Cent. Eur. J. Math. • 9(6) • 2011 • 1389-1402
DOI: 10.2478/s11533-011-0080-5

VERSITA

Central European Journal of **Mathematics**

Generation of Hauptmoduln of $\Gamma_1(N)$ by Weierstrass units and application to class fields

Research Article

Chang Heon Kim[1]*, Ja Kyung Koo[2]†

1 *Department of Mathematics and Research Institute for Natural Sciences, Hanyang University, Seoul, 133-791, Korea*

2 *Korea Advanced Institute of Science and Technology, Department of Mathematics, Taejon, 305-701, Korea*

Received 18 May 2011; accepted 9 July 2011

Abstract: We show that the modular functions $j_{1,N}$ generate function fields of the modular curve $X_1(N)$, $N \in \{7, 8, 9, 10, 12\}$, and apply them to construct ray class fields over imaginary quadratic fields.

MSC: 11F03, 11F06, 11F11, 14H55

Keywords: Modular curve • Modular function • Class field

1. Introduction

Let $\mathfrak{H}$ be the complex upper half plane and let $\Gamma_1(N)$ be a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$ whose elements are congruent to $\left(\begin{smallmatrix}1 & *\\ 0 & 1\end{smallmatrix}\right)$ modulo N, $N = 1, 2, 3, \ldots$ Since the group $\Gamma_1(N)$ acts on $\mathfrak{H}$ by linear fractional transformations, we may define the modular curve $X_1(N) = \Gamma_1(N)\backslash\mathfrak{H}^*$, as the projective closure of the smooth affine curve $\Gamma_1(N)\backslash\mathfrak{H}$, whose genus shall be denoted $g_{1,N}$. Since $g_{1,N} = 0$ only for the eleven cases $1 \le N \le 10$ and $N = 12$ [7], for such N the function field $K(X_1(N))$ of the curve $X_1(N)$ is a rational function field over $\mathbb{C}$.

In [3, 5, 11, 12, 21] the division values of the Weierstrass $\wp$-function were used to construct modular functions on $\Gamma_1(N)$ of positive genus. In Section 3 of this article, we find the field generator $j_{1,N}$ for $7 \le N \le 10$ and $N = 12$ using the aforementioned functions. In Section 4, we construct the normalized generators (or Hauptmoduln) $\mathcal{N}(j_{1,N})$. When $\tau \in \mathfrak{H} \cap \mathbb{Q}(\sqrt{-d})$ for a square free positive integer d, we shall show that $\mathcal{N}(j_{1,N})(\tau)$ is an algebraic integer. When applied

* *E-mail: chhkim@hanyang.ac.kr*
† *E-mail: jkkoo@math.kaist.ac.kr*

to explicit class field theory, it is important to work with modular functions with rational Fourier coefficients. The modular function $j_{1,N}$ has this property and can therefore be used to construct class fields over an imaginary quadratic field K. This is done in Section 4 following an idea of Chen–Yui [1]. Given an ideal $\mathfrak{A} = [\alpha_1, \alpha_2]$ of maximal order in K, let $\alpha = \alpha_1/\alpha_2 \in \mathfrak{H}$. Then we shall show that the modular function $j_{1,N}(\alpha)$ in the above generates the ray class field $K_{\mathfrak{f}}$ over K for a conductor $\mathfrak{f}$ dividing N.

Throughout the article we adopt the following notation:

$\mathfrak{H}^*$ – the extended complex upper half plane,

Γ – a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$,

$\Gamma(N) = \{\gamma \in \mathrm{SL}_2(\mathbb{Z}) : \gamma \equiv I \bmod N\}$,

$\Gamma_0(N)$ – the Hecke subgroup $\left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma(1) : c \equiv 0 \bmod N \right\}$,

$\Gamma_1(N) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma(1) : a \equiv d \equiv 1,\ c \equiv 0 \bmod N \right\}$,

$X(\Gamma) = \Gamma \setminus \mathfrak{H}^*$,

$X(N) = \Gamma(N) \setminus \mathfrak{H}^*$,

$X_0(N) = \Gamma_0(N) \setminus \mathfrak{H}^*$,

$X_1(N) = \Gamma_1(N) \setminus \mathfrak{H}^*$,

$K(X(\Gamma))$ – the function field of the curve $X(\Gamma)$,

$\overline{\Gamma}$ – the inhomogeneous group of Γ $(= \Gamma / \pm I)$

$q_h = e^{2\pi i z/h}$, $z \in \mathfrak{H}$,

$f|_{[A]_k} = (\det A)^{k/2}(cz+d)^{-k} f(Az)$ where $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$,

$f|_{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)} = f\left(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \cdot z\right)$,

$M_k(\Gamma)$ – the space of modular forms of weight k with respect to the group Γ,

$z \to i\infty$ denotes that $z = it$, $t \in \mathbb{R}$, and $t \to \infty$,

$\sum'_m$ – a sum over $m \neq 0$.

We shall always take the branch of the square root having argument in $(-\pi/2, \pi/2]$. Thus, $\sqrt{z}$ is a holomorphic function on the complex plane with the negative real axis $(-\infty, 0]$ removed. For any integer k, we define $z^{k/2}$ to mean $(\sqrt{z})^k$.

2. Cusps of $\Gamma_1(N)$

We denote by S_Γ the set of inequivalent cusps of Γ. From [7, 13, 15],

$$\begin{aligned} S_{\Gamma_1(7)} &= \{\infty,\ 4/7,\ 5/7,\ 0,\ 1/2,\ 1/3\}; \\ S_{\Gamma_1(8)} &= \{\infty,\ 3/8,\ 0,\ 1/3,\ 1/2,\ 1/4\}; \\ S_{\Gamma_1(9)} &= \{\infty,\ 5/9,\ 7/9,\ 0,\ 1/2,\ 3/4,\ 1/3,\ 2/3\}; \\ S_{\Gamma_1(10)} &= \{\infty,\ 3/10,\ 0,\ 1/3,\ 1/2,\ 1/4,\ 1/5,\ 2/5\}; \quad \text{and} \\ S_{\Gamma_1(12)} &= \{\infty,\ 5/12,\ 0,\ 1/5,\ 1/2,\ 1/3,\ 1/9,\ 1/4,\ 1/8,\ 1/6\}. \end{aligned}$$

For later use we calculate the widths of the cusps. We recall that the width of the cusp a/c in $X_1(N)$ is the smallest positive integer h such that $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)^{-1} \in \pm\Gamma_1(N)$. The lemma below is [8, Lemma 3].

Lemma 2.1.
Let $a/c \in \mathbb{P}^1(\mathbb{Q})$ be a cusp where $(a,c)=1$. Choose an element $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$. Then the width of a/c in $X_1(N)$ is given by $N/(c,N)$ if $N \neq 4$.

We then have the following tables of inequivalent cusps of $\Gamma_1(N)$ for $7 \le N \le 10$ and $N = 12$:

Table 1. Cusps of $\Gamma_1(7)$

cusp	∞	4/7	5/7	0	1/2	1/3
width	1	1	1	7	7	7

Table 2. Cusps of $\Gamma_1(8)$

cusp	∞	3/8	0	1/3	1/2	1/4
width	1	1	8	8	4	2

Table 3. Cusps of $\Gamma_1(9)$

cusp	∞	5/9	7/9	0	1/2	3/4	1/3	2/3
width	1	1	1	9	9	9	3	3

Table 4. Cusps of $\Gamma_1(10)$

cusp	∞	3/10	0	1/3	1/2	1/4	1/5	2/5
width	1	1	10	10	5	5	2	2

Table 5. Cusps of $\Gamma_1(12)$

cusp	∞	5/12	0	1/5	1/2	1/3	1/9	1/4	1/8	1/6
width	1	1	12	12	6	4	4	3	3	2

3. Modular functions $j_{1,N}$ for $7 \le N \le 10$ and $N = 12$

In this section we construct a generator of $K(X_1(N))$ using the $\wp$-division values when $N \in \{7,8,9,10,12\}$. Let L be a lattice in $\mathbb{C}$. The *Weierstrass $\wp$-function* (*relative to L*) is defined by the series

$$\wp_L(z) = \frac{1}{z^2} + \sum_{w \in L,\, w \neq 0} \frac{1}{(z-w)^2} - \frac{1}{w^2}\,.$$

Let $\mathbf{a} = (a_1, a_2)$ be a row vector with entries in $\mathbb{Z}$. Then we define the *N-th division value* $\wp_{N,\mathbf{a}}$ [16, Chapter VII, §3] of $\wp$ to be

$$\wp_{N,\mathbf{a}}(z) = \wp_{L_z}\left(\frac{a_1 z + a_2}{N}\right)$$

where $L_z = \mathbb{Z}z + \mathbb{Z}$ for $z \in \mathfrak{H}$.

Lemma 3.1 ([16, Chapter VII, §2 and §3]).

(i) $\wp_{N,\mathbf{a}}|_{[\gamma]_2} = \wp_{N,\mathbf{a}\gamma}$ *for* $\gamma \in \Gamma(1)$.

(ii) $\wp_{N,\mathbf{a}}(z) = N^2\big(G^*_{N,2,\mathbf{a}}(z) - G^*_{N,2,\mathbf{0}}(z)\big) \in M_2(\Gamma(N))$ *where* $G^*_{N,2,\mathbf{a}}$ *is the Eisenstein series of weight* 2 *and level* N*, which is defined by the value at* $s = 0$ *of the analytic continuation of the series*

$$\sum_{m_\nu \equiv a_\nu \bmod N}{}' (m_1 z + m_2)^{-2} |m_1 z + m_2|^{-s}, \qquad z \in \mathfrak{H}.$$

(iii) $G^*_{N,2,\mathbf{a}}(z)$ *has the following* q_N*-expansion:*

$$G^*_{N,2,\mathbf{a}}(z) = \frac{-2\pi i}{N^2(z - \bar{z})} + \sum_{\nu \geq 0} \alpha_\nu(N, \mathbf{a})\, {q_N}^\nu,$$

where

$$\alpha_0(N, \mathbf{a}) = \delta\left(\frac{a_1}{N}\right) \sum_{m_2 \equiv a_2 (N)}{}' {m_2}^{-2}$$

with $\delta(a_1/N) = 1$ *if* $a_1/N \in \mathbb{Z}$, 0 *otherwise, and*

$$\alpha_\nu(N, \mathbf{a}) = -\frac{4\pi^2}{N^2} \cdot \sum_{m|\nu,\ \nu/m \equiv a_1 (N)}{}' |m|\, {\zeta_N}^{a_2 m}, \qquad \nu \geq 1.$$

Lemma 3.2.
Let $\mathbf{a}$ *and* $\mathbf{b}$ *be two row vectors such that* $\pm\mathbf{a}$ *is not congruent to* $\mathbf{b}$ *modulo* N*. Then* $\wp_{N,\mathbf{a}} - \wp_{N,\mathbf{b}}$ *has no zeros in* $\mathfrak{H}$.

Proof. It is well known that

$$\wp_L(z_1) = \wp_L(z_2) \qquad \text{if and only if} \qquad \pm z_1 \equiv z_2 \bmod L. \tag{1}$$

Now suppose that there exists some $z_0 \in \mathfrak{H}$ such that $\wp_{N,\mathbf{a}}(z_0) = \wp_{N,\mathbf{b}}(z_0)$. Then

$$\wp_{L_{z_0}}\left(\frac{a_1 z_0 + a_2}{N}\right) = \wp_{L_{z_0}}\left(\frac{b_1 z_0 + b_2}{N}\right).$$

Now by (1), $\pm(a_1 z_0 + a_2)/N \equiv (b_1 z_0 + b_2)/N \bmod L$. Thus $\pm(a_1, a_2) \equiv (b_1, b_2) \bmod N$, which is a contradiction. □

We identify the cusps of $X(N)$ with $\left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right)$ where $x, y \in \mathbb{Z}/N\mathbb{Z}$ and are relatively prime.

Lemma 3.3 ([15, Proposition 1]).
The ramification degree of the projection $X(N) \to X_1(N)$ *at each cusp* $\left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right)$ *is given by* $\gcd(y, N)$.

Lemma 3.4 ([15, Proposition 3]).
Let $G_{N,2,\mathbf{a}}$ *be defined by the holomorphic part of* $G^*_{N,2,\mathbf{a}}$*. Let* $\{x\}_N$ *be defined by* $0 \leq \{x\}_N \leq N/2$ *and* $\{x\}_N \equiv \pm x \bmod N$*. Then* $G_{N,2,\mathbf{a}}$ *has a zero of order* $\geq \{a_1 x + a_2 y\}_N$ *at the cusp* $\left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right)$ *of* $X(N)$.

Lemma 3.5.
Let $\mathbf{a} = (0, a_2)$*. Then,*

$$\wp_{N,(0,a_2)} \in M_2(\Gamma_1(N)), \quad \textit{and} \tag{i}$$

$$W_N\big(\wp_{N,(0,a_2)}(z)\big) \overset{\text{def}}{=} \wp_{N,(0,a_2)}(z)|_{\left[\left(\begin{smallmatrix} 0 & -1 \\ N & 0 \end{smallmatrix}\right)\right]_2} = \wp_{N,(a_2,0)}(Nz). \tag{ii}$$

Proof. By Lemma 3.1 (ii), it suffices to check the slash operator invariance under $\Gamma_1(N)$. For each $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_1(N)$, consider

$$\begin{aligned} \mathbf{a}\gamma = (0, a_2)\begin{pmatrix} a & b \\ c & d \end{pmatrix} &\equiv (0, a_2)\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \mod N \\ &\equiv \mathbf{a} \mod N. \end{aligned}$$

From Lemma 3.1 (i) and the definition of the $\wp$-division value it follows that $\wp_{N,\mathbf{a}}|_{[\gamma]_2} = \wp_{N,\mathbf{a}\gamma} = \wp_{N,\mathbf{a}}$. To prove (ii):

$$\begin{aligned} W_N(\wp_{N,(0,a_2)}(z)) = \wp_{N,(0,a_2)}(z)|_{\left[\left(\begin{smallmatrix} 0 & -1 \\ N & 0 \end{smallmatrix}\right)\right]_2} &= \wp_{N,(0,a_2)}(z)|_{\left[\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)\right]_2\left[\left(\begin{smallmatrix} N & 0 \\ 0 & 1 \end{smallmatrix}\right)\right]_2} \\ &= \wp_{N,(a_2,0)}(z)|_{\left[\left(\begin{smallmatrix} N & 0 \\ 0 & 1 \end{smallmatrix}\right)\right]_2} \qquad \text{by Lemma 3.1 (i)} \\ &= \wp_{N,(a_2,0)}(Nz). \end{aligned}$$

□

Lemma 3.6.

We have

$$\sum_{m_2 \equiv a_2 \bmod N}{}' m_2^{-2} = \frac{2\pi^2}{N^2} \cdot \frac{1}{1 - \cos(2a_2\pi/N)}$$

for a_2 not congruent to 0 modulo N.

Proof. First note that for $z \in \mathfrak{H}$, $\sum_{n\in\mathbb{Z}}(z+n)^{-2} = (2\pi i)^2 \sum_{n=1}^{\infty} nq^n$. Also $\sum_{n=1}^{\infty} nq^n = q(1-q)^{-2}$. Hence

$$\sum_{n\in\mathbb{Z}} \frac{1}{(z+n)^2} = (2\pi i)^2 \frac{q}{(1-q)^2}, \qquad z \in \mathfrak{H}. \tag{2}$$

We observe that the LHS of (2) converges uniformly and absolutely in $\mathbb{C}\setminus\mathbb{Z}$. Hence as z approaches a_2/N, (2) becomes

$$\sum_{n\in\mathbb{Z}} \frac{1}{(a_2/N+n)^2} = (2\pi i)^2 \frac{e^{2\pi i a_2/N}}{(1-e^{2\pi i a_2/N})^2}, \qquad z \in \mathfrak{H}. \tag{3}$$

Now we consider the absolute value of the RHS of (3), which is equal to

$$\frac{4\pi^2}{|1-\cos(2\pi a_2/N) - i\sin(2\pi a_2/N)|^2} = \frac{4\pi^2}{(1-\cos(2\pi a_2/N))^2 + \sin^2(2\pi a_2/N)} = \frac{2\pi^2}{1-\cos(2\pi a_2/N)}.$$

Since the LHS of (3) is positive, the RHS of (3) must be $2\pi^2/(1-\cos(2\pi a_2/N))$. Hence

$$\begin{aligned} \sum_{m_2\equiv a_2 \bmod N}{}' m_2^{-2} &= \sum_{m_2\equiv a_2 \bmod N} m_2^{-2} \qquad \text{since } a_2 \not\equiv 0 \bmod N \\ &= \sum_{n\in\mathbb{Z}} \frac{1}{(a_2+Nn)^2} = \frac{2\pi^2}{N^2} \cdot \frac{1}{1-\cos(2a_2\pi/N)}. \end{aligned}$$

This proves the lemma. □

Theorem 3.7.

Let $N \in \{7, 8, 9, 10, 12\}$. Put

$$j_{1,N} = \frac{\wp_{N,(1,0)}(Nz) - \wp_{N,(2,0)}(Nz)}{\wp_{N,(1,0)}(Nz) - \wp_{N,(4,0)}(Nz)}, \quad N \neq 12, \qquad j_{1,12} = \frac{\wp_{12,(1,0)}(12z) - \wp_{12,(2,0)}(12z)}{\wp_{12,(1,0)}(12z) - \wp_{12,(5,0)}(12z)}.$$

Then $j_{1,N} \in K(X_1(N))$ and hence $K(X_1(N)) = \mathbb{C}(j_{1,N})$.

Proof. Considering the above lemmas, it is enough to show that $j_{1,N}$ has only one simple zero and one simple pole at the cusps. For simplicity, we let $\varphi_j = G_{N,2,(0,j)}$ and $\varphi_{ij} = \varphi_i - \varphi_j$. Using Lemmas 3.3 and 3.4 we can estimate the order of φ_{ij} at each cusp. First we consider the case $N = 7$. Let (φ_j) denote the divisor of the function φ_j. Then,

$$(\varphi_1) \geq (0) + 2\left(\frac{1}{2}\right) + 3\left(\frac{1}{3}\right), \qquad (\varphi_2) \geq 2(0) + 3\left(\frac{1}{2}\right) + \left(\frac{1}{3}\right), \qquad (\varphi_4) \geq 3(0) + \left(\frac{1}{2}\right) + 2\left(\frac{1}{3}\right).$$

Thus we have

$$(\varphi_{12}) \geq (0) + 2\left(\frac{1}{2}\right) + \left(\frac{1}{3}\right) \quad \text{and} \quad (\varphi_{14}) \geq (0) + \left(\frac{1}{2}\right) + 2\left(\frac{1}{3}\right). \tag{4}$$

In general, a modular form of weight k for a subgroup of index μ in $\Gamma(1)$ has $k\mu/12$ zeroes in any fundamental domain. In our case, $\mu = [\Gamma(1) : \pm\Gamma_1(7)] = 24$ and $k = 2$. Therefore $k\mu/12 = 4$, hence the inequality in (4) is an equality.

Similarly, in the other cases we have the following equalities. When $N = 8$,

$$(\varphi_{12}) = (0) + 2\left(\frac{1}{3}\right) + \left(\frac{1}{2}\right) \quad \text{and} \quad (\varphi_{14}) = (0) + 3\left(\frac{1}{3}\right).$$

When $N = 9$,

$$(\varphi_{12}) = (0) + 2\left(\frac{1}{2}\right) + \left(\frac{3}{4}\right) + \left(\frac{1}{3}\right) + \left(\frac{2}{3}\right) \quad \text{and} \quad (\varphi_{14}) = (0) + \left(\frac{1}{2}\right) + 2\left(\frac{3}{4}\right) + \left(\frac{1}{3}\right) + \left(\frac{2}{3}\right).$$

When $N = 10$,

$$(\varphi_{12}) = (0) + 3\left(\frac{1}{3}\right) + \left(\frac{1}{2}\right) + \left(\frac{1}{4}\right) \quad \text{and} \quad (\varphi_{14}) = (0) + 2\left(\frac{1}{3}\right) + \left(\frac{1}{2}\right) + 2\left(\frac{1}{4}\right).$$

When $N = 12$,

$$(\varphi_{12}) = (0) + 2\left(\frac{1}{5}\right) + \left(\frac{1}{2}\right) + \left(\frac{1}{3}\right) + \left(\frac{1}{9}\right) + \left(\frac{1}{4}\right) + \left(\frac{1}{8}\right) \quad \text{and}$$
$$(\varphi_{15}) = (0) + \left(\frac{1}{5}\right) + \left(\frac{1}{2}\right) + \left(\frac{1}{3}\right) + \left(\frac{1}{9}\right) + \left(\frac{1}{4}\right) + \left(\frac{1}{6}\right) + \left(\frac{1}{8}\right) + \left(\frac{1}{9}\right).$$

Thus in the case $N \in \{7, 8, 9, 10\}$ (resp. $N = 12$) the quotient $\varphi_{12}/\varphi_{14}$ (resp. $\varphi_{12}/\varphi_{15}$) generates the function field of $X_1(N)$. Since W_N normalizes $\Gamma_1(N)$, its action induces an automorphism of the function field of $X_1(N)$ and therefore $j_{1,N}$ generates $K(X_1(N))$, as desired. □

4. Normalized generators

For a modular function f, we call f *normalized* if its q-series is

$$\frac{1}{q} + 0 + a_1 q + a_2 q^2 + \dots$$

The following lemma is a simple consequence of basic properties of compact Riemann surfaces (or algebraic curves).

Lemma 4.1.
The normalized generator of a genus zero function field is unique.

Proof. Let Γ be a Fuchsian group such that the genus of the curve $\Gamma\backslash\mathfrak{H}^*$ is zero. Assume that $K(X(\Gamma)) = \mathbb{C}(J_1) = \mathbb{C}(J_2)$ where J_1 and J_2 are normalized. We can then write their Fourier expansions as $J_1 = q^{-1} + 0 + a_1 q + a_2 q^2 + \ldots$ and $J_2 = q^{-1} + 0 + b_1 q + b_2 q^2 + \ldots$ Observe that $1 = [K(X(\Gamma)) : \mathbb{C}(J_i)] = \nu_0(J_i) = \nu_\infty(J_i)$ for $i = 1, 2$. Hence, J_1 and J_2 have only one zero and one pole whose orders are simple. We see that the only poles of J_i occur at ∞. Then, $J_1 - J_2$ has no poles (because the series for each of J_1 and J_2 start with q^{-1}) and is thus constant. Since $J_1 - J_2 = (a_1 - b_1)q + \ldots$, this constant must be zero. This proves the lemma. □

Now, we will construct the normalized generator (or the Hauptmodul) of the function field $K(X_1(N))$ from the modular function $j_{1,N}$ mentioned in Theorem 3.7. Let

$$\begin{aligned}
\mathcal{N}(j_{1,7}) &= \frac{-1}{j_{1,7}(z) - 1} - 3 = \frac{1}{q} + 4q + 3q^2 - 5q^4 - 7q^5 - 2q^6 + 8q^7 + 16q^8 + 12q^9 - 7q^{10} + \ldots, \\
\mathcal{N}(j_{1,8}) &= \frac{-1}{j_{1,8}(z) - 1} - 2 = \frac{1}{q} + 3q + 2q^2 + q^3 - 2q^4 - 4q^5 - 4q^6 + 6q^8 + 9q^9 + 8q^{10} + \ldots, \\
\mathcal{N}(j_{1,9}) &= \frac{-1}{j_{1,9}(z) - 1} - 2 = \frac{1}{q} + 2q + 2q^2 + q^3 - q^4 - 2q^5 - 3q^6 - 2q^7 + q^8 + 4q^9 + 6q^{10} + \ldots, \\
\mathcal{N}(j_{1,10}) &= \frac{-1}{j_{1,10}(z) - 1} - 2 = \frac{1}{q} + 2q + q^2 + q^3 + 0q^4 - q^5 - 2q^6 - 2q^7 - q^8 + q^9 + 3q^{10} + \ldots, \\
\mathcal{N}(j_{1,12}) &= \frac{-1}{j_{1,12}(z) - 1} - 2 = \frac{1}{q} + q + q^2 + q^3 - q^6 - q^7 - q^8 - q^9 + \ldots
\end{aligned}$$

which are in $q^{-1}\mathbb{Z}[[q]]$. Then the above computation shows that $\mathcal{N}(j_{1,N})$ is the normalized generator of $K(X_1(N))$. Using Lemmas 3.1 and 3.6 we can compute the cusp values of $\mathcal{N}(j_{1,N})$, summarized in the following tables:

Table 6. Cusp values of $\mathcal{N}(j_{1,7})$

s	∞	$4/7$	$5/7$	0	$1/2$	$1/3$
$\mathcal{N}(j_{1,7})(s)$	∞	-3	-2	$\frac{u^{-1}-w^{-1}}{v^{-1}-w^{-1}} - 3$	$\frac{w^{-1}-v^{-1}}{u^{-1}-v^{-1}} - 3$	$\frac{v^{-1}-u^{-1}}{w^{-1}-u^{-1}} - 3$

where $u = 1 - \cos(2\pi/7)$, $v = 1 - \cos(4\pi/7)$, $w = 1 - \cos(8\pi/7)$.

Table 7. Cusp values of $\mathcal{N}(j_{1,8})$

s	∞	$3/8$	0	$1/3$	$1/2$	$1/4$
$\mathcal{N}(j_{1,8})(s)$	∞	-2	$2\sqrt{2}+1$	$-2\sqrt{2}+1$	-3	-1

Table 8. Cusp values of $\mathcal{N}(j_{1,9})$

s	∞	$5/9$	$7/9$	0	$1/2$	$3/4$	$1/3$	$2/3$
$\mathcal{N}(j_{1,9})(s)$	∞	-2	-1	$\frac{u^{-1}-w^{-1}}{v^{-1}-w^{-1}} - 2$	$\frac{w^{-1}-v^{-1}}{u^{-1}-v^{-1}} - 2$	$\frac{v^{-1}-u^{-1}}{w^{-1}-u^{-1}} - 2$	$(-3-\sqrt{3}i)/2$	$(-3+\sqrt{3}i)/2$

where $u = 1 - \cos(2\pi/9)$, $v = 1 - \cos(4\pi/9)$, $w = 1 - \cos(8\pi/9)$.

Table 9. Cusp values of $\mathcal{N}(j_{1,10})$

s	∞	$3/10$	0	$1/3$	$1/2$	$1/4$	$1/5$	$2/5$
$\mathcal{N}(j_{1,10})(s)$	∞	-1	$1+\sqrt{5}$	$1-\sqrt{5}$	$(-3-\sqrt{5})/2$	$(-3+\sqrt{5})/2$	0	-2

Table 10. Cusp values of $\mathcal{N}(j_{1,12})$

s	∞	5/12	0	1/5	1/2	1/3	1/9	1/4	1/8	1/6
$\mathcal{N}(j_{1,12})(s)$	∞	-1	$1+\sqrt{3}$	$1-\sqrt{3}$	-2	$-1-i$	$-1+i$	$(-1-\sqrt{3}i)/2$	$(-1+\sqrt{3}i)/2$	0

Theorem 4.2.

Let d be a square free positive integer and $t=\mathcal{N}(j_{1,N})$ be the normalized generator of $K(X_1(N))$. For a cusp s of $\Gamma_1(N)$ let h_s denote its width. If $t\in q^{-1}\mathbb{Z}[[q]]$ and

$$\prod_{s\in S_{\Gamma_1(N)}\setminus\{\infty\}}(t(z)-t(s))^{h_s}$$

is a polynomial in $\mathbb{Z}[t]$, then $t(\tau)$ is an algebraic integer for $\tau\in\mathbb{Q}(\sqrt{-d})\cap\mathfrak{H}$.

Proof. Let $j(z)=1/q+744+196884q+\ldots$ It is well-known that $j(\tau)$ is an algebraic integer for $\tau\in\mathbb{Q}(\sqrt{-d})\cap\mathfrak{H}$ [10, 18]. For algebraic proofs, see [4, 14, 17, 19]. View j as a function on the modular curve $X_1(N)$. Then j has a pole of order h_s at the cusp s. On the other hand, $t(z)-t(s)$ has a simple zero at s. Thus

$$j\times\prod_{s\in S_{\Gamma_1(N)}\setminus\{\infty\}}(t(z)-t(s))^{h_s} \tag{5}$$

has a pole only at ∞ whose degree is $\mu_N=\left[\overline{\Gamma}(1):\overline{\Gamma}_1(N)\right]$, and is thus a monic polynomial in t of degree μ_N which we denote by $f(t)$. Since the multiplier of j in (5) is a polynomial in $\mathbb{Z}[t]$ and since j and t have integer coefficients in the q-expansions, $f(t)$ is a monic polynomial in $\mathbb{Z}[t]$ of degree μ_N. This shows that $t(\tau)$ is integral over $\mathbb{Z}[j(\tau)]$. Therefore $t(\tau)$ is integral over $\mathbb{Z}$ for $\tau\in\mathbb{Q}(\sqrt{-d})\cap\mathfrak{H}$. □

Corollary 4.3.

For $\tau\in\mathbb{Q}(\sqrt{-d})\cap\mathfrak{H}$, $\mathcal{N}(j_{1,N})(\tau)$ is an algebraic integer for $N\in\{7,8,9,10,12\}$.

Proof. Since $\mathcal{N}(j_{1,N})$ has integral Fourier coefficients, it is enough to show that

$$\prod_{s\in S_{\Gamma_1(N)}\setminus\{\infty\}}(t(z)-t(s))^{h_s}\in\mathbb{Z}[t]. \tag{6}$$

When $N\in\{8,10,12\}$, from Tables 2, 4, 5, 7, 9 and 10 we can check that this product is in $\mathbb{Z}[t]$. When $N=7$ we show that

$$(t-t(0))\left(t-t\left(\frac{1}{2}\right)\right)\left(t-t\left(\frac{1}{3}\right)\right)\in\mathbb{Z}[t]$$

where $t=\mathcal{N}(j_{1,7})$. And when $N=9$ we show that

$$(t-t(0))\left(t-t\left(\frac{1}{2}\right)\right)\left(t-t\left(\frac{3}{4}\right)\right)\in\mathbb{Z}[t]$$

where $t=\mathcal{N}(j_{1,9})$. Then from Tables 1, 3, 6 and 8 we have (6).

<u>$N=7$</u> Let t_0 be the Hauptmodul of $\Gamma_0(7)$. Then by [2, Tables 3 and 4],

$$t_0=\frac{\eta(z)^4}{\eta(7z)^4}+4=\frac{1}{q}+0+2q+8q^2-5q^3-4q^4-10q^5+12q^6-7q^7+8q^8+46q^9-36q^{10}+\ldots$$

If we view t_0 as a function on $X_1(7)$, then t_0 has simple poles only at ∞, 4/7, 5/7. Thus $t_0 \times (t - t(4/7))(t - t(5/7))$ has poles only at ∞ whose degree is 3 and so it is a monic polynomial in t of degree 3. Then we can write

$$t_0 \times \left(t - t\left(\frac{4}{7}\right)\right)\left(t - t\left(\frac{5}{7}\right)\right) = t^3 + at^2 + bt + c$$

for some $a, b, c \in \mathbb{C}$. From Table 4 it follows that

$$t_0 \times (t+3)(t+2) = t^3 + at^2 + bt + c.$$

By replacing t_0, t by their q-series,

$$\begin{aligned}(L.H.S.) &= q^{-3} + \frac{5}{q^2} + \frac{16}{q} + 44 + 94q + \dots \\ (R.H.S.) &= q^{-3} + \frac{a}{q^2} + \frac{12+b}{q} + 9 + 8a + c + (48 + 6a + 4b)\,q + \dots\end{aligned}$$

Therefore $a = 5$, $b = 4$, $c = -5$. Also from the transformation formula of eta functions it follows that

$$t_0|_{\left(\begin{smallmatrix}0 & -1\\ 1 & 0\end{smallmatrix}\right)} = \frac{\eta(z)^4}{\eta(7z)^4}\Big|_{\left(\begin{smallmatrix}0 & -1\\ 1 & 0\end{smallmatrix}\right)} + 4 = \frac{\eta(-1/z)^4}{\eta(-7/z)^4} + 4 = \frac{\sqrt{-iz}^4\eta(z)^4}{\sqrt{-iz/7}^4\eta(z/7)^4} + 4 \to 4.$$

Since 0, 1/2, and 1/3 are equivalent to 0 under $\Gamma_0(7)$, $t(0)$, $t(1/2)$, and $t(1/3)$ are roots of the polynomial

$$X^3 + 5X^2 + 4X - 5 - 4(X+3)(X+2) = X^3 + X^2 - 16X - 29.$$

$\underline{N = 9}$ Let t_0 be the Hauptmodul of $\Gamma_0(9)$. Again by [2, Tables 3 and 4]

$$t_0 = \frac{\eta(z)^3}{\eta(9z)^3} + 3 = \frac{1}{q} + 0 + 0q + 5q^2 + 0q^3 + 0q^4 - 7q^5 + 0q^6 + 0q^7 + 3q^8 + 0q^9 + 0q^{10} + \dots$$

Similarly to the case $N = 7$,

$$t_0 \times \left(t - t\left(\frac{5}{9}\right)\right)\left(t - t\left(\frac{7}{9}\right)\right) = t^3 + at^2 + bt + c$$

for some $a, b, c \in \mathbb{C}$. From Table 5

$$t_0 \times (t+2)(t+1) = t^3 + at^2 + bt + c.$$

By replacing t_0, t by their q-series,

$$\begin{aligned}(L.H.S.) &= \frac{1}{q^3} + \frac{3}{q^2} + \frac{6}{q} + 15 + 27q + 39q^2 + \dots \\ (R.H.S.) &= \frac{1}{q^3} + \frac{a}{q^2} + \frac{6+b}{q} + 6 + 4a + c + (15 + 4a + 2b)\,q + (21 + 6a + 2b)\,q^2 + \dots\end{aligned}$$

Thus $a = 3$, $b = 0$, $c = -3$. And

$$t_0|_{\left(\begin{smallmatrix}0 & -1\\ 1 & 0\end{smallmatrix}\right)} = \frac{\eta(z)^3}{\eta(9z)^3}\Big|_{\left(\begin{smallmatrix}0 & -1\\ 1 & 0\end{smallmatrix}\right)} + 3 = \frac{\eta(-1/z)^3}{\eta(-9/z)^3} + 3 = \frac{\sqrt{-iz}^3\eta(z)^3}{\sqrt{-iz/9}^3\eta(z/9)^3} + 3 \to 3.$$

Now that 0, 1/2, and 3/4 are equivalent to 0 under $\Gamma_0(9)$, $t(0)$, $t(1/2)$, and $t(3/4)$ are roots of the polynomial

$$X^3 + 3X^2 - 3 - 3(X+2)(X+1) = X^3 - 9X - 9. \qquad \square$$

Remark 4.4.

(1) Let $t = \mathcal{N}(j_{1,N})$. There is an explicit description of how the Galois group of $\mathbb{Q}(e^{2\pi i/N})$ over $\mathbb{Q}$ acts on $t(s)$ for each cusp s (see [15] and also [18, Chapter 6] and [20, Chapter 1]). Using this description one can show that the assumption in Theorem 4.2 is met.

(2) The function $j_{1,N}$ is a modular unit with integer coefficients [9, Theorem 6.4]. In other words, $j_{1,N}$ is a unit inside the integral closure of the ring $\mathbb{Z}[j]$. Therefore, the values of $j_{1,N}$ at imaginary quadratic irrationalities are not only algebraic integers, but also units in the ring of integers. Now, the normalized Hauptmodul $\mathcal{N}(j_{1,N})(z)$ is equal to $\pm j_{1,N}(\gamma z)^{\pm 1} + c$ for a suitably chosen $\gamma \in \Gamma_0(N)$ and some integer c. More explicitly, the following equalities hold:

$$\mathcal{N}(j_{1,7})(z) = j_{1,7}\left(\left(\begin{smallmatrix} 4 & 1 \\ 7 & 2 \end{smallmatrix}\right) z\right) - 3, \qquad \mathcal{N}(j_{1,8})(z) = -j_{1,8}\left(\left(\begin{smallmatrix} 3 & 1 \\ 8 & 3 \end{smallmatrix}\right) z\right) - 1, \qquad \mathcal{N}(j_{1,9})(z) = j_{1,9}\left(\left(\begin{smallmatrix} 5 & 1 \\ 9 & 2 \end{smallmatrix}\right) z\right) - 2,$$
$$\mathcal{N}(j_{1,10})(z) = -\frac{1}{j_{1,10}\left(\left(\begin{smallmatrix} 3 & 2 \\ 10 & 7 \end{smallmatrix}\right) z\right)}, \qquad \mathcal{N}(j_{1,12})(z) = \frac{1}{j_{1,12}\left(\left(\begin{smallmatrix} 5 & 2 \\ 12 & 5 \end{smallmatrix}\right) z\right)} - 2.$$

Therefore, $\mathcal{N}(j_{1,N})$ takes algebraic integers as values at imaginary quadratic numbers.

5. Application to class fields

Let G be an algebraic group GL_2 defined over $\mathbb{Q}$ and $G_{\mathbb{A}}$ be the adelization of G. We set $G_{\infty+} = \{x \in \mathrm{GL}_2(\mathbb{R}) : \det x > 0\}$ and $G_{\mathbb{Q}_+} = \{x \in \mathrm{GL}_2(\mathbb{Q}) : \det x > 0\}$. Note that we define the topology of $G_{\mathbb{A}}$ by taking $U = \prod_p \mathrm{GL}_2(\mathbb{Z}_p) \times G_{\infty+}$ to be an open subgroup. Let K be an imaginary quadratic field, and let ξ be an embedding of K into $M_2(\mathbb{Q})$. We call ξ *normalized* if it is defined by $u\left(\begin{smallmatrix} z \\ 1 \end{smallmatrix}\right) = \xi(u)\left(\begin{smallmatrix} z \\ 1 \end{smallmatrix}\right)$ for $u \in K$ where z is a fixed point of $\xi(K^\times)$ $(\subset G_{\mathbb{Q}_+})$ in $\mathfrak{H}$. We observe that the embedding ξ defines a continuous homomorphism of $K_{\mathbb{A}}^\times$ into $G_{\mathbb{A}+}$, where $K_{\mathbb{A}}^\times$ is the idele group of K and $G_{\mathbb{A}+}$ denotes the group $G_0 G_{\infty+}$ with G_0 the non-archimedean part of $G_{\mathbb{A}}$. The following lemma is a slight modification of the argument in [1, (3.7.6)] which originally comes from the Shimura reciprocity law.

Lemma 5.1 ([8, sublemma of Theorem 17]).

With K and α as in the introduction, let $az^2 + bz + c = 0$ be the equation of α such that $a > 0$ and $(a, b, c) = 1$. Let f be a modular function of level N with rational Fourier coefficients and (β) a principal ideal of $\mathcal{O}_K$ relatively prime to N. Write $\beta = n(a\alpha) + m$ in $\mathbb{Z}(a\alpha) + \mathbb{Z}$ $(= \mathcal{O}_K)$. And let $\mathcal{A}_\beta$ be a matrix in $\mathrm{SL}_2(\mathbb{Z})$ whose image in $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ is equal to

$$\begin{pmatrix} -bn + m & -cn \\ anN(\beta)^{-1} & mN(\beta)^{-1} \end{pmatrix}.$$

Here $N(\beta)$ means the norm of β. Then the action of (β) on $f(\alpha)$ is given by

$$f(\alpha)^{[(\beta), K_{(N)}/K]} = f(\mathcal{A}_\beta \cdot \alpha) \tag{7}$$

where $[(\beta), K_{(N)}/K]$ denotes the Artin symbol.

Theorem 5.2.

Let K and α be as before. Let $az^2 + bz + c = 0$ be the equation of α such that $a > 0$ and $(a, b, c) = 1$. Then $j_{1,N}(\alpha)$ generates the ray class field $K_{\mathfrak{f}}$ with conductor

$$\mathfrak{f} = \frac{N}{(a, N)} \cdot [(a, N), a\alpha + b]$$

where d_K is the discriminant of K and $N \in \{7, 8, 9, 10, 12\}$.

Proof. We treat only the case $N = 7$ — the other cases can be treated in almost the same way. Since $j_{1,7}$ is a modular function of level 7 with rational Fourier coefficients, $j_{1,7}(\alpha)$ belongs to $K_{(7)}$. Let $I_K(7)$ be the group of all fractional $\mathcal{O}_K$-ideals relatively prime to $7\mathcal{O}_K$ and $\Phi_{L/K}\colon I_K(7) \to \mathrm{Gal}(L/K)$ be the Artin map for a subfield L of $K_{(7)}$. We set $L_1 = K(j_{1,7}(\alpha))$ for simplicity. Since $K \subseteq L_1 \subseteq K_{(7)}$, we have $P_{K,1}(7) \subseteq \ker(\Phi_{L_1/K})$ where $P_{K,1}(7)$ is the subgroup of $I_K(7)$ generated by the principal ideals $x\mathcal{O}_K$ with $x \equiv 1 \bmod 7\mathcal{O}_K$. We will show that $\ker(\Phi_{L_1/K}) = P_{K,1}(\mathfrak{f}) \cap I_K(7)$, where $P_{K,1}(\mathfrak{f})$ is the subgroup of $I_K(\mathfrak{f})$ generated by principal ideals $x\mathcal{O}_K$ with $x \equiv 1 \bmod \mathfrak{f}$ and $I_K(\mathfrak{f})$ is the group of all fractional $\mathcal{O}_K$-ideals relatively prime to $\mathfrak{f}$. Let $\mathfrak{a} \in \ker(\Phi_{L_1/K})$. Then $\Phi_{L_1/K}(\mathfrak{a}) = [\mathfrak{a}, L_1/K]$ fixes $j_{1,7}(\alpha)$ and hence it fixes $j(\alpha)$ too. Here j denotes the modular invariant. Since $K(j(\alpha))$ is the Hilbert class field of K, $\mathfrak{a}$ belongs to $P_K(7)$, the subgroup of $I_K(7)$ generated by principal ideals. Thus we can write $\mathfrak{a} = \beta\mathcal{O}_K$ where β is an element of $\mathcal{O}_K$ with $(N(\beta), 7) = 1$. If $\beta = n(a\alpha) + m$ is in $\mathbb{Z}\cdot(a\alpha) + \mathbb{Z} = \mathcal{O}_K$, then by (7) we claim that $(\beta) \in \ker(\Phi_{L_1/K})$ if and only if $A_\beta \in \pm\Gamma_1(7)\cdot\Gamma_\alpha$ where $\Gamma_\alpha = \{\gamma \in \mathrm{SL}_2(\mathbb{Z}) : \gamma\alpha = \alpha\}$. Here we observe that Γ_α is nontrivial if and only if α is equivalent to i $(= \sqrt{-1})$ or ρ $(= e^{2\pi i/3})$ under $\mathrm{SL}_2(\mathbb{Z})$. First we consider the trivial case for Γ_α. For $(\beta) \in I_K(7)$,

$$\begin{aligned}
(\beta) \in \ker(\Phi_{L_1/K}) \quad &\Longleftrightarrow \quad A_\beta \in \pm\Gamma_1(7) \quad \Longleftrightarrow \quad 7 \mid an \ \text{ and } \ -bn + m \equiv \pm 1 \bmod 7 \\
\Longleftrightarrow \quad &\frac{7}{(a,7)} \mid n \ \text{ and } \ m \in \pm 1 + bn + 7\mathbb{Z} \quad \Longleftrightarrow \quad \frac{7}{(a,7)} \mid n \ \text{ and } \ \beta \in \pm 1 + n(a\alpha + b) + 7\mathbb{Z} \\
\Longleftrightarrow \quad &\pm\beta \in 1 + \frac{7}{(a,7)}\cdot[(a,7), a\alpha + b] \quad \Longleftrightarrow \quad (\beta) \in P_{K,1}(\mathfrak{f}),
\end{aligned}$$

as desired. Next, assume that Γ_α is nontrivial. Thus α is equivalent to i or ρ under $\mathrm{SL}_2(\mathbb{Z})$. Suppose first that α is equivalent to i (i.e. the discriminant $d_K = b^2 - 4ac = -4$). We then obtain that for $(\beta) \in I_K(7)$,

$$\begin{aligned}
(\beta) \in \ker(\Phi_{L_1/K}) \quad &\Longleftrightarrow \quad A_\beta \in \pm\Gamma_1(7)\cdot\Gamma_\alpha \\
&\Longleftrightarrow \quad A_\beta \in \pm\Gamma_1(7) \quad \text{or} \quad A_\beta\cdot\gamma^{-1}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\gamma \in \pm\Gamma_1(7)
\end{aligned}$$

where we write $\alpha = \gamma^{-1}\cdot i$ for some $\gamma = \left(\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$. Since α is a root of the polynomial $[1,0,1]\circ\left(\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right)\left(\begin{smallmatrix} z \\ 1 \end{smallmatrix}\right) = (p^2 + r^2)z^2 + 2(pq + rs)z + q^2 + s^2$, $a = p^2 + r^2$, $b = 2(pq + rs)$ and $c = q^2 + s^2$. Here $[A, B, C]\circ\left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right)$ denotes the quadratic form $Ax^2 + Bxy + Cy^2$. Thus

$$\gamma^{-1}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\gamma = \begin{pmatrix} -b/2 & -c \\ a & b/2 \end{pmatrix},$$

and thus

$$A_\beta\cdot\gamma^{-1}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\gamma = \begin{pmatrix} b^2n/2 - bm/2 - acn & -c(m - bn/2) \\ a(m - bn/2)k_\beta & * \end{pmatrix}$$

where $k_\beta \in \mathbb{Z}$ is such that $k_\beta N(\beta) \equiv 1 \bmod 7$. Therefore

$$\begin{aligned}
&A_\beta \in \pm\Gamma_1(7) \quad \text{or} \quad A_\beta\cdot\gamma^{-1}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\gamma \in \pm\Gamma_1(7) \\
\Longleftrightarrow \quad &7 \mid an \quad \text{and} \quad m \in \pm 1 + bn + 7\mathbb{Z}, \\
&\text{or} \quad 7 \mid a\left(m - \frac{bn}{2}\right) \quad \text{and} \quad \frac{b^2n}{2} - \frac{bm}{2} - acn \equiv \pm 1 \bmod 7 \\
\Longleftrightarrow \quad &\frac{7}{(a,7)} \mid n \quad \text{and} \quad \beta \in \pm 1 + n(a\alpha + b) + 7\mathbb{Z}, \\
&\text{or} \quad \frac{7}{(a,7)} \mid \left(m - \frac{bn}{2}\right) \quad \text{and} \quad \frac{b^2n}{2} - \frac{bm}{2} - acn \equiv \pm 1 \bmod 7 \\
\Longleftrightarrow \quad &\pm\beta \in 1 + \frac{7}{(a,7)}[(a,7), a\alpha + b], \\
&\text{or} \quad \frac{7}{(a,7)} \mid \left(m - \frac{bn}{2}\right) \quad \text{and} \quad \frac{b^2n}{2} - \frac{bm}{2} - acn \equiv \pm 1 \bmod 7.
\end{aligned}$$

On the other hand,

$$(\beta) \in P_{K,1}(\mathfrak{f}) \qquad \Longleftrightarrow \qquad \pm\beta \equiv 1 \bmod \mathfrak{f} \quad \text{or} \quad \pm\beta \cdot i \equiv 1 \bmod \mathfrak{f}.$$

From the equality $(a\alpha)^2 + b(a\alpha) + ac = 0$ it follows that $a\alpha = -b/2 + i$. And

$$\begin{aligned}\beta \cdot i &= (na\alpha + m)\left(a\alpha + \frac{b}{2}\right) = \left(-\frac{bn}{2} + m\right) a\alpha + \frac{bm}{2} - nac \\ &= \left(-\frac{bn}{2} + m\right)(a\alpha + b) - b\left(-\frac{bn}{2} + m\right) + \frac{bm}{2} - nac = \left(-\frac{bn}{2} + m\right)(a\alpha + b) + \frac{b^2 n}{2} - \frac{bm}{2} - acn.\end{aligned}$$

Thus

$$\begin{aligned}&\pm\beta \equiv 1 \bmod \mathfrak{f} \quad \text{or} \quad \pm\beta \cdot i \equiv 1 \bmod \mathfrak{f} \qquad \Longleftrightarrow \\ &\qquad \pm\beta \in 1 + \frac{7}{(a,7)} \cdot [(a,7), a\alpha + b], \quad \text{or} \quad \frac{7}{(a,7)} \mid \left(m - \frac{bn}{2}\right) \quad \text{and} \quad \frac{b^2 n}{2} - \frac{bm}{2} - acn \equiv \pm 1 \bmod 7.\end{aligned}$$

Suppose instead that α is equivalent to ρ under $\mathrm{SL}_2(\mathbb{Z})$ (i.e. the discriminant $d_K = -3$). Since $\Gamma_\rho = \left\{ \pm I, \pm\left(\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix}\right), \pm\left(\begin{smallmatrix} 1 & 1 \\ -1 & 0 \end{smallmatrix}\right) \right\}$, we see that $\Gamma_\alpha = \left\{ \pm I, \pm\gamma^{-1}\left(\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix}\right)\gamma, \pm\gamma^{-1}\left(\begin{smallmatrix} 1 & 1 \\ -1 & 0 \end{smallmatrix}\right)\gamma \right\}$ if we write $\alpha = \gamma^{-1}\rho$ for some $\gamma = \left(\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$. We then obtain that for $(\beta) \in I_K(7)$,

$$\begin{aligned}&(\beta) \in \ker(\Phi_{L_1/K}) \qquad \Longleftrightarrow \qquad A_\beta \in \pm\Gamma_1(7) \cdot \Gamma_\alpha \\ &\Longleftrightarrow \qquad A_\beta \in \pm\Gamma_1(7) \quad \text{or} \quad A_\beta \cdot \gamma^{-1} \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix} \gamma \in \pm\Gamma_1(7) \quad \text{or} \quad A_\beta \cdot \gamma^{-1} \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} \gamma \in \pm\Gamma_1(7).\end{aligned}$$

Since α is a root of the polynomial

$$[1,1,1] \circ \begin{pmatrix} p & q \\ r & s \end{pmatrix} \begin{pmatrix} z \\ 1 \end{pmatrix} = \left(p^2 + pr + r^2\right) z^2 + (2pq + ps + qr + 2rs) z + \left(q^2 + qs + s^2\right),$$

we get $a = p^2 + pr + r^2$, $b = 2pq + ps + qr + 2rs$ $(= 2(pq + ps + rs) - 1 = 2(pq + qr + rs) + 1)$ and $c = q^2 + qs + s^2$. Thus

$$\gamma^{-1} \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix} \gamma = \begin{pmatrix} ps + pq + rs & q^2 + qs + s^2 \\ -(p^2 + pr + r^2) & -(pq + qr + rs) \end{pmatrix} = \begin{pmatrix} (b+1)/2 & c \\ -a & -(b-1)/2 \end{pmatrix},$$

and

$$\begin{aligned}A_\beta \cdot \left(\gamma^{-1} \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix} \gamma\right) &= \begin{pmatrix} -bn + m & -cn \\ ank_\beta & mk_\beta \end{pmatrix} \begin{pmatrix} (b+1)/2 & c \\ -a & -(b-1)/2 \end{pmatrix} \\ &= \begin{pmatrix} (b+1)(-bn+m)/2 + acn & -((b+1)n/2 - m)c \\ ((b+1)n/2 - m)ak_\beta & * \end{pmatrix}.\end{aligned}$$

Likewise, we have

$$\gamma^{-1} \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} \gamma = \left(\gamma^{-1} \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix} \gamma\right)^{-1} = \begin{pmatrix} -(b-1)/2 & -c \\ a & (b+1)/2 \end{pmatrix}$$

and

$$A_\beta \cdot \gamma^{-1} \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} \gamma = \begin{pmatrix} -(b-1)(-bn+m)/2 - acn & ((b-1)n/2 - m)c \\ (-(b-1)n/2 + m)ak_\beta & * \end{pmatrix}.$$

Therefore

$$\begin{aligned} & A_\beta \in \pm\Gamma_1(7) \quad \text{or} \quad A_\beta \cdot \gamma^{-1}\begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}\gamma \in \pm\Gamma_1(7) \quad \text{or} \quad A_\beta \cdot \gamma^{-1}\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}\gamma \in \pm\Gamma_1(7) \\ \Longleftrightarrow \quad & 7 \mid an \quad \text{and} \quad m \in \pm 1 + bn + 7\mathbb{Z}, \\ & \text{or} \quad 7 \mid a\left(\frac{(b+1)n}{2} - m\right) \quad \text{and} \quad (b+1)\frac{-bn+m}{2} + acn \equiv \pm 1 \bmod 7 \\ & \text{or} \quad 7 \mid a\left(\frac{(b-1)n}{2} - m\right) \quad \text{and} \quad (b-1)\frac{-bn+m}{2} + acn \equiv \pm 1 \bmod 7 \\ \Longleftrightarrow \quad & \pm\beta \in 1 + \frac{7}{(a,7)}[(a,7), a\alpha + b], \\ & \text{or} \quad \frac{7}{(a,7)} \mid \frac{(b+1)n}{2} - m \quad \text{and} \quad (b+1)\frac{-bn+m}{2} + acn \equiv \pm 1 \bmod 7 \\ & \text{or} \quad \frac{7}{(a,7)} \mid \frac{(b-1)n}{2} - m \quad \text{and} \quad (b-1)\frac{-bn+m}{2} + acn \equiv \pm 1 \bmod 7. \end{aligned}$$

On the other hand,

$$(\beta) \in P_{K,1}(\mathfrak{f}) \quad \Longleftrightarrow \quad \pm\beta \equiv 1 \bmod \mathfrak{f} \quad \text{or} \quad \pm\,\beta\cdot\rho \equiv 1 \bmod \mathfrak{f} \quad \text{or} \quad \pm\,\beta\cdot\rho^2 \equiv 1 \bmod \mathfrak{f}.$$

From the equality $(a\alpha)^2 + b(a\alpha) + ac = 0$ it follows that

$$a\alpha = \frac{-b+1-1+\sqrt{-3}}{2} = -\frac{b-1}{2} + \rho = \frac{-b-1+1+\sqrt{-3}}{2} = -\frac{b+1}{2} - \rho^2.$$

Thus we have $\rho = a\alpha + (b-1)/2$ and $-\rho^2 = a\alpha + (b+1)/2$. And

$$\begin{aligned} \beta\cdot\rho = (na\alpha + m)\left(a\alpha + \frac{b-1}{2}\right) &= \left(m - \frac{(b+1)n}{2}\right)a\alpha + \frac{m(b-1)}{2} - nac \\ &= \left(m - \frac{(b+1)n}{2}\right)(a\alpha + b) - b\left(m - \frac{(b+1)n}{2}\right) + \frac{m(b-1)}{2} - nac \\ &= \left(m - \frac{(b+1)n}{2}\right)(a\alpha + b) - (b+1)\frac{-bn+m}{2} - nac. \end{aligned}$$

Similarly,

$$\begin{aligned} \beta\cdot(-\rho^2) = (na\alpha + m)\left(a\alpha + \frac{b+1}{2}\right) &= \left(m - \frac{(b-1)n}{2}\right)a\alpha + \frac{m(b+1)}{2} - nac \\ &= \left(m - \frac{(b-1)n}{2}\right)(a\alpha + b) - b\left(m - \frac{(b-1)n}{2}\right) + \frac{m(b+1)}{2} - nac \\ &= \left(m - \frac{(b-1)n}{2}\right)(a\alpha + b) + (b-1)\frac{bn-m}{2} - nac. \end{aligned}$$

Thus we get that

$$\begin{aligned} & \pm\,\beta \equiv 1 \bmod \mathfrak{f} \quad \text{or} \quad \pm\,\beta\cdot\rho \equiv 1 \bmod \mathfrak{f} \quad \text{or} \quad \pm\,\beta\cdot\rho^2 \equiv 1 \bmod \mathfrak{f} \\ \Longleftrightarrow \quad & \pm\beta \in 1 + \frac{7}{(a,7)}\cdot[(a,7), a\alpha + b], \\ & \text{or} \quad \frac{7}{(a,7)} \mid \left(m - \frac{(b+1)n}{2}\right) \quad \text{and} \quad (b+1)\frac{-bn+m}{2} + nac \equiv \pm 1 \bmod 7 \\ & \text{or} \quad \frac{7}{(a,7)} \mid \left(m - \frac{(b-1)n}{2}\right) \quad \text{and} \quad (b-1)\frac{-bn+m}{2} + nac \equiv \pm 1 \bmod 7. \end{aligned}$$

Consequently, $(\beta) \in \ker(\Phi_{L_1/K})$ is equivalent to $(\beta) \in I_K(7) \cap P_{K,1}(\mathfrak{f})$. We recall from [6, Chapter V, Lemma 6.1] that the canonical map $I_K(7) \to I_K(\mathfrak{f})/P_{K,1}(\mathfrak{f})$ induces an isomorphism $I_K(7)/(I_K(7) \cap P_{K,1}(\mathfrak{f})) \approx I_K(\mathfrak{f})/P_{K,1}(\mathfrak{f})$. Therefore by class field theory we prove that L_1 is the ray class field $K_{\mathfrak{f}}$. □

Acknowledgements

This work was partially supported by Basic Science Research Program through the NRF of Korea funded by MEST (2011-0001184).

References

[1] Chen I., Yui N., Singular values of Thompson series, In: Groups, Difference Sets, and the Monster, Columbus, 1993, Ohio State Univ. Math. Res. Inst. Publ., 4, de Gruyter, Berlin, 1996, 255–326

[2] Conway J.H., Norton S.P., Monstrous moonshine, Bull. London Math. Soc., 1979, 11(3), 308–339

[3] Darmon H., Note on a polynomial of Emma Lehmer, Math. Comp., 1991, 56(194), 795–800

[4] Deuring M., Die Typen der Multiplikatorenringe elliptischer Funktionenkörper, Abh. Math. Sem. Hansischen Univ., 1941, 14, 197–272

[5] Ishida N., Ishii N., Generators and defining equation of the modular function field of the group $\Gamma_1(N)$, Acta Arith., 2002, 101(4), 303–320

[6] Janusz G.J., Algebraic Number Fields, Pure Appl. Math., 55, Academic Press, New York–London, 1973

[7] Kim C.H., Koo J.K., On the genus of some modular curve of level N, Bull. Austral. Math. Soc., 1996, 54(2), 291–297

[8] Kim C.H., Koo J.K., Arithmetic of the modular function $j_{1,8}$, Ramanujan J., 2000, 4(3), 317–338

[9] Kubert D.S., Lang S., Modular Units, Grundlehren Math. Wiss., 244 Springer, New York–Berlin, 1981

[10] Lang S., Elliptic Functions, 2nd ed., Grad. Texts in Math., 112, Springer, New York, 1987

[11] Lecacheux O., Unités d'une famille de corps cycliques réeles de degré 6 liés à la courbe modulaire $X_1(13)$, J. Number Theory, 1989, 31(1), 54–63

[12] Lecacheux O., Unités d'une famille de corps liés à la courbe $X_1(25)$, Ann. Inst. Fourier (Grenoble), 1990, 40(2), 237–253

[13] Miyake T., Modular Forms, Springer, Berlin, 1989

[14] Néron A., Modèles minimaux des variétés abéliennes sur les corps locaux et globaux, Publ. Math. Inst. Hautes Études Sci., 1964, 21, 5–125

[15] Ogg A.P., Rational points on certain elliptic modular curves, In: Analytic Number Theory, St. Louis University, St. Louis, 1972, Proc. Sympos. Pure Math., 24, American Mathematical Society, Providence, 1973, 221–231

[16] Schoeneberg B., Elliptic Modular Functions, Grundlehren Math. Wiss., 203, Springer, New York–Heidelberg, 1974

[17] Serre J.-P., Tate J., Good reduction of abelian varieties, Ann. of Math., 1968, 88, 492–517

[18] Shimura G., Introduction to the Arithmetic Theory of Automorphic Functions, Publications of the Mathematical Society of Japan, 11, Iwanami Shoten, Tokyo, 1971

[19] Silverman J.H., Advanced Topics in the Arithmetic of Elliptic Curves, Grad. Texts in Math., 151, Springer, New York, 1994

[20] Stevens G., Arithmetic on Modular Curves, Progr. Math., 20, Birkhäuser, Boston, 1982

[21] Washington L.C., A family of cyclic quartic fields arising from modular curves, Math. Comp., 1991, 57(196), 763–775