JOURNAL OF THE
CHUNGCHEONG MATHEMATICAL SOCIETY
Volume **34**, No. 4, November 2021
http://dx.doi.org/10.14403/jcms.2021.34.4.317

# GENERATION OF RAY CLASS FIELDS OF IMAGINARY QUADRATIC FIELDS

Ho Yun Jung

Abstract. Let $K$ be an imaginary quadratic field other than $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-3})$, and let $\mathcal{O}_K$ be its ring of integers. Let $N$ be a positive integer such that $N = 5$ or $N \geq 7$. In this paper, we generate the ray class field modulo $N\mathcal{O}_K$ over $K$ by using a single $x$-coordinate of an elliptic curve with complex multiplication by $\mathcal{O}_K$.

## 1. Introduction

Let $K$ be an imaginary quadratic field with ring of integers $\mathcal{O}_K$. Assume that $K$ is different from $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-3})$. For each non-negative integer $n$, let $E_{K,n}$ be the elliptic curve with $j$-invariant $j(\mathcal{O}_K)$ given by the Weierstrass equation

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

where

$$J_K = \frac{1}{1728}\, j(\mathcal{O}_K) \quad \text{and} \quad C_K = J_K^2(J_K-1)^3.$$

Then we have a complex analytic isomorphism of complex Lie groups

$$\begin{array}{rcl} \mathbb{C}/\mathcal{O}_K & \xrightarrow{\sim} & E_{K,n}(\mathbb{C}) \ (\subset \mathbb{P}^2(\mathbb{C})) \\ z + \mathcal{O}_K & \mapsto & [x_{K,n}(z) : y_{K,n}(z) : 1] \end{array}$$

Received August 12, 2021; Accepted September 23, 2021.
2010 Mathematics Subject Classification: Primary 11F03; Secondary 11G15, 11R37.
Key words and phrases: Class field theory, complex multiplication, modular functions.
This research was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIT)(No. 2020R1F1A1A01073055).

with

$$x_{K,\,n}(z) = C_K^n \frac{g_2(\mathcal{O}_K)g_3(\mathcal{O}_K)}{\Delta(\mathcal{O}_K)}\wp(z;\,\mathcal{O}_K),$$

$$y_{K,\,n}(z) = \sqrt{\left(C_K^n \frac{g_2(\mathcal{O}_K)g_3(\mathcal{O}_K)}{\Delta(\mathcal{O}_K)}\right)^3}\wp'(z;\,\mathcal{O}_K).$$

(See [13, Chapter VI].)

Let $H_K$ be the Hilbert class field of $K$. Furthermore, for a nontrivial ideal $\mathfrak{m}$ of $\mathcal{O}_K$, let $K_\mathfrak{m}$ be the ray class field of $K$ modulo $\mathfrak{m}$. (See [1, §8] or [3, Chapter V].) Now, let $\mathfrak{m} \neq \mathcal{O}_K$ and $\omega$ be an element of $K$ such that $\omega + \mathcal{O}_K$ is a generator of the $\mathcal{O}_K$-module $\mathfrak{m}^{-1}\mathcal{O}_K/\mathcal{O}_K$. As is well known, $x_{K,\,n}(\omega)$ for such $\omega$ are all Galois conjugate over $H_K$ ([10, Theorem 7 and its corollary in Chapter 10]). Set

$$B_{K,\,\mathfrak{m}} = \frac{\frac{13}{24}\pi\sqrt{|d_K|} + 6\ln(\frac{229}{76}N_\mathfrak{m})}{\frac{5}{2}\pi\sqrt{|d_K|} - \ln 877383} - \frac{1}{6} \quad (\in \mathbb{R})$$

where $d_K$ $(< 0)$ is the discriminant of $K$ and $N_\mathfrak{m}$ is the least positive integer in $\mathfrak{m}$. Recently, Jung, Koo and Shin ([6, Theorem 5.2]) proved that if $K_\mathfrak{m}$ properly contains $H_K$, then

$$K_\mathfrak{m} = K\left(x_{K,\,n}(\omega)\right) \quad \text{for all } n \geq B_{K,\,\mathfrak{m}},$$

which would be an answer to a problem of Hasse and Ramachandra on generation of class fields in terms of the Weber function ([2, p. 91] and [11, p. 105]).

In this paper, we focus on the special case where $\mathfrak{m} = N\mathcal{O}_K$ for a positive integer $N$ such that $N = 5$ or $N \geq 7$. By utilizing Shimura's reciprocity law and some inequalities on special values of meromorphic modular functions, we shall reduce the bound $B_{K,\,\mathfrak{m}}$ of $n$ so that

$$K_\mathfrak{m} = K_{(N)} = K\left(x_{K,\,n}(\omega)\right) \quad \text{for all } n \geq \frac{\frac{1}{8}\pi\sqrt{|d_K|} + 2\ln(4.263N)}{\frac{5}{2}\pi\sqrt{|d_K|} - \ln 877383} - \frac{1}{6}$$

(Theorem 5.2). Besides, Koo, Shin and Yoon showed in [9] that

$$K_{(N)} = K\left(x_{K,\,0}(\tfrac{1}{N})\right) \text{ or } K\left(x_{K,\,0}(\tfrac{2}{N})\right)$$

by using the second Kronecker's limit formula.

## 2. Fields of modular functions

We shall briefly review some basic properties of Fricke functions and Siegel functions as modular functions.

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

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

(See [1, §10.B] or [10, §3.3].) For $\mathbf{v} = \begin{bmatrix} v_1 & v_2 \end{bmatrix} \in M_{1,2}(\mathbb{Q}) \setminus M_{1,2}(\mathbb{Z})$, let $f_{\mathbf{v}}$ and $g_{\mathbf{v}}$ be the Fricke function and the Siegel function on $\mathbb{H}$, respectively, defined as follows:

$$(2.1)\quad f_{\mathbf{v}}(\tau) = -2^7 3^5\,\frac{g_2(\tau)g_3(\tau)}{\Delta(\tau)}\,\wp(z;\, \mathbb{Z}\tau + \mathbb{Z}),$$

$$(2.2)\quad g_{\mathbf{v}}(\tau) = -e^{\pi \mathrm{i} v_2(v_1-1)} q_\tau^{\frac{1}{2}(v_1^2 - v_1 + \frac{1}{6})}(1-q_z)\prod_{n=1}^{\infty}(1-q_\tau^n q_z)(1-q_\tau^n q_z^{-1}),$$

where $z = v_1\tau + v_2$, $q_\tau = e^{2\pi \mathrm{i}\tau}$ and $q_z = e^{2\pi \mathrm{i} z}$. (For the original definition of $g_{\mathbf{v}}$, one can refer to [8, §2.1]. ) For a positive integer $N$, let

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

The field $\mathcal{F}_N$ is a Galois extension of $\mathcal{F}_1$ such that

$$\mathrm{Gal}(\mathcal{F}_N/\mathcal{F}_1) \;\simeq\; \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\langle -I_2 \rangle.$$

Moreover, it coincides with the field of meromorphic modular functions of level $N$ whose Fourier coefficients lie in the $N$th cyclotomic field ([12, Theorem 6.6 and Proposition 6.9]).

Proposition 2.1. *Let $N \geq 2$ and $\mathbf{v} \in \frac{1}{N} M_{1,2}(\mathbb{Z}) \setminus M_{1,2}(\mathbb{Z})$.*

(i) *The function $g_{\mathbf{v}}^{12N}$ belongs to $\mathcal{F}_N$. It has no zeros and poles on $\mathbb{H}$.*

(ii) *If $\mathbf{u} \in M_{1,2}(\mathbb{Q})$ satisfies $\mathbf{u} \equiv \mathbf{v}$ or $-\mathbf{v} \pmod{M_{1,2}(\mathbb{Z})}$, then*

$$f_{\mathbf{u}} = f_{\mathbf{v}} \quad \text{and} \quad g_{\mathbf{u}}^{12N} = g_{\mathbf{v}}^{12N}.$$

(iii) *For $\gamma \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\langle -I_2 \rangle$ $(\simeq \mathrm{Gal}(\mathcal{F}_N/\mathcal{F}_1))$ we have*

$$f_{\mathbf{v}}^{\gamma} = f_{\mathbf{v}\gamma} \quad \text{and} \quad \left(g_{\mathbf{v}}^{12N}\right)^{\gamma} = g_{\mathbf{v}\gamma}^{12N}.$$

*Proof.* (i) See [8, Theorem 1.2 in Chapter 2].

(ii) See [1, Lemma 10.4] and [8, pp. 28–29].

(iii) See [12, Theorem 6.6 (2)] and [8, Proposition 1.3 in Chapter 2].

□

## 3. Theory of complex multiplication

In this section, we shall present some consequences of the main theorems of complex multiplication and Shimura's reciprocity law.

Let $K$ be an imaginary quadratic field of discriminant $d_K$. 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 so $\mathcal{O}_K = \mathbb{Z}\tau_K + \mathbb{Z}$ ([1, (7.1)]).

PROPOSITION 3.1. *The theory of complex multiplication yields the following results*:

(i) $H_K = K(j(\tau_K))$.
(ii) $K_{(N)} = K(f(\tau_K) \mid f \in \mathcal{F}_N$ *is finite at* $\tau_K)$ *if* $N \geq 2$.
(iii) $K_{(N)} = H_K\left(f_{\left[0\ \frac{1}{N}\right]}(\tau_K)\right)$ *if* $K \neq \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3})$ *and* $N \geq 2$.

*Proof.* (i) See [10, Theorem 1 in Chapter 10].
(ii) See [10, Corollary to Theorem 2 in Chapter 10] or [12, Proposition 6.33].
(iii) See [10, Corollary to Theorem 7 in Chapter 10].

□

Let $\mathcal{R}(d_K)$ be the set of reduced binary quadratic forms of discriminant $d_K$, that is, the set of quadratic forms $Q(x,y) = a_Q x^2 + b_Q xy + c_Q y^2$ in $\mathbb{Z}[x, y]$ whose coefficients satisfy the following four conditions:

(i) $a_Q > 0$.
(ii) $\gcd(a_Q, b_Q, c_Q) = 1$.
(iii) $b_Q^2 - 4a_Q c_Q = d_K$.
(iv) $-a_Q < b_Q \leq a_Q < c_Q$ or $0 \leq b_Q \leq a_Q = c_Q$.

Let $Q_{\mathrm{pr}} = x^2 + b_K xy + c_K y^2$ be the principal form in $\mathcal{R}(d_K)$, namely,

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

Note that every nonprincipal reduced form $Q$ satisfies $a_Q \geq 2$. For each $Q \in \mathcal{R}(d_K)$, let $\tau_Q$ be the zero of the quadratic polynomial $Q(x, 1)$ lying in $\mathbb{H}$, that is,

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

In particular, we see that $\tau_{Q_{\mathrm{pr}}} = \tau_K$. For a positive integer $N$, let $W_{K,N}$ be the subgroup of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ given by

$$W_{K,N} = \left\{ \gamma = \begin{bmatrix} t - b_K s & -c_K s \\ s & t \end{bmatrix} \mid s,\, t \in \mathbb{Z}/N\mathbb{Z} \text{ such that } \gamma \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) \right\}.$$

Proposition 3.2 (Shimura's reciprocity law). *Assume that $K$ is different from $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-3})$. Then there is a bijective map*

$$\begin{aligned} W_{K,N}/\langle -I_2 \rangle \times \mathcal{R}(d_K) &\to \mathrm{Gal}(K_{(N)}/K) \\ (\alpha,\, Q) &\mapsto \left( f(\tau_K) \mapsto f^{\beta(\alpha,Q)}(\tau_Q) \mid f \in \mathcal{F}_N \text{ is finite at } \tau_K \right), \end{aligned}$$

*where $\beta(\alpha, Q)$ is a certain element of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\langle -I_2 \rangle$ ($\simeq \mathrm{Gal}(\mathcal{F}_N/\mathcal{F}_1)$), such that its restriction to $W_{K,N}/\langle -I_2 \rangle \times \{Q_{\mathrm{pr}}\}$ induces an isomorphism onto $\mathrm{Gal}(K_{(N)}/H_K)$.*

*Proof.* See [14, §3 and 6] or [7, Proposition 3.1 and Remark 3.2]. □

Remark 3.3. Let $h_K$ denote the class number of $K$.

(i) We have $h_K = [H_K : K] = |\mathcal{R}(d_K)|$ ([1, Theorems 2.8 and 7.7]).
(ii) If $h_K \geq 2$, then $d_K \leq -15$ ([1, Theorem 12.34]).

## 4. Inequalities on special values of modular functions

We shall introduce and develop some inequalities on special values of modular functions which are necessary to prove our main theorem.

Throughout this section, we let $K$ be an imaginary quadratic field other than $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-3})$. Define a function $J$ on $\mathbb{H}$ by

$$J(\tau) = \frac{1}{1728}\, j(\tau) \quad (\tau \in \mathbb{H}).$$

Lemma 4.1. *If $h_K \geq 2$ (so, $d_K \leq -15$), then we get*

$$\left| \frac{J(\tau_Q)^2 (J(\tau_Q) - 1)^3}{J(\tau_K)^2 (J(\tau_K) - 1)^3} \right| \;<\; 877383\, |q_{\tau_K}|^{\frac{5}{2}} \;(< 1)$$

*for all $Q \in \mathcal{R}(d_K) \setminus \{Q_{\mathrm{pr}}\}$.*

*Proof.* See [5, Lemma 6.3 (ii)] and [6, Remark 4.2]. □

Remark 4.2. Note that $C_K = J_K^2 (J_K - 1)^3 \neq 0$ ([1, p. 200]). We obtain by Proposition 3.1 (i), 3.2 for $N = 1$ and Lemma 4.1 that

$$H_K = K\,(C_K^n) \quad \text{for every nonzero integer } n$$

([6, Lemma 4.3]).

LEMMA 4.3. *If* $\mathbf{v} \in \frac{1}{N}M_{1,2}(\mathbb{Z}) \setminus M_{1,2}(\mathbb{Z})$ *for an integer* $N \geq 2$ *and* $Q \in \mathcal{R}(d_K) \setminus \{Q_{\mathrm{pr}}\}$*, then we have*

$$\left| \frac{g_{\left[0\ \frac{1}{N}\right]}(\tau_K)}{g_{\mathbf{v}}(\tau_Q)} \right| \ < \ 1.$$

*Proof.* See [4, Lemma 3.2 and Remark 3.6]. □

LEMMA 4.4. *Let* $\mathbf{v} \in M_{1,2}(\mathbb{Q}) \setminus M_{1,2}(\mathbb{Z})$*, and let* $\tau \in \mathbb{H}$ *such that* $|q_\tau| \leq e^{-\pi\sqrt{3}}$*.*

(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*

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

*Proof.* See [6, Lemma 5.1]. □

LEMMA 4.5. *Let* $N$ *and* $t$ *be positive integers such that* $N \geq 4$ *and* $2 \leq t \leq N-2$*. If* $h_K \geq 2$*, then we have*

$$\left| \frac{g_{\left[0\ \frac{t}{N}\right]}(\tau_K)^2}{g_{\left[0\ \frac{t+1}{N}\right]}(\tau_K)\, g_{\left[0\ \frac{t-1}{N}\right]}(\tau_K)} \right| \ < \ 2.0002.$$

*Proof.* We derive by the definition (2.2) that

$$\begin{aligned}
&\left| \frac{g_{\left[0\ \frac{t}{N}\right]}(\tau_K)^2}{g_{\left[0\ \frac{t+1}{N}\right]}(\tau_K)\, g_{\left[0\ \frac{t-1}{N}\right]}(\tau_K)} \right| \\
= \ &\left| \frac{(1-\zeta_N^t)^2}{(1-\zeta_N^{t+1})(1-\zeta_N^{t-1})} \right| \\
&\times \left| \frac{\prod_{n=1}^{\infty}(1-q_{\tau_K}^n\zeta_N^t)^2(1-q_{\tau_K}^n\zeta_N^{-t})^2}{\prod_{n=1}^{\infty}(1-q_{\tau_K}^n\zeta_N^{t+1})(1-q_{\tau_K}^n\zeta_N^{-t-1})(1-q_{\tau_K}^n\zeta_N^{t-1})(1-q_{\tau_K}^n\zeta_N^{-t+1})} \right| \\
\leq \ &\frac{\sin^2\frac{t\pi}{N}}{\sin\frac{(t+1)\pi}{N}\sin\frac{(t-1)\pi}{N}} \prod_{n=1}^{\infty}\left(\frac{1+r^n}{1-r^n}\right)^4 \quad \text{where } r = e^{-\pi\sqrt{|d_K|}}
\end{aligned}$$

$$\begin{aligned}
&\leq \frac{\sin^2\frac{t\pi}{N}}{\sin^2\frac{t\pi}{N}-\sin^2\frac{\pi}{N}}\prod_{n=1}^{\infty}e^{12r^n}\\
&\qquad \text{because } r\leq e^{-\pi\sqrt{3}}<\frac{1}{3} \text{ and } \frac{1+x}{1-x}<e^{3x} \text{ for } 0<x<\frac{1}{3}\\
&\leq \frac{\sin^2\frac{t\pi}{N}}{\sin^2\frac{t\pi}{N}-\frac{1}{2}\sin^2\frac{t\pi}{N}}\,e^{\sum_{n=1}^{\infty}12r^n}\\
&\qquad \text{because } \sin\frac{\pi}{N}=\frac{\sin\frac{2\pi}{N}}{2\cos\frac{\pi}{N}}\leq\frac{\sin\frac{t\pi}{N}}{2\cos\frac{\pi}{4}}=\frac{1}{\sqrt{2}}\sin\frac{t\pi}{N}\\
&\leq 2e^{\frac{12e^{-\pi\sqrt{15}}}{1-e^{-\pi\sqrt{15}}}} \quad \text{since } r\leq e^{-\pi\sqrt{15}}\\
&< 2.0002.
\end{aligned}$$

□

## 5. Generation of ray class fields

Now, we are ready to prove our main theorem on generation of $K_{(N)}$ by using a single $x$-coordinate of an $N$-torsion point on the elliptic curve $E_{K,n}$.

LEMMA 5.1. *Let* $\mathbf{u}, \mathbf{v}\in M_{1,2}(\mathbb{Q})\setminus M_{1,2}(\mathbb{Z})$ *such that*

$$\mathbf{u}\not\equiv\mathbf{v}, -\mathbf{v} \pmod{M_{1,2}(\mathbb{Z})}.$$

*Then we have the relation*

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

*Proof.* See [8, p. 51]. □

THEOREM 5.2. *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 such that* $N=5$ *or* $N\geq 7$. *Let* $\omega$ *be an element of* $K$ *such that* $\omega+\mathcal{O}_K$ *is a generator of the* $\mathcal{O}_K$*-module* $N^{-1}\mathcal{O}_K/\mathcal{O}_K$. *If* $n$ *is a nonnegative integer satisfying*

$$n \geq \frac{\frac{1}{8}\pi\sqrt{|d_K|}+2\ln(4.263N)}{\frac{5}{2}\pi\sqrt{|d_K|}-\ln 877383}-\frac{1}{6}, \tag{5.1}$$

*then we have*

$$K_{(N)}=K\left(x_{K,n}(\omega)\right).$$

*Proof.* If $h_K = 1$, then the assertion holds for all $n \geq 0$ by the proof (Case 1) of [6, Proposition 4.5].

Now, we let $h_K \geq 2$. Since $N = 5$ or $N \geq 7$, there is at least one integer $t$ such that $2 \leq t \leq N-2$ and $\gcd(N, t) = 1$ ([15, §I.1]). Since each of $\omega + \mathcal{O}_K$, $\frac{1}{N} + \mathcal{O}_K$ and $\frac{t}{N} + \mathcal{O}_K$ is a generator of the $\mathcal{O}_K$-module $N^{-1}\mathcal{O}_K/\mathcal{O}_K$, the $x$-coordinates $x_{K,n}(\omega)$, $x_{K,n}(\frac{1}{N})$ and $x_{K,n}(\frac{t}{N})$ of the elliptic curve $E_{K,n}$ are all Galois conjugate over $H_K$ ([10, Theorem 7 and its corollary in Chapter 10]). Thus we get

$$K\left(x_{K,n}(\omega)\right) = K\left(x_{K,n}(\tfrac{1}{N})\right) = K\left(x_{K,n}(\tfrac{t}{N})\right) \tag{5.2}$$

as an intermediate field of the abelian extension $K_{(N)}/K$. Note further that $x_{K,n}(\frac{t}{N})$ and $x_{K,n}(\frac{1}{N})$ are distinct because $\frac{t}{N} \not\equiv \frac{1}{N}, -\frac{1}{N} \pmod{\mathcal{O}_K}$ ([1, Lemma 10.4]).

Suppose on the contrary that $x_{K,n}(\omega)$ does not generate $K_{(N)}$ over $K$. Then there exists a nonidentity element $\sigma$ of $\mathrm{Gal}(K_{(N)}/K)$ which leaves $x_{K,n}(\omega)$ fixed. Since

$$\begin{aligned}
K_{(N)} &= H_K\left(f_{\left[0\ \frac{1}{N}\right]}(\tau_K)\right) \quad \text{by Proposition 3.1 (iii)} \\
&= H_K\left(C_K^n f_{\left[0\ \frac{1}{N}\right]}(\tau_K)\right) \quad \text{by Remark 4.2} \\
&= H_K\left(x_{K,n}(\tfrac{1}{N})\right) \\
&\qquad \text{by the definition (2.1) and the fact } \mathcal{O}_K = \mathbb{Z}\tau_K + \mathbb{Z} \\
&= H_K\left(x_{K,n}(\omega)\right) \quad \text{by (5.2)},
\end{aligned}$$

we observe that

$$\sigma \notin \mathrm{Gal}(K_{(N)}/H_K). \tag{5.3}$$

Now we derive that

$$\begin{aligned}
1 &= \left| \frac{\left(x_{K,n}(\frac{t}{N}) - x_{K,n}(\frac{1}{N})\right)^{\sigma}}{x_{K,n}(\frac{t}{N}) - x_{K,n}(\frac{1}{N})} \right| \\
&\qquad \text{by (5.2) and the fact that } \sigma \text{ is the identity on } K\left(x_{K,n}(\omega)\right) \\
&= \left| \frac{\left\{J(\tau_K)^{2n}(J(\tau_K)-1)^{3n}(f_{\left[0\ \frac{t}{N}\right]}(\tau_K) - f_{\left[0\ \frac{1}{N}\right]}(\tau_K))\right\}^{\sigma}}{J(\tau_K)^{2n}(J(\tau_K)-1)^{3n}(f_{\left[0\ \frac{t}{N}\right]}(\tau_K) - f_{\left[0\ \frac{1}{N}\right]}(\tau_K))} \right| \\
&\qquad \text{by the definition (2.1)}
\end{aligned}$$

$$= \left|\frac{J(\tau_Q)^2(J(\tau_Q)-1)^3}{J(\tau_K)^2(J(\tau_K)-1)^3}\right|^n \left|\frac{f_{\mathbf{u}}(\tau_Q)-f_{\mathbf{v}}(\tau_Q)}{f_{\left[0\ \frac{t}{N}\right]}(\tau_K)-f_{\left[0\ \frac{1}{N}\right]}(\tau_K)}\right|$$

for some $Q \in \mathcal{R}(d_K) \setminus \{Q_{\mathrm{pr}}\}$ and $\mathbf{u}$, $\mathbf{v} \in \frac{1}{N}M_{1,2}(\mathbb{Z}) \setminus M_{1,2}(\mathbb{Z})$ such that $\mathbf{u} \not\equiv \mathbf{v}, -\mathbf{v} \pmod{M_{1,2}(\mathbb{Z})}$ by Proposition 2.1 (iii), 3.2 and (5.3)

$$= \left|\frac{J(\tau_Q)^2(J(\tau_Q)-1)^3}{J(\tau_K)^2(J(\tau_K)-1)^3}\right|^{n+\frac{1}{6}} \left|\frac{\left(\frac{g_{\mathbf{u}+\mathbf{v}}(\tau_Q)g_{\mathbf{u}-\mathbf{v}}(\tau_Q)}{g_{\mathbf{u}}(\tau_Q)^2 g_{\mathbf{v}}(\tau_Q)^2}\right)}{\left(\frac{g_{\left[0\ \frac{t+1}{N}\right]}(\tau_K)g_{\left[0\ \frac{t-1}{N}\right]}(\tau_K)}{g_{\left[0\ \frac{t}{N}\right]}(\tau_K)^2 g_{\left[0\ \frac{1}{N}\right]}(\tau_K)^2}\right)}\right|$$

by Lemma 5.1

$$= \left|\frac{J(\tau_Q)^2(J(\tau_Q)-1)^3}{J(\tau_K)^2(J(\tau_K)-1)^3}\right|^{n+\frac{1}{6}} \left|\frac{g_{\left[0\ \frac{t}{N}\right]}(\tau_K)^2}{g_{\left[0\ \frac{t+1}{N}\right]}(\tau_K)g_{\left[0\ \frac{t-1}{N}\right]}(\tau_K)}\right|$$

$$\times \left|\frac{g_{\left[0\ \frac{1}{N}\right]}(\tau_K)}{g_{\mathbf{v}}(\tau_Q)}\right|^2 |g_{\mathbf{u}+\mathbf{v}}(\tau_Q)|\,|g_{\mathbf{u}-\mathbf{v}}(\tau_Q)| \left|\frac{1}{g_{\mathbf{u}}(\tau_Q)}\right|^2$$

$$< \left(877383|q_{\tau_K}|^{\frac{5}{2}}\right)^{n+\frac{1}{6}} \cdot 2.0002 \cdot 1^2 \cdot \left(2.29|q_{\tau_Q}|^{-\frac{1}{24}}\right)^2 \left(\frac{0.76}{N}|q_{\tau_Q}|^{\frac{1}{12}}\right)^{-2}$$

by Lemmas 4.1, 4.3, 4.4 and 4.5

$$\leq \left(877383|q_{\tau_K}|^{\frac{5}{2}}\right)^{n+\frac{1}{6}} (4.263N)^2 |q_{\tau_Q}|^{-\frac{1}{4}}$$

$$\leq \left(877383|q_{\tau_K}|^{\frac{5}{2}}\right)^{n+\frac{1}{6}} (4.263N)^2 |q_{\tau_K}|^{-\frac{1}{8}}$$

because $|q_{\tau_Q}| = |q_{\tau_K}|^{\frac{1}{a_Q}} \geq |q_{\tau_K}|^{\frac{1}{2}}$ due to the facts $|q_{\tau_K}| < 1$ and $a_Q \geq 2$

$$= \left(877383e^{-\frac{5}{2}\pi\sqrt{|d_K|}}\right)^{n+\frac{1}{6}} (4.263N)^2 e^{\frac{1}{8}\pi\sqrt{|d_K|}}.$$

We then obtain by taking logarithm that

$$0 < \left(n+\frac{1}{6}\right)\left(\ln 877383 - \frac{5}{2}\pi\sqrt{|d_K|}\right) + 2\ln(4.263N) + \frac{1}{8}\pi\sqrt{|d_K|},$$

which contradicts the inequality (5.1) for $n$.

Therefore we conclude that $K_{(N)} = K(x_{K,n}(\omega))$. □

## References


[1] D. A. Cox, *Primes of the Form $x^2 + ny^2$: Fermat, Class Field Theory, and Complex Multiplication*, 2nd edition, Pure Appl. Math., (Hoboken), John Wiley & Sons, Inc., Hoboken, NJ, 2013.

[2] G. Frei, F. Lemmermeyer and P. J. Roquette, *Emil Artin and Helmut Hasse-the Correspondence 1923-1958*, Comm App Math Comp Sci., **5** (2014) Springer, Heidelberg.

[3] G. J. Janusz, *Algebraic Number Fields*, 2nd ed., Grad. Studies in Math. 7, Amer. Math. Soc., Providence, RI, 1996.

[4] H. Y. Jung, J. K. Koo and D. H. Shin, *Ray class invariants over imaginary quadratic fields*, Tohoku Math. J. (2) **63** (2011), no. 3, 413-426.

[5] 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.

[6] H. Y. Jung, J. K. Koo and D. H. Shin, *Class fields generated by coordinates of elliptic curves*, submitted. https://arxiv.org/abs/2111.01021

[7] J. K. Koo and D. H. Shin, *Construction of class fields over imaginary quadratic fields using y-coordinates of elliptic curves*, J. Korean Math. Soc., **50** (2013), no. 4, 847-864.

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

[9] 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.

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

[11] K. Ramachandra, *Some applications of Kronecker's limit formula*, Ann. of Math., (2) **80** (1964), 104-148.

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

[13] J. H. Silverman, *The Arithmetic of Elliptic Curves*, 2nd ed., Grad. Texts in Math., 106, Springer, Dordrecht, 2009.

[14] P. Stevenhagen, *Hilbert's 12th problem, complex multiplication and Shimura reciprocity*, Adv. Stud. Pure Math., **30**, Math. Soc., Japan, Tokyo, 2001.

[15] J. Sándor, D. S. Mitrinović and B. Crstici, *Handbook of Number Theory I*, Springer, Dordrecht, 1995.



Department of Mathematics
Dankook University
Cheonan-si, Chungnam 31116, Republic of Korea
*E-mail*: hoyunjung@dankook.ac.kr