e_k} \text{ for some } k\} \\ \leq \;& \sum_{k=1}^{n} \#\{\chi \text{ of } \mathrm{Gal}(K_{\mathfrak{f}\mathfrak{p}_k^{-e_k}}/K)\} = \sum_{k=1}^{n} [K_{\mathfrak{f}\mathfrak{p}_k^{-e_k}} : K]. \end{aligned} \tag{6.5}$$

Now, suppose that F is properly contained in $K_{\mathfrak{f}}$. Then we get from the hypothesis (6.3) that

$$[K_{\mathfrak{f}} : K] - [F : K] = [K_{\mathfrak{f}} : K]\left(1 - \frac{1}{[K_{\mathfrak{f}} : F]}\right) > 2\sum_{k=1}^{n} [K_{\mathfrak{f}\mathfrak{p}_k^{-e_k}} : K]\left(1 - \frac{1}{2}\right) = \sum_{k=1}^{n} [K_{\mathfrak{f}\mathfrak{p}_k^{-e_k}} : K].$$

Thus there exists a character ψ of $\mathrm{Gal}(K_{\mathfrak{f}}/K)$ such that

$$\psi|_{\mathrm{Gal}(K_{\mathfrak{f}}/F)} \neq 1 \quad \text{and} \quad \mathfrak{p}_k \mid \mathfrak{f}_\psi \text{ for all } k$$

by (6.4) and (6.5). Hence we obtain by (6.2)

$$0 \neq L_{\mathfrak{f}_\psi}(1,\ \psi_0) = TS_{\mathfrak{f}}(\overline{\psi},\ g_{\mathfrak{f}}) \tag{6.6}$$

for certain nonzero constant T and the proper character ψ_0 of $\mathrm{Cl}(\mathfrak{f}_\psi)$ corresponding to ψ. On the other hand, we achieve that

$$\begin{aligned} \big(\psi(C') - 4\big)S_{\mathfrak{f}}(\overline{\psi},\ g_{\mathfrak{f}}) &= \big(\overline{\psi}(C'^{-1}) - 4\big) \sum_{C \in \mathrm{Cl}(\mathfrak{f})} \overline{\psi}(C) \log|g_{\mathfrak{f}}(C)| \\ &= \sum_{C \in \mathrm{Cl}(\mathfrak{f})} \overline{\psi}(C) \left| \left(\frac{g_{\mathfrak{f}}(C')}{g_{\mathfrak{f}}(C_0)^4}\right)^{\sigma(C)} \right| \\ &= \sum_{\substack{C_1 \in \mathrm{Gal}(K_{\mathfrak{f}}/K) \\ C_1 \pmod{\mathrm{Gal}(K_{\mathfrak{f}}/F)}}} \sum_{C_2 \in \mathrm{Gal}(K_{\mathfrak{f}}/F)} \overline{\psi}(C_1C_2) \log|\varepsilon^{\sigma(C_1C_2)}| \\ &= \sum_{C_1} \overline{\psi}(C_1) \log|\varepsilon^{\sigma(C_1)}| \left(\sum_{C_2} \overline{\psi}(C_2)\right) \quad \text{by (6.1) and the fact } \varepsilon \in F \\ &= 0 \quad \text{by the fact } \psi|_{\mathrm{Gal}(K_{\mathfrak{f}}/F)} \neq 1, \end{aligned}$$

which contradicts (6.6) because $\psi(C') - 4 \neq 0$. Therefore $F = K_{\mathfrak{f}}$ as desired. □

Remark 6.3. Any nonzero power of ε can also generate $K_{\mathfrak{f}}$ over K in the proof of Theorem 6.2.

Corollary 6.4. *Let $N \geq 3$ be an odd integer and assume (6.3) with $\mathfrak{f} = N\mathcal{O}_K$. Then the singular value $y_{(0,\ \frac{1}{N})}(\theta)^4$ generates $K_{(N)}$ over K.*

Proof. Observe that for the unit class C_0 we have

$$g_{\mathfrak{f}}(C_0) = g_{(0,\ \frac{1}{N})}(\theta)^{12N}.$$

Since N is odd, $\alpha = \left(\begin{smallmatrix} 2 & 0 \\ 0 & 2 \end{smallmatrix}\right)$ belongs to $W_{N,\ \theta}$. Then by Propositions 4.2 and 4.4 we deduce that

$$g_{(0,\ \frac{2}{N})}(\theta)^{12N} = g_{(0,\ \frac{1}{N})\alpha}(\theta)^{12N} = \left(g_{(0,\ \frac{1}{N})}(\theta)^{12N}\right)^{\alpha} = g_{\mathfrak{f}}(C_0)^{\sigma(C')}$$

for some $C' \in \mathrm{Cl}(\mathfrak{f})$. Therefore the singular value

$$y_{(0,\ \frac{1}{N})}(\theta)^{12N} = \frac{g_{(0,\ \frac{2}{N})}(\theta)^{12N}}{g_{(0,\ \frac{1}{N})}(\theta)^{48N}} = \frac{g_{\mathfrak{f}}(C')}{g_{\mathfrak{f}}(C_0)^4}$$

generates $K_{\mathfrak{f}} = K_{(N)}$ over K by Theorem 6.2. Since $y_{(0,\ \frac{1}{N})}(\theta)^{\frac{4}{\gcd(4,\ N)}}$ belongs to $K_{(N)}$, it also generates $K_{(N)}$ over K. □

Remark 6.5. Let K be an imaginary quadratic field with $d_K \leq -7$ and $N(\geq 3)$ be an odd integer.

(i) Suppose that $N = p^n (n \geq 1)$ where p is an odd prime which is inert or ramified in $K/\mathbb{Q}$. One can derive by Lemma 6.1 that

$$[K_{(N)} : K] = \begin{cases} \frac{h_K(p^2-1)p^{2(n-1)}}{2} \geq \frac{h_K(3^2-1)3^{2\cdot 0}}{2} > 2h_K & \text{if } p \text{ is inert in } K/\mathbb{Q} \\ \frac{h_K(p-1)p^{2n-1}}{2} \geq \frac{h_K(3-1)3^{2\cdot 1-1}}{2} > 2h_K & \text{if } p \text{ is ramified in } K/\mathbb{Q}. \end{cases}$$

Thus $\mathfrak{f} = N\mathcal{O}_K$ satisfies the condition (6.3) and hence we are able to apply Corollary 6.4 for such N.

(ii) Suppose, in general

$$\mathfrak{f} = N\mathcal{O}_K = \prod_{k=1}^{n} \mathfrak{p}_k^{e_k} \quad \text{with } n \geq 2.$$

Then it follows from Lemma 6.1 that the condition (6.3) is equivalent to

$$\frac{1}{2} > \sum_{k=1}^{n} \frac{1}{\phi(\mathfrak{p}_k^{e_k})}. \tag{6.7}$$

Therefore one can also apply Corollary 6.4 under the assumption (6.7).

References

1. D. A. Cox, *Primes of the form $x^2 + ny^2$: Fermat, Class Field, and Complex Multiplication*, John Wiley & Sons, Inc., 1989.
2. A. Gee, *Class invariants by Shimura's reciprocity law*, J. Theor. Nombres Bordeaux 11 (1999), no. 1, 45-72.
3. K. J. Hong and J. K. Koo, *Singular values of some modular functions and their applications to class fields*, Ramanujan J. 16 (2008), no. 3, 321-337.
4. 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), no. 1, 167-175.
5. G. J. Janusz, *Algebraic Number Fields*, Academic Press, 1973.
6. H. Y. Jung, J. K. Koo and D. H. Shin, *On some ray class invariants over imaginary quadratic fields*, submitted.
7. J. K. Koo and D. H. Shin, *On some arithmetic properties of Siegel functions*, Math. Zeit., DOI 10.1007/s00209-008-0456-9.
8. D. Kubert and S. Lang, *Modular Units*, Grundlehren der mathematischen Wissenschaften 244, Spinger-Verlag, 1981.
9. S. Lang, *Algebraic Number Theory, 2nd edition*, Springer, 1994.
10. S. Lang, *Elliptic Functions, 2nd edition*, Spinger-Verlag, 1987.
11. R. Miranda, *Algebraic Curves and Riemann Surfaces*, AMS, 1995.
12. K. Ramachandra, *Some applications of Kronecker's limit formula*, Ann. of Math. (2) 80(1964), 104-148.
13. R. Schertz, *Construction of ray class fields by elliptic units*, J. Theor. Nombres Bordeaux 9 (1997), no. 2, 383-394.
14. G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Iwanami Shoten and Princeton University Press, 1971.
15. J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer-verlag, 1985.
16. P. Stevenhagen, *Hilbert's 12th problem, complex multiplication and Shimura reciprocity*, Class Field Theory-Its Centenary and Prospect (Tokyo, 1998), 161-176, Adv. Stud. Pure Math., 30, Math. Soc. Japan, Tokyo, 2001.

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

Department of Mathematical Sciences, KAIST
Current address: Daejeon 373-1, Korea
E-mail address: yds1850@kaist.ac.kr