Singular values of generalized $\lambda$ functions

October 21, 2011

Noburo Ishii

1 Introduction

For a positive integer $N$, let $\Gamma_1(N)$ be the subgroup of $\text{SL}_2(\mathbb{Z})$ defined by

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(\mathbb{Z}) \mid a - 1 \equiv c \equiv 0 \mod N \right\}.$$ 

We denote by $A_1(N)$ the modular function field with respect to $\Gamma_1(N)$. For a positive integer $N \geq 6$, let $a = [a_1, a_2, a_3]$ be a triple of integers with the properties $0 < a_i \leq N/2$ and $a_i \neq a_j$ for any $i, j$. For an element $\tau$ of the complex upper half plane $\mathcal{H}$, we denote by $L_\tau$ the lattice of $\mathbb{C}$ generated by $1$ and $\tau$ and by $\wp(z; L_\tau)$ the Weierstrass $\wp$-function relative to the lattice $L_\tau$. In [4], we defined a modular function $W_a(\tau)$ with respect to $\Gamma_1(N)$ by

$$W_a(\tau) = \frac{\wp(a_1/N; \tau) - \wp(a_3/N; \tau)}{\wp(a_2/N; \tau) - \wp(a_3/N; \tau)}.$$ 

This function is one of generalized $\lambda$ functions introduced by S.Lang in Chapter 18, §6 of [5]. He describes that it is interesting to investigate special values of generalized $\lambda$ functions at imaginary quadratic points, to see if they generate the ray class field. Here a point of $\mathcal{H}$ is called an imaginary quadratic point if it generates an imaginary quadratic field over $\mathbb{Q}$. In Theorem 3.7 of [5], we showed, under a rather strong condition that $a_1a_2a_3(a_1 - a_3)(a_2 - a_3)$...
is prime to $N$, that the values of $W_a$ at imaginary quadratic points are units of ray class fields. Let $j$ be the modular invariant function. We showed in Theorem 5 of [4] that each of the functions $W_{[3,2,1]}, W_{[5,2,1]}$ generates $A_1(N)$ over $C(j)$. In this article, we shall study the functions $W_a$ in the particular case: $a_2 = 2, a_3 = 1$. To simplify the notation, henceforth we denote by $\Lambda_k$ the function $W_{[k,2,1]}$. We shall prove that if $2 < k < N/2$, then $\Lambda_k$ generates $A_1(N)$ over $C(j)$. In this article, we shall study the functions $W_a$ in the particular case: $a_2 = 2, a_3 = 1$. To simplify the notation, henceforth we denote by $\Lambda_k$ the function $W_{[k,2,1]}$. We shall prove that if $2 < k < N/2$, then $\Lambda_k$ generates $A_1(N)$ over $C(j)$. This result implies that for an imaginary quadratic point $\alpha$ such that $\mathbb{Z}[[\alpha]]$ is the maximal order of the field $K = \mathbb{Q}(\alpha)$, the values $\Lambda_k(\alpha)$ and $e^{2\pi i N}$ generate the ray class field of $K$ modulo $N$ over the Hilbert class field of $K$. Let $\delta = (k, N)$ be the greatest common divisor of $k$ and $N$. On the assumption that $k$ satisfies either (i) $\delta = 1$ or (ii) $\delta > 1, (\delta, 3) = 1$ and $N/\delta$ is not a power of a prime number, we shall prove that values of $\Lambda_k$ at imaginary quadratic points are algebraic integers. Throughout this article, we use the following notation:

For a function $f(\tau)$ and $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(\mathbb{Z})$, $f[A]_2, f \circ A$ represent

$$f[A]_2 = f \left( \frac{a\tau + b}{c\tau + d} \right) \left( c\tau + d \right)^{-2}, \quad f \circ A = f \left( \frac{a\tau + b}{c\tau + d} \right).$$

The greatest common divisor of $a, b \in \mathbb{Z}$ is denoted by $(a, b)$. For an integral domain $R$, $R((q))$ represents the ring of power series of a variable $q$ with coefficients in $R$ and $R[[q]]$ is a subring of $R((q))$ of power series with non-negative order. For elements $\alpha, \beta$ of $R$, the notation $\alpha | \beta$ represents that $\beta$ is divisible by $\alpha$, thus $\beta = \alpha \gamma$ for an element $\gamma \in R$.

2 Auxiliary results

Let $N$ be a positive integer greater than 6. Put $q = \exp(2\pi i \tau/N), \zeta = \exp(2\pi i /N)$. For an integer $x$, let $\{x\}$ and $\mu(x)$ be the integers defined by the following conditions:

$$0 \leq \{x\} \leq \frac{N}{2}, \quad \mu(x) = \pm 1,$$

$$\begin{cases} 
\mu(x) = 1 & \text{if } x \equiv 0, N/2 \mod N, \\
 x \equiv \mu(x)\{x\} \mod N & \text{otherwise}. 
\end{cases}$$

2
For an integer $s$ not congruent to $0 \mod N$, let

$$
\phi_s(\tau) = \frac{1}{(2\pi i)^2} \varphi \left( \frac{s}{N}, L_\tau \right) - 1/12.
$$

Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(\mathbb{Z})$. Put $s^* = \mu(sc)s, u_s = \zeta^{s^*}q^{(sc)\tau}$. Then by Lemma 1 of [4], we have

$$
\phi_s[A]_2 = \begin{cases} 
\frac{\zeta^{s^*}}{(1 - \zeta^{s^*})^2} - \sum_{m=1}^{\infty} \sum_{n=1}^{\infty} n(1 - \zeta^{n^*})(1 - \zeta^{-n^*})q^{mnN} & \text{if } \{sc\} = 0, \\
\sum_{n=1}^{\infty} nu_n^* - \sum_{m=1}^{\infty} \sum_{n=1}^{\infty} n(1 - u_n^*)(1 - u_s^{-n})q^{mnN} & \text{otherwise.}
\end{cases}
$$

(1)

We shall need next lemmas and propositions in the following sections.

**Lemma 2.1.** Let $r, s, c, d$ be integers such that $0 < r \neq s \leq N/2$, $(c, d) = 1$. Assume that $\{rc\} = \{sc\}$. Put $r^* = \mu(rc)r, s^* = \mu(sc)s$. Then we have $\zeta^{r^* - s^*} \neq 1$. Further if $\{rc\} = \{sc\} = 0, N/2$, then $\zeta^{r^* + s^*} \neq 1$.

**Proof.** The assumption $\{rc\} = \{sc\}$ implies that $(\mu(rc)r - \mu(sc)s)c \equiv 0 \mod N$. If $\zeta^{r^* - s^*} = 1$, then $(\mu(rc)r - \mu(sc)s)d \equiv 0 \mod N$. From $(c, d) = 1$, we obtain $\mu(rc)r - \mu(sc)s \equiv 0 \mod N$. This shows $r = s$. Suppose $\{rc\} = \{sc\} = 0, N/2$ and $\zeta^{r^* + s^*} = 1$. Then we have $(r+s)c \equiv 0 \mod N, (r+s)d \equiv 0 \mod N$. Therefore $r + s \equiv 0 \mod N$. This is impossible, because $0 < r \neq s \leq N/2$. $\square$

**Lemma 2.2.** Let $k \in \mathbb{Z}, \delta = (k, N)$.

(i) For an integer $\ell$, if $\delta | \ell$, then $(1 - \zeta^\ell)/(1 - \zeta^k) \in \mathbb{Z}[\zeta]$.

(ii) If $N/\delta$ is not a power of a prime number, then $1 - \zeta^k$ is a unit of $\mathbb{Z}[\zeta]$.

**Proof.** If $\delta | \ell$, then there exist an integer $m$ such that $\ell \equiv mk \mod N$. Therefore $\zeta^\ell = \zeta^{mk}$ and $(1 - \zeta^k) | (1 - \zeta^\ell)$. This shows (i). Let $p_i (i = 1, 2)$ be distinct prime factors of $N/\delta$. Since $N/p_i = \delta(N/(\delta p_i)), 1 - \zeta^\delta \mid 1 - \zeta^{N/p_i}$. Therefore $1 - \zeta^\delta | p_i (i = 1, 2)$. This implies that $1 - \zeta^\delta$ is a unit. Because of $(k/\delta, N/\delta) = 1, 1 - \zeta^k$ is also a unit.$\square$

From [11] and Lemma 2.1, we immediately obtain the following two propositions.
Proposition 2.3. Let \( r, s \in \mathbb{Z} \) such that \( 0 < r \neq s \leq N/2 \).

(i) If \( \{rc\}, \{sc\} \neq 0 \), then

\[
(\phi_r - \phi_s)[A]_2 \equiv \sum_{n=1}^{\infty} n(u_r^n - u_s^n) + u_r^{-1}q^N - u_s^{-1}q^N \mod q^N \mathbb{Z}[[\zeta]][[q]].
\]

(ii) If \( \{rc\} = 0 \) and \( \{sc\} \neq 0 \), then

\[
(\phi_r - \phi_s)[A]_2 \equiv \frac{\zeta^{rd}}{(1 - \zeta^{rd})^2} - \sum_{n=1}^{\infty} nu_r^n - u_s^{-1}q^N \mod q^N \mathbb{Z}[[\zeta]][[q]].
\]

(iii) If \( \{rc\} = \{sc\} = 0 \), then

\[
(\phi_r - \phi_s)[A]_2 \equiv -\zeta^{sd}(1 - \zeta^{(r-s)d})(1 - \zeta^{(r+s)d}) \mod q^N \mathbb{Z}[[\zeta]][[q]].
\]

Proposition 2.4. Let \( r, s \in \mathbb{Z} \) such that \( 0 < r \neq s \leq N/2 \). Put \( \ell = \min(\{rc\}, \{sc\}) \). Then

\[
(\phi_r - \phi_s)[A]_2 = \theta_{r,s}(A)q^\ell(1 + qh(q)),
\]

where \( h(q) \in \mathbb{Z}[\zeta][[q]] \) and \( \theta_{r,s}(A) \) is a non-zero element of \( \mathbb{Q}(\zeta) \) given as follows. In the case \( \{rc\} = \{sc\} \),

\[
\theta_{r,s}(A) = \begin{cases} 
-\zeta^s(1 - \zeta^{r-s}) & \text{if } \ell \neq 0, N/2, \\
-\zeta^s(1 - \zeta^{r-s})(1 - \zeta^{r+s}) & \text{if } \ell = N/2, \\
-\zeta^s(1 - \zeta^{r-s})(1 - \zeta^{r+s}) & \text{if } \ell = 0.
\end{cases}
\]

In the case \( \{rc\} \neq \{sc\} \), assuming that \( \{rc\} < \{sc\} \),

\[
\theta_{r,s}(A) = \begin{cases} 
\zeta^r & \text{if } \ell \neq 0, \\
\zeta^r & \text{if } \ell = 0.
\end{cases}
\]
3 Values of \( \Lambda_k \) at imaginary quadratic points

In this section, we shall prove that the values of \( \Lambda_k = W_{[k,2,1]} \) at imaginary quadratic points are algebraic integers.

**Proposition 3.1.** Let \( k \) be an integer such that \( 3 \leq k < N/2 \). Put \( \delta = (k, N) \). Assume either (i) \( \delta = 1 \) or (ii) \( \delta > 1, (\delta, 3) = 1 \) and \( N/\delta \) is not a power of a prime number. Then for \( A \in \text{SL}_2(\mathbb{Z}) \), we have

\[
\Lambda_k \circ A \in \mathbb{Z}[\zeta]((q)).
\]

**Proof.** Put \( A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \). Proposition 2.4 shows

\[
\Lambda_k \circ A = \omega f(q),
\]

where \( \omega = \theta_{k,1}(A)/\theta_{2,1}(A) \) and \( f \) is a power series in \( \mathbb{Z}[\zeta]((q)) \). Therefore it is sufficient to prove that \( \omega \in \mathbb{Z}[\zeta] \). First we consider the case \( \{c\} \neq \emptyset \). Let \( \{2c\} \neq \{c\} \). By (ii) of Proposition 2.4, we see \( 1/(\phi_2 - \phi_1)[A]_2 \in \mathbb{Z}[\zeta]((q)) \).

Further if \( \{kc\} \neq \emptyset \), then \( (\phi_k - \phi_1)[A]_2 \in \mathbb{Z}[\zeta][[q]] \). If \( \{kc\} = \emptyset \), then \( \delta > 1 \) and \( c \equiv 0 \mod N/\delta \). Therefore \( \zeta^{kd} \) is a primitive \( N/\delta \)-th root of unity. The assumption (ii) shows \( 1 - \zeta^{kd} \) is a unit. Thus \( (\phi_k - \phi_1)[A]_2 \in \mathbb{Z}[\zeta][[q]] \).

Hence we have \( \omega \in \mathbb{Z}[\zeta] \). Let \( \{2c\} = \{c\} \). Then, since \( \{c\} \neq \emptyset \), we have \( N \equiv 0 \mod 3 \), \( (k,3) = 1 \) and \( \{c\} = \{2c\} = \{kc\} = N/3 \), \( \mu(2c) = -\mu(c) \), \( \mu(kc) = (\frac{c}{k})\mu(c) \), where \((\frac{c}{k})\) is the Legendre symbol. By the same proposition, we know that \( \omega = (1 - \zeta^{(\mu(kc)k-\mu(c)d)})/(1 - \zeta^{3\mu(c)d}) \). Since \( \mu(kc)k - \mu(c) \equiv 0 \mod 3 \), we have \( \omega \in \mathbb{Z}[\zeta] \). Next consider the case \( \{c\} = \emptyset \). Then we have \( \{c\} = \{2c\} = \{kc\} = 0 \), \( \mu(c) = \mu(2c) = \mu(kc) = 1 \), \( (d, N) = 1 \) and

\[
\omega = \left( \frac{1 - \zeta^{2d}}{1 - \zeta^{kd}} \right)^2 \cdot \frac{(1 - \zeta^{(k-1)d})(1 - \zeta^{(k+1)d})}{(1 - \zeta^d)(1 - \zeta^{3d})}.
\]

If \( \delta = 1 \), then \( (kd, N) = 1 \). If \( \delta \neq 1 \), then the assumption (ii) implies \( 1 - \zeta^{kd} \) is a unit. Therefore \( (1 - \zeta^{2d})/(1 - \zeta^{kd}) \in \mathbb{Z}[\zeta] \). If \( N \neq 0 \) \mod 3, then since \( (3d, N) = 1 \), we know

\[
\frac{(1 - \zeta^{(k-1)d})(1 - \zeta^{(k+1)d})}{(1 - \zeta^d)(1 - \zeta^{3d})} \in \mathbb{Z}[\zeta].
\]
If $N \equiv 0 \mod 3$, then $(k, 3) = 1$ and one of $k + 1, k - 1$ is divisible by 3. Lemma 2.1 (i) gives
\[
\frac{(1 - \zeta^{(k-1)d})(1 - \zeta^{(k+1)d})}{(1 - \zeta^d)(1 - \zeta^{3d})} \in \mathbb{Z}[\zeta].
\]
Hence we obtain $\omega \in \mathbb{Z}[\zeta]$. □

**Theorem 3.2.** Let $\alpha$ be an imaginary quadratic point. Then $\Lambda_k(\alpha)$ is an algebraic integer.

**Proof.** Let $\mathcal{R}$ be a transversal of the coset decomposition of $\text{SL}_2(\mathbb{Z})$ by $\Gamma_1(N)\{\pm E_2\}$, where $E_2$ is the unit matrix. Consider a modular equation $\Phi(X, j) = \prod_{A \in \mathcal{R}} (X - \Lambda_k \circ A)$. Since $\Lambda_k \circ A$ has no poles in $\mathcal{H}$ and $\Lambda_k \circ A \in \mathbb{Z}[\zeta][\!(q)\!]$ by Proposition 3.1, the coefficients of $\Phi(X, j)$ are polynomials of $j$ with coefficients in $\mathbb{Z}[\zeta]$. Since $j(\alpha)$ is an algebraic integer (see Theorem 10.23 in [1]), $\Phi(X, j(\alpha))$ is a monic polynomial with algebraic integer coefficients. Because $\Lambda_k(\alpha)$ is a root of $\Phi(X, j(\alpha))$, it is an algebraic integer. □

Further we can show that $\Phi(X, j) \in \mathbb{Z}[j][X]$ and that $\Lambda_k(\alpha)$ belongs to the ray class field of $\mathbb{Q}(\alpha)$ modulo $N$. For details, see §3 of [5].

**Corollary 3.3.** Let $A \in \text{SL}_2(\mathbb{Z})$. Then the values of the function $\Lambda_k \circ A$ at imaginary quadratic points are algebraic integers. In particular, the function
\[
\frac{\varphi(k\tau/N; \tau) - \varphi(\tau/N; \tau)}{\varphi(2\tau/N; \tau) - \varphi(\tau/N; \tau)}
\]
takes algebraic and integral values at imaginary quadratic points, for $2 < k < N/2$.

**Proof.** Let $\alpha$ be an imaginary quadratic point. Then, $A(\alpha)$ is an imaginary quadratic point. Therefore, we have the former part of the assertion. If we put $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, then from the transformation formula of $\varphi((r\tau+s)/N; L_\tau)$ in §2 of [4], we obtain the latter part. □

4 Generators of $A_1(N)$

Let $A(N)$ be the modular function field of the principal congruence subgroup $\Gamma(N)$ of level $N$. For a subfield $\mathfrak{F}$ of $A(N)$, let us denote by $\mathfrak{F}_{\mathbb{Q}(\zeta)}$ the subfield of $\mathfrak{F}$ consisted of all modular functions having Fourier coefficients in $\mathbb{Q}(\zeta)$.  

6
Theorem 4.1. Let \( k \) be an integer such that \( 2 < k < N/2 \). Then we have \( A_1(N)_{\mathbb{Q}(\zeta)} = \mathbb{Q}(\zeta)(\Lambda_k,j) \)

Proof. By Theorem 3 of Chapter 6 of [6], the field \( A(N)_{\mathbb{Q}(\zeta)} \) is a Galois extension over \( \mathbb{Q}(\zeta)(j) \) with the Galois group \( SL_2(\mathbb{Z})/\Gamma(N)\{\pm E_2\} \) and the field \( A_1(N)_{\mathbb{Q}(\zeta)} \) is the fixed field of the subgroup \( \Gamma_1(N)\{\pm E_2\} \). Since \( \Lambda_k \in A_1(N)_{\mathbb{Q}(\zeta)} \), to prove the assertion, we have only to show \( A \in \Gamma_1(N)\{\pm E_2\} \), for \( A \in SL_2(\mathbb{Z}) \) such that \( \Lambda_k \cdot A = \Lambda_k \). Let \( A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \) such that \( \Lambda_k \cdot A = \Lambda_k \). Since the order of \( q \)-expansion of \( \Lambda_k \) is 0 and that of \( \Lambda_k \cdot A \) is \( \min(\{kc\}, \{c\}) \) - \( \min(\{2c\}, \{c\}) \) by Proposition 2.4, we have

\[
\min(\{kc\}, \{c\}) = \min(\{2c\}, \{c\}).
\]  

(2)

By considering power series modulo \( q^N \), thus modulo \( q^N \mathbb{Q}(\zeta)[[q]] \), from Proposition 3.1 we obtain

\[
\theta_{2,1}(E_2)(\phi_k - \phi_1)[A]_2 \equiv \theta_{k,1}(E_2)(\phi_2 - \phi_1)[A]_2 \pmod{q^N} \tag{3}
\]

For an integer \( i \), put \( u_i = \zeta^{\mu(i)c}d, \omega_i = \zeta^{\mu(i)c-\mu(c)d} \). First of all, we shall prove that \( c \equiv 0 \pmod{N} \). Let us assume \( c \neq 0 \pmod{N} \). Suppose that \( \{2c\} = \{c\} \). Since \( \{c\} \neq 0 \), we see \( \{c\} = N/3 \). Further since by \( \{kc\} \geq \{c\} \), we have \( (k,3) = 1, \{c\} = \{2c\} = \{kc\} = N/3 \) and \( u_k = \omega_k u_1, u_2 = \omega_2 u_1 \). Lemma 2.1 gives that \( \omega_k, \omega_2 \neq 1, \omega_k \neq \omega_2 \). By (3) and Proposition 2.3

\[
\theta_{2,1}(E_2) \left( \sum_n n(u_k^n - u_1^n) + u_k^{-1}q^N - u_1^{-1}q^N \right) \equiv \theta_{k,1}(E_2) \left( \sum_n n(u_2^n - u_1^n) + u_2^{-1}q^N - u_1^{-1}q^N \right) \pmod{q^N}.
\]

Therefore

\[
\theta_{2,1}(E_2) \left( \sum_n n(\omega_k^n - 1)u_1^n + (\omega_k^{-1} - 1)u_1^{-1}q^N \right) \equiv \theta_{k,1}(E_2) \left( \sum_n n(\omega_2^n - 1)u_1^n + (\omega_2^{-1} - 1)u_1^{-1}q^N \right) \pmod{q^N}.
\]
Since \( q^N = \zeta^{-3\mu(c)d}u_1^2 \),

\[ \theta_{2,1}(E_2)((\omega_k - 1)u_1 + (2(\omega_k^2 - 1) + \zeta^{-3\mu(c)d}(\omega_k^{-1} - 1)u_1^2) \equiv \theta_{k,1}(E_2)((\omega_k - 1)u_1 + (2(\omega_k^2 - 1) + \zeta^{-3\mu(c)d}(\omega_k^{-1} - 1)u_1^2) \mod u_1^3. \]

By comparing the coefficients of \( u_1, u_1^2 \) on both sides, we have

\[ 2(\omega_k + 1) - \omega_k^{-1}\zeta^{-3\mu(c)d} = 2(\omega_k + 1) - \omega_k^{-1}\zeta^{-3\mu(c)d}. \]

This equation implies that \( \zeta^{3\mu(c)d}\omega_k = -1/2 \). We have a contradiction.

Suppose \( \{2c\} > \{c\} \). Then by [2], we know \( \{kc\} \geq \{c\} \). If \( \{kc\} > \{c\} \), then the \( q \)-expansion of \( \Lambda \circ A \) begins with 1. Thus \( \theta_{k,1}(E_2) = \theta_{2,1}(E_2) \). This gives that \( (1 - \zeta^{k+2})(1 - \zeta^{k-2}) = 0 \). We have a contradiction. If \( \{kc\} = \{c\} \), then \( \{kc\}, \{c\} \neq 0, N/2 \) and \( u_k = \omega_ku_1 \). By considering \( \mod q^N \) as above, we obtain

\[ \theta_{2,1}(E_2) \left( \sum_n n(\omega_k^n - 1)u_1^n + (\omega_k^{-1} - 1)u_1^{-1}q^N \right) \equiv \theta_{k,1}(E_2) \left( \sum_n n(u_2^n - u_1^n) + u_2^{-1}q^N - u_1^{-1}q^N \right) \mod q^N. \]

Thus

\[ u_1 + 2(\omega_k + 1)u_1^2 - \omega_k^{-1}u_1^{-1}q^N \equiv u_1 - u_2 + 2u_1^2 - u_2^{-1}q^N + u_1^{-1}q^N - 2u_2^2 + \cdots \mod q^N. \]

Therefore

\[ 2\omega_ku_1^2 - (\omega_k^{-1} + 1)u_1^{-1}q^N + h_1(u_1) \equiv -u_2 - u_2^{-1}q^N - 2u_2 + h_2(u_2) \mod q^N, \]

where \( h_i(u_i) \) is a polynomial of \( u_i \) with terms \( u_i^n, n > 2 \). Since \( \{2c\} > \{c\} \), we see \( \{2c\} \leq N - \{2c\} < N - \{c\} \). Therefore we have \( \{2c\} < N - \{c\} \) and \( 2\{c\} = \{2c\} = N - \{2c\} \) or \( 2\{c\} = \{2c\} < N - \{2c\} \). By comparing the coefficients of first terms, we obtain \( 2\omega_k\zeta^{2\mu(c)d} = -\zeta^{\mu(2c)2d} + \zeta^{-\mu(2c)2d} \) in the case \( \{2c\} = N - \{2c\} \) and \( 2\omega_k\zeta^{2\mu(c)d} = -\zeta^{\mu(2c)2d} \) in the case \( \{2c\} < N - \{2c\} \).

In the former case, \( N \) is even and \( \{2c\} = N/2 \). So we have \( \mu(2c)2c \equiv 0 \mod N/2 \) and \( \mu(2c)2d \equiv 0 \mod N/2 \). Therefore from \( (c, d) = 1 \) we obtain \( 2 \equiv 0 \mod N/2 \). This is impossible. In the latter case, clearly we have a
contradiction. Suppose \( \{2c\} < \{c\} \). Then \( \{kc\} = \{2c\} \). If \( \{2c\} = 0 \), then \( k, N \) are even and \( \{c\} = N/2 \). From Proposition 2.3 we get

\[
(\phi_k - \phi_1)[A]_2 = \frac{\zeta^{kd}}{(1 - \zeta^{kd})^2} - (\zeta^{d} + \zeta^{-d})q^{N/2} \mod q^N,
\]

\[
(\phi_2 - \phi_1)[A]_2 = \frac{\zeta^{2d}}{(1 - \zeta^{2d})^2} - (\zeta^{d} + \zeta^{-d})q^{N/2} \mod q^N.
\]

By using (3),

\[
\theta_{2,1}(E_2)\frac{\zeta^{kd}}{(1 - \zeta^{kd})^2} = \theta_{k,1}(E_2)\frac{\zeta^{2d}}{(1 - \zeta^{2d})^2},
\]

\[
\theta_{2,1}(E_2)(\zeta^{d} + \zeta^{-d}) = \theta_{k,1}(E_2)(\zeta^{d} + \zeta^{-d}).
\]

If \( \zeta^{d} + \zeta^{-d} = 0 \), then \( 2d \equiv 0 \mod N/2 \). Since \( 2c \equiv 0 \mod N/2 \) and \( (c, d) = 1 \), we see \( 2 \equiv 0 \mod N/2 \). This is impossible. Therefore \( \theta_{2,1}(E_2) = \theta_{k,1}(E_2) \) and \( \frac{\zeta^{kd}}{(1 - \zeta^{kd})^2} = \frac{\zeta^{2d}}{(1 - \zeta^{2d})^2} \). This implies that \((1 - \zeta^{(k+2)d})(1 - \zeta^{(k-2)d}) = 0\). Lemma 2.4 gives a contradiction. Hence \( \{2c\}, \{c\} \neq 0, N/2 \). Let \( u_k = \omega u_2 \), where \( \omega = \omega_k/\omega_2 \). By (3),

\[
\theta_{2,1}(E_2)(\sum_n n(\omega^n u_2^n - u_1^n) + \omega^{-1}u_2^{-1}q^N - u_1^{-1}q^N) \equiv \theta_{k,1}(E_2)(\sum_n n(u_2^n - u_1^n) + u_2^{-1}q^N - u_1^{-1}q^N) \mod q^N.
\]

Therefore \( \theta_{2,1}(E_2)\omega = \theta_{k,1}(E_2) \) and

\[
\sum_n n(\omega^n - \omega)u_2^n + (\omega^{-1} - \omega)u_2^{-1}q^N \equiv \sum_n n(1 - \omega)u_1^n + (1 - \omega)u_1^{-1}q^N \mod q^N.
\]

Since by Lemma 2.4, \( \omega \neq 1 \), we have

\[
2\omega u_2^2 - (1 + \omega^{-1})u_2^{-1}q^N + h_2(u_2) \equiv -u_1 - u_1^{-1}q^N - 2u_1^2 + h_1(u_1) \mod q^N,
\]

where \( h_i(u_i) \) is a polynomial of \( u_i \) with terms \( u_i^n, n > 2 \). Since \( \{c\} < N - \{c\} < N - \{2c\} \), we have \( 2\{2c\} = \{c\} \) and \( 2\omega \zeta^{2\mu(2c)2d} = -\zeta^{\mu(c)c} \). This gives a contradiction. Hence we have \( c \equiv 0 \mod N \). Let \( c \equiv 0 \mod N \). Then
by the definition of $\phi_s$, we have $\Lambda_k \circ A = \frac{\phi_{kd} - \phi_{d}}{\phi_{2kd} - \phi_{2d}}$. From now on, to save labor, we put $r = \{2d\}$, $s = \{kd\}$, $t = \{d\}$. Then since $r, s, t$ are distinct from each other and $\min(s, t) = \min(r, t)$, $(d, N) = 1$, we have $r, s, t \neq 0, N/2$ and $t < r, s$. We have only to prove $t = 1$. Let us assume $t > 1$. Let $T = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$.

Then

$$\Lambda_k \circ T = \left(\frac{\phi_s - \phi_t}{\phi_r - \phi_t}\right) \circ T. \quad (4)$$

If $\ell$ is an integer such that $0 < \ell < N/2$, then $\mu(\ell) = 1$, $\ell = \ell$. Let $u = \zeta q$. Then

$$\phi_\ell[T]_2 \equiv \sum_n nu^{\ell n} + u^{N-\ell} \mod q^N. \quad (5)$$

From (4),

$$(\phi_r\phi_1 + \phi_s\phi_2 + \phi_t\phi_k)[T]_2 = (\phi_t\phi_2 + \phi_s\phi_1 + \phi_r\phi_k)[T]_2.$$  

By comparing the order of $q$-series in the both sides, we see $r = t + 1 < s$. Since $t \geq 2$ and $t + 2 \leq s < N/2$, we know that $2t \geq t + 2, N > 2t + 4$. By (5) and by the inequality relations that $r = t + 1, s \geq t + 2, 2t \geq t + 2, N > 2t + 4$, we have modulo $u^{t+4},$

$$\phi_r\phi_1[T]_2 \equiv u^{t+2} + 2u^{t+3} \mod u^{t+4}, \phi_s\phi_2[T]_2 \equiv 0 \mod u^{t+4},$$

$$\phi_t\phi_1[T]_2 \equiv u^{t+k} \mod u^{t+4}, \phi_t\phi_2[T]_2 \equiv u^{t+2} \mod u^{t+4},$$

$$\phi_s\phi_1[T]_2 \equiv u^{s+1} \mod u^{t+4}, \phi_r\phi_k[T]_2 \equiv 0 \mod u^{t+4}.$$  

Therefore we obtain a congruence:

$$2u^{t+3} + u^{t+k} \equiv u^{s+1} \mod u^{t+4}.$$  

The coefficients of $u^{t+3}$ on both sides are distinct from each other, we have a contradiction. Hence $t = 1$. $\square$

We obtain the following theorem from the Gee-Stevenhagen theory in [2] and [3]. See also Chapter 6 of [7].

**Theorem 4.2.** Let $N$ and $k$ be as above. Let $\alpha \in \mathcal{S}$ such that $\mathbb{Z}[\alpha]$ is the maximal order of an imaginary quadratic field $K$. Then the ray class field of $K$ is generated by $\Lambda_l(\alpha)$ over $\mathbb{Q}(\zeta, j(\alpha))$.

**Proof.** The assertion is deduced from Theorems 1 and 2 of [2] and Theorem 4.1. $\square$
References

[1] D.Cox, Primes of the form $x^2 + ny^2$, A Wiley-Interscience Publication, John Wiley and Sons, Inc., New York, 1989.

[2] A.Gee, “Class invariants by Shimura’s reciprocity law,” J. Théor. Nombres Bordeaux 11 (1999), 45-72.

[3] A.Gee and P.Stevenhagen, “Generating class fields using Shimura reciprocity,” Algorithmic number theory, Springer LNCS 1423, 1998, pp. 441-453.

[4] N.Ishida and N.Ishii, “Generators and defining equation of the modular function field of the group $\Gamma_1(N)$,” Acta Arith. 101.4 (2002), 303-320.

[5] N.Ishii and M.Kobayashi, “Singular values of some modular functions”, Ramanujan J. 24 (2011), 67-83, DOI 10.1007/s11139-010-9249-y.

[6] S.Lang, Elliptic Functions, Adison-Wesley, London, 1973.

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

Faculty of Liberal Arts and Sciences
Osaka Prefecture University
1-1 Gakuen-cho, Naka-ku Sakai
Osaka, 599-8531 Japan

e-mail: ishii@las.osakafu-u.ac.jp