Special values of generalized $\lambda$ functions at imaginary quadratic points

November 1, 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

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

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 [1, 5], we defined a modular function $W_a(\tau)$ with respect to $\Gamma_1(N)$ by

$$W_a(\tau) = \frac{\wp(a_1/N; \tau) - \wp(a_3/N; \tau)}{\wp(a_2/N; \tau) - \wp(a_3/N; \tau)}.$$ \hspace{1cm} (1)

This function is one of generalized $\lambda$ functions defined by S.Lang in Chapter 18, §6 of [6]. He describes that it is interesting to investigate special values of generalized $\lambda$ functions at imaginary quadratic points and to see if they generate the ray class fields. Here a point of $\mathcal{H}$ is called an imaginary

*2000 Mathematics Subject Classification 11F03, 11G15*
quadratic point if it generates an imaginary quadratic field over $\mathbb{Q}$. Let $j$ be
the modular invariant function. In Theorem 3.6 of [5], we showed that $W_a$ is
integral over $\mathbb{Z}[j]$ under a condition that $a_1a_2a_3(a_1 \pm a_3)(a_2 \pm a_3)$ is prime to
$N$. From this we obtained that values of $W_a$ at imaginary quadratic points
are algebraic integers. Further, 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 $\mathbb{C}(j)$. In this article, we
study the functions $W_a$ in the particular case: $a_3 = 1$. To simplify the no-
tation, henceforth we denote by $\Lambda_{k,\ell}$ the function $W_{[k,\ell,1]}$. We prove that for
integers $k, \ell$ such that $1 < \ell \neq k < N/2$, the function $\Lambda_{k,\ell}$ generates $A_1(N)$
over $\mathbb{C}(j)$. 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 value $\Lambda_{k,\ell}(\alpha)$
and $e^{2\pi i/N}$ generate the ray class field of $K$ modulo $N$ over the Hilbert class
field $K((j(\alpha)))$ of $K$. On the assumption $k(\ell \pm 1)$ is prime to $N$, we prove
that $\Lambda_{k,\ell}$ is integral over $\mathbb{Z}[j]$. Further in the case $\ell = 2$, we can weaken the
assumption. Let $\delta = (k, N)$ be the greatest common divisor of $k$ and $N$. If
we assume either (i) $\delta = 1$ or (ii) $\delta < 1, (\delta, 3) = 1$ and $N/\delta$ is not a power of
a prime number, then $\Lambda_{k,2}$ is integral over $\mathbb{Z}[j]$. In particular the values of
$\Lambda_{k,\ell}$ at imaginary quadratic points are algebraic integers. Our results can be
extended easily to the functions $W_a$ in the case that $a_3$ is prime to $N$. See
Corollaries 3.2, 4.7. Throughout this article, we use the following notation:

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

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

The greatest common divisor of $a, b \in \mathbb{Z}$ is denoted by $(a, b)$. For an integral
domain $R$, $R((q))$ represents the power series ring of a variable $q$ over $R$ and
$R[[q]]$ is a subring of $R((q))$ of power series of non-negative order.

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 determined
by the following conditions:

\[ 0 \leq \{x\} \leq \frac{N}{2}, \quad \mu(x) = \pm 1, \]
\[ \begin{cases} \mu(x) = 1 & \text{if } x \equiv 0, N/2 \pmod{N}, \\ x \equiv \mu(x)\{x\} \pmod{N} & \text{otherwise.} \end{cases} \]

For an integer \( s \) not congruent to 0 mod \( N \), let

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

Obviously we have \( W_a = (\phi_{a_1} - \phi_{a_3})/(\phi_{a_2} - \phi_{a_3}) \). Let \( A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \).

Put \( s^* = \mu(sc)sd, u_s = \zeta^{s^*}q^{\{sc\}} \). Then by Lemma 1 of [4], we have

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

(2)

Therefore, \( \phi_s[A]_2 \in \mathbb{Q}(\zeta)[[q]] \) and its order is \( \{sc\} \). If \( c \equiv 0 \pmod{N} \), then by [2] or the transformation formula of \( \varphi((r\tau + s)/N; L_\tau) \) in §2 of [4], we have

\[ \phi_s[A]_2 = \phi_{\{sd\}}. \]

(3)

The next lemmas and propositions are required 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 \( r^* = \mu(rc)rd, s^* = \mu(sc)sd \). 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 \( \mu(rc)r - \mu(sc)s \equiv 0 \pmod{N} \). This is impossible, because of \( 0 < r \neq s \leq N/2 \). Suppose \( \{rc\} = \{sc\} = 0, N/2 \) and \( \zeta^{r^*+s^*} = 1 \). Then we have \((r + s)c \equiv 0 \pmod{N}, \ (r + s)d \equiv 0 \pmod{N} \). Therefore \( r + s \equiv 0 \pmod{N} \). This is also impossible. \( \square \)

**Lemma 2.2.** Let \( k \in \mathbb{Z} \). Put \( \delta = (k, N) \).
(i)  For $\ell \in \mathbb{Z}$, if $\ell$ is divisible by $\delta$, 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 $\ell$ is divisible by $\delta$, then there exist an integer $m$ such that $\ell \equiv mk \mod N$. Therefore $\zeta^\ell = \zeta^{mk}$ and $(1 - \zeta^\ell)$ is divisible by $(1 - \zeta^k)$. This shows (i). Let $p_i (i = 1, 2)$ be distinct prime factors of $N/\delta$. Since $N/p_i = \delta(N/(\delta p_i))$, $1 - \zeta^{N/p_i}$ is divisible by $1 - \zeta^\delta$. Therefore $p_i (i = 1, 2)$ are divisible by $1 - \zeta^\delta$. This implies that $1 - \zeta^\delta$ is a unit. Because of $(k/\delta, N/\delta) = 1$, $1 - \zeta^k$ is also a unit. \hfill \Box

From (2) and Lemma 2.1 we immediately obtain the following 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

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

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

$$(\phi_r - \phi_s)[A]_2 \equiv \frac{-\zeta^d(1 - \zeta^{(r-s)d})(1 - \zeta^{(r+s)d})}{(1 - \zeta^d)^2(1 - \zeta^sd)^2} \mod q^N \mathbb{Z}[\zeta][[q]],$$

**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 $\mathbb{Q}(\zeta)$ defined 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 \( \{rc\} < \{sc\} \),

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

## 3 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 \( \mathfrak{f}_{Q(\zeta)} \) a subfield of \( \mathfrak{f} \) consisted of all modular functions having Fourier coefficients in \( Q(\zeta) \).

**Theorem 3.1.** Let \( k, \ell \) be integers such that \( 1 < \ell < k < N/2 \). Then we have \( A_1(N)_{Q(\zeta)} = Q(\zeta)(\Lambda_{k,\ell}, j) \)

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

\[
\min(\{kc\}, \{c\}) = \min(\{\ell c\}, \{c\}). \tag{4}
\]

From Propositions 2.3 and 2.4 by considering power series modulo \( q^N \), thus modulo \( q^N Q(\zeta)[[q]] \), we obtain

\[
\theta_{\ell}(\phi_k - \phi_1)[A]_2 \equiv \theta_k(\phi_{\ell} - \phi_1)[A]_2 \mod q^N,
\]

where \( \theta_{\ell} = \theta_{\ell,1}(E_2), \theta_k = \theta_{k,1}(E_2) \). Thus

\[
(\theta_{\ell}\phi_k - \theta_k\phi_\ell)[A]_2 \equiv (\theta_{\ell} - \theta_k)\phi_1[A]_2 \mod q^N. \tag{5}
\]

If \( \theta_{\ell} = \theta_k \), then we have \( (1 - \zeta^{k+\ell})(1 - \zeta^{k-\ell}) = 0 \). Therefore we have \( \theta_{\ell} \neq \theta_k \). For an integer \( i \), put \( u_i = \zeta^{(\mu(i)c)d}q^{(i)c}, \omega_i = \zeta^{(\mu(i)c) - (\mu(i)c)d} \). We shall show that \( c \equiv 0 \mod N \). Let us assume \( c \not\equiv 0 \mod N \). Then first of all we shall prove \( \{\ell c\} = \{kc\} = \{c\} \) by contradiction. Since we can interchange the roles of \( \ell, k \), we have only to consider the case \( \{\ell c\} \neq \{c\} \).
(i) Suppose that \( \{\ell c\} < \{c\} \). Then \( \{kc\} = \{\ell c\}, u_k = \omega u_\ell \ (\omega = \omega_k / \omega_\ell) \). We note \( \omega \neq 1 \) by Lemma 2.1. Since order of the power series on the right hand side of \((5)\) is \( \{c\} \neq 0 \), we see \( \{\ell c\} \neq 0 \), because if \( \{\ell c\} = 0 \), then order of the series on the left hand side is a multiple of \( N \). Further the coefficient \( \theta_\ell \omega - \theta_k \) of \( u_\ell \) of the series on the left hand side should be 0. Thus from Proposition 2.3 and \((5)\), we obtain

\[
(\phi_k - \omega \phi_\ell)[A]_2 \equiv (1 - \omega) \phi_1[A]_2 \mod q^N.
\]

This gives

\[
\sum_{n \geq 2} n\omega(\omega^{n-1} - 1)u_n^\ell - \omega^-(n + 1)u_n^\ell q^N \equiv - \sum_{n \geq 1} nu_1^n - u_1^{-1}q^N \mod q^N.
\]

Since \( \{c\} \leq N - \{c\} < N - \{\ell c\} \), we have \( 2\{\ell c\} = \{c\} \). If \( \{c\} = N/2 \), then \( \{\ell c\} = 0, N/2 \) according to the parity of \( \ell \). Therefore we know \( \{\ell c\} \neq N/2 \) and by comparing the coefficients of \( q^{\ell c} \) on both sides, we have \( 2\omega \xi^{2\mu(\ell c)\ell d} = -\zeta^{\mu(c)c} \). This gives a contradiction.

(ii) Suppose that \( \{\ell c\} > \{c\} \). The congruence \((5)\) implies \( \{kc\} = \{c\} \) and

\[
\theta_k \phi_\ell[A]_2 \equiv (\theta_k \phi_\ell - (\theta_k - \theta_k) \phi_1)[A]_2 \mod q^N.
\]

Since \( \{c\} \neq 0, N/2 \) and \( u_k = \omega_k u_1 \), we have \( \theta_k = (1 - \omega_k) \theta_\ell \) and, noting \( \omega_k \neq 1 \),

\[
\sum_{n \geq 1} nu_n^\ell + u_1 q^N \equiv \sum_{n \geq 2} n \left(1 - \frac{\omega_n^{n-1}}{\omega_k - 1}\right) u_1^n + (\omega_k^{-1} + 1)u_1^{-1}q^N \mod q^N.
\]

Since \( N - \{c\} > N - \{\ell c\} \), we have \( 2\{c\} = \{\ell c\} \). By comparing the coefficients of first terms on both sides, we obtain \( 2\omega_k \xi^{2\mu(c)d} = -\zeta^{\ell d}+\xi^{-\ell d} \) in the case \( \{\ell c\} = N/2 \) and \( 2\omega_k \xi^{2\mu(c)d} = -\zeta^{\ell d} \) in the case \( \{\ell c\} \neq N/2 \). In the former case, we have \( |\cos 2\pi \ell d / N| = 1 \). Therefore \( \ell c \equiv 0 \mod N/2 \) and \( \ell d \equiv 0 \mod N/2 \). Since \( (c,d) = 1 \), we know \( \ell \equiv 0 \mod N/2 \). This is impossible. In the latter case, clearly we have a contradiction. Therefore we have \( \{\ell c\} = \{kc\} = \{c\} \). Assume that \( \{\ell c\} = \{kc\} = \{c\} \). Then \( u_\ell = \omega_k u_1, u_\ell = \omega_k u_1 \). By congruence \((5)\), by comparing the coefficients of \( u_1 \) on both sides, we have \( \theta_\ell (\omega_k - 1) = \theta_k (\omega_\ell - 1) \). Since \( \omega_k, \omega_\ell, \omega_k / \omega_\ell \neq 1 \), from \((5)\), we obtain

\[
2u_1^2 + (\omega_k \omega_\ell)^{-1} u_1^{-1} q^N \equiv 0 \mod u_1^3.
\]
This gives a contradiction. Hence we have $c \equiv 0 \mod N$. Hereafter we assume that $k > \ell$, if necessary by considering $1/\Lambda_{k,\ell} = \Lambda_{\ell,k}$ instead of $\Lambda_{k,\ell}$.

Let $c \equiv 0 \mod N$. Then $(d, N) = 1$. By (3), we have $\Lambda_{k,\ell} \circ A = \frac{\phi_{kd} - \phi_{d}}{\phi_{kd} - \phi_{d}}$.

From now on, to save labor, we put $r = \{\ell d\}, s = \{kd\}, t = \{d\}$. Since $r, s, t$ are distinct from each other and $\min(s, t) = \min(r, t)$, 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

$$\Lambda_{k,\ell} \circ T = \Lambda_{k,\ell} \circ AT = \left( \frac{\phi_{s} - \phi_{t}}{\phi_{r} - \phi_{t}} \right) \circ T.$$  

(6)

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

$$\phi_{i}[T]_2 \equiv \sum_{n} nu^{in} + u^{N-i} \mod qN.$$  

(7)

From (6),

$$(\phi_{r}\phi_{s} + \phi_{s}\phi_{\ell} + \phi_{t}\phi_{k})[T]_2 = (\phi_{t}\phi_{\ell} + \phi_{s}\phi_{1} + \phi_{r}\phi_{k})[T]_2.$$  

Since $s + \ell, t + k, r + k > t + \ell$ and order of $\phi_{i}[T]_2$ is $i$, we have

$$\phi_{r}\phi_{1}[T]_2 - \phi_{s}\phi_{1}[T]_2 \equiv \phi_{t}\phi_{1}[T]_2 \mod u^{t+\ell+1}.$$  

If $s < r$, then $s + 1 = t + \ell$. However in this case the coefficients of $u^{t+\ell}$ on both sides are distinct. Therefore $r < s$, $r + 1 = t + \ell$. Since $t + \ell \leq s < N/2$, we know that $N > 2t + 2\ell$. By (7) and by the inequality relations that $t \geq 2$, $k > \ell, r = t + \ell - 1, s \geq t + \ell, N > 2t + 2\ell$, we have modulo $u^{t+\ell+2}$,

$$\begin{align*}
(\phi_{r}\phi_{1})[T]_2 &\equiv u^{t+\ell} + 2u^{t+\ell+1} \mod u^{t+\ell+2}, 
(\phi_{s}\phi_{1})[T]_2 \equiv 0 \mod u^{t+\ell+2}, \\
(\phi_{t}\phi_{k})[T]_2 &\equiv u^{t+k} \mod u^{t+\ell+2}, 
(\phi_{t}\phi_{\ell})[T]_2 \equiv u^{t+\ell} \mod u^{t+\ell+2}, \\
(\phi_{s}\phi_{1})[T]_2 &\equiv u^{s+1} \mod u^{t+\ell+2}, 
(\phi_{r}\phi_{k})[T]_2 \equiv 0 \mod u^{t+\ell+2}.
\end{align*}$$

Therefore we obtain a congruence:

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

The coefficients of $u^{t+\ell+1}$ on both sides cannot be equal. Hence we have a contradiction.  

\[\square\]
Corollary 3.2. Let $W_a$ be the function defined by (1). If $a_1, a_2 \neq N/2$ and $(a_3, N) = 1$, then $A_1(N)Q(\zeta) = Q(\zeta)(W_a, j)$

Proof. Let $M \in \text{SL}_2(\mathbb{Z})$ such that $M \equiv \begin{pmatrix} a_3^{-1} & 0 \\ 0 & a_3 \end{pmatrix}$ mod $N$. By (3), we know that $W_a = \Lambda_{k,\ell} \circ M$, where $k, \ell \in \mathbb{Z}$ such that $a_1 = \{ka_3\}, a_2 = \{\ell k\}$ and $1 < \ell \neq k < N/2$. Let $A \in \text{SL}_2(\mathbb{Z})$. If $W_a \circ A = W_a$, then $A_{k,\ell} \circ (MAM^{-1}) = A_{k,\ell}$. Therefore we have $MAM^{-1} \in \Gamma_1(N)\{\pm E_2\}$. Since $M$ is a normalizer of $\Gamma_1(N), A \in \Gamma_1(N)\{\pm E_2\}$. This shows our assertion. □

4 Values of $\Lambda_{k,\ell}$ at imaginary quadratic points

In this section, we shall study values of $\Lambda_{k,\ell}$ at imaginary quadratic points.

Proposition 4.1. Let $k, \ell$ be integers such that $1 < \ell \neq k \leq N/2$. Assume $(k(\ell \pm 1), N) = 1$. Then for $A \in \text{SL}_2(\mathbb{Z})$, we have $\Lambda_{k,\ell} \circ A \in \mathbb{Z}[\zeta]((q))$.

Proof. Put $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Proposition 2.4 shows $\Lambda_{k,\ell} \circ A = \omega f(q)$, where $\omega = \theta_{k,1}(A)/\theta_{\ell,1}(A)$ 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 $\{c\} \neq 0$. By the assumption, we know $\{\ell c\} \neq \{c\}$. Proposition 2.4 implies that $\theta_{k,1}(A)^{-1} \in \mathbb{Z}[\zeta]$. Since $(k, N) = 1, \{kc\} \neq 0$. Thus $\theta_{k,1}(A) \in \mathbb{Z}[\zeta]$. Hence we have $\omega \in \mathbb{Z}[\zeta]$. Next consider the case $\{c\} = 0$. Then we have $\{c\} = \{\ell c\} = \{kc\} = 0, \mu(c) = \mu(\ell c) = \mu(kc) = 1$, $(d, N) = 1$ and

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

Using the assumption, Lemma 2.2 (i) shows

$$\frac{1 - \zeta^{\ell d}}{1 - \zeta^{kd}}, \frac{1 - \zeta^{(k-1)d}}{1 - \zeta^{(\ell-1)d}}, \frac{1 - \zeta^{(k+1)d}}{1 - \zeta^{(\ell+1)d}} \in \mathbb{Z}[\zeta].$$

Hence we obtain $\omega \in \mathbb{Z}[\zeta]$. □
Proposition 4.2. Let $k$ be an integer such that $2 < k < N/2$. 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

$$
\Lambda_{k,2} \circ A \in \mathbb{Z}[\zeta((q))].
$$

Proof. Similarly in the proof of Proposition 4.1, we have only to prove $\omega = \theta_{k,1}(A)/\theta_{2,1}(A) \in \mathbb{Z}[\zeta]$. First we consider the case $\{c\} \neq 0$. Let $\{2c\} \neq \{c\}$. By (ii) of Proposition 2.4, we see $\theta_{k,1}(A)^{-1} \in \mathbb{Z}[\zeta]$. Further if $\{kc\} \neq 0$, then $\theta_{k,1}(A) \in \mathbb{Z}[\zeta]$. If $\{kc\} = 0$, 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 $\theta_{k,1}(A) \in \mathbb{Z}[\zeta]$. Hence we have $\omega \in \mathbb{Z}[\zeta]$. Let $\{2c\} = \{c\}$. Then, since $\{c\} \neq 0$, we have $N \equiv 0 \mod 3$, $(k, 3) = 1$ and $\{c\} = \{2c\} = \{kc\} = N/3$, $\mu(2c) = -\mu(c)$, $\mu(kc) = (\frac{k}{3})\mu(c)$, where $(\frac{k}{3})$ 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 $\{c\} = 0$. Then we have $\{c\} = \{2c\} = \{kc\} = 0$, $\mu(c) = \mu(2c) = \mu(kc) = 1$, $(d, N) = 1$ and

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

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 $N \not\equiv 0 \mod 3$, then since $(3d, N) = 1$, we know

$$
\frac{(1-\zeta^{(k-1)d})(1-\zeta^{(k+1)d})}{(1-\zeta^{3d})(1-\zeta^{kd})} \in \mathbb{Z}[\zeta].
$$

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

$$
\frac{(1-\zeta^{(k-1)d})(1-\zeta^{(k+1)d})}{(1-\zeta^{3d})(1-\zeta^{kd})} \in \mathbb{Z}[\zeta].
$$

Hence we obtain $\omega \in \mathbb{Z}[\zeta]$. 

To study the modular equation of $\Lambda_{k,\ell}$ over $\mathbb{C}(j)$, we construct a transversal $R$ of the coset decomposition of $\text{SL}_2(\mathbb{Z})$ by $\Gamma_1(N)\{\pm E_2\}$, where $E_2$ is the unit matrix. For $\nu \in (\mathbb{Z}/N\mathbb{Z})^\times/\{\pm 1\}$, take $M_\nu \in \text{SL}_2(\mathbb{Z})$ so that $M_\nu \equiv \begin{pmatrix} v^{-1} & 0 \\ 0 & 0 \end{pmatrix} \mod N$. For a positive divisor $t$ of $N$, let $\Theta_t$ be a set of
\( \phi((t, N/t)) \) integers \( u \) such that \( u \) is prime to \( t \) and runs over a transversal of the factor group \((\mathbb{Z}/(t, N/t)\mathbb{Z})^\times\). For an integer \( u \) prime to \( t \) and an integer \( k \) with the property \( ku \equiv 1 \pmod{t} \), consider a matrix in \( \text{SL}_2(\mathbb{Z}) \)

\[
B(t, u, k) = \begin{pmatrix} u & (uk - 1)/t \\ t & k \end{pmatrix}.
\]

We denote by \( \mathfrak{M}_t \) the set of matrices

\[
\{B(t, u, k) \mid u \in \Theta_t, \ k \mod N/t, uk \equiv 1 \mod t\}.
\]

Lemma 3.1 in [5] shows a set of matrices

\[
R = \{M_v B \mid v \in (\mathbb{Z}/N\mathbb{Z})^\times/\{\pm 1\}, B \in \bigcup_{t \mid N} \mathfrak{M}_t \}
\]

is a transversal of the coset decomposition of \( \text{SL}_2(\mathbb{Z}) \) by \( \Gamma_1(N)\{\pm E_2\} \). For an integer \( h \) prime to \( N \), let \( h^* \) be an integer such that \( hh^* \equiv 1 \mod N \). Put, for the set \( \Theta_t \),

\[
\Theta_t = \{h^* u \mid u \in \Theta_t\}.
\]

Then obviously a set of matrices

\[
\{M_v B \mid v \in (\mathbb{Z}/N\mathbb{Z})^\times/\{\pm 1\}, B \in \bigcup_{t \mid N} \mathfrak{M}_{h\Theta_t} \}
\]

is also a transversal of the coset decomposition. For details, see §3 of [5].

Let \( \sigma_h \) be the automorphism of \( \mathbb{Q}(\zeta) \) defined by \( \zeta^{\sigma_h} = \zeta^h \). On a power series \( f = \sum m a_m q^m \) with \( a_m \in \mathbb{Q}(\zeta) \), \( \sigma_h \) acts by \( f^{\sigma_h} = \sum m a_m^h q^m \). From Lemma 3.2 of [5], we obtain

\[
(\Lambda_{k,\ell} \circ M_v B(t, u, k))^{\sigma_h} = \Lambda_{k,\ell} \circ M_v B(t, h^* u, hk).
\]  \( (8) \)

**Remark 4.3.** We do not need to separate the case \( \{st\} = 0 \) from the case \( \{st\} \neq 0 \) in Lemma 3.2 of [5]. Therefore we can omit the assumption \( a_1 a_2 a_3 \) is prime to \( N \) in Proposition 3.4,[5].

**Theorem 4.4.** Let the assumption be the same as in Proposition 4.1. Further in the case \( \ell = 2 \), let the assumption be the same as in Proposition 4.2. Then \( \Lambda_{k,\ell} \) is integral over \( \mathbb{Z}[j] \).

**Proof.** Let \( R \) be the above set. Consider a modular equation \( \Phi(X, j) = \prod_{A \in R} (X - \Lambda_{k,\ell} \circ A) \). Since \( \Lambda_{k,\ell} \circ A \) has no poles in \( \hat{\mathbb{H}} \) and \( \Lambda_{k,\ell} \circ A \in \mathbb{Z}[[\zeta]]((q)) \) by Propositions 4.1 and 4.2, the coefficients of \( \Phi(X, j) \) are polynomials of \( j \) with coefficients in \( \mathbb{Z}[[\zeta]] \). By \( (8) \), for every automorphism \( \sigma \) of \( \mathbb{Q}(\zeta) \), the correspondence: \( \Lambda_{k,\ell} \circ A \rightarrow (\Lambda_{k,\ell} \circ A)^\sigma \) induces a permutation on the set \( \{\Lambda_{k,\ell} \circ A \mid A \in R\} \). Therefore \( \Phi(X, j) \in \mathbb{Z}[j] \). \( \square \)
Theorem 4.5. Let the assumption be the same as in Theorem 4.4. Let \( \alpha \) be an imaginary quadratic point. Then \( \Lambda_{k,\ell}(\alpha) \) is an algebraic integer.

Proof. Since \( j(\alpha) \) is an algebraic integer (see [1], Theorem 10.23) and \( \Lambda_{k,\ell}(\alpha) \) is integral over \( \mathbb{Z}[j(\alpha)] \), \( \Lambda_{k,\ell}(\alpha) \) is an algebraic integer. \( \square \)

Corollary 4.6. Let \( A \in \text{SL}_2(\mathbb{Z}) \). Let the assumption be the same as in Theorem 4.4. Then the values of the function \( \Lambda_{k,\ell} \circ A \) at imaginary quadratic points are algebraic integers. In particular, the function

\[
\frac{\wp(k\tau/N; \tau) - \wp(\tau/N; \tau)}{\wp(\ell\tau/N; \tau) - \wp(\tau/N; \tau)}
\]

takes algebraic, integral values at imaginary quadratic points.

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 \( \wp((r\tau+s)/N; L_{\tau}) \) in \( \S 2 \) of [4], we obtain the latter part. \( \square \)

Corollary 4.7. Let \( W_a \) be the function defined by (1). If \( a_1a_3(a_2 \pm a_3) \) is prime to \( N \), then \( W_a \) is integral over \( \mathbb{Z}[j] \) and values of \( W_a \) at imaginary quadratic points are algebraic integers.

Proof. Let \( M \in \text{SL}_2(\mathbb{Z}) \) such that \( M \equiv \begin{pmatrix} a_1^{-1} & 0 \\ 0 & a_3 \end{pmatrix} \mod N \). Then \( W_a = \Lambda_{k,\ell} \circ M \), where \( k, \ell \in \mathbb{Z} \) such that \( a_1 = \{ka_3\}, a_2 = \{\ell a_3\} \). The assumption implies \( k(\ell \pm 1) \) is prime to \( N \). By Theorem 4.4 for \( A \in \text{SL}_2(\mathbb{Z}) \), \( \Lambda_{k,\ell} \circ A \) is integral over \( \mathbb{Z}[j] \). Hence \( W_a \) is integral over \( \mathbb{Z}[j] \). \( \square \)

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

Theorem 4.8. Let \( k, \ell \in \mathbb{Z} \) such that \( 1 < \ell \neq k < N/2 \). Let \( K \) be an imaginary quadratic field with the discriminant \( D \). Then the ray class field of \( K \) modulo \( N \) is generated by \( \Lambda_{k,\ell}((D + \sqrt{D})/2) \) and \( \zeta \) over the Hilbert class field of \( K \).

Proof. The assertion is deduced from Theorems 1 and 2 of [2] and Theorem 3.1. \( \square \)
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), 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.