Research Article

Ho Yun Jung*, Ja Kyung Koo, and Dong Hwa Shin

Class fields generated by coordinates of elliptic curves

https://doi.org/10.1515/math-2022-0502
received November 7, 2021; accepted September 9, 2022

Abstract: Let K be an imaginary quadratic field different from $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-3})$. For a nontrivial integral ideal $\mathfrak{m}$ of K, let $K_\mathfrak{m}$ be the ray class field modulo $\mathfrak{m}$. By using some inequalities on special values of modular functions, we show that a single x-coordinate of a certain elliptic curve generates $K_\mathfrak{m}$ over K.

Keywords: class field theory, complex multiplication, modular functions

MSC 2020: 11F03, 11G15, 11R37

1 Introduction

Let K be an imaginary quadratic field with ring of integers $\mathcal{O}_K$. Let E be the elliptic curve with complex multiplication by $\mathcal{O}_K$ given by the Weierstrass equation:

$$E : y^2 = 4x^3 - g_2x - g_3 \quad \text{with } g_2 = g_2(\mathcal{O}_K) \quad \text{and} \quad g_3 = g_3(\mathcal{O}_K).$$

For $z \in \mathbb{C}$, let $[z]$ denote the coset $z + \mathcal{O}_K$ in $\mathbb{C}/\mathcal{O}_K$. Then the map

$$\begin{aligned}\varphi_K : \mathbb{C}/\mathcal{O}_K &\to E(\mathbb{C}) \quad (\subset \mathbb{P}^2(\mathbb{C}))\\ [z] &\mapsto [\wp(z; \mathcal{O}_K) : \wp'(z; \mathcal{O}_K) : 1],\end{aligned}$$

where $\wp$ is the Weierstrass $\wp$-function relative to $\mathcal{O}_K$, is a complex analytic isomorphism of complex Lie groups ([1, Proposition 3.6 in Chapter VI]). Corresponding to E, we consider the Weber function $\mathfrak{h}_K : E(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$ given by

$$\mathfrak{h}_K(x, y) = \begin{cases} \dfrac{g_2g_3}{\Delta}x & \text{if } j(E) \neq 0,\ 1{,}728, \\ \dfrac{g_2^2}{\Delta}x^2 & \text{if } j(E) = 1{,}728, \\ \dfrac{g_3}{\Delta}x^3 & \text{if } j(E) = 0, \end{cases}$$

where $\Delta = g_2^3 - 27g_3^2$ $(\neq 0)$ and $j(E) = j(\mathcal{O}_K)$ is the j-invariant of E. For a nontrivial ideal $\mathfrak{m}$ of $\mathcal{O}_K$, by $K_\mathfrak{m}$ we mean the ray class field of K modulo $\mathfrak{m}$. In particular, $K_{\mathcal{O}_K}$ is the Hilbert class field H_K of K. Then we obtain by the theory of complex multiplication that $H_K = K(j(E))$ and

$$K_\mathfrak{m} = H_K(\mathfrak{h}_K(x, y)) \text{ for some } \mathfrak{m}\text{-torsion point } (x, y) \text{ on } E$$

* **Corresponding author: Ho Yun Jung,** Department of Mathematics, Dankook University, Cheonan-si, Chungnam 31116, Republic of Korea, e-mail: hoyunjung@dankook.ac.kr
Ja Kyung Koo: Department of Mathematical Sciences, KAIST, Daejeon 34141, Republic of Korea, e-mail: jkgoo@kaist.ac.kr
Dong Hwa Shin: Department of Mathematics, Hankuk University of Foreign Studies, Yongin-si, Gyeonggi-do 17035, Republic of Korea, e-mail: dhshin@hufs.ac.kr

if $\mathfrak{m}$ is proper [2, Chapter 10]. In a letter to Hecke concerning Kronecker's Jugendtraum (= Hilbert 12th problem), Hasse asked whether every abelian extension of K can be generated only by a single value of the Weber function $\mathfrak{h}_K$ over K [3, p. 91] and Sugawara first gave partial answers to this question [4,5]. Recently, Jung et al. [6] proved that if $\mathfrak{m} = NO_K$ and $N \in \{2, 3, 4, 6\}$, then

$$K_{\mathfrak{m}} = K\left(\mathfrak{h}_K\left(\varphi_K\left(\left[\frac{1}{N}\right]\right)\right)\right) \quad \text{or} \quad K_{\mathfrak{m}} = K\left(\mathfrak{h}_K\left(\varphi_K\left(\left[\frac{2}{N}\right]\right)\right)\right). \tag{1}$$

Koo et al. [7] further showed by utilizing the second Kronecker's limit formula that (1) holds for $N = 5$ and $N \geq 7$. Besides, it is worth noting that Ramachandra [8] constructed a complicated primitive generator of $K_{\mathfrak{m}}$ over K by using special values of the product of high powers of the discriminant Δ function and Siegel functions, which is beautiful in theory.

Now, we assume that K is different from $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-3})$, and so $g_2g_3 \neq 0$ and $j(O_K) \neq 0, 1{,}728$ ([9, p. 200]). Let $\{E_{K,n}\}_{n\in\mathbb{Z}_{\geq 0}}$ be the family of elliptic curves isomorphic to E given by the affine models

$$E_{K,n} : y^2 = 4x^3 - \frac{J_K(J_K - 1)}{27}\ell_K{}^{2n}x - \frac{J_K(J_K - 1)^2}{27^2}\ell_K{}^{3n}, \tag{2}$$

where

$$J_K = \frac{1}{1{,}728}j(O_K) \quad \text{and} \quad \ell_K = J_K^2(J_K - 1)^3.$$

Then for each $n \in \mathbb{Z}_{\geq 0}$ we have a parametrization

$$\begin{aligned} \mathbb{C}/O_K &\to E_{K,n}(\mathbb{C}) \quad (\subset \mathbb{P}^2(\mathbb{C})) \\ [z] &\mapsto [x_{K,n}(z) : y_{K,n}(z) : 1], \end{aligned}$$

with

$$x_{K,n}(z) = \ell_K{}^n\frac{g_2g_3}{\Delta}\wp(z; O_K) \quad \text{and} \quad y_{K,n}(z) = \sqrt{\left(\ell_K{}^n\frac{g_2g_3}{\Delta}\right)^3}\wp'(z; O_K).$$

Here we note that

$$x_{K,n}(z) = \ell_K{}^n\mathfrak{h}_K(\varphi_K([z])) \quad (z \in \mathbb{C}). \tag{3}$$

Let $\mathfrak{m}$ be a proper nontrivial ideal of O_K in such a way that $K_{\mathfrak{m}}$ properly contains H_K. Let ω be an element of K so that $[\omega] = \omega + O_K$ is a generator of the O_K-module $\mathfrak{m}^{-1}O_K/O_K$. In this article, we shall prove the following three assertions (Theorems 4.4, 5.2, and 6.4):

(i) We have $K_{\mathfrak{m}} = K(x_{K,n}(\omega), y_{K,n}(\omega)^2)$ for every $n \in \mathbb{Z}_{\geq 0}$.

(ii) We obtain $K_{\mathfrak{m}} = K(x_{K,n}(\omega))$ for every $n \in \mathbb{Z}_{\geq 0}$ satisfying

$$n \geq \frac{\frac{13}{24}\pi\sqrt{|d_K|} + 6\ln\left(\frac{229}{76}N_{\mathfrak{m}}\right)}{\frac{5}{2}\pi\sqrt{|d_K|} - \ln 877{,}383} - \frac{1}{6},$$

where d_K is the discriminant of K and $N_{\mathfrak{m}}$ is the least positive integer in $\mathfrak{m}$.

(iii) If $\mathfrak{m} = NO_K$ for an integer N (≥ 2) whose prime factors are all inert in K, then $K_{\mathfrak{m}} = K(x_{K,n}(\omega))$ for every $n \in \mathbb{Z}_{\geq 0}$.

To this end, we shall make use of some inequalities on special values of the elliptic modular function and Siegel functions (Lemmas 4.1 and 5.1), rather than using L-function arguments adopted in [7,8,10].

Finally, we hope to utilize the aforementioned results (i), (ii), and (iii) to investigate the images of (higher dimensional) Galois representations attached to elliptic curves with complex multiplication.

2 Fricke and Siegel functions

In this preliminary section, we recall the definitions and basic properties of Fricke and Siegel functions.

Let $\mathbb{H}$ be the complex upper half-plane, that is, $\mathbb{H} = \{\tau \in \mathbb{C} | \mathrm{Im}(\tau) > 0\}$. Let j be the elliptic modular function on $\mathbb{H}$ given by

$$j(\tau) = j([\tau, 1]) \quad (\tau \in \mathbb{H}),$$

where $[\tau, 1]$ stands for the lattice $\mathbb{Z}\tau + \mathbb{Z}$ in $\mathbb{C}$ and $j([\tau, 1])$ is the j-invariant of an elliptic curve isomorphic to $\mathbb{C}/[\tau, 1]$. Define the function J on $\mathbb{H}$ by

$$J(\tau) = \frac{1}{1{,}728} j(\tau) \quad (\tau \in \mathbb{H}).$$

Furthermore, for $\mathbf{v} = [v_1 \;\; v_2] \in M_{1,2}(\mathbb{Q}) \setminus M_{1,2}(\mathbb{Z})$ we define the Fricke function $f_{\mathbf{v}}$ on $\mathbb{H}$ by

$$f_{\mathbf{v}}(\tau) = -2^7 3^5 \frac{g_2(\tau) g_3(\tau)}{\Delta(\tau)} \wp(v_1\tau + v_2;\, [\tau, 1]) \quad (\tau \in \mathbb{H}),$$

where $g_2(\tau) = g_2([\tau, 1])$, $g_3(\tau) = g_3([\tau, 1])$, and $\Delta(\tau) = \Delta([\tau, 1])$. Note that for $\mathbf{u}, \mathbf{v} \in M_{1,2}(\mathbb{Q}) \setminus M_{1,2}(\mathbb{Z})$

$$f_{\mathbf{u}} = f_{\mathbf{v}} \;\Leftrightarrow\; \mathbf{u} \equiv \mathbf{v} \text{ or } -\mathbf{v} \pmod{M_{1,2}(\mathbb{Z})} \tag{4}$$

([9, Lemma 10.4]). For a positive integer N, let $\mathcal{F}_N$ be the field given by

$$\mathcal{F}_N = \begin{cases} \mathbb{Q}(j) & \text{if } N = 1, \\ \mathcal{F}_1\left(f_{\mathbf{v}} | \mathbf{v} \in \frac{1}{N} M_{1,2}(\mathbb{Z}) \setminus M_{1,2}(\mathbb{Z}) \right) & \text{if } N \geq 2. \end{cases}$$

Then, $\mathcal{F}_N$ is a Galois extension of $\mathcal{F}_1$ whose Galois group is isomorphic to $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\langle -I_2 \rangle$ ([11, Theorem 6.6]). It coincides with the field of meromorphic modular functions of level N whose Fourier coefficients belong to the Nth cyclotomic field ([11, Proposition 6.9]).

Proposition 2.1. *If $N \geq 2$, $\mathbf{v} \in \frac{1}{N} M_{1,2}(\mathbb{Z}) \setminus M_{1,2}(\mathbb{Z})$, and $\gamma \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\langle -I_2 \rangle$, then*

$$f_{\mathbf{v}}^{\gamma} = f_{\mathbf{v}\gamma}.$$

Moreover, if $\gamma \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\langle -I_2 \rangle$, then

$$f_{\mathbf{v}}^{\gamma} = f_{\mathbf{v}} \circ \alpha,$$

where α is any element of $\mathrm{SL}_2(\mathbb{Z})$ (acting on $\mathbb{H}$ as fractional linear transformation) whose image in $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\langle -I_2 \rangle$ is γ.

Proof. See [2, Theorem 3 in Chapter 6] or [11, Theorem 6.6]. □

For $\mathbf{v} = [v_1 \;\; v_2] \in M_{1,2}(\mathbb{Q}) \setminus M_{1,2}(\mathbb{Z})$, the Siegel function $g_{\mathbf{v}}$ on $\mathbb{H}$ is given by the infinite product expansion

$$g_{\mathbf{v}}(\tau) = -e^{\pi \mathrm{i} v_2(v_1 - 1)} q_\tau^{\frac{1}{2}(v_1^2 - v_1 + \frac{1}{6})} (1 - q_z) \prod_{n=1}^{\infty} (1 - q_\tau^n q_z)(1 - q_\tau^n q_z^{-1}) \quad (\tau \in \mathbb{H}), \tag{5}$$

where $q_\tau = e^{2\pi \mathrm{i}\tau}$ and $q_z = e^{2\pi \mathrm{i} z}$ with $z = v_1\tau + v_2$. Observe that $g_{\mathbf{v}}$ has neither a zero nor a pole on $\mathbb{H}$.

Proposition 2.2. *Let N be an integer such that $N \geq 2$, and let $\mathbf{v} \in \frac{1}{N} M_{1,2}(\mathbb{Z}) \setminus M_{1,2}(\mathbb{Z})$.*

(*i*) *If $\mathbf{u} \in \frac{1}{N} M_{1,2}(\mathbb{Z}) \setminus M_{1,2}(\mathbb{Z})$ such that $\mathbf{u} \equiv \mathbf{v}$ or $-\mathbf{v} \pmod{M_{1,2}(\mathbb{Z})}$, then $g_{\mathbf{u}}^{12N} = g_{\mathbf{v}}^{12N}$.*

(*ii*) *The function $g_{\mathbf{v}}^{12N}$ belongs to $\mathcal{F}_N$ and satisfies*

$$(g_{\mathbf{v}}^{12N})^{\gamma} = g_{\mathbf{v}\gamma}^{12N} \quad (\gamma \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\langle -I_2 \rangle \simeq \mathrm{Gal}(\mathcal{F}_N/\mathcal{F}_1)).$$

Proof.
(i) See [12, Theorem 1.1 in Chapter 2 and p. 29].
(ii) See [12, Theorem 1.2 and Proposition 1.3 in Chapter 2]. □

Lemma 2.3. *Let* $\mathbf{u}, \mathbf{v} \in M_{1,2}(\mathbb{Q})\backslash M_{1,2}(\mathbb{Z})$ *such that* $\mathbf{u} \not\equiv \mathbf{v}$ *and* $-\mathbf{v} \pmod{M_{1,2}(\mathbb{Z})}$*. Then we have*

$$(f_{\mathbf{u}} - f_{\mathbf{v}})^6 = \frac{J^2(J-1)^3}{3^9} \frac{g_{\mathbf{u}+\mathbf{v}}^6 g_{\mathbf{u}-\mathbf{v}}^6}{g_{\mathbf{u}}^{12} g_{\mathbf{v}}^{12}}.$$

Proof. See [12, p. 51]. □

3 Extended form class groups

In this section, we review some necessary consequences of the theory of complex multiplication, and introduce extended form class groups which might be an extension of Gauss' form class group.

Let K be an imaginary quadratic field of discriminant d_K. For a positive integer N, let $\mathcal{Q}_N(d_K)$ be the set of primitive positive definite binary quadratic forms of discriminant d_K whose leading coefficients are relatively prime to N, that is,

$$\mathcal{Q}_N(d_K) = \left\{ Q\left(\begin{bmatrix} x \\ y \end{bmatrix}\right) = a_Q x^2 + b_Q xy + c_Q y^2 \in \mathbb{Z}[x,y] \;\middle|\; \begin{array}{l} \gcd(a_Q, b_Q, c_Q) = 1, \\ \gcd(a_Q, N) = 1, \\ a_Q > 0, \\ b_Q^2 - 4a_Q c_Q = d_K \end{array} \right\}.$$

The congruence subgroup

$$\Gamma_1(N) = \left\{ \gamma \in \mathrm{SL}_2(\mathbb{Z}) | \gamma \equiv \begin{bmatrix} 1 & * \\ 0 & 1 \end{bmatrix} \pmod{NM_2(\mathbb{Z})} \right\}$$

defines an equivalence relation $\sim_N$ on the set $\mathcal{Q}_N(d_K)$ as

$$Q \sim_N Q' \iff Q' = Q\left(\gamma \begin{bmatrix} x \\ y \end{bmatrix}\right) \text{ for some } \gamma \in \Gamma_1(N).$$

Let

$$\mathrm{C}_N(d_K) = \mathcal{Q}_N(d_K)/\sim_N$$

be the set of equivalence classes. For each $Q = a_Q x^2 + b_Q xy + c_Q y^2 \in \mathcal{Q}_N(d_K)$, let $[Q]_N$ be its class in $\mathrm{C}_N(d_K)$, and let

$$\tau_Q = \frac{-b_Q + \sqrt{d_K}}{2a_Q},$$

which is the zero of the quadratic polynomial $Q(x, 1)$ lying in $\mathbb{H}$. For a nontrivial ideal $\mathfrak{m}$ of $\mathcal{O}_K$, let us denote by $\mathrm{Cl}(\mathfrak{m})$ the ray class group modulo $\mathfrak{m}$, namely, $\mathrm{Cl}(\mathfrak{m}) = I_K(\mathfrak{m})/P_{K,1}(\mathfrak{m})$, where $I_K(\mathfrak{m})$ is the group of fractional ideals of K relatively prime to $\mathfrak{m}$ and $P_{K,1}(\mathfrak{m})$ is the subgroup of $P_K(\mathfrak{m})$ (the subgroup of $I_K(\mathfrak{m})$ consisting of principal fractional ideals) defined by

$$P_{K,1}(\mathfrak{m}) = \langle \nu\mathcal{O}_K | \nu \in \mathcal{O}_K\backslash\{0\} \quad \text{such that } \nu \equiv 1 \pmod{\mathfrak{m}} \rangle.$$

Then, when $\mathfrak{m} = N\mathcal{O}_K$, the map

$$\begin{aligned} \mathrm{C}_N(d_K) &\to \mathrm{Cl}(N\mathcal{O}_K) \\ [Q]_N &\mapsto [[\tau_Q, 1]] = [\mathbb{Z}\tau_Q + \mathbb{Z}] \end{aligned}$$

is a well-defined bijection, through which we may regard $\mathrm{C}_N(d_K)$ as a group isomorphic to $\mathrm{Cl}(N\mathcal{O}_K)$ ([13, Theorem 2.9] or [14, Theorem 2.5 and Proposition 5.3]). The identity element of $\mathrm{C}_N(d_K)$ is the class $[Q_{\mathrm{pr}}]_N$ of the principal form

$$Q_{\mathrm{pr}} := x^2 + b_K xy + c_K y^2 = \begin{cases} x^2 - \dfrac{d_K}{4}y^2 & \text{if } d_K \equiv 0 \pmod 4, \\ x^2 + xy + \dfrac{1-d_K}{4}y^2 & \text{if } d_K \equiv 1 \pmod 4. \end{cases}$$

We call this group $\mathrm{C}_N(d_K)$ the extended form class group of discriminant d_K and level N.

In particular, $\mathrm{C}_1(d_K)$ is the classical form class group of discriminant d_K, originated and developed by Gauss [15] and Dirichlet [16]. A form $Q = a_Q x^2 + b_Q xy + c_Q y^2$ in $\mathcal{Q}_1(d_K)$ is said to be reduced if

$$-a_Q < b_Q \le a_Q < c_Q \quad \text{or} \quad 0 \le b_Q \le a_Q = c_Q.$$

This condition yields

$$a_Q \le \sqrt{\frac{|d_K|}{3}}. \tag{6}$$

If we let $Q_1, Q_2, \ldots, Q_h$ be all the reduced forms of discriminant d_K, then we have $h = |\mathrm{C}_1(d_K)|$ and

$$\mathrm{C}_1(d_K) = \{[Q_1]_1, [Q_2]_1, \ldots, [Q_h]_1\} \tag{7}$$

([9, Theorem 2.8]). Set

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

and then $\tau_K = \tau_{Q_{\mathrm{pr}}}$ and $\mathcal{O}_K = [\tau_K, 1]$. By the theory of complex multiplication, we obtain the following results.

Proposition 3.1. *Let K be an imaginary quadratic field and $\mathfrak{m}$ be a nontrivial ideal of $\mathcal{O}_K$.*

(*i*) *If $\mathfrak{m} = \mathcal{O}_K$, then we obtain*

$$K_{\mathfrak{m}} = H_K = K(j(\tau_K)).$$

Furthermore, if Q_i ($i = 1, 2, \ldots, h = |\mathrm{C}_1(d_K)|$) are reduced forms of discriminant d_K, then the singular values $j(\tau_{Q_i})$ are distinct (Galois) conjugates of $j(\tau_K)$ over K.

(*ii*) *If $\mathfrak{m} \neq \mathcal{O}_K$, then we have*

$$K_{\mathfrak{m}} = H_K(\mathfrak{h}_K(\varphi_K([\omega])))$$

for any element ω of K for which $[\omega] = \omega + \mathcal{O}_K$ is a generator of the $\mathcal{O}_K$-module $\mathfrak{m}^{-1}\mathcal{O}_K/\mathcal{O}_K$. All such $\mathfrak{h}_K(\varphi_K([\omega]))$ are conjugate over H_K. More precisely, if ξ_i ($i = 1, 2, \ldots, [K_{\mathfrak{m}} : H_K]$) are nonzero elements of $\mathcal{O}_K$ such that

$$\{(\xi_i)P_{K,1}(\mathfrak{m}) \mid i = 1, 2, \ldots, [K_{\mathfrak{m}} : H_K]\} = P_K(\mathfrak{m})/P_{K,1}(\mathfrak{m})(\simeq \mathrm{Gal}(K_{\mathfrak{m}}/H_K)),$$

then $\mathfrak{h}_K(\varphi_K([\xi_i\omega]))$ are all distinct conjugates of $\mathfrak{h}_K(\varphi_K([\omega]))$ over H_K.

Proof.

(i) See [2, Theorem 1 in Chapter 10] and [9, Theorem 7.7 (ii)].

(ii) See [2, Theorem 7 and its Corollary in Chapter 10]. □

By modifying Shimura's reciprocity law ([11, Theorem 6.31, Propositions 6.33 and 6.34]), Eum et al. established the following proposition.

Proposition 3.2. *Let K be an imaginary quadratic field, N be a positive integer, and $K_{(N)}$ be the ray class field of K modulo the ideal (N). Then the map*

$$\begin{aligned} \mathrm{C}_N(d_K) &\to \mathrm{Gal}(K_{(N)}/K) \\ [Q]_N &\mapsto \left(f(\tau_K) \mapsto f^{\begin{bmatrix} a_Q & (b_Q-b_K)/2 \\ 0 & 1 \end{bmatrix}}(\tau_Q) \mid f \in \mathcal{F}_N \text{ is finite at } \tau_K \right) \end{aligned}$$

is a well-defined isomorphism.

Proof. See [13, Remark 3.3 and Theorem 3.10]. □

Remark 3.3. If M and N are positive integers such that $M \mid N$, then the natural map

$$\begin{aligned} \mathrm{C}_N(d_K) &\to \mathrm{C}_M(d_K) \\ [Q]_N &\mapsto [Q]_M \end{aligned}$$

is a surjective homomorphism ([13, Remark 2.10 (i)]).

4 Some applications of inequality on singular values of *j*

Let K be an imaginary quadratic field of discriminant d_K. By using inequality argument on singular values of j developed in [6], we show that coordinates of elliptic curves in the family $\{E_{K,n}\}_{n\in\mathbb{Z}_{\geq 0}}$ described in (2) can be used in order to generate the ray class fields of K.

Let h_K denote the class number of K, i.e., $h_K = |\mathrm{C}_1(d_K)| = [H_K : K]$. It is well known that

$$h_K = 1 \;\Leftrightarrow\; d_K = -3, -4, -7, -8, -11, -19, -43, -67, -163$$

([9, Theorem 12.34]). So, if $h_K \geq 2$, then we have $d_K \leq -15$.

Lemma 4.1. *If $h_K \geq 2$ and $d_K \leq -20$, then we achieve*

$$\left| \frac{J(\tau_Q)^2(J(\tau_Q)-1)^3}{J(\tau_K)^2(J(\tau_K)-1)^3} \right| < 877{,}383 \quad |q_{\tau_K}|^{\frac{5}{2}}(<1) \tag{8}$$

for all nonprincipal reduced forms Q of discriminant d_K.

Proof. See [6, Lemma 6.3 (ii)]. □

Remark 4.2. If $d_K = -15$, then we obtain $\mathrm{C}_1(d_K) = \{[Q_1]_1, [Q_2]_1\}$ with

$$Q_1 = x^2 + xy + 4y^2 \quad \text{and} \quad Q_2 = 2x^2 + xy + 2y^2.$$

Moreover, we have

$$j(\tau_K) = j\left(\tau_{Q_1}\right) = -52{,}515 - 85{,}995\frac{1+\sqrt{5}}{2} \quad \text{and} \quad j\left(\tau_{Q_2}\right) = -52{,}515 - 85{,}995\ \frac{1-\sqrt{5}}{2}$$

([1, Example 6.2.2]). One can check that inequality (8) also holds true.

Lemma 4.3. *Let K be an imaginary quadratic field other than $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-3})$. Then we attain*

$$H_K = K(\ell_K{}^n) \quad \text{for every } n \in \mathbb{Z}_{>0}.$$

Proof. If $h_K = 1$, then the assertion is obvious because $H_K = K$.

Now, assume that $h_K \geq 2$. Let σ be an element of $\mathrm{Gal}(H_K/K)$, which fixes $\ell_K{}^n$. Then we find by Proposition 3.1 (i) that

$$1 = \left|\frac{(\ell_K{}^n)^\sigma}{\ell_K{}^n}\right| = \left|\frac{\{J(\tau_K)^2(J(\tau_K)-1)^3\}^\sigma}{J(\tau_K)^2(J(\tau_K)-1)^3}\right|^n = \left|\frac{J(\tau_Q)^2(J(\tau_Q)-1)^3}{J(\tau_K)^2(J(\tau_K)-1)^3}\right|^n$$

for some reduced form Q of discriminant d_K. Thus, Q must be Q_{pr} by Lemma 4.1 and Remark 4.2, and hence σ is the identity element of $\mathrm{Gal}(H_K/K)$ again by Proposition 3.1 (i). This observation implies by the Galois theory that H_K is generated by $\ell_K{}^n$ over K. □

Theorem 4.4. *Let K be an imaginary quadratic field other than $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-3})$, and let $\mathfrak{m}$ be a nontrivial proper integral ideal of $\mathcal{O}_K$. Let ω be an element of K such that $\omega + \mathcal{O}_K$ is a generator of the $\mathcal{O}_K$-module $\mathfrak{m}^{-1}/\mathcal{O}_K$. If $K_\mathfrak{m}$ properly contains H_K, then we have*

$$K_\mathfrak{m} = K(x_{K,n}(\omega), y_{K,n}(\omega)^2) \quad \text{for every } n \in \mathbb{Z}_{\geq 0}.$$

Proof. For simplicity, let

$$X = x_{K,n}(\omega) = \ell_K{}^n \mathfrak{h}_K(\varphi_K([\omega])) \quad \text{and} \quad Y = y_{K,n}(\omega).$$

Set $L = K(X, Y^2)$ which is a subfield of $K_\mathfrak{m}$ by Proposition 3.1 and the Weierstrass equation for $E_{K,n}$ stated in (2).

Suppose on the contrary that $K_\mathfrak{m} \neq L$. Then there is a nonidentity element σ of $\mathrm{Gal}(K_\mathfrak{m}/K)$, which leaves both X and Y^2 fixed. Note further that

$$\sigma \notin \mathrm{Gal}(K_\mathfrak{m}/H_K) \tag{9}$$

because $K_\mathfrak{m} = H_K(X)$ by Proposition 3.1 (ii). By applying σ on both sides of the equality

$$Y^2 = 4X^3 - AX - B \quad \text{with } A = \frac{J_K(J_K-1)}{27}\ell_K{}^{2n} \quad \text{and} \quad B = \frac{J_K(J_K-1)^2}{27^2}\ell_K{}^{3n},$$

we obtain

$$Y^2 = 4X^3 - A^\sigma X - B^\sigma.$$

It then follows that

$$(A^\sigma - A)X = B - B^\sigma. \tag{10}$$

Since

$$AB = \frac{\ell_K{}^{5n+1}}{27^3}$$

generates H_K over K by Lemma 4.3, we deduce by (9) and (10) that $A^\sigma - A \neq 0$ and

$$X = -\frac{B^\sigma - B}{A^\sigma - A} \in H_K.$$

Then we obtain

$$H_K = H_K(X) = K_\mathfrak{m},$$

which contradicts the hypothesis $K_\mathfrak{m} \supsetneq H_K$.

Therefore, we conclude that

$$K_\mathfrak{m} = L = K(x_{K,n}(\omega), y_{K,n}(\omega)^2).$$

□

Proposition 4.5. *Let K be an imaginary quadratic field other than $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-3})$, and let $\mathfrak{m}$ be a nontrivial proper integral ideal of $\mathcal{O}_K$. Let ω be an element of K such that $\omega + \mathcal{O}_K$ is a generator of the $\mathcal{O}_K$-module $\mathfrak{m}^{-1}/\mathcal{O}_K$. Then we have*

$$K_\mathfrak{m} = K(x_{K,n}(\omega)) \quad \textit{for sufficiently large } n \in \mathbb{Z}_{\geq 0}.$$

Proof. Note that $\ell_K = J(\tau_K)^2(J(\tau_K) - 1)^3$ is nonzero because K is different from $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-3})$. There are two possible cases: $h_K = 1$ or $h_K \geq 2$.

Case 1. If $h_K = 1$ (and so $H_K = K$), then for any $n \in \mathbb{Z}_{\geq 0}$

$$\begin{aligned} K(x_{K,n}(\omega)) &= H_K(\ell_K{}^n \mathfrak{h}_K(\varphi_K([\omega]))) \quad \text{by (3)} \\ &= H_K(\mathfrak{h}_K(\varphi_K([\omega]))) \quad \text{by Proposition 3.1 (i)} \\ &= K_\mathfrak{m} \quad \text{by Proposition 3.1 (ii)}. \end{aligned}$$

Case 2. Consider the case where $h_K \geq 2$. Let $\mathrm{Gal}(H_K/K) = \{\sigma_1 = \mathrm{id}, \sigma_2, \ldots, \sigma_{h_K}\}$ and $d = [K_\mathfrak{m} : H_K]$. Observe by Proposition 3.1 (i) that for each $i = 1, 2, \ldots, h_K$ there is a unique reduced form Q_i of discriminant d_K, and so $J(\tau_K)^{\sigma_i} = J(\tau_{Q_i})$. By Lemma 4.1 and Remark 4.2 we can take a sufficiently large positive integer m so that

$$\left|\frac{\ell_K{}^{\sigma_i}}{\ell_K}\right|^{md} = \left|\frac{J(\tau_{Q_i})^2(J(\tau_{Q_i}) - 1)^3}{J(\tau_K)^2(J(\tau_K) - 1)^3}\right|^{md} < \left|\frac{\mathrm{N}_{K_\mathfrak{m}/H_K}(\mathfrak{h}_K(\varphi_K([\omega])))}{\mathrm{N}_{K_\mathfrak{m}/H_K}(\mathfrak{h}_K(\varphi_K([\omega])))^{\sigma_i}}\right| \quad \text{for all } i = 2, 3, \ldots, h_K.$$

We then see by (3) and Proposition 3.1 (i) that if $n \in \mathbb{Z}_{\geq 0}$ satisfies $n \geq m$ and $2 \leq i \leq h_K$, then

$$\left|\frac{\mathrm{N}_{K_\mathfrak{m}/H_K}(x_{K,n}(\omega))^{\sigma_i}}{\mathrm{N}_{K_\mathfrak{m}/H_K}(x_{K,n}(\omega))}\right| = \left|\frac{\ell_K{}^{\sigma_i}}{\ell_K}\right|^{nd} \left|\frac{\mathrm{N}_{K_\mathfrak{m}/H_K}(\mathfrak{h}_K(\varphi_K([\omega])))^{\sigma_i}}{\mathrm{N}_{K_\mathfrak{m}/H_K}(\mathfrak{h}_K(\varphi_K([\omega])))}\right| < 1.$$

This observation implies that

$$K(N_{K_\mathfrak{m}/H_K}(x_{K,n}(\omega))) = H_K. \tag{11}$$

Hence we derive that if $n \geq m$, then

$$\begin{aligned} K(x_{K,n}(\omega)) &= K(x_{K,n}(\omega), N_{K_\mathfrak{m}/H_K}(x_{K,n}(\omega))) \quad \text{since } K(x_{K,n}(\omega)) \quad (\subseteq K_\mathfrak{m}) \quad \text{is an abelian extension of} \\ &\qquad K \\ &= H_K(x_{K,n}(\omega)) \quad \text{by (11)} \\ &= K_\mathfrak{m} \quad \text{by (3) and Proposition 3.1.} \end{aligned}$$

□

5 Generation of ray class fields by x-coordinates of elliptic curves

By using some interesting inequalities on special values of Siegel functions, we shall find a concrete bound of n in Proposition 4.5 for which if n is greater than or equal to this, then $x_{K,n}(\omega)$ generates $K_\mathfrak{m}$ over K.

Lemma 5.1. *Let $\mathbf{v} \in M_{1,2}(\mathbb{Q}) \setminus M_{1,2}(\mathbb{Z})$, and let $\tau \in \mathbb{H}$ such that $|q_\tau| = |e^{2\pi i \tau}| \leq e^{-\pi\sqrt{3}}$.*

(*i*) *We have*

$$|g_\mathbf{v}(\tau)| < 2.29|q_\tau|^{-\frac{1}{24}}.$$

(*ii*) *If $\mathbf{v} \in \frac{1}{N}M_{1,2}(\mathbb{Z}) \setminus M_{1,2}(\mathbb{Z})$ for an integer $N \geq 2$, then we obtain*

$$|g_\mathbf{v}(\tau)| > \frac{0.76|q_\tau|^{\frac{1}{12}}}{N}.$$

Proof. Let $\mathbf{v} = [v_1 \;\; v_2]$ and $z = v_1\tau + v_2$. By Proposition 2.2 (i) we may assume that $0 \leq v_1 \leq \frac{1}{2}$. Set $s = |q_\tau|$.

(i) We then derive that

$$\begin{aligned}
|g_{\mathbf{v}}(\tau)| &\leq |q_\tau|^{\frac{1}{2}(v_1^2-v_1+\frac{1}{6})}(1+|q_z|)\prod_{n=1}^{\infty}(1+|q_\tau|^n|q_z|)(1+|q_\tau|^n|q_z|^{-1}) \quad \text{by (5)}\\
&= s^{\frac{1}{2}(v_1^2-v_1+\frac{1}{6})}\left(1+s^{v_1}\right)\prod_{n=1}^{\infty}\left(1+s^{n+v_1}\right)\left(1+s^{n-v_1}\right)\\
&\leq s^{-\frac{1}{24}}(1+1)\prod_{n=1}^{\infty}(1+s^{n-\frac{1}{2}})^2 \quad \text{since}\, 0 \leq v_1 \leq \frac{1}{2} \text{ and } v_1^2 - v_1 + \frac{1}{6} \geq -\frac{1}{12}\\
&\leq 2s^{-\frac{1}{24}}\prod_{n=1}^{\infty}e^{2(e^{-\pi\sqrt{3}})^{n-\frac{1}{2}}} \quad \text{because } 1+x<e^x \text{ for } x>0\\
&= 2s^{-\frac{1}{24}}e^{2\sum_{n=1}^{\infty}(e^{-\pi\sqrt{3}})^{n-\frac{1}{2}}}\\
&= 2s^{-\frac{1}{24}}e^{\frac{2e^{-\frac{\pi\sqrt{3}}{2}}}{1-e^{-\pi\sqrt{3}}}}\\
&< 2.29\ s^{-\frac{1}{24}}.
\end{aligned}$$

(ii) Furthermore, we see that

$$\begin{aligned}
|g_{\mathbf{v}}(\tau)| &\geq s^{\frac{1}{2}(v_1^2-v_1+\frac{1}{6})}|1-q_z|\prod_{n=1}^{\infty}\left(1-s^{n+v_1}\right)\left(1-s^{n-v_1}\right) \quad \text{by (5)}\\
&\geq s^{\frac{1}{12}}\min\left\{|1-e^{\frac{2\pi\mathrm{i}}{N}}|,\, 1-s^{\frac{1}{N}}\right\}\prod_{n=1}^{\infty}(1-s^{n-\frac{1}{2}})^2 \quad \text{because } v_1^2-v_1+\frac{1}{6} \leq \frac{1}{6}\\
&\geq s^{\frac{1}{12}}\min\left\{\sin\frac{\pi}{N},\, 1-(e^{-\pi\sqrt{3}})^{\frac{1}{N}}\right\}\prod_{n=1}^{\infty}e^{-4(e^{-\pi\sqrt{3}})^{n-\frac{1}{2}}} \quad \text{since } 1-x>e^{-2x} \text{ for } 0<x<\frac{1}{2}\\
&> s^{\frac{1}{12}}\frac{1}{N}e^{-4\sum_{n=1}^{\infty}(e^{-\pi\sqrt{3}})^{n-\frac{1}{2}}} \quad \text{because both } \sin(\pi x) \text{ and } 1-e^{-\pi\sqrt{3}x} \text{ are } > x \text{ for } 0<x\leq\frac{1}{2}\\
&= s^{\frac{1}{12}}\frac{1}{N}e^{\frac{-4e^{-\frac{\pi\sqrt{3}}{2}}}{1-e^{-\pi\sqrt{3}}}}\\
&> \frac{0.76s^{\frac{1}{12}}}{N}.
\end{aligned}$$

□

Theorem 5.2. *Let K be an imaginary quadratic field other than $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-3})$. Let $\mathfrak{m}$ be a proper nontrivial ideal of $\mathcal{O}_K$ in which $N_\mathfrak{m}$ (≥ 2) is the least positive integer. Let ω be an element of K such that $\omega + \mathcal{O}_K$ is a generator of the $\mathcal{O}_K$-module $\mathfrak{m}^{-1}/\mathcal{O}_K$. If $K_\mathfrak{m}$ properly contains H_K, then*

$$K_\mathfrak{m} = K(x_{K,n}(\omega))$$

for every nonnegative integer n satisfying

$$n \geq \frac{\frac{13}{24}\pi\sqrt{|d_K|} + 6\ln\left(\frac{229}{76}N_\mathfrak{m}\right)}{\frac{5}{2}\pi\sqrt{|d_K|} - \ln 877{,}383} - \frac{1}{6}. \tag{12}$$

Proof. Since $N_\mathfrak{m}\mathcal{O}_K \subseteq \mathfrak{m}$ and $\omega \in \mathfrak{m}^{-1}\backslash\mathcal{O}_K$, we have

$$N_\mathfrak{m}\omega = a\tau_K + b \quad \text{for some } a, b \in \mathbb{Z} \text{ such that } [a \;\; b] \notin N_\mathfrak{m}M_{1,2}(\mathbb{Z}). \tag{13}$$

Let n be a nonnegative integer satisfying (12). If $h_K = 1$, then the assertion holds by the proof (Case 1) of Proposition 4.5.

Now, we assume $h_K \geq 2$. Since $K_\mathfrak{m}$ properly contains H_K, one can take a nonidentity element ρ of $\mathrm{Gal}(K_\mathfrak{m}/H_K)$. Note that ρ does not fix $x_{K,n}(\omega)$ due to the fact $K_\mathfrak{m} = H_K(x_{K,n}(\omega))$ by (3) and Proposition 3.1 (ii). Suppose on the contrary that $x_{K,n}(\omega)$ does not generate $K_\mathfrak{m}$ over K. Then there exists at least one nonidentity element σ in $\mathrm{Gal}(K_\mathfrak{m}/K(x_{K,n}(\omega))) = \mathrm{Gal}(H_K(x_{K,n}(\omega))/K(x_{K,n}(\omega)))$. Let P be a quadratic form in $\mathcal{Q}_{N_\mathfrak{m}}(d_K)$ such that $[P]_{N_\mathfrak{m}}$ maps to σ through the surjection

$$\begin{array}{ccccc} \mathrm{C}_{N_\mathfrak{m}}(d_K) & \xrightarrow{\sim} & \mathrm{Gal}\big(K_{(N_\mathfrak{m})}/K\big) & \xrightarrow{\text{restriction}} & \mathrm{Gal}(K_\mathfrak{m}/K) \\ & & \mu & \mapsto & \mu\,|_{K_\mathfrak{m}} \end{array}$$

whose first map is the isomorphism given in Proposition 3.2. It follows from (7), Proposition 3.2, and Remark 3.3 that

$$P = Q^\gamma \quad \text{for some nonpricipal reduced form } Q \quad \text{and } \gamma \in \mathrm{SL}_2(\mathbb{Z}).$$

Here we observe that

$$\tau_P = \gamma^{-1}(\tau_Q) \quad \text{and} \quad a_Q \geq 2. \tag{14}$$

Then we deduce that

$$\begin{aligned}
1 &= \left| \frac{(x_{K,n}(\omega) - x_{K,n}(\omega)^\rho)^\sigma}{x_{K,n}(\omega) - x_{K,n}(\omega)^\rho} \right| \\
&\quad \text{because } \sigma \text{ is the identity on } K(x_{K,n}(\omega)) \text{ which contains } x_{K,n}(\omega)^\rho \\
&= \left| \frac{(\ell_K{}^n f_\mathbf{u}(\tau_K) - (\ell_K{}^n f_\mathbf{u}(\tau_K))^\rho)^\sigma}{\ell_K{}^n f_\mathbf{u}(\tau_K) - (\ell_K{}^n f_\mathbf{u}(\tau_K))^\rho} \right| \quad \text{with } \mathbf{u} = \begin{bmatrix} \frac{a}{N_\mathfrak{m}} & \frac{b}{N_\mathfrak{m}} \end{bmatrix} \\
&\quad \text{by (3), (13), and the definitions of } \mathfrak{h}_K,\ \varphi_K \text{ and a Fricke function} \\
&= \left| \frac{\{J(\tau_K)^{2n}(J(\tau_K)-1)^{3n}(f_\mathbf{u}(\tau_K) - f_\mathbf{v}(\tau_K))\}^\sigma}{J(\tau_K)^{2n}(J(\tau_K)-1)^{3n}(f_\mathbf{u}(\tau_K) - f_\mathbf{v}(\tau_K))} \right| \\
&\quad \text{for some } \mathbf{v} \in \frac{1}{N_\mathfrak{m}} M_{1,2}(\mathbb{Z}) \setminus M_{1,2}(\mathbb{Z}) \text{ such that } \mathbf{u} \not\equiv \mathbf{v} \text{ and } -\mathbf{v} \pmod{M_{1,2}(\mathbb{Z})} \\
&\quad \text{by Proposition 3.1(ii) and (4) since } \rho \in \mathrm{Gal}(K_\mathfrak{m}/H_K) \setminus \big\{\mathrm{id}_{K_\mathfrak{m}}\big\} \\
&= \left| \frac{J(\tau_P)^2(J(\tau_P)-1)^3}{J(\tau_K)^2(J(\tau_K)-1)^3} \right|^n \left| \frac{f_{\mathbf{u}'}(\tau_P) - f_{\mathbf{v}'}(\tau_P)}{f_\mathbf{u}(\tau_K) - f_\mathbf{v}(\tau_K)} \right| \\
&\quad \text{for some } \mathbf{u}', \mathbf{v}' \in \frac{1}{N_\mathfrak{m}} M_{1,2}(\mathbb{Z}) \setminus M_{1,2}(\mathbb{Z}) \text{ such that } \mathbf{u}' \not\equiv \mathbf{v}' \text{ and } -\mathbf{v}' \pmod{M_{1,2}(\mathbb{Z})} \\
&\quad \text{by Proposition 3.2} \\
&= \left| \frac{J(\gamma^{-1}(\tau_Q))^2(J(\gamma^{-1}(\tau_Q))-1)^3}{J(\tau_K)^2(J(\tau_K)-1)^3} \right|^n \left| \frac{f_{\mathbf{u}'}(\gamma^{-1}(\tau_Q)) - f_{\mathbf{v}'}(\gamma^{-1}(\tau_Q))}{f_\mathbf{u}(\tau_K) - f_\mathbf{v}(\tau_K)} \right| \quad \text{by (14)} \\
&= \left| \frac{J(\tau_Q)^2(J(\tau_Q)-1)^3}{J(\tau_K)^2(J(\tau_K)-1)^3} \right|^n \left| \frac{f_{\mathbf{u}''}(\tau_Q) - f_{\mathbf{v}''}(\tau_Q)}{f_\mathbf{u}(\tau_K) - f_\mathbf{v}(\tau_K)} \right| \quad \text{with } \mathbf{u}'' = \mathbf{u}'\gamma^{-1} \text{ and } \mathbf{v}'' = \mathbf{v}'\gamma^{-1} \\
&\quad \text{by the fact } J \in \mathcal{F}_1 \text{ and Proposition 2.1} \\
&= \left| \frac{J(\tau_Q)^2(J(\tau_Q)-1)^3}{J(\tau_K)^2(J(\tau_K)-1)^3} \right|^{n+\frac{1}{6}} \left| \frac{g_{\mathbf{u}''+\mathbf{v}''}(\tau_Q) g_{\mathbf{u}''-\mathbf{v}''}(\tau_Q) g_\mathbf{u}(\tau_K)^2 g_\mathbf{v}(\tau_K)^2}{g_{\mathbf{u}+\mathbf{v}}(\tau_K) g_{\mathbf{u}-\mathbf{v}}(\tau_K) g_{\mathbf{u}''}(\tau_Q)^2 g_{\mathbf{v}''}(\tau_Q)^2} \right| \quad \text{by Lemma 2.3} \\
&< \left(877{,}383\ |q_{\tau_K}|^{\frac{5}{2}} \right)^{n+\frac{1}{6}} \frac{2.29^6 |q_{\tau_Q}|^{-\frac{1}{12}} |q_{\tau_K}|^{-\frac{1}{6}}}{\left(\frac{0.76}{N_\mathfrak{m}}\right)^6 |q_{\tau_K}|^{\frac{1}{6}} |q_{\tau_Q}|^{\frac{1}{3}}} \quad \text{by Lemmas 4.1, 5.1, and Remark 4.2} \\
&\quad \text{because } |q_{\tau_K}| = e^{-\pi\sqrt{|d_K|}} \leq e^{-\pi\sqrt{15}} \text{ and } |q_{\tau_Q}| = e^{-\frac{\pi\sqrt{|d_K|}}{a_Q}} \leq e^{-\pi\sqrt{3}} \text{ by (6)} \\
&= \left(877{,}383\ |q_{\tau_K}|^{\frac{5}{2}} \right)^{n+\frac{1}{6}} \left(\frac{229}{76} N_\mathfrak{m} \right)^6 |q_{\tau_Q}|^{-\frac{5}{12}} |q_{\tau_K}|^{-\frac{1}{3}} \\
&\leq \left(877{,}383\ |q_{\tau_K}|^{\frac{5}{2}} \right)^{n+\frac{1}{6}} \left(\frac{229}{76} N_\mathfrak{m} \right)^6 |q_{\tau_K}|^{-\frac{5}{24}} |q_{\tau_K}|^{-\frac{1}{3}} \\
&\quad \text{since } |q_{\tau_K}|^{-1} > 1 \text{ and } |q_{\tau_Q}|^{-1} = (|q_{\tau_K}|^{-1})^{\frac{1}{a_Q}} \leq (|q_{\tau_K}|^{-1})^{\frac{1}{2}} \text{ by (14)} \\
&= \left(877{,}383\ e^{-\frac{5}{2}\pi\sqrt{|d_K|}} \right)^{n+\frac{1}{6}} \left(\frac{229}{76} N_\mathfrak{m} \right)^6 e^{\frac{13}{24}\pi\sqrt{|d_K|}}.
\end{aligned}$$

Now, by taking logarithm we obtain the inequality

$$0<\left(n+\frac{1}{6}\right)\left(\ln 877{,}383-\frac{5}{2}\pi\sqrt{|d_K|}\right)+6\ln\left(\frac{229}{76}N_{\mathfrak{m}}\right)+\frac{13}{24}\pi\sqrt{|d_K|}$$

with

$$\ln 877{,}383-\frac{5}{2}\pi\sqrt{|d_K|}\le \ln 877{,}383-\frac{5}{2}\pi\sqrt{15}<0.$$

But this contradicts (12). Therefore, we conclude that $K_{\mathfrak{m}}=K(x_{K,n}(\omega))$. □

Example 5.3. Let $K=\mathbb{Q}(\sqrt{-5})$, and so $d_K=-20$. Note that

$$\begin{cases} 2\text{ is ramified in } K & \text{since } 2\mid d_K,\\ 13\text{ is inert in } K & \text{due to } \left(\dfrac{d_K}{13}\right)=-1,\\ 23\text{ splits completely in } K & \text{because } \left(\dfrac{d_K}{23}\right)=1 \end{cases}$$

([9, Proposition 5.16]). Let $\mathfrak{m}=\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$ be the product of three prime ideals

$$\mathfrak{p}_1=[1+\sqrt{-5},2],\quad \mathfrak{p}_2=[13\sqrt{-5},13],\quad\text{and}\quad \mathfrak{p}_3=[15+\sqrt{-5},23]$$

of $\mathcal{O}_K$ satisfying $2\mathcal{O}_K=\mathfrak{p}_1^2$, $13\mathcal{O}_K=\mathfrak{p}_2$, and $23\mathcal{O}_K=\mathfrak{p}_3\overline{\mathfrak{p}}_3$. In this case, by checking the degree formula for $[K_{\mathfrak{m}}:H_K]$ we see that $K_{\mathfrak{m}}$ properly contains H_K. Since

$$\mathfrak{m}=\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\supset\mathfrak{p}_1^2\mathfrak{p}_2\mathfrak{p}_3\overline{\mathfrak{p}}_3=(2\cdot 13\cdot 23)\mathcal{O}_K,$$

we obtain $N_{\mathfrak{m}}=2\cdot 13\cdot 23=598$, and hence one can estimate

$$\frac{\frac{13}{24}\pi\sqrt{|d_K|}+6\ln\left(\frac{229}{76}N_{\mathfrak{m}}\right)}{\frac{5}{2}\pi\sqrt{|d_K|}-\ln 877{,}383}-\frac{1}{6}=\frac{\frac{13}{24}\pi\sqrt{20}+6\ln\left(\frac{229}{76}\cdot 598\right)}{\frac{5}{2}\pi\sqrt{20}-\ln 877{,}383}-\frac{1}{6}\approx 2.286282.$$

If ω is an element of K such that $\omega+\mathcal{O}_K$ is a generator of the $\mathcal{O}_K$-module $\mathfrak{m}^{-1}/\mathcal{O}_K$, then we obtain by Theorem 5.2 that

$$K_{\mathfrak{m}}=K(x_{K,n}(\omega))\quad\text{for all } n\ge 3.$$

Remark 5.4. At this stage, we conjecture that Theorem 5.2 may hold for every $n\in\mathbb{Z}_{\ge 0}$.

6 Ray class fields of special moduli

Let K be an imaginary quadratic field other than $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-3})$, and let N (≥ 2) be an integer whose prime factors are all inert in K. In this last section, we consider the special case where $\mathfrak{m}=N\mathcal{O}_K$ and show that Theorem 5.2 is also true for every $n\in\mathbb{Z}_{\ge 0}$.

Lemma 6.1. *Let $f\in\mathcal{F}_1$. If f has neither a zero nor a pole on $\mathbb{H}$, then it is a nonzero rational number.*

Proof. See [2, Theorem 2 in Chapter 5] and [17, Lemma 2.1]. □

For an integer $N\ge 2$, let

$$S_N=\{[s\quad t]\in M_{1,2}(\mathbb{Z})\mid 0\le s,t<N\text{ and }\gcd(N,s,t)=1\}.$$

We define an equivalence relation $\equiv_N$ on the set S_N as follows: for $\mathbf{u},\mathbf{v}\in S_N$

$$\mathbf{u} \equiv_N \mathbf{v} \quad \Leftrightarrow \quad \mathbf{u} \equiv \mathbf{v} \text{ or } -\mathbf{v} \pmod{NM_{1,2}(\mathbb{Z})}.$$

Let

$$P_N = \{(\mathbf{u},\mathbf{v}) \mid \mathbf{u},\mathbf{v} \in S_N \text{ such that } \mathbf{u} \not\equiv_N \mathbf{v}\} \quad \text{and} \quad m_N = |P_N|.$$

Since $[1 \ \ 0]$, $[0 \ \ 1]$ represent distinct classes in $S_N/\equiv_N$, we claim $m_N \geq 2$.

Lemma 6.2. *If N is an integer such that $N \geq 2$, then we have*

$$\prod_{(\mathbf{u},\mathbf{v})\in P_N} \left(f_{\frac{1}{N}\mathbf{u}} - f_{\frac{1}{N}\mathbf{v}}\right)^6 = k\{J^2(J-1)^3\}^{m_N} \quad \textit{for some } k \in \mathbb{Q}\setminus\{0\}.$$

Proof. For $[a \ \ b] \in M_{1,2}(\mathbb{Z})$ with $\gcd(N,a,b) = 1$, let $\pi_N([a \ \ b])$ denote the unique element of S_N satisfying

$$\pi_N([a \ \ b]) \equiv [a \ \ b] \pmod{NM_{1,2}(\mathbb{Z})}.$$

Let $\alpha \in M_2(\mathbb{Z})$ with $\gcd(N, \det(\alpha)) = 1$, and let $\tilde{\alpha}$ be its image in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\langle -I_2\rangle$ ($\simeq \mathrm{Gal}(\mathcal{F}_N/\mathcal{F}_1)$). Setting

$$f = \prod_{(\mathbf{u},\mathbf{v})\in P_N} \left(f_{\frac{1}{N}\mathbf{u}} - f_{\frac{1}{N}\mathbf{v}}\right)^6,$$

we find that

$$f^{\tilde{\alpha}} = \prod_{(\mathbf{u},\mathbf{v})\in P_N} \left(f_{\frac{1}{N}\mathbf{u}\tilde{\alpha}} - f_{\frac{1}{N}\mathbf{v}\tilde{\alpha}}\right)^6 \quad \text{by Proposition 2.1} = \prod_{(\mathbf{u},\mathbf{v})\in P_N} \left(f_{\frac{1}{N}\pi_N(\mathbf{u}\alpha)} - f_{\frac{1}{N}\pi_N(\mathbf{v}\alpha)}\right)^6 \quad \text{by (4)} \ = f$$

because the mapping $S_N \to S_N$, $\mathbf{u} \mapsto \pi_N(\mathbf{u}\alpha)$, gives rise to an injection (and so, a bijection) of P_N into itself. This observation implies by the Galois theory that f lies in $\mathcal{F}_1$.

On the other hand, we attain

$$\begin{aligned} f &= \prod_{(\mathbf{u},\mathbf{v})\in P_N} \frac{J^2(J-1)^3}{3^9} \frac{g^6_{\frac{1}{N}(\mathbf{u}+\mathbf{v})} g^6_{\frac{1}{N}(\mathbf{u}-\mathbf{v})}}{g^{12}_{\frac{1}{N}\mathbf{u}} g^{12}_{\frac{1}{N}\mathbf{v}}} \quad \text{by Lemma 2.3} \\ &= g\left\{\frac{J^2(J-1)^3}{3^9}\right\}^{m_N} \quad \text{with } g = \prod_{(\mathbf{u},\mathbf{v})\in P_N} \frac{g^6_{\frac{1}{N}(\mathbf{u}+\mathbf{v})} g^6_{\frac{1}{N}(\mathbf{u}-\mathbf{v})}}{g^{12}_{\frac{1}{N}\mathbf{u}} g^{12}_{\frac{1}{N}\mathbf{v}}}. \end{aligned}$$

Since f and J belong to $\mathcal{F}_1$, so does g. Moreover, since g has neither a zero nor a pole on $\mathbb{H}$, it is a nonzero rational number by Lemma 6.1. Therefore, we obtain

$$f = k\{J^2(J-1)^3\}^{m_N} \quad \text{for some } k \in \mathbb{Q}\setminus\{0\}.$$

□

Lemma 6.3. *Let K be an imaginary quadratic field and N be an integer with $N \geq 2$. If every prime factor of N is inert in K, then the principal ideal $(s\tau_K + t)\mathcal{O}_K$ is relatively prime to $N\mathcal{O}_K$ for all $s, t \in \mathbb{Z}$ such that* $\gcd(N, s, t) = 1$.

Proof. We see that

$$\mathrm{N}_{K/\mathbb{Q}}(s\tau_K + t) = (s\tau_K + t)(s\overline{\tau}_K + t) = \tau_K\overline{\tau}_K s^2 + (\tau_K + \overline{\tau}_K)st + t^2 = c_K s^2 - b_K st + t^2.$$

Now, we claim that $\mathrm{N}_{K/\mathbb{Q}}(s\tau_K + t)$ is relatively prime to N. Indeed, we have two cases: $d_K \equiv 0 \pmod 4$ or $d_K \equiv 1 \pmod 4$.

Case 1. Consider the case where $d_K \equiv 0 \pmod 4$, and then $b_K = 0$ and $c_K = -\frac{d_K}{4}$. Let p be a prime factor of N. Since p is inert in K, it must be odd and satisfy $\left(\frac{d_K}{p}\right) = -1$. If

$$\mathrm{N}_{K/\mathbb{Q}}(s\tau_K + t) = -\frac{d_K}{4}s^2 + t^2 \equiv 0 \pmod p,$$

then the fact $\left(\frac{d_K}{p}\right) = -1$ forces us to obtain $s \equiv 0 \pmod{p}$ and so $t \equiv 0 \pmod{p}$. But this contradicts the fact $\gcd(N, s, t) = 1$. Therefore, $\mathrm{N}_{K/\mathbb{Q}}(s\tau_K + t)$ is relatively prime to p, and hence to N.

Case 2. Let $d_K \equiv 1 \pmod{4}$, and so $b_K = 1$ and $c_K = \frac{1-d_K}{4}$. Let p be a prime factor of N. Since p is inert in K, we derive

$$\begin{cases} d_K \equiv 5 \pmod{8} & \text{if } p = 2, \\ \left(\dfrac{d_K}{p}\right) = -1 & \text{if } p > 2. \end{cases}$$

Then we find that

$$\mathrm{N}_{K/\mathbb{Q}}(s\tau_K + t) = \frac{1-d_K}{4}s^2 - st + t^2 \equiv \begin{cases} s^2 + st + t^2 \pmod{p} & \text{if } p = 2, \\ 4'\{(s-2t)^2 - d_K s^2\} \pmod{p} & \text{if } p > 2, \end{cases}$$

where $4'$ is an integer such that $4 \cdot 4' \equiv 1 \pmod{p}$. When $p = 2$, we see that $s^2 + st + t^2 \equiv 1 \pmod{p}$ because s and t are not both even. When $p > 2$, if $\mathrm{N}_{K/\mathbb{Q}}(s\tau_K + t) \equiv 0 \pmod{p}$, then the fact $\left(\frac{d_K}{p}\right) = -1$ yields that $s \equiv 0 \pmod{p}$ and so $t \equiv 0 \pmod{p}$. But this again contradicts $\gcd(N, s, t) = 1$. Hence $\mathrm{N}_{K/\mathbb{Q}}(s\tau_K + t)$ is relatively prime to p, and so to N. Therefore, the principal ideal $(s\tau_K + t)\mathcal{O}_K$ is relatively prime to $N\mathcal{O}_K$. □

Theorem 6.4. *Let K be an imaginary quadratic field other than $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-3})$, and let N be an integer such that $N \geq 2$. Let ω be an element of K so that $\omega + \mathcal{O}_K$ is a generator of the $\mathcal{O}_K$-module $N^{-1}\mathcal{O}_K/\mathcal{O}_K$. If every prime factor of N is inert in K, then we attain*

$$K_{(N)} = K(x_{K,n}(\omega)) \quad \textit{for every } n \in \mathbb{Z}_{\geq 0}.$$

Proof. Since $K_{(N)}$ is an abelian extension of K, $K(x_{K,n}(\omega))$ is also an abelian extension of K containing $x_{K,n}\left(\frac{1}{N}\right)$ by Proposition 3.1 (ii). Since

$$(s\tau_K + t)\mathcal{O}_K \in P_K(N\mathcal{O}_K) \quad \text{for all } [s \;\; t] \in S_N$$

by Lemma 6.3, we obtain by Proposition 3.1 (ii) that

$$x_{K,n}\left(\frac{s\tau_K + t}{N}\right) \in K(x_{K,n}(\omega)) \quad \text{for all } [s \;\; t] \in S_N.$$

We then deduce that

$$\begin{aligned} K(x_{K,n}(\omega)) \ni & \prod_{(\mathbf{u},\mathbf{v})\in P_N} \left(x_{K,n}\left(\frac{u_1\tau_K + u_2}{N}\right) - x_{K,n}\left(\frac{v_1\tau_K + v_2}{N}\right)\right)^6 \quad \text{with } \mathbf{u} = [u_1 \;\; u_2] \text{ and } \mathbf{v} = [v_1 \;\; v_2] \\ = & \prod_{(\mathbf{u},\mathbf{v})\in P_N} \left(\ell_K{}^n \mathfrak{h}_K\left(\varphi_K\left(\left[\frac{u_1\tau_K + u_2}{N}\right]\right)\right) - \ell_K{}^n \mathfrak{h}_K\left(\varphi_K\left(\left[\frac{v_1\tau_K + v_2}{N}\right]\right)\right)\right)^6 \quad \text{by (3)} \\ = & \prod_{(\mathbf{u},\mathbf{v})\in P_N} \left\{\left(\frac{\ell_K{}^n}{2^7 3^5}\right)^6 \left(f_{\frac{1}{N}\mathbf{u}}(\tau_K) - f_{\frac{1}{N}\mathbf{v}}(\tau_K)\right)^6\right\} \\ & \text{by the definitions of } \varphi_K, \mathfrak{h}_K \text{ and Fricke functions} \\ = & \left(\frac{\ell_K{}^n}{2^7 3^5}\right)^{6m_N} \left\{\prod_{(\mathbf{u},\mathbf{v})\in P_N} \left(f_{\frac{1}{N}\mathbf{u}} - f_{\frac{1}{N}\mathbf{v}}\right)^6\right\}(\tau_K) \\ = & \left(\frac{\ell_K{}^n}{2^7 3^5}\right)^{6m_N} [k\{J^2(J-1)^3\}^{m_N}](\tau_K) \quad \text{for some } k \in \mathbb{Q}\setminus\{0\} \text{ by Lemma 6.2} \\ = & k\left(\frac{\ell_K{}^{6n+1}}{2^{42}3^{30}}\right)^{m_N}. \end{aligned}$$

Therefore, we achieve that

$$\begin{aligned} K(x_{K,n}(\omega)) &= K\left(x_{K,n}(\omega),\, k\left(\frac{\ell_K{}^{6n+1}}{2^{42}3^{30}}\right)^{m_N}\right) \\ &= H_K(x_{K,n}(\omega)) \quad \text{by Lemma 4.3} \\ &= K_{(N)} \quad \text{by (3) and Proposition 3.1.} \end{aligned}$$

□

Acknowledgments: Ho Yun Jung was supported by the research fund of Dankook University in 2020 and by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (No. 2020R1F1A1A01073055). Dong Hwa Shin was supported by Hankuk University of Foreign Studies Research Fund of 2022 and by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (No. 2020R1F1A1A01048633).

Conflict of interest: All authors state no conflict of interest.

References

[1] J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, 2nd ed., Springer New York, Dordrecht, 2009.

[2] S. Lang, *Elliptic functions*, With an appendix by J. Tate, Graduate Texts in Mathematics, 2nd ed., Spinger-Verlag, New York, 1987.

[3] G. Frei, F. Lemmermeyer, and P. Roquette, *Emil Artin and Helmut Hasse-the Correspondence 1923-1958, Contributions in Mathematical and Computational Sciences*, Vol. 5, Springer Basel, Heidelberg, 2014.

[4] M. Sugawara, *On the so-called Kronecker's dream in youngdays*, Proc. Phys. Math. Soc. Jpn. **15** (1993), 99–107.

[5] M. Sugawara, *Zur theorie der Komplexen multiplikation. I, II*, J. Reine Angew. Math. **1936** (1936), no. 175, 189–191, 65–68.

[6] H. Y. Jung, J. K. Koo, and D. H. Shin, *Generation of ray class fields modulo 2, 3, 4, or 6 by using the Weber function*, J. Korean Math. Soc. **55** (2018), no. 2, 343–372.

[7] J. K. Koo, D. H. Shin, and D. S. Yoon, *On a problem of Hasse and Ramachandra*, Open Math. **17** (2019), no. 1, 131–140.

[8] K. Ramachandra, *Some applications of Kronecker's limit formula*, Ann. of Math. (2) **80** (1964), no. 1, 104–148.

[9] D. A. Cox, *Primes of the form $x^2 + ny^2$: Fermat, class field theory, and complex multiplication*, Pure and Applied Mathematics (Hoboken), 2nd ed., John Wiley & Sons, Inc., Hoboken, NJ, 2013.

[10] R. Schertz, *Complex Multiplication, New Mathematical Monographs 15*, Cambridge University Press, Cambridge, 2010.

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

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

[13] I. S. Eum, J. K. Koo, and D. H. Shin, *Binary quadratic forms and ray class groups*, Proc. Roy. Soc. Edinburgh Sect. A **150** (2020), no. 2, 695–720.

[14] H. Y. Jung, J. K. Koo, and D. H. Shin, *On some extensions of Gauss' work and applications*, Open Math **18** (2020), no. 1, 1915–1934.

[15] C. F. Gauss, *Disquisitiones Arithmeticae*, In commiss. apud Gerh. Fleischer, jun, Leipzig, 1801.

[16] J. P. G. L. Dirichlet, *Zahlentheorie*, 4th ed., Vieweg, Braunschweig, 1894.

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