J. Korean Math. Soc. **50** (2013), No. 4, pp. 847–864
http://dx.doi.org/10.4134/JKMS.2013.50.4.847

CONSTRUCTION OF CLASS FIELDS OVER IMAGINARY QUADRATIC FIELDS USING y-COORDINATES OF ELLIPTIC CURVES

Ja Kyung Koo and Dong Hwa Shin

Abstract. By a change of variables we obtain new y-coordinates of elliptic curves. Utilizing these y-coordinates as meromorphic modular functions, together with the elliptic modular function, we generate the fields of meromorphic modular functions. Furthermore, by means of the special values of the y-coordinates, we construct the ray class fields over imaginary quadratic fields as well as normal bases of these ray class fields.

1. Introduction

Let E be an elliptic curve over $\mathbb{C}$. Then there exist a lattice $\Lambda = [\omega_1, \omega_2]$ in $\mathbb{C}$ and a complex analytic isomorphism

$$\begin{array}{rcl} \mathbb{C}/\Lambda & \rightarrow & E(\mathbb{C}):\ y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda) \\ z & \mapsto & [\wp(z;\Lambda) : \wp'(z;\Lambda) : 1] \end{array} \tag{1.1}$$

of complex Lie groups, where

$$g_2(\Lambda) = 60 \sum_{\omega\in\Lambda\setminus\{0\}} 1/\omega^4, \quad g_3(\Lambda) = 140 \sum_{\omega\in\Lambda\setminus\{0\}} 1/\omega^6$$

and

$$\wp(z;\Lambda) = 1/z^2 + \sum_{\omega\in\Lambda\setminus\{0\}} (1/(z-\omega)^2 - 1/\omega^2) \quad (z \in \mathbb{C}) \tag{1.2}$$

is the Weierstrass $\wp$-function (relative to Λ) with derivative $\wp'(z;\Lambda)$ [13, Chapter VI, Proposition 3.6(b)].

Received April 16, 2012; Revised February 14, 2013.
2010 *Mathematics Subject Classification.* Primary 11G16; Secondary 11F03, 11G15, 11R37.
Key words and phrases. class field theory, complex multiplication, elliptic and modular units, modular functions.
The first author was partially supported by the NRF of Korea grant funded by MEST (2012-0000798). The second author was supported by Hankuk University of Foreign Studies Research Fund of 2013.

For an integer N (≥ 2) and a pair of rational numbers $(r_1, r_2) \in (1/N)\mathbb{Z}^2 \setminus \mathbb{Z}^2$, we define the Fricke function $f_{(r_1,r_2)}(\tau)$ on the complex upper-half plane $\mathbb{H}$ as

$$f_{(r_1,r_2)}(\tau) = -(2^7 3^5 g_2(\tau) g_3(\tau)/\Delta(\tau))\wp(r_1\tau + r_2; [\tau, 1]) \quad (\tau \in \mathbb{H}),$$

where

$$g_2(\tau) = g_2([\tau, 1]),\ g_3(\tau) = g_3([\tau, 1]) \ \text{ and } \ \Delta(\tau) = g_2(\tau)^3 - 27g_3(\tau)^2. \tag{1.3}$$

This belongs to the field $\mathcal{F}_N$ of all meromorphic modular functions of level N whose Fourier coefficients with respect to $q_\tau^{1/N} = e^{2\pi i\tau/N}$ lie in the Nth cyclotomic field $\mathbb{Q}(\zeta_N)$, where $\zeta_N = e^{2\pi i/N}$. We further define the elliptic modular function $j(\tau)$ as

$$j(\tau) = 1728 g_2(\tau)^3/\Delta(\tau) \quad (\tau \in \mathbb{H}),$$

which is a generator of $\mathcal{F}_1$ over $\mathbb{Q}$ [10, Chaper 6].

Let K be an imaginary quadratic field of discriminant d_K. We denote its ring of algebraic integers by $\mathcal{O}_K$ and set

$$\theta_K = \begin{cases} \sqrt{d_K}/2 & \text{if } d_K \equiv 0 \pmod 4, \\ (-1+\sqrt{d_K})/2 & \text{if } d_K \equiv 1 \pmod 4 \end{cases} \tag{1.4}$$

so that $\theta_K \in \mathbb{H}$ and $\mathcal{O}_K = [\theta_K, 1]$. For a positive integer N, let $K_{(N)}$ be the ray class field modulo (N) $(= N\mathcal{O}_K)$ of K. Then the main theorem of complex multiplication implies that

$$K_{(N)} = K(f(\theta_K)\ ;\ f \in \mathcal{F}_N \text{ is defined and finite at } \theta_K) \tag{1.5}$$

$$= K(j(\theta_K), h_N(\theta_K)), \tag{1.6}$$

where

$$h_N(\theta_K) = \begin{cases} (g_2(\theta_K)^2/\Delta(\theta_K))\wp(1/N; \mathcal{O}_K)^2 & \text{if } K = \mathbb{Q}(\sqrt{-1}), \\ (g_3(\theta_K)/\Delta(\theta_K))\wp(1/N; \mathcal{O}_K)^3 & \text{if } K = \mathbb{Q}(\sqrt{-3}), \\ (g_2(\theta_K)g_3(\theta_K)/\Delta(\theta_K))\wp(1/N; \mathcal{O}_K) & \text{otherwise} \end{cases}$$

([6] or [10, Chapter 10, Theorems 2, 8 and their Corollaries]). Furthermore, Cho and Koo [1] combined these two generators, $j(\theta_K)$ and $h_N(\theta_K)$, by using the result of Gross and Zagier [5] and Dorman [4] to obtain a primitive generator of $K_{(N)}$ over K. Note that the value $h_N(\theta_K)$ comes from the x-coordinate of some N-torsion point of the elliptic curve (1.1) with $\Lambda = [\theta_K, 1]$. However, it is not known that $h_N(\theta_K)$ alone generates $K_{(N)}$ over K. On the other hand, Jung et al. [7] showed that the special value $g_{(0,1/N)}(\theta_K)^{12N}$ generates $K_{(N)}$ over K (§2), conjectured by Lang [10, p. 292] and Schertz [11]. But unfortunately, the value is not directly related to a torsion point of an elliptic curve.

Consider the special case when $K = \mathbb{Q}(\sqrt{-3})$ and $\theta_K = (-1+\sqrt{-3})/2$. Setting $\Lambda = [\theta_K, 1]$ and $z = 1/N$ $(N \geq 2)$ in (1.1), one can derive that

$$\begin{aligned} &(g_3(\theta_K)/\sqrt{\Delta(\theta_K)})\wp'(1/N; \mathcal{O}_K)^2/\sqrt{\Delta(\theta_K)} \\ &\quad = 4(g_3(\theta_K)/\Delta(\theta_K))\wp(1/N; \mathcal{O}_K)^3 - (g_2(\theta_K)g_3(\theta_K)/\Delta(\theta_K))\wp(1/N; \mathcal{O}_K) \end{aligned} \tag{1.7}$$

$$- g_3(\theta_K)^2/\Delta(\theta_K).$$

Moreover, we get from the fact $g_2(\theta_K) = 0$ [10, p. 37] and the definition (1.3) that

$$j(\theta_K) = 0 \quad \text{and} \quad g_3(\theta_K)/\sqrt{\Delta(\theta_K)} = \pm 1/3\sqrt{-3}.$$

Hence the equation (1.7) becomes

$$\pm(1/3\sqrt{-3})\wp'(1/N; \mathcal{O}_K)^2/\sqrt{\Delta(\theta_K)} = 4h_N(\theta_K) + 1/27,$$

which shows that the value $\wp'(1/N; \mathcal{O}_K)^2/\sqrt{\Delta(\theta_K)}$ generates $K_{(N)}$ over K by (1.6).

Let $\eta(\tau)$ be the Dedekind η-function defined by

$$\eta(\tau) = \sqrt{2\pi}\zeta_8 q_\tau^{1/24} \prod_{n=1}^{\infty}(1 - q_\tau^n) \quad (\tau \in \mathbb{H}). \tag{1.8}$$

This satisfies the relation $\eta(\tau)^{24} = \Delta(\tau)$ [10, Chapter 18, Theorem 5]. In this paper we shall prove that if $d_K \leq -19$ and $N \geq 3$, then any nonzero power of the value

$$y = (\wp'(1/N; \mathcal{O}_K)/\eta(\theta_K)^6)^{4/\gcd(4,N)}$$

generates $K_{(N)}$ over K (Theorem 3.4) by using the idea of [7]. The value y is obtained from certain y-coordinate of an elliptic curve associated with $\mathcal{O}_K$, and is suitable for computing the minimal polynomial because it can be expressed as an infinite product (§2). As an application we shall also find a normal basis of $K_{(N)}$ over K (Corollary 3.9).

2. Fields of modular functions

In this section we shall examine the fields of modular functions in terms of y-coordinates of elliptic curves together with the elliptic modular function $j(\tau)$.

For a positive integer N, let $\mathbb{C}(X(N))$ be the field of meromorphic functions on the modular curve $X(N) = \Gamma(N)\backslash\mathbb{H}^*$, where $\mathbb{H}^* = \mathbb{H} \cup \mathbb{Q} \cup \{\infty\}$. As is well-known, $\mathbb{C}(X(N))$ is a Galois extension of $\mathbb{C}(X(1)) = \mathbb{C}(j(\tau))$ whose Galois group is given by

$$\Gamma(1)/\pm\Gamma(N) \simeq \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I_2\}$$

as fractional linear transformations [3, Proposition 7.5.1]. Furthermore, the subfield $\mathcal{F}_N$ of $\mathbb{C}(X(N))$ is a Galois extension of $\mathcal{F}_1$ whose Galois group is represented by

$$\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I_2\} = G_N \cdot \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I_2\} = \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I_2\} \cdot G_N,$$

where

$$G_N = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix} : d \in (\mathbb{Z}/N\mathbb{Z})^* \right\}.$$

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

$$\sum_{n>-\infty}^{\infty} c_n q_\tau^{n/N}\mapsto \sum_{n>-\infty}^{\infty} c_n^{\sigma_d} q_\tau^{n/N},$$

where σ_d is the automorphism of $\mathbb{Q}(\zeta_N)$ induced by $\zeta_N\mapsto\zeta_N^d$. Second, for an element $\gamma\in\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I_2\}$, let $\gamma'\in\mathrm{SL}_2(\mathbb{Z})$ be a preimage of γ via the natural surjection $\mathrm{SL}_2(\mathbb{Z})\to\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I_2\}$. Then γ acts on $h\in\mathcal{F}_N$ by

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

([10, Chapter 6, Theorem 3] or [12, Proposition 6.9(1)]).

For a lattice Λ in $\mathbb{C}$, the Weierstrass σ-function (relative to Λ) is defined by

$$\sigma(z;\Lambda)=z\prod_{\omega\in\Lambda\setminus\{0\}}(1-z/\omega)e^{z/\omega+(1/2)(z/\omega)^2}\quad(z\in\mathbb{C}).$$

Taking the logarithmic derivative, we define the Weierstrass ζ-function (relative to Λ) as

$$\zeta(z;\Lambda)=\sigma'(z;\Lambda)/\sigma(z;\Lambda)=1/z+\sum_{\omega\in\Lambda\setminus\{0\}}(1/(z-\omega)+1/\omega+z/\omega^2)\quad(z\in\mathbb{C}).$$

Differentiating the function $\zeta(z+\omega;\Lambda)-\zeta(z;\Lambda)$ for any $\omega\in\Lambda$ results in 0 since $\zeta'(z;\Lambda)=-\wp(z;\Lambda)$, by (1.2) and $\wp(z;\Lambda)$, is periodic with respect to Λ. Hence there is a constant $\eta(\omega;\Lambda)$ so that

$$\zeta(z+\omega;\Lambda)=\zeta(z;\Lambda)+\eta(\omega;\Lambda).$$

For $(r_1,r_2)\in\mathbb{Q}^2\setminus\mathbb{Z}^2$, we define the Siegel function $g_{(r_1,r_2)}(\tau)$ as

(2.1)

$$g_{(r_1,r_2)}(\tau)=e^{-(1/2)(r_1\eta(\tau;[\tau,1])+r_2\eta(1;[\tau,1]))(r_1\tau+r_2)}\sigma(r_1\tau+r_2;[\tau,1])\eta(\tau)^2\ (\tau\in\mathbb{H}),$$

where $\eta(\tau)$ is the Dedekind η-function defined in (1.8).

Proposition 2.1. *Let $(r_1,r_2)\in\mathbb{Q}^2\setminus\mathbb{Z}^2$.*

(i) *We have*

$$g_{(-r_1,-r_2)}(\tau)=-g_{(r_1,r_2)}(\tau).$$

(ii) *If $\gamma\in\mathrm{SL}_2(\mathbb{Z})$, then*

$$g_{(r_1,r_2)}(\tau)\circ\gamma=\zeta g_{(r_1,r_2)\gamma}(\tau)$$

for a 12th root of unity ζ depending on γ and (r_1,r_2).

(iii) *If $(s_1,s_2)\in\mathbb{Z}^2$, then*

$$g_{(r_1+s_1,r_2+s_2)}(\tau)=\varepsilon((r_1,r_2),(s_1,s_2))g_{(r_1,r_2)}(\tau),$$

where $\varepsilon((r_1,r_2),(s_1,s_2))=(-1)^{s_1s_2+s_1+s_2}e^{-\pi i(s_1r_2-s_2r_1)}$.

Proof. See [9, Chapter 2, §1] and [10, Chapter 18, Theorem 6]. ☐

A Siegel function has a fairly simple q_τ-order formula. Let

$$\mathbf{B}_2(X) = X^2 - X + 1/6$$

be the second Bernoulli polynomial. Using the product formula of the Weierstrass σ-function, we get the product expression

$$g_{(r_1,r_2)}(\tau) = -q_\tau^{(1/2)\mathbf{B}_2(r_1)} e^{\pi i r_2(r_1-1)}(1-q_z)\prod_{n=1}^{\infty}(1-q_\tau^n q_z)(1-q_\tau^n/q_z), \tag{2.2}$$

where $z = r_1\tau + r_2$ [10, Chapter 18, Theorem 4 and Chapter 19, §2]. Regarding (2.2) as a Laurent series expansion with respect to q_τ, we see that

$$\mathrm{ord}_{q_\tau}(g_{(r_1,r_2)}(\tau)) = (1/2)\mathbf{B}_2(\langle r_1\rangle) \quad (\in \mathbb{Q}), \tag{2.3}$$

where $\langle X\rangle$ is the fractional part of $X \in \mathbb{R}$ such that $0 \le \langle X\rangle < 1$ [9, Chapter 2, §1].

Proposition 2.2. *Let N (≥ 2) be an integer and let $\{m(r)\}_{r=(r_1,r_2)\in(1/N)\mathbb{Z}^2\setminus\mathbb{Z}^2}$ be a family of integers such that $m(r) = 0$ except for finitely many r. Then a product of Siegel functions*

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

belongs to $\mathcal{F}_N$ if $\{m(r)\}_r$ satisfies the quadratic relation modulo N, namely,

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

and 12 divides $\gcd(12,N)\cdot\sum_r m(r)$. In particular, $g_r(\tau)^{12N/\gcd(6,N)}$ belongs to $\mathcal{F}_N$ for any $r \in (1/N)\mathbb{Z}^2\setminus\mathbb{Z}^2$.

Proof. See [9, Chapter 3, Theorems 5.2 and 5.3]. □

Proposition 2.3. *Let N (≥ 2) be an integer and let $r \in (1/N)\mathbb{Z}^2\setminus\mathbb{Z}^2$.*

(i) *Both $g_r(\tau)$ and $N/g_r(\tau)$ are integral over $\mathbb{Z}[j(\tau)]$.*

(ii) *If $\alpha \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I_2\} \simeq \mathrm{Gal}(\mathcal{F}_N/\mathcal{F}_1)$, then*

$$(g_r(\tau)^{12N/\gcd(6,N)})^\alpha = g_{r\alpha}(\tau)^{12N/\gcd(6,N)}.$$

Proof. (i) See [8, §3].

(ii) This follows from Proposition 2.1 and (2.2). □

Let Λ be a lattice in $\mathbb{C}$ of the form $\Lambda = [\tau, 1]$ with $\tau \in \mathbb{H}$. Diving both sides of the equation

$$\wp'(z;\Lambda)^2 = 4\wp(z;\Lambda)^3 - g_2(\tau)\wp(z;\Lambda) - g_3(\tau)$$

by the nonzero constant $\eta^{12}(\tau)$ and using the relation

$$\wp'(z;\Lambda) = -\sigma(2z;\Lambda)/\sigma(z;\Lambda)^4$$

[13, p. 166], we get

$$\begin{aligned}&(\sigma(2z;\Lambda)\eta(\tau)^2/\sigma(z;\Lambda)^4\eta(\tau)^8)^2\\&= 4(\wp(z;\Lambda)/\eta(\tau)^4)^3-(g_2(\tau)/\eta(\tau)^8)(\wp(z;\Lambda)/\eta(\tau)^4)-g_3(\tau)/\eta(\tau)^{12}.\end{aligned}$$

Hence we obtain a change of variables

$$\begin{array}{ccc}\mathbb{C}/\Lambda & \overset{\sim}{\to} & y^2=4x^3-(g_2(\tau)/\eta(\tau)^8)x-g_3(\tau)/\eta(\tau)^{12}\\ z & \mapsto & [\wp(z;\Lambda)/\eta(\tau)^4 : \sigma(2z;\Lambda)\eta(\tau)^2/\sigma(z;\Lambda)^4\eta(\tau)^8 : 1].\end{array}$$

If $z=r_1\tau+r_2$ with $(r_1,r_2)\in\mathbb{Q}^2\setminus\mathbb{Z}^2$, then the corresponding y-coordinate satisfies

$$\sigma(2r_1\tau+2r_2;\Lambda)\eta(\tau)^2/\sigma(r_1\tau+r_2;\Lambda)^4\eta(\tau)^8=g_{(2r_1,2r_2)}(\tau)/g_{(r_1,r_2)}(\tau)^4$$

by (2.1). Regarding τ as a variable on $\mathbb{H}$, we define the function $y_{(r_1,r_2)}(\tau)$ on $\mathbb{H}$ as

$$y_{(r_1,r_2)}(\tau)=g_{(2r_1,2r_2)}(\tau)/g_{(r_1,r_2)}(\tau)^4. \tag{2.4}$$

Lemma 2.4. *Let N (≥ 2) be an integer and let $(r_1,r_2)\in(1/N)\mathbb{Z}^2\setminus\mathbb{Z}^2$. Then $y_{(r_1,r_2)}(\tau)^{4/\gcd(4,N)}$ belongs to $\mathcal{F}_N$.*

Proof. If $(2r_1,2r_2)\in\mathbb{Z}^2$, then $y_{(r_1,r_2)}(\tau)^{4/\gcd(4,N)}=0\in\mathcal{F}_N$. So we assume $(2r_1,2r_2)\notin\mathbb{Z}^2$. Now that the product of Siegel functions

$$(g_{(2r_1,2r_2)}(\tau)/g_{(r_1,r_2)}(\tau)^4)^{4/\gcd(4,N)}$$

satisfies the quadratic relation modulo N and

$$\gcd(12,N)\cdot\text{sum of exponents}=-12\gcd(12,N)/\gcd(4,N)\equiv 0 \pmod{12},$$

it belongs to $\mathcal{F}_N$ by Proposition 2.2. □

Remark 2.5. Note that a Siegel function has no zeros or poles on $\mathbb{H}$ by (2.2). Hence the special value $y_{(r_1,r_2)}(\theta_K)^{4/\gcd(4,N)}$ lies in $K_{(N)}$ by the definition (2.4), Lemma 2.4 and (1.5).

Lemma 2.6. *Let N (≥ 3) and m $(\neq 0)$ be integers. If $\gamma\in\mathrm{SL}_2(\mathbb{Z})$ acts trivially on both $y_{(1/N,0)}(\tau)^m$ and $y_{(0,1/N)}(\tau)^m$ as a fractional linear transformation, then $\gamma\in\pm\Gamma(N)$.*

Proof. For convenience, we use the notation $\doteq$ to denote the equality up to a root of unity. Letting $\gamma=\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)\in\mathrm{SL}_2(\mathbb{Z})$, we derive by the definition (2.4) and Proposition 2.1(ii) that

$$\begin{aligned}(y_{(1/N,0)}(\tau)^m)^\gamma &\doteq g_{(2/N,0)\gamma}(\tau)^m/g_{(1/N,0)\gamma}(\tau)^{4m}\\&= g_{(2a/N,2b/N)}(\tau)^m/g_{(a/N,b/N)}(\tau)^{4m},\\(y_{(0,1/N)}(\tau)^m)^\gamma &\doteq g_{(0,2/N)\gamma}(\tau)^m/g_{(0,1/N)\gamma}(\tau)^{4m}\\&= g_{(2c/N,2d/N)}(\tau)^m/g_{(c/N,d/N)}(\tau)^{4m}.\end{aligned}$$

Since we are assuming that the action of γ on $y_{(1/N,0)}(\tau)^m$ and $y_{(1/N,0)}(\tau)^m$ is trivial, we get

$$g_{(2a/N,2b/N)}(\tau)^m/g_{(a/N,b/N)}(\tau)^{4m} \doteq g_{(2/N,0)}(\tau)^m/g_{(1/N,0)}(\tau)^{4m}, \tag{2.5}$$

$$g_{(2c/N,2d/N)}(\tau)^m/g_{(c/N,d/N)}(\tau)^{4m} \doteq g_{(0,2/N)}(\tau)^m/g_{(0,1/N)}(\tau)^{4m}. \tag{2.6}$$

It then follows from the action of $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ on both sides of (2.5) and (2.6) as a fractional linear transformation that

$$g_{(2b/N,-2a/N)}(\tau)^m/g_{(b/N,-a/N)}(\tau)^{4m} \doteq g_{(0,-2/N)}(\tau)^m/g_{(0,-1/N)}(\tau)^{4m}, \tag{2.7}$$

$$g_{(2d/N,-2c/N)}(\tau)^m/g_{(d/N,-c/N)}(\tau)^{4m} \doteq g_{(2/N,0)}(\tau)^m/g_{(1/N,0)}(\tau)^{4m} \tag{2.8}$$

by Proposition 2.1(ii). Now by using the q_τ-order formula (2.3), we can compare the q_τ-orders of both sides of (2.5)$\sim$(2.8) to conclude

$$\begin{aligned}
m(1/2)\mathbf{B}_2(\langle 2a/N\rangle)-4m(1/2)\mathbf{B}_2(\langle a/N\rangle) &= m(1/2)\mathbf{B}_2(2/N) - 4m(1/2)\mathbf{B}_2(1/N),\\
m(1/2)\mathbf{B}_2(\langle 2c/N\rangle) - 4m(1/2)\mathbf{B}_2(\langle c/N\rangle) &= m(1/2)\mathbf{B}_2(0) - 4m(1/2)\mathbf{B}_2(0),\\
m(1/2)\mathbf{B}_2(\langle 2b/N\rangle) - 4m(1/2)\mathbf{B}_2(\langle b/N\rangle) &= m(1/2)\mathbf{B}_2(0) - 4m(1/2)\mathbf{B}_2(0),\\
m(1/2)\mathbf{B}_2(\langle 2d/N\rangle) - 4m(1/2)\mathbf{B}_2(\langle d/N\rangle) &= m(1/2)\mathbf{B}_2(2/N) - 4m(1/2)\mathbf{B}_2(1/N).
\end{aligned}$$

Considering the fact $\det(\gamma) = ad - bc = 1$, we achieve $a \equiv d \equiv \pm 1 \pmod N$ and $b \equiv c \equiv 0 \pmod N$. Hence γ lies in $\pm\Gamma(N)$, as desired. □

Theorem 2.7. *Let N (≥ 3) and m $(\neq 0)$ be integers.*

(i) $\mathbb{C}(X(N)) = \mathbb{C}(j(\tau), y_{(1/N,0)}(\tau)^{4m/\gcd(4,N)}, y_{(0,1/N)}(\tau)^{4m/\gcd(4,N)})$.

(ii) $\mathcal{F}_N = \mathbb{Q}(j(\tau), \zeta_N y_{(1/N,0)}(\tau)^{4m/\gcd(4,N)}, y_{(0,1/N)}(\tau)^{4m/\gcd(4,N)})$.

Proof. (i) Put $F=\mathbb{C}(j(\tau), y_{(1/N,0)}(\tau)^{4m/\gcd(4,N)}, y_{(0,1/N)}(\tau)^{4m/\gcd(4,N)})$, which is a subfield of $\mathbb{C}(X(N))$ containing $\mathbb{C}(X(1)) = \mathbb{C}(j(\tau))$ by Lemma 2.4. Assume that an element $\gamma \in \Gamma(1)$ acts trivially on F. Then γ must be in $\pm\Gamma(N)$ by Lemma 2.6. Thus F is all of $\mathbb{C}(X(N))$ by the fact $\mathrm{Gal}(\mathbb{C}(X(N))/\mathbb{C}(X(1))) \simeq \Gamma(1)/\pm\Gamma(N)$ and Galois theory.

(ii) Set $F = \mathbb{Q}(j(\tau), \zeta_N y_{(1/N,0)}(\tau)^{4m/\gcd(4,N)}, y_{(0,1/N)}(\tau)^{4m/\gcd(4,N)})$, which is a subfield of $\mathcal{F}_N$ containing $\mathcal{F}_1 = \mathbb{Q}(j(\tau))$ by Lemma 2.4. By (i) and [8, Lemma 4.1], we have $\mathcal{F}_N = F(\zeta_N)$. Hence $\mathrm{Gal}(\mathcal{F}_N/F)$ is isomorphic to a subgroup of $G_N = \{\left(\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix}\right) : d \in (\mathbb{Z}/N\mathbb{Z})^*\}$. Assume that $\beta = \left(\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix}\right) \in G_N$ acts trivially on F. Since

$$\begin{aligned}
y_{(1/N,0)}(\tau) &= \frac{g_{(2/N,0)}(\tau)}{g_{(1/N,0)}(\tau)^4}\\
&= \frac{-q_\tau^{(1/2)\mathbf{B}_2(2/N)}(1-q_\tau^{2/N})\prod_{n=1}^\infty(1-q_\tau^{n+2/N})(1-q_\tau^{n-2/N})}{(-q_\tau^{(1/2)\mathbf{B}_2(2/N)}(1-q_\tau^{2/N})\prod_{n=1}^\infty(1-q_\tau^{n+2/N})(1-q_\tau^{n-2/N}))^4}
\end{aligned}$$

has rational Fourier coefficients by (2.2), we get

$$\begin{aligned}
\zeta_N y_{(1/N,0)}(\tau)^{4m/\gcd(4,N)} &= (\zeta_N y_{(1/N,0)}(\tau)^{4m/\gcd(4,N)})^\beta\\
&= \zeta_N^d y_{(1/N,0)}(\tau)^{4m/\gcd(4,N)}.
\end{aligned}$$

Therefore, $d \equiv 1 \pmod{N}$, which implies that F is all of $\mathcal{F}_N$ by Galois theory. $\square$

3. Ray class invariants over imaginary quadratic fields

Throughout this section, let K be an imaginary quadratic field of discriminant d_K and let θ_K be as in (1.4). We shall prove our main theorem which claims that if $d_K \leq -19$ and $N \geq 3$, then for any nonzero integer m, the special value $y_{(0,1/N)}(\theta_K)^{4m/\gcd(4,N)}$ generates the ray class field $K_{(N)}$ over K. To this end, we shall introduce an explicit description of Shimura's reciprocity law due to Stevenhagen [14], from which we are able to determine all the conjugates of the special value of a meromorphic modular function.

Let $\mathrm{C}(d_K)$ be the group of all reduced (binary quadratic) forms $Q = [a, b, c] = aX^2 + bXY + cY^2 \in \mathbb{Z}[X, Y]$ characterized by the conditions

$$b^2 - 4ac = d_K,\ \gcd(a, b, c) = 1 \text{ and } (-a < b \leq a < c \text{ or } 0 \leq b \leq a = c) \tag{3.1}$$

[2, §2, A]. Note that the above conditions imply

$$a \leq \sqrt{-d_K/3} \tag{3.2}$$

[2, p. 29], and the identity of $\mathrm{C}(d_K)$ is

$$\begin{cases} [1, 0, -d_K/4] & \text{if } d_K \equiv 0 \pmod{4}, \\ [1, 1, (1 - d_K)/4] & \text{if } d_K \equiv 1 \pmod{4} \end{cases}$$

[2, Theorem 3.9]. For a reduced form $Q = [a, b, c] \in \mathrm{C}(d_K)$, we let

$$\theta_Q = (-b + \sqrt{d_K})/2a, \tag{3.3}$$

and define $u_Q = (u_p)_p \in \prod_{p\,:\,\mathrm{prime}} \mathrm{GL}_2(\mathbb{Z}_p)$ by

Case 1 : $d_K \equiv 0 \pmod{4}$

$$u_p = \begin{cases} \begin{pmatrix} a & b/2 \\ 0 & 1 \end{pmatrix} & \text{if } p \nmid a, \\ \begin{pmatrix} -b/2 & -c \\ 1 & 0 \end{pmatrix} & \text{if } p \mid a \text{ and } p \nmid c, \\ \begin{pmatrix} -a - b/2 & -c - b/2 \\ 1 & -1 \end{pmatrix} & \text{if } p \mid a \text{ and } p \mid c. \end{cases} \tag{3.4}$$

Case 2 : $d_K \equiv 1 \pmod{4}$

$$u_p = \begin{cases} \begin{pmatrix} a & (b-1)/2 \\ 0 & 1 \end{pmatrix} & \text{if } p \nmid a, \\ \begin{pmatrix} -(b+1)/2 & -c \\ 1 & 0 \end{pmatrix} & \text{if } p \mid a \text{ and } p \nmid c, \\ \begin{pmatrix} -a - (b+1)/2 & -c - (b-1)/2 \\ 1 & -1 \end{pmatrix} & \text{if } p \mid a \text{ and } p \mid c. \end{cases} \tag{3.5}$$

Let $\min(\theta_K,\mathbb{Q}) = X^2+BX+C$. For a positive integer N, we define a matrix group

$$W_{N,K} = \left\{ \begin{pmatrix} t-Bs & -Cs \\ s & t \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) : t,s \in \mathbb{Z}/N\mathbb{Z} \right\}.$$

Proposition 3.1 (Shimura's reciprocity law)**.** *Let K be an imaginary quadratic field other than $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-3})$, and let N be a positive integer. There is a one-to-one correspondence*

$$\begin{array}{rcl} W_{N,K}/\{\pm I_2\} \times \mathrm{C}(d_K) & \rightarrow & \mathrm{Gal}(K_{(N)}/K) \\ (\alpha, Q) & \mapsto & (h(\theta_K) \mapsto h^{\alpha\cdot u_Q}(\theta_Q)\ ; \\ & & \quad h \in \mathcal{F}_N \textit{ is defined and finite at } \theta_K). \end{array}$$

Proof. See [14, §3 and 6]. □

Remark 3.2. (i) There exists a 2×2 integral matrix β such that $\det(\beta) > 0$ and $\beta \equiv u_p \pmod{N\mathbb{Z}_p}$ for all p dividing N by the Chinese remainder theorem. The action of u_Q on $\mathcal{F}_N$ is understood as the action of $\beta \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I_2\}$ on $\mathcal{F}_N$.

(ii) The identity of $W_{N,K}/\{\pm I_2\} \times \mathrm{C}(d_K)$ corresponds to the identity of $\mathrm{Gal}(K_{(N)}/K)$ by the definitions (3.3)∼(3.5).

For simplicity, we let

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

Then one can readily verify the inequality

(3.6)
$$1/(1-A^{X/a}) < 1 + A^{X/1.03a} \quad \text{for } a, X \in \mathbb{R} \text{ such that } 1 \le a \le D \text{ and } X \ge 1/2.$$

It is also obvious that

$$1 + X < e^X \quad \text{for all } X > 0. \tag{3.7}$$

Lemma 3.3. (i) *Assume that $d_K \le -20$ and $N \ge 3$. Let $Q = [a,b,c] \in \mathrm{C}(d_K)$. If $a \ge 2$, then the inequality*

$$|g_{(2s/N,2t/N)}(\theta_Q)/g_{(s/N,t/N)}(\theta_Q)^4| < 0.996|g_{(0,2/N)}(\theta_K)/g_{(0,1/N)}(\theta_K)^4|$$

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

(ii) *Assume that $d_K \le -11$ and $N \ge 3$. Then the inequality*

$$|g_{(2s/N,2t/N)}(\theta_K)/g_{(s/N,t/N)}(\theta_K)^4| < 0.614|g_{(0,2/N)}(\theta_K)/g_{(0,1/N)}(\theta_K)^4|$$

holds for any $(s,t) \in \mathbb{Z}^2 \setminus N\mathbb{Z}^2$ such that $(s,t) \not\equiv (0,\pm 1) \pmod N$.

Proof. (i) We may assume that $0 \le s \le N/2$ and $0 \le t < N$ by Proposition 2.1(i) and (iii). Also note that $2 \le a \le D$ by (3.2) and $A \le e^{-\pi\sqrt{20}} < 1$. It follows from (2.2) that

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

$$
\begin{aligned}
&\le A^{1/4+(1/a)(s/N-1/4)}\left|\frac{(1-\zeta_N)^4}{1-\zeta_N^2}\right|\left|\frac{1-e^{2\pi i((2s/N)\theta_Q+2t/N)}}{(1-e^{2\pi i((s/N)\theta_Q+t/N)})^4}\right| \\
&\quad\times\prod_{n=1}^{\infty}\frac{(1+A^n)^8(1+A^{(1/a)(n+2s/N)})(1+A^{(1/a)(n-2s/N)})}{(1-A^n)^2(1-A^{(1/a)(n+s/N)})^4(1-A^{(1/a)(n-s/N)})^4} \\
&\le T(N,s,t)\prod_{n=1}^{\infty}\frac{(1+A^n)^8(1+A^{n/a})(1+A^{(1/a)(n-1)})}{(1-A^n)^2(1-A^{n/a})^4(1-A^{(1/a)(n-1/2)})^4} \\
&\qquad\text{by the fact } 0\le s\le N/2 \\
&\le T(N,s,t)\prod_{n=1}^{\infty}\frac{(1+A^n)^8(1+A^{n/D})(1+A^{(1/D)(n-1)})}{(1-A^n)^2(1-A^{n/D})^4(1-A^{(1/D)(n-1/2)})^4} \\
&\qquad\text{by the fact } 2\le a\le D,
\end{aligned}
$$

where

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

If $s=0$, then

$$
\begin{aligned}
T(N,s,t)&=A^{1/4-1/4a}\left|\left(\frac{1-\zeta_N}{1-\zeta_N^t}\right)^3\right|\left|\frac{1+\zeta_N^t}{1+\zeta_N}\right| \\
&=A^{1/4-1/4a}\left|\left(\frac{\sin(\pi/N)}{\sin(t\pi/N)}\right)^3\right|\left|\frac{\cos(t\pi/N)}{\cos(\pi/N)}\right| \\
&\le A^{1/8}\quad\text{by the fact } 2\le a\le D \\
&\le e^{-\pi\sqrt{20}/8}\quad\text{by the fact } d_K\le -20 \\
&<0.173.
\end{aligned}
$$

If $s\ne 0$, then

$$
\begin{aligned}
T(N,s,t)&\le A^{1/4+(1/a)(1/N-1/4)}\left|\frac{(1-\zeta_N)^3}{1+\zeta_N}\right|\frac{1+A^{1/Na}}{(1-A^{1/Na})^3} \\
&\qquad\text{by the fact } 1\le s\le N/2 \\
&\le A^{1/4+(1/2)(1/N-1/4)}\left|\frac{(1-\zeta_N)^3}{1+\zeta_N}\right|\frac{1+A^{1/ND}}{(1-A^{1/ND})^3} \\
&\qquad\text{by the fact } 2\le a\le D \\
&=e^{-\pi\sqrt{20}(1/8+1/2N)}\frac{4\sin^3(\pi/N)}{\cos(\pi/N)}\frac{1+e^{-\pi\sqrt{3}/N}}{(1-e^{-\pi\sqrt{3}/N})^3} \\
&\qquad\text{by the facts } d_K\le -20 \text{ and } A^{1/D}=e^{-\pi\sqrt{3}} \\
&<0.267\quad\text{from the graph for } N\ge 3 \text{ (Figure 1).}
\end{aligned}
$$

Therefore, we derive that

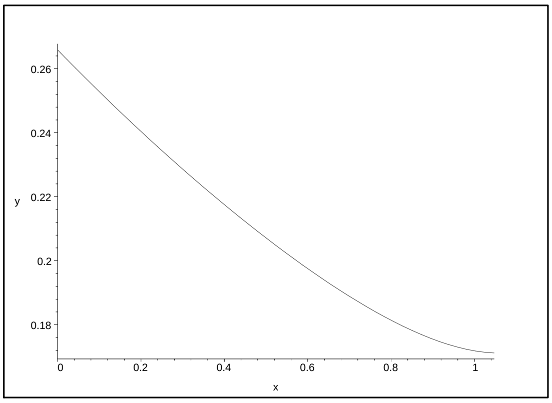

FIGURE 1. $Y = e^{-\pi\sqrt{20}(1/8+X/2\pi)}\frac{4\sin^3 X}{\cos X}\frac{1+e^{-\sqrt{3}X}}{(1-e^{-\sqrt{3}X})^3}$ for $0 < X \le \pi/3$

$$\begin{aligned}
&\left|\frac{g_{(2s/N,2t/N)}(\theta_Q)/g_{(s/N,t/N)}(\theta_Q)^4}{g_{(0,2/N)}(\theta_K)/g_{(0,1/N)}(\theta_K)^4}\right| \\
&< 0.267\prod_{n=1}^{\infty}\frac{(1+A^n)^8(1+A^{n/D})(1+A^{(1/D)(n-1)})}{(1+A^{n/1.03})^{-2}(1+A^{n/1.03D})^{-4}(1+A^{(1/1.03D)(n-1/2)})^{-4}} \\
&\qquad \text{by (3.6)} \\
&< 0.267\prod_{n=1}^{\infty} e^{8A^n+A^{n/D}+A^{(1/D)(n-1)}+2A^{n/1.03}+4A^{n/1.03D}+4A^{(1/1.03D)(n-1/2)}} \\
&\qquad \text{by (3.7)} \\
&= 0.267e^{8A/(1-A)+(A^{1/D}+1)/(1-A^{1/D})+2A^{1/1.03}/(1-A^{1/1.03})+(4A^{1/1.03D}+4A^{1/2.06D})/(1-A^{1/1.03D})} \\
&\le 0.267e^{8e^{-\pi\sqrt{20}}/(1-e^{-\pi\sqrt{20}})+(e^{-\pi\sqrt{3}}+1)/(1-e^{-\pi\sqrt{3}})+2e^{-\pi\sqrt{20}/1.03}/(1-e^{-\pi\sqrt{20}/1.03})} \\
&\quad \times e^{(4e^{-\pi\sqrt{3}/1.03}+4e^{-\pi\sqrt{3}/2.06})/(1-e^{-\pi\sqrt{3}/1.03})} \\
&\qquad \text{by the facts } A \le e^{-\pi\sqrt{20}} \text{ and } A^{1/D} = e^{-\pi\sqrt{3}} \\
&< 0.996.
\end{aligned}$$

(ii) We may also assume that $0 \le s \le N/2$ and $0 \le t < N$ by Proposition 2.1(i) and (iii). We establish by (2.2) that

$$\begin{aligned}
&\left|\frac{g_{(2s/N,2t/N)}(\theta_K)/g_{(s/N,t/N)}(\theta_K)^4}{g_{(0,2/N)}(\theta_K)/g_{(0,1/N)}(\theta_K)^4}\right| \\
&\le A^{s/N}\left|\frac{(1-\zeta_N)^4}{1-\zeta_N^2}\right|\left|\frac{1-e^{2\pi i((2s/N)\theta_K+2t/N)}}{(1-e^{2\pi i((s/N)\theta_K+t/N)})^4}\right|\prod_{n=1}^{\infty}\frac{(1+A^n)^8(1+A^{n+2s/N})(1+A^{n-2s/N})}{(1-A^n)^2(1-A^{n+s/N})^4(1-A^{n-s/N})^4}
\end{aligned}$$

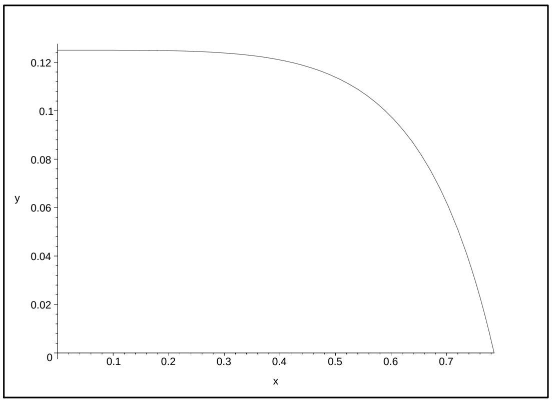

FIGURE 2. $Y = \frac{2\cos^2 X - 1}{8\cos^4 X}$ for $0 < X \leq \pi/4$

$$\leq T(N,s,t) \prod_{n=1}^{\infty} \frac{(1+A^n)^9(1+A^{n-1})}{(1-A^n)^6(1-A^{n-1/2})^4} \quad \text{by the fact } 0 \leq s \leq N/2,$$

where

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

If $s = 0$, then $N \geq 4$ and $2 \leq t \leq N-2$ by the assumption $(s,t) \not\equiv (0, \pm 1) \pmod N$; hence

$$\begin{aligned} T(N,s,t) &= \left| \left(\frac{1-\zeta_N}{1-\zeta_N^t} \right)^3 \right| \left| \frac{1+\zeta_N^t}{1+\zeta_N} \right| \\ &= \left| \left(\frac{\sin(\pi/N)}{\sin(t\pi/N)} \right)^3 \right| \left| \frac{\cos(t\pi/N)}{\cos(\pi/N)} \right| \\ &\leq \left(\frac{\sin(\pi/N)}{\sin(2\pi/N)} \right)^3 \frac{\cos(2\pi/N)}{\cos(\pi/N)} \\ &= \frac{2\cos^2(\pi/N) - 1}{8\cos^4(\pi/N)} \\ &< 0.125 \quad \text{from the graph for } N \geq 4 \text{ (Figure 2).} \end{aligned}$$

If $s \neq 0$, then

$$\begin{aligned} T(N,s,t) &\leq A^{1/N} \left| \frac{(1-\zeta_N)^3}{1+\zeta_N} \right| \frac{1+A^{1/N}}{(1-A^{1/N})^3} \\ &= \frac{4\sin^3(\pi/N)}{\cos(\pi/N)} \frac{A^{1/N}(1+A^{1/N})}{(1-A^{1/N})^3} \end{aligned}$$

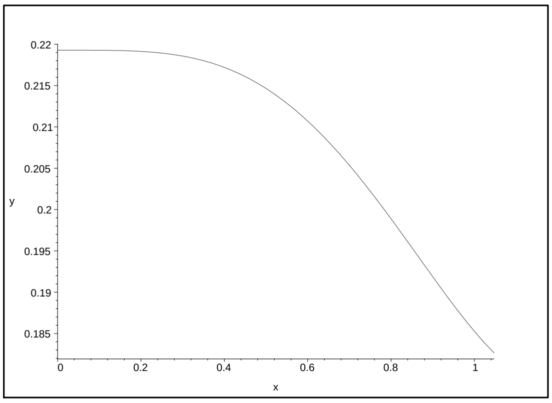

FIGURE 3. $Y = \frac{4\sin^3 X}{\cos X}\frac{e^{-\sqrt{11}X}(1+e^{-\sqrt{11}X})}{(1-e^{-\sqrt{11}X})^3}$ for $0 < X \leq \frac{\pi}{3}$

$$\begin{aligned} &\leq \frac{4\sin^3(\pi/N)}{\cos(\pi/N)}\frac{e^{-\pi\sqrt{11}/N}(1+e^{-\pi\sqrt{11}/N})}{(1-e^{-\pi\sqrt{11}/N})^3} \quad \text{by the fact } d_K \leq -11 \\ &< 0.22 \quad \text{from the graph for } N \geq 3 \text{ (Figure 3).} \end{aligned}$$

Therefore, we get that

$$\begin{aligned} &\left| \frac{g_{(2s/N,2t/N)}(\theta_K)/g_{(s/N,t/N)}(\theta_K)^4}{g_{(0,2/N)}(\theta_K)/g_{(0,1/N)}(\theta_K)^4} \right| \\ &< 0.22\prod_{n=1}^{\infty}\frac{(1+A^n)^9(1+A^{n-1})}{(1+A^{n/1.03})^{-6}(1+A^{(1/1.03)(n-1/2)})^{-4}} \quad \text{by (3.6)} \\ &< 0.22\prod_{n=1}^{\infty} e^{9A^n+A^{n-1}+6A^{n/1.03}+4A^{(1/1.03)(n-1/2)}} \quad \text{by (3.7)} \\ &= 0.22e^{(9A+1)/(1-A)+(6A^{1/1.03}+4A^{1/2.06})/(1-A^{1/1.03})} \\ &\leq 0.22e^{(9e^{-\pi\sqrt{11}}+1)/(1-e^{-\pi\sqrt{11}})+(6e^{-\pi\sqrt{11}/1.03}+4e^{-\pi\sqrt{11}/2.06})/(1-e^{-\pi\sqrt{11}/1.03})} \\ &\qquad \text{by the facts } A \leq e^{-\pi\sqrt{11}} \\ &< 0.614. \end{aligned}$$

This proves the lemma. $\square$

Theorem 3.4. *Let K be an imaginary quadratic field of discriminant d_K (≤ -19) and let N (≥ 3) be an integer. Then for any nonzero integer m, the special value $y_{(0,1/N)}(\theta_K)^{4m/\gcd(4,N)}$ generates the ray class field $K_{(N)}$ over K.*

Proof. Put $y(\tau) = y_{(0,1/N)}(\tau)^{4m/\gcd(4,N)}$. Then we get $y(\tau) \in \mathcal{F}_N$ by Lemma 2.4 and $y(\theta_K) \in K_{(N)}$ by Remark 2.5. Hence if we show that the only element of $\mathrm{Gal}(K_{(N)}/K)$ leaving $y(\theta_K)$ fixed is the identity, then we can conclude that $y(\theta_K)$ generates $K_{(N)}$ over K by Galois theory.

Any conjugate of $y(\theta_K)$ is of the form $y^{\alpha\cdot u_Q}(\theta_Q)$ for some $\alpha = \left(\begin{smallmatrix} t-Bs & -Cs \\ s & t \end{smallmatrix}\right) \in W_{N,K}$ and a reduced form $Q = [a,b,c] \in \mathrm{C}(d_K)$ by Proposition 3.1. Assume that $y(\theta_K) = y^{\alpha\cdot u_Q}(\theta_Q)$. If $d_K = -19$, then $h_K = 1$ [2, Theorem 12.34], and so $a = 1$. If $d_K \le -20$, then Lemma 3.3(i) leads us to take $a = 1$. Also, we derive from the condition (3.1) for reduced forms that

$$Q = \begin{cases} [1, 0, -d_K/4] & \text{for } d_K \equiv 0 \pmod 4, \\ [1, 1, (1-d_K)/4] & \text{for } d_K \equiv 1 \pmod 4, \end{cases}$$

which is the identity of $\mathrm{C}(d_K)$. It follows that $\theta_Q = \theta_K$ and that

$$u_Q = \begin{cases} \begin{pmatrix} 1 & b/2 \\ 0 & 1 \end{pmatrix} & \text{if } d_K \equiv 0 \pmod 4, \\ \begin{pmatrix} 1 & (b-1)/2 \\ 0 & 1 \end{pmatrix} & \text{if } d_K \equiv 1 \pmod 4 \end{cases}$$

as an element of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ by the definitions (3.3)$\sim$(3.5). Thus we deduce by the definition (2.4) and Proposition 2.3(ii) that

$$\begin{aligned} y(\theta_K) &= y^{\alpha\cdot u_Q}(\theta_Q) \\ &\doteq \left(\frac{g_{(0,2/N)\alpha u_Q}(\theta_Q)}{g_{(0,1/N)\alpha u_Q}(\theta_Q)^4} \right)^{4m/\gcd(4,N)} \\ &\doteq \begin{cases} \left(\dfrac{g_{(2s/N,(2s/N)(b/2)+2t/N)}(\theta_K)}{g_{(s/N,(s/N)(b/2)+t/N)}(\theta_K)^4} \right)^{4m/\gcd(4,N)} & \text{if } d_K \equiv 0 \pmod 4, \\ \left(\dfrac{g_{(2s/N,(2s/N)(b-1)/2+2t/N)}(\theta_K)}{g_{(s/N,(s/N)(b-1)/2+t/N)}(\theta_K)^4} \right)^{4m/\gcd(4,N)} & \text{if } d_K \equiv 1 \pmod 4, \end{cases} \end{aligned}$$

where $\doteq$ stands for the equality up to a root of unity. We get $(s,t) \equiv (0, \pm 1) \pmod N$ by Lemma 3.3(ii), which shows that α is the identity of $W_{N,K}/\{\pm I_2\}$. Hence $(\alpha, Q) \in W_{N,K}/\{\pm I_2\} \times \mathrm{C}(d_K)$ represents the identity of $\mathrm{Gal}(K_{(N)}/K)$ by Remark 3.2(ii). Therefore, $y(\theta_K)$ indeed generates $K_{(N)}$ over K. □

Corollary 3.5. *Let K be an imaginary quadratic field of discriminant d_K (≤ -19) and let N (≥ 3) be an odd integer. Then for any nonzero integer m, the special value $g_{(0,1/N)}(\theta_K)^{12Nm/\gcd(6,N)}$ generates $K_{(N)}$ over K.*

Proof. Let $g(\tau) = g_{(0,1/N)}(\tau)^{12Nm/\gcd(6,N)}$. Since $g(\tau) \in \mathcal{F}_N$ by Proposition 2.2, its special value $g(\theta_K)$ lies in $K_{(N)}$ by (1.5). On the other hand, since $K(g(\theta_K))$ is an abelian extension of K as a subfield of $K_{(N)}$, it contains all the conjugates of $g(\theta_K)$. Now that we are assuming N (≥ 3) is odd, $\left(\begin{smallmatrix} 2 & 0 \\ 0 & 2 \end{smallmatrix}\right) \in$

$\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I_2\}$ belongs to $W_{N,K}$ and satisfies

$$g(\theta_K)^{\left(\begin{smallmatrix}2&0\\0&2\end{smallmatrix}\right)} = g_{(0,1/N)\left(\begin{smallmatrix}2&0\\0&2\end{smallmatrix}\right)}(\theta_K)^{12Nm/\gcd(6,N)} = g_{(0,2/N)}(\theta_K)^{12Nm/\gcd(6,N)}$$

by Proposition 2.3(ii). Thus $K(g(\theta_K))$ contains the value

$$\begin{aligned}&(g_{(0,2/N)}(\theta_K)/g_{(0,1/N)}(\theta_K)^4)^{12Nm/\gcd(6,N)}\\ &= (y_{(0,1/N)}(\theta_K)^{4m/\gcd(4,N)})^{3N\gcd(4,N)/\gcd(6,N)},\end{aligned}$$

which implies that $K(g(\theta_K))$ is all of $K_{(N)}$ by Theorem 3.4. □

Proposition 3.6. *Let K be an imaginary quadratic field and let N (≥ 3) be an integer. Then the special values $g_{(0,1/N)}(\theta_K)^{12N/\gcd(6,N)}$ and*

$$\begin{cases} y_{(0,1/N)}(\theta_K)^{12N/\gcd(6,N)} & \textit{if } N \textit{ has at least two distinct prime factors in } \mathbb{Z},\\ N^{48N/\gcd(6,N)}y_{(0,1/N)}(\theta_K)^{12N/\gcd(6,N)} & \textit{if } N \textit{ is a prime power}\end{cases}$$

are real algebraic integers. Hence their minimal polynomials over K have integer coefficients.

Proof. Let $g(\tau) = g_{(0,1/N)}(\tau)^{12N/\gcd(6,N)}$ and

$$h(\tau) = \begin{cases} y_{(0,1/N)}(\tau)^{12N/\gcd(6,N)} & \text{if } N \text{ has at least two distinct prime factors in } \mathbb{Z},\\ N^{48N/\gcd(6,N)}y_{(0,1/N)}(\tau)^{12N/\gcd(6,N)} & \text{if } N \text{ is a prime power.}\end{cases}$$

Then $g(\tau)$ and $h(\tau)$ are integral over $\mathbb{Z}[j(\tau)]$ by Proposition 2.3(i) and the definition (2.4); hence their special values $g(\theta_K)$ and $h(\theta_K)$ are algebraic integers since $j(\theta_K)$ is an algebraic integer [10, Chapter 5, Theorem 4]. On the other hand, the infinite product formula (2.2) yields

$$\begin{aligned}&g(\theta_K)\\ &= q_{\theta_K}^{N/\gcd(6,N)}(2\sin(2\pi/N))^{12N/\gcd(6,N)}\prod_{n=1}^{\infty}(1-2\cos(4\pi/N)q_{\theta_K}^n+q_{\theta_K}^{2n})^{12N/\gcd(6,N)},\end{aligned}$$

and

$$\begin{aligned}&y(\theta_K)^{12N/\gcd(6,N)}\\ &= \frac{q_{\theta_K}^{N/\gcd(6,N)}(2\sin(2\pi/N))^{12N/\gcd(6,N)}\prod_{n=1}^{\infty}(1-2\cos(4\pi/N)q_{\theta_K}^n+q_{\theta_K}^{2n})^{12N/\gcd(6,N)}}{q_{\theta_K}^{4N/\gcd(6,N)}(2\sin(\pi/N))^{48N/\gcd(6,N)}\prod_{n=1}^{\infty}(1-2\cos(2\pi/N)q_{\theta_K}^n+q_{\theta_K}^{2n})^{48N/\gcd(6,N)}},\end{aligned}$$

where

$$q_{\theta_K} = e^{2\pi i\theta_K} = \begin{cases} e^{-\pi\sqrt{-d_K}} & \text{if } d_K \equiv 0 \pmod 4,\\ -e^{-\pi\sqrt{-d_K}} & \text{if } d_K \equiv 1 \pmod 4.\end{cases}$$

Therefore, $g(\theta_K)$ and $h(\theta_K)$ are real numbers. If we set $x = g(\theta_K)$ or $h(\theta_K)$, then

$$[\mathbb{Q}(x) : \mathbb{Q}] = \frac{[K(x) : K] \cdot [K : \mathbb{Q}]}{[K(x) : \mathbb{Q}(x)]} = \frac{[K(x) : K] \cdot 2}{2} = [K(x) : K],$$

which implies that the coefficients of the minimal polynomial of x over K are integers. $\square$

Example 3.7. Let $K = \mathbb{Q}(\sqrt{-10})$ and $\theta_K = \sqrt{-10}$. The reduced forms of discriminant $d_K = -40$ are exactly $Q_1 = [1, 0, 10]$ and $Q = [2, 0, 5]$, and we find

$$\theta_{Q_1} = \sqrt{-10},\ u_{Q_1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \theta_{Q_2} = \sqrt{-10}/2,\ u_{Q_2} = \begin{pmatrix} 2 & -3 \\ 3 & 4 \end{pmatrix}.$$

Furthermore, if $N = 6$, then

$$\begin{aligned} W_{6,K}/\{\pm I_2\} = \Big\{ & \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 4 \\ 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 4 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 4 \\ 5 & 1 \end{pmatrix}, \\ & \begin{pmatrix} 3 & 2 \\ 1 & 3 \end{pmatrix}, \begin{pmatrix} 3 & 4 \\ 2 & 3 \end{pmatrix} \Big\}. \end{aligned}$$

The special value $y_{(0,1/6)}(\theta_K)^{12}$ generates $K_{(6)}$ over K by Theorem 3.4, and one can find its minimal polynomial as follows (by using MAPLE 8 for the numerical computation of infinite products):

$$\begin{aligned}
&\min(y_{(0,1/6)}(\theta_K)^{12}, K) \\
= &\prod_{r=1}^{2} \prod_{\alpha \in W_{6,K}/\{\pm I_2\}} (X - (g_{(0,2/6)}(\tau)^{12}/g_{(0,1/6)}(\tau)^{48})^{\alpha u_{Q_r}}(\theta_{Q_r})) \\
= &\prod_{r=1}^{2} \prod_{\alpha \in W_{6,K}/\{\pm I_2\}} (X - g_{(0,2/6)\alpha U_{Q_r}}(\theta_{Q_r})^{12}/g_{(0,1/6)\alpha U_{Q_r}}(\theta_{Q_r})^{48}) \\
= &X^{16} - 5622749976591821668944491121 6X^{15} \\
&+ 28198738767573877103982180845427211416X^{14} \\
&- 6100629439282245697354378735343342652885917275 2X^{13} \\
&+ 24191545040559618198685578078066621024919984909895925564X^{12} \\
&- 1457219992512158403396945180026448081831307850098282381377715440X^{11} \\
&- 18752470866345884189001610098477497577054910903316185989551458784993 52X^{10} \\
&- 32042580545366914035595667456826388569591861662792064759274743450384537793 44X^{9} \\
&+ 3837981102128004098408468513928508790437791343975460837886051703270106222358 78X^{8} \\
&- 1154239742001591344102441518921573611681795924258535508207102881840723966924784 16X^{7} \\
&+ 3341072845825657939339745542850139076972151681140122802515727700239942604742952 08X^{6} \\
&- 2413062017539132381926952150397596657649211631905734942002508919329018160X^{5} \\
&+ 5947186157319106561144943221021199418610488121986658654341036924X^{4}
\end{aligned}$$

$$- 5317595247800083950930014176690955051475061944750295248X^3$$
$$+ 797299465586120177639706616225451835994220376X^2$$
$$- 29812156397602328057777202393119664X + 282429536481.$$

Lemma 3.8. *Let L be a finite Galois extension of a number field K with $G = \mathrm{Gal}(L/K)$. Assume that there exists an element $x \in L$ such that*

$$|x^\gamma/x| < 1 \quad \textit{for all} \;\; \gamma \in G \setminus \{\mathrm{Id}\}.$$

Take a suitably large positive integer s such that

$$|x^\gamma/x|^s \leq 1/|G| \quad \textit{for all} \;\; \gamma \in G \setminus \{\mathrm{Id}\}.$$

Then the conjugates of x^s form a normal basis of L over K (that is, $\{(x^s)^\gamma;\ \gamma \in \mathrm{Gal}(L/K)\}$ is a basis of the vector space L over K).

Proof. See [7, Theorem 2.4]. □

Corollary 3.9. *Let K be an imaginary quadratic field of discriminant d_K (≤ -19) and let N (≥ 3) be an integer. If s is any positive integer such that*

$$s \geq (\gcd(4, N)/4) \log_{1/0.996}[K_{(N)} : K],$$

then the conjugates of the special value $y_{(0,1/N)}(\theta_K)^{4s/\gcd(4,N)}$ form a normal basis of $K_{(N)}$ over K.

Proof. Let $x = y_{(0,1/N)}(\theta_K)^{4/\gcd(4,N)}$. In the proof of Theorem 3.4, we showed that

$$|x^\gamma/x| < 0.996^{4/\gcd(4,N)} \quad \text{for all } \gamma \in \mathrm{Gal}(K_{(N)}/K) \setminus \{\mathrm{Id}\}$$

by virtue of Lemma 3.3. Hence Lemma 3.8 proves the assertion. □

References

[1] B. Cho and J. K. Koo, *Constructions of class fields over imaginary quadratic fields and applications*, Q. J. Math. **61** (2010), no. 2, 199–216.

[2] D. A. Cox, *Primes of the form $x^2 + ny^2$*, Fermat, Class Field, and Complex Multiplication, A Wiley-Interscience Publication, John Wiley & Sons, Inc., New York, 1989.

[3] F. Diamond and J. Shurman, *A First Course in Modular Forms*, Grad. Texts in Math. 228, Springer-Verlag, New York, 2005.

[4] D. R. Dorman, *Singular moduli, modular polynomials, and the index of the closure of $\mathbb{Z}[j(\tau)]$ in $\mathbb{Q}(j(\tau))$*, Math. Ann. **283** (1989), no. 2, 177–191.

[5] B. Gross and D. Zagier, *On singular moduli*, J. Reine Angew. Math. **355** (1985), 191–220.

[6] H. Hasse, *Neue Begründung der komplexen Multiplikation. I*, J. Reine Angew. Math. **157** (1927), 115–139.

[7] H. Y. Jung, J. K. Koo, and D. H. Shin, *Normal bases of ray class fields over imaginary quadratic fields*, Math. Z. **271** (2012), no. 1-2, 109–116.

[8] J. K. Koo and D. H. Shin, *On some arithmetic properties of Siegel functions*, Math. Z. **264** (2010), no. 1, 137–177.

[9] D. Kubert and S. Lang, *Modular Units*, Grundlehren der mathematischen Wissenschaften 244, Spinger-Verlag, New York-Berlin, 1981.

[10] S. Lang, *Elliptic Functions*, With an appendix by J. Tate, 2nd edition, Grad. Texts in Math. 112, Springer-Verlag, New York, 1987.

[11] R. Schertz, *Construction of ray class fields by elliptic units*, J. Théor. Nombres Bordeaux **9** (1997), no. 2, 383–394.

[12] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Iwanami Shoten and Princeton University Press, Princeton, N. J., 1971.

[13] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Grad. Texts in Math. 106, Springer-Verlag, New York, 1992.

[14] 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.

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

Dong Hwa Shin
Department of Mathematics
Hankuk University of Foreign Studies
Gyeonggi-do 449-791, Korea
E-mail address: dhshin@hufs.ac.kr