TOKYO J. MATH.
VOL. 37, NO. 1, 2014

Generalized Lambda Functions and Modular Function Fields of Principal Congruence Subgroups

Noburo ISHII

Osaka Prefecture University

(Communicated by S. Nakano)

Abstract. Let N be a positive integer greater than 1. We define a modular function of level N which is a generalization of the elliptic modular lambda function. We show this function and the modular invariant function j generate the modular function field with respect to the principal congruence subgroup of level N. Further we study its values at imaginary quadratic points.

1. Introduction

For a positive integer N, let $\Gamma(N)$ be the principal congruence subgroup of level N of $\mathrm{SL}_2(\mathbf{Z})$, thus,

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z}) \;\middle|\; a-1 \equiv b \equiv c \equiv 0 \mod N \right\}.$$

We denote by $A(N)$ the modular function field with respect to $\Gamma(N)$. For an element τ of the complex upper half plane, we denote by L_τ the lattice of $\mathbf{C}$ generated by 1 and τ and by $\wp(z; L_\tau)$ the Weierstrass $\wp$-function relative to the lattice L_τ. Let $e_i\,(i = 1, 2, 3)$ be the 2-division points of the group $\mathfrak{E}_\tau = \mathbf{C}/L_\tau$. The elliptic modular lambda function $\lambda(\tau)$ is defined by

$$\lambda(\tau) = \frac{\wp(e_1; L_\tau) - \wp(e_3; L_\tau)}{\wp(e_2; L_\tau) - \wp(e_3; L_\tau)}.$$

The function λ generates $A(2)$ and is used instead of the modular invariant function $j(\tau)$ to parametrize elliptic curves. Further $2^4\lambda$ is integral over $\mathbf{Z}[j]$ (see [6] 18, §6). Note that $e_3 = e_1 + e_2$. In the case the genus of $A(N)$ is not 0, thus $N \geq 6$, $A(N)$ has at least two generators. It is well known that $A(N)$ is a Galois extension over $\mathbf{C}(j)$ with the Galois group $\mathrm{SL}_2(\mathbf{Z})/\{\pm E_2\}\Gamma(N)$, where E_2 is a unit matrix. Therefore $A(N)$ is generated by a function over $\mathbf{C}(j)$. Henceforth let $N \geq 2$. For the group $\mathfrak{E}_\tau[N]$ of N-division points of $\mathfrak{E}_\tau$, there exists

Received April 25, 2013; revised July 3, 2013
2010 *Mathematics Subject Classification*: 11F03; 11G15
Key words and phrases: modular function field, generator, lambda function

an isomorphism φ_τ of the group $\mathbf{Z}/N\mathbf{Z} \oplus \mathbf{Z}/N\mathbf{Z}$ to $\mathfrak{E}_\tau[N]$ given by $\varphi_\tau((r, s)) \equiv (r\tau + s)/N \mod L_\tau$. If $\{Q_1, Q_2\}$ is a basis of $\mathbf{Z}/N\mathbf{Z} \oplus \mathbf{Z}/N\mathbf{Z}$, then $\{\varphi_\tau(Q_1), \varphi_\tau(Q_2)\}$ is a basis of $\mathfrak{E}_\tau[N]$. In this article, we consider a modular function associated with a basis of the group $\mathfrak{E}_\tau[N]$ which is a generalization of $\lambda(\tau)$, defined by

$$\Lambda(\tau; Q_1, Q_2) = \frac{\wp(\varphi_\tau(Q_1); L_\tau) - \wp(\varphi_\tau(Q_1 + Q_2); L_\tau)}{\wp(\varphi_\tau(Q_2); L_\tau) - \wp(\varphi_\tau(Q_1 + Q_2); L_\tau)}. \tag{1}$$

For $N \neq 6$, we shall show that $\Lambda(\tau; Q_1, Q_2)$ generates $A(N)$ over $\mathbf{C}(j)$. In the case $N = 6$, $\Lambda(\tau; Q_1, Q_2)$ is not a generator of $A(6)$ over $\mathbf{C}(j)$, for any basis $\{Q_1, Q_2\}$ (see Remark 3.4). For N, let us define an integer C_N as follows. Put $C_2 = 2^4$. Let $N > 2$. If $N = p^m$ is a power of a prime number p, then put

$$C_N = \begin{cases} p^2 & \text{if } p = 2, 3, \\ p & \text{if } p > 3. \end{cases}$$

If N is not a power of a prime number, then put $C_N = 1$. We shall show that $C_N \Lambda(\tau; Q_1, Q_2)$ is integral over $\mathbf{Z}[j]$, and the value of $C_N \Lambda(\tau; Q_1, Q_2)$ at an imaginary quadratic point is an algebraic integer. Further if $N \neq 6$, then it generates a ray class field modulo N over a Hilbert class field. For the modular subgroups $\Gamma_1(N)$ and $\Gamma_0(N)$, we have obtained similar results by using generalized lambda functions of different types. See Remark 4.6 and for more details, refer to [4] and [5]. Throughout this article, we use the following notation:

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

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

The greatest common divisor of $a, b \in \mathbf{Z}$ is denoted by $\mathrm{GCD}(a, b)$. For an integral domain R, $R((q))$ represents the ring of formal Laurent series of a variable q with coefficients in R and $R[[q]]$ is the power series ring of a variable q with coefficients in R. For $f, g \in R((q))$ and a positive integer m, the relation $f - g \in q^m R[[q]]$ is denoted by $f \equiv g \mod q^m$.

2. Auxiliary results

Let N be an integer greater than 1. Put $q = \exp(2\pi i\tau/N)$ and $\zeta = \exp(2\pi i/N)$. For an integer x, let $\{x\}$ and $\mu(x)$ be the integers defined by the following conditions:

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

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

For a pair of integers (r, s) such that $(r, s) \not\equiv (0, 0) \mod N$, consider a function

$$E(\tau; r, s) = \frac{1}{(2\pi i)^2}\wp\left(\frac{r\tau + s}{N}; L_\tau\right) - 1/12$$

on the complex upper half plane. Clearly,

$$\begin{aligned} &E(\tau; r + aN, s + bN) = E(\tau; r, s) \text{ for any integers } a, b\,, \\ &E(\tau; r, s) = E(\tau; -r, -s)\,, \end{aligned} \tag{2}$$

since $\wp(z; L_\tau)$ is an even function. It follows that $E(\tau; r, s)$ is a modular form of weight 2 with respect to $\Gamma(N)$ from the transformation formula:

$$E(\tau; r, s)[A]_2 = E(\tau; ar + cs, br + ds), \text{ for } A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})\,. \tag{3}$$

Put $\omega = \zeta^{\mu(r)s}$ and $u = \omega q^{\{r\}}$. From proof of Lemma 1 of [3], the q-expansion of $E(\tau; r, s)$ is obtained as follows:

$$E(\tau; r, s) = \begin{cases} \dfrac{\omega}{(1-\omega)^2} + \displaystyle\sum_{m=1}^{\infty}\sum_{n=1}^{\infty} n(\omega^n + \omega^{-n} - 2)q^{mnN} & \text{if } \{r\} = 0\,, \\ \displaystyle\sum_{n=1}^{\infty} nu^n + \sum_{m=1}^{\infty}\sum_{n=1}^{\infty} n(u^n + u^{-n} - 2)q^{mnN} & \text{otherwise.} \end{cases} \tag{4}$$

Therefore $E(\tau; r, s) \in \mathbf{Q}(\zeta)[[q]]$. For an integer ℓ prime to N, let σ_ℓ be the automorphism of $\mathbf{Q}(\zeta)$ defined by $\zeta^{\sigma_\ell} = \zeta^\ell$. On a power series $f = \sum_m a_m q^m$ with $a_m \in \mathbf{Q}(\zeta)$, σ_ℓ acts by $f^{\sigma_\ell} = \sum_m a_m^{\sigma_\ell} q^m$. By (4),

$$E(\tau; r, s)^{\sigma_\ell} = E(\tau; r, s\ell)\,. \tag{5}$$

If (r_1, s_1) and (r_2, s_2) are pairs of integers such that (r_1, s_1), $(r_2, s_2) \not\equiv (0, 0) \mod N$ and $(r_1, s_1) \not\equiv (r_2, s_2), (-r_2, -s_2) \mod N$, then $E(\tau; r_1, s_1) - E(\tau; r_2, s_2)$ is not 0 and has neither zeros nor poles on the complex upper half plane, because the function $\wp(z; L_\tau) - \wp((r_2\tau + s_2)/N; L_\tau)$ has zeros (resp.poles) only at the points $z \equiv \pm(r_2\tau + s_s)/N$ (resp.0) $\mod L_\tau$. The next lemma and propositions are required in the following sections.

LEMMA 2.1. *Let $k \in \mathbf{Z}$ and $\delta = \mathrm{GCD}(k, N)$.*

(i) *For an integer ℓ, if ℓ is divisible by δ, then $(1 - \zeta^\ell)/(1 - \zeta^k) \in \mathbf{Z}[\zeta]$.*

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

PROOF. If ℓ is divisible by δ, 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/δ. Since $N/p_i = \delta(N/\delta p_i)$, $1 - \zeta^{N/p_i}$ is divisible by $1 - \zeta^\delta$. Therefore p_i $(i = 1, 2)$ is divisible by $1 - \zeta^\delta$. This implies that $1 - \zeta^\delta$ is a unit. Because of $\mathrm{GCD}(k/\delta, N/\delta) = 1$, $1 - \zeta^k$ is also a unit. $\square$

The following propositions are immediate results of (4).

PROPOSITION 2.2. *Let* (r_i, s_i) $(i = 1, 2)$ *be as above. Assume that* $\{r_1\} \leq \{r_2\}$. *Put* $\omega_i = \zeta^{\mu(r_i)s_i}$ *and* $u_i = \omega_i q^{\{r_i\}}$.

(i) *If* $\{r_1\} \neq 0$, *then*

$$E(\tau; r_1, s_1) - E(\tau; r_2, s_2) \equiv \sum_{n=1}^{N-1} n(u_1^n - u_2^n) + u_1^{-1} q^N - u_2^{-1} q^N \mod q^N .$$

(ii) *If* $\{r_1\} = 0$ *and* $\{r_2\} \neq 0$, *then*

$$E(\tau; r_1, s_1) - E(\tau; r_2, s_2) \equiv \frac{\omega_1}{(1-\omega_1)^2} - \sum_{n=1}^{N-1} n u_2^n - u_2^{-1} q^N \mod q^N .$$

(iii) *If* $\{r_1\} = \{r_2\} = 0$, *then*

$$E(\tau; r_1, s_1) - E(\tau; r_2, s_2) \equiv \frac{(\omega_1 - \omega_2)(1 - \omega_1\omega_2)}{(1-\omega_1)^2(1-\omega_2)^2} \mod q^N .$$

PROPOSITION 2.3. *Let the assumption and the notation be the same as in Proposition* 2.2. *Then*

$$E(\tau; r_1, s_1) - E(\tau; r_2, s_2) = \theta q^{\{r_1\}}(1 + q h(q)) ,$$

where $h(q) \in \mathbf{Z}[\zeta][[q]]$ *and* θ *is a non-zero element of* $\mathbf{Q}(\zeta)$ *defined as follows. In the case of* $\{r_1\} = \{r_2\}$,

$$\theta = \begin{cases} \omega_1 - \omega_2 & \text{if } \{r_1\} \neq 0, N/2 , \\ -\dfrac{(\omega_1 - \omega_2)(1 - \omega_1\omega_2)}{\omega_1\omega_2} & \text{if } \{r_1\} = N/2 , \\ \dfrac{(\omega_1 - \omega_2)(1 - \omega_1\omega_2)}{(1-\omega_1)^2(1-\omega_2)^2} & \text{if } \{r_1\} = 0 . \end{cases}$$

In the case of $\{r_1\} < \{r_2\}$,

$$\theta = \begin{cases} \omega_1 & \text{if } \{r_1\} \neq 0 , \\ \dfrac{\omega_1}{(1-\omega_1)^2} & \text{if } \{r_1\} = 0 . \end{cases}$$

3. Generalized lambda functions

For a basis $\{Q_1, Q_2\}$ of the group $\mathbf{Z}/N\mathbf{Z} \oplus \mathbf{Z}/N\mathbf{Z}$, let $\Lambda(\tau; Q_1, Q_2)$ be the function defined by (1). Henceforth, for an integer k prime to N, the function $\Lambda(\tau; (1,0), (0,k))$ is denoted by $\Lambda_k(\tau)$ to simplify the notation, thus,

$$\begin{aligned}\Lambda_k(\tau) &= \frac{\wp(\tau/N; L_\tau) - \wp((\tau+k)/N; L_\tau)}{\wp(k/N; L_\tau) - \wp((\tau+k)/N; L_\tau)} \\ &= \frac{E(\tau; 1, 0) - E(\tau; 1, k)}{E(\tau; 0, k) - E(\tau; 1, k)}\,.\end{aligned} \tag{6}$$

PROPOSITION 3.1. *Let $\{Q_1, Q_2\}$ be a basis of the group $\mathbf{Z}/N\mathbf{Z} \oplus \mathbf{Z}/N\mathbf{Z}$. Then there exist an integer k prime to N and a matrix $A \in \mathrm{SL}_2(\mathbf{Z})$ such that*

$$\Lambda(\tau; Q_1, Q_2) = \Lambda_k \circ A\,.$$

PROOF. Each basis $\{Q_1, Q_2\}$ of $\mathbf{Z}/N\mathbf{Z} \oplus \mathbf{Z}/N\mathbf{Z}$ is given by $\{(1,0)B, (0,1)B\}$ for $B \in \mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$. It is easy to see that $B \equiv \begin{pmatrix} 1 & 0 \\ 0 & k \end{pmatrix} A \mod N$, for an integer k prime to N and $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$. Therefore $Q_1 \equiv (a, b)$, $Q_2 \equiv (ck, dk) \mod N$. Since

$$\Lambda_k(\tau) = \frac{E(\tau; 1, 0) - E(\tau; 1, k)}{E(\tau; 0, k) - E(\tau; 1, k)}\,,$$

by (3)

$$\Lambda_k \circ A = \frac{E(\tau; a, b) - E(\tau; a+ck, b+dk)}{E(\tau; ck, dk) - E(\tau; a+ck, b+dk)} = \Lambda(\tau; Q_1, Q_2)\,.$$

□

Let $A(N)_{\mathbf{Q}(\zeta)}$ be the subfield of $A(N)$ consisted of all modular functions having Fourier coefficients in $\mathbf{Q}(\zeta)$. By (4),

$$\Lambda(\tau; Q_1, Q_2) \in A(N)_{\mathbf{Q}(\zeta)}\,. \tag{7}$$

Theorem 3 of Chapter 6 of [6] shows that $A(N)_{\mathbf{Q}(\zeta)}$ is a Galois extension over $\mathbf{Q}(\zeta)(j)$ with Galois group $\mathrm{SL}_2(\mathbf{Z})/\Gamma(N)\{\pm E_2\}$.

PROPOSITION 3.2. *Let $N \neq 6$ and let k be an integer prime to N. Then*

$$A(N)_{\mathbf{Q}(\zeta)} = \mathbf{Q}(\zeta)(\Lambda_k, j)\,.$$

PROOF. By (5), $\Lambda_k^{\sigma_\ell} = \Lambda_{k\ell}$. If $A(N)_{\mathbf{Q}(\zeta)} = \mathbf{Q}(\zeta)(\Lambda_1, j)$, then we can write $\Lambda_{k^{-1}} = F(\Lambda_1, j)$ for a rational function $F(X, Y)$ of X and Y with coefficients in $\mathbf{Q}(\zeta)$. By applying σ_k to this equality, we have $\Lambda_1 = F^{\sigma_k}(\Lambda_k, j)$, and $A(N)_{\mathbf{Q}(\zeta)} = \mathbf{Q}(\zeta)(\Lambda_k, j)$. Therefore we have only to prove the assertion in the case $k = 1$. Let $k = 1$ and H the invariant subgroup of Λ_1 in $\mathrm{SL}_2(\mathbf{Z})$. Since $\Lambda_1 \in A(N)_{\mathbf{Q}(\zeta)}$, it is sufficient to show $H \subset \Gamma(N)\{\pm E_2\}$. Let

$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in H$, thus, $\Lambda_1 \circ A = \Lambda_1$. Then by (3) and (6),

$$\begin{aligned} &(E(\tau; a, b) - E(\tau; a+c, b+d))(E(\tau; 0, 1) - E(\tau; 1, 1)) \\ &\quad = (E(\tau; c, d) - E(\tau; a+c, b+d))(E(\tau; 1, 0) - E(\tau; 1, 1)) . \end{aligned} \tag{8}$$

From Proposition 2.2 it follows:

$$\begin{aligned} E(\tau; 0, 1) - E(\tau; 1, 1) &\equiv \theta - \zeta q - 2\zeta^2 q^2 \mod q^3 , \\ E(\tau; 1, 0) - E(\tau; 1, 1) &\equiv (1-\zeta)q + 2(1-\zeta^2)q^2 \mod q^3 , \end{aligned} \tag{9}$$

where $\theta = \zeta/(1-\zeta)^2$. By considering the order of q-series in the both side of (8), it follows from Proposition 2.3 that

$$\min(\{a\}, \{a+c\}) = \min(\{c\}, \{a+c\}) + 1 . \tag{10}$$

This equality implies that $\{a\}, \{a+c\} \neq 0$. At first we shall show that $c \equiv 0 \mod N$. Let us assume that $\{c\} \neq 0$. We have three cases: (i) $\{a\} < \{a+c\}$, (ii) $\{a\} > \{a+c\}$, (iii) $\{a\} = \{a+c\}$. Let us consider the case (i). Then $\{c\} = \{a\} - 1 \neq 0$. Therefore $0 < \{a\}, \{c\} < \{a+c\} \leq N/2$. By comparing the coefficient of $q^{\{a\}}$ of q-series in the both side of (8), from Proposition 2.3 it follows that

$$\zeta^{\mu(a)b}\theta = \zeta^{\mu(c)d}(1-\zeta) .$$

This gives $|1-\zeta| = 1$, hence $N = 6$, which contradicts the assumption. In the case (ii), $\{c\} = \{a+c\} - 1$. Therefore $0 < \{c\} < \{a+c\} < \{a\} \leq N/2$. An argument similar to that in the case (i) gives that $N = 6$. Now we deal with the case (iii). Put $\{c\} = t$. Then $\{a\} = \{a+c\} = t+1 \leq N/2$, and $t \neq 0, N/2$. Since $t \neq 0$, the equality $\{a\} = \{a+c\}$ implies that $c \equiv -2a \mod N$, $\mu(a) = -\mu(a+c)$. Therefore $t = 2\{a\}$ (resp.$N - 2\{a\}$) if $2\{a\} \leq N/2$ (resp.$2\{a\} > N/2$). The equality $\{a\} = t+1$ implies that $t = N - 2\{a\}$,thus $N = 3t+2$. Hence $N \geq 5$ and $\{a\} \neq N/2$. From comparing the coefficient of q^{t+1} of q-series in the both side of (8), from Proposition 2.3 it follows that

$$\frac{\zeta}{(1-\zeta)^2}(\omega_1 - \omega_3) = (1-\zeta)\omega_2 , \tag{11}$$

where $\omega_1 = \zeta^{\mu(a)b}$, $\omega_2 = \zeta^{\mu(c)d}$, $\omega_3 = \zeta^{\mu(a+c)(b+d)}$. Therefore,

$$\zeta\omega_1\omega_2^{-1}\left(\frac{1-\omega_3\omega_1^{-1}}{1-\zeta}\right) = (1-\zeta)^2 .$$

Let $N = 5$. Then $(1-\zeta)$ is not a unit but by Lemma 2.1, $\left(\dfrac{1-\omega_3\omega_1^{-1}}{1-\zeta}\right)$ is 0 or a unit. This gives a contradiction. Let $N \geq 6$. Then $t > 1$ and noting that $t < N/2-1, 2t-1, N-(t+3)$, the following congruences are obtained from Proposition 2.2:

$$\begin{aligned} E(\tau; a, b) - E(\tau; a+c, b+d) &\equiv (\omega_1 - \omega_3)q^{t+1} \mod q^{t+3}, \\ E(\tau; c, d) - E(\tau; a+c, b+d) &\equiv \omega_2 q^t - \omega_3 q^{t+1} \mod q^{t+2}. \end{aligned} \tag{12}$$

Therefore, comparing the coefficient of q^{t+2} of q-series in (8), we have:

$$\zeta(\omega_1 - \omega_3) = (1-\zeta)\omega_3 - 2(1-\zeta^2)\omega_2 .$$

From this, by using (11), it follows that $3 + \zeta^2 = \omega_3/\omega_2$. Therefore $|3+\zeta^2| = 1$. However $|3+\zeta^2| > 1$. This is a contradiction. Hence we obtain $c \equiv 0 \mod N$. From (10), it is deduced that $a \equiv d \equiv \pm 1 \mod N$. If necessary, by replacing A by $-A$, we can assume that $A = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$. By (8),

$$\begin{aligned} &(E(\tau; 1, b) - E(\tau; 1, b+1))(E(\tau; 0, 1) - E(\tau; 1, 1)) \\ &\qquad = (E(\tau; 0, 1) - E(\tau; 1, b+1))(E(\tau; 1, 0) - E(\tau; 1, 1)) . \end{aligned} \tag{13}$$

By comparing the coefficients of q,

$$(\zeta^b - \zeta^{b+1})\theta = (1-\zeta)\theta .$$

This implies that $\zeta^b = 1$. Hence we obtain $A \in \Gamma(N)$. □

THEOREM 3.3. *Let $\{Q_1, Q_2\}$ be a basis of the group $\mathbf{Z}/N\mathbf{Z} \oplus \mathbf{Z}/N\mathbf{Z}$. Then $A(N)_{\mathbf{Q}(\zeta)} = \mathbf{Q}(\zeta)(\Lambda(\tau; Q_1, Q_2), j)$.*

PROOF. By Proposition 3.1, there exists an integer k prime to N and an element $A \in \mathrm{SL}_2(\mathbf{Z})$ such that $\Lambda(\tau; Q_1, Q_2) = \Lambda_k \circ A$. Since $\Gamma(N)$ is a normal subgroup of $\mathrm{SL}_2(\mathbf{Z})$, the assertion is deduced from (7) and Proposition 3.2. □

REMARK 3.4. Let $N = 6$. Then the matrix $M = \begin{pmatrix} 3 & 11 \\ 1 & 4 \end{pmatrix} \notin \Gamma(6)$ fixes the function $\Lambda_1(\tau)$. This fact is proved as follows. Let us consider the function

$$\begin{aligned} F(\tau) &= (E(\tau; 1, 0) - E(\tau; 1, 1))[M]_2(E(\tau; 0, 1) - E(\tau; 1, 1)) \\ &\quad - (E(\tau; 0, 1) - E(\tau; 1, 1))[M]_2(E(\tau; 1, 0) - E(\tau; 1, 1)) \\ &= (E(\tau; 3, 1) - E(\tau; 2, 3))(E(\tau; 0, 1) - E(\tau; 1, 1)) \\ &\quad - (E(\tau; 1, 4) - E(\tau; 2, 3))(E(\tau; 1, 0) - E(\tau; 1, 1)) . \end{aligned}$$

Here we used (2) and (3). Then F is a cusp form of weight 4 with respect to $\Gamma(6)$. If $F \neq 0$, then F has 24 zeros in the fundamental domain. See [7], III-6, Proposition 10. Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z})$. Then the order of F at the cusp $a/c = A(i\infty)$ is greater than or equal to minimum of two integers $\min(\{3a+c\}, \{2a+3c\}) + \min(\{c\}, \{a+c\})$ and $\min(\{a+4c\}, \{2a+3c\}) + \min(\{a\}, \{a+c\})$. It is easy to see that F has at least 22 zeros at cusps other than $i\infty$ and the coefficient of q^2 of the q-expansion of F is 0. This shows that F has at least 25 zeros. Hence $F = 0$.

4. Values of $\Lambda(\tau; Q_1, Q_2)$ at imaginary quadratic points

In this section, we study values of $\Lambda(\tau; Q_1, Q_2)$ at imaginary quadratic points. In the case $N = 2$, it is well known that $2^4\lambda$ is integral over $\mathbf{Z}[j]$. For example see [6] 18, §6. We shall consider the case $N > 2$.

LEMMA 4.1. *Let k be an integer prime to N and $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z})$. Let A_k be a matrix of $\mathrm{SL}_2(\mathbf{Z})$ such that $A_k \equiv \begin{pmatrix} a & bk^{-1} \\ ck & d \end{pmatrix} \mod N$. Then*

$$\Lambda_k \circ A = (\Lambda_1 \circ A_k)^{\sigma_k}.$$

PROOF. Let $A_k = \begin{pmatrix} t & u \\ v & w \end{pmatrix}$. Then

$$\begin{aligned}(\Lambda_1 \circ A_k)^{\sigma_k} &= \frac{E(\tau; t, uk) - E(\tau; t+v, (u+w)k)}{E(\tau; v, wk) - E(\tau; t+v, (u+w)k)} \\ &= \frac{E(\tau; a, b) - E(\tau; a+ck, b+dk)}{E(\tau; ck, dk) - E(\tau; a+ck, b+dk)} \\ &= \Lambda_k \circ A.\end{aligned}$$

□

PROPOSITION 4.2. *Let $N > 2$ and k be an integer prime to N. Then for any $A \in \mathrm{SL}_2(\mathbf{Z})$, $(1-\zeta^k)^3 \Lambda_k \circ A \in \mathbf{Z}[\zeta]((q))$.*

PROOF. By Lemma 4.1, we have only to prove the assertion in the case $k = 1$. Put $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Proposition 2.3 shows that

$$\begin{aligned} E(\tau; a, b) - E(\tau; a+c, b+d) &= \theta_1 q^{t_1}(1 + h_1(q)), \\ E(\tau; c, d) - E(\tau; a+c, b+d) &= \theta_2 q^{t_2}(1 + h_2(q)), \end{aligned} \tag{14}$$

where t_i are non-negative integers, θ_i are non-zero elements of $\mathbf{Q}(\zeta)$ and $h_i \in \mathbf{Z}[\zeta][[q]]$ $(i = 1, 2)$. This shows $\Lambda_k \circ A = \omega f(q)$, where $\omega = \theta_1/\theta_2$ and $f \in \mathbf{Z}[\zeta]((q))$. Therefore it is sufficient to prove that $(1-\zeta)^3\omega \in \mathbf{Z}[\zeta]$. By Proposition 2.3, if $\min(\{a\}, \{a+c\}) \neq 0$ and $\{c\} \neq \{a+c\}$, then $\theta_1, \theta_2^{-1} \in \mathbf{Z}[\zeta]$. Therefore $\omega \in \mathbf{Z}[\zeta]$. Let $\{c\} = \{a+c\}$. If $\mu(c) = \mu(a+c)$, then $a \equiv 0 \mod N$. This implies that $\mathrm{GCD}(c, N) = 1$ and $\{a\} = 0 < \{c\} = \{a + c\} < N/2$. Therefore

$$\theta_1 = \zeta^b/(1 - \zeta^b)^2, \theta_2 = \zeta^{\mu(c)d} - \zeta^{\mu(c)(b+d)},$$

and $\omega = \zeta^\ell/(1 - \zeta^b)^3$ for an integer ℓ. Since $\mathrm{GCD}(b, N) = 1$, by (i) of Lemma 2.1, $(1 - \zeta)^3\omega \in \mathbf{Z}[\zeta]$. Let $\mu(c) = -\mu(a + c)$. Then $a \equiv -2c \mod N$. Since $\mathrm{GCD}(a, c) = 1$, $\mathrm{GCD}(c, N) = 1$. It follows that $\{c\} \neq 0, N/2$ and $\{a\}, \{a + c\} \neq 0$. Therefore $\theta_1 \in \mathbf{Z}[\zeta]$ and $\theta_2 = \zeta^{\mu(c)d}(1 - \zeta^{-\mu(c)(b+2d)})$. Let $\mathrm{GCD}(b + 2d, N) = D$, then $b \equiv -2d \mod D, a \equiv -2c \mod D$. It follows that $1 = ad - bc \equiv 0 \mod D$. This shows $b+2d$ is prime to N. Lemma 2.1 shows that $(1 - \zeta)\omega \in \mathbf{Z}[\zeta]$. Let $\min(\{a\}, \{a + c\}) = 0$ and $\{a + c\} \neq \{c\}$. Then $\{a + c\} = 0$ and $\{a\}, \{c\} \neq 0$. Therefore $0 = \{a + c\} < \{a\}, \{c\}$, and $\theta_1 = \theta_2$, thus $\omega = 1$. □

Let $C_2 = 2^4$ and for $N > 2$ put

$$C_N = \begin{cases} p^2 & \text{if } N = p^\ell (p = 2, 3)\,, \\ p & \text{if } N = p^\ell (p : \text{a prime number} > 3)\,, \\ 1 & \text{if } N \text{ is not a power of a prime number}\,. \end{cases}$$

COROLLARY 4.3. *Let $N > 2$ and k be an integer prime to N. Then $C_N \Lambda_k \circ A \in \mathbf{Z}[\zeta]((q))$ for any $A \in \mathrm{SL}_2(\mathbf{Z})$.*

PROOF. Lemma 2.1 implies that $C_N/(1 - \zeta^k)^3 \in \mathbf{Z}[\zeta]$. The assertion follows from Proposition 4.2. □

THEOREM 4.4. *Let $\{Q_1, Q_2\}$ be a basis of the group $\mathbf{Z}/N\mathbf{Z} \oplus \mathbf{Z}/N\mathbf{Z}$. Then the function $C_N \Lambda(\tau; Q_1, Q_2)$ is integral over $\mathbf{Z}[j]$. Further Let θ be an element of the complex upper half plane such that $\mathbf{Q}(\theta)$ is an imaginary quadratic field. Then $C_N \Lambda(\theta; Q_1, Q_2)$ is an algebraic integer.*

PROOF. For $N = 2$, the assertion has been already proved. Let $N > 2$. For an integer k prime to N, let us consider a polynomial of X:

$$\Psi_k(X) = \prod_A (X - C_N \Lambda_k \circ A)\,,$$

where A runs over all representatives of $\mathrm{SL}_2(\mathbf{Z})/\Gamma(N)\{\pm E_2\}$. Then each coefficient of $\Psi_k(X)$ is belong to $\mathbf{Z}[\zeta]((q))$ and is $\mathrm{SL}_2(\mathbf{Z})$-invariant, and has no poles in the complex half plane. Therefore $\Psi_k(X)$ is a monic polynomial with coefficients in $\mathbf{Z}[\zeta][j]$. Since $C_N \Lambda_k \circ A$ is a root of $\Psi_k(X) = 0$, $C_N \Lambda_k \circ A$ is integral over $\mathbf{Z}[\zeta][j]$. From Proposition 3.1 and the fact that $\mathbf{Z}[\zeta][j]$ is integral over $\mathbf{Z}[j]$, it follows that $C_N \Lambda(\tau; Q_1, Q_2)$ is integral over $\mathbf{Z}[j]$. Since $j(\theta)$ is an algebraic integer (see [1],Theorem 10.23) and $C_N \Lambda(\theta; Q_1, Q_2)$ is integral over $\mathbf{Z}[j(\theta)]$, $C_N \Lambda(\theta; Q_1, Q_2)$ is an algebraic integer. □

THEOREM 4.5. *Let $N \neq 6$ and $\{Q_1, Q_2\}$ be a basis of the group $\mathbf{Z}/N\mathbf{Z} \oplus \mathbf{Z}/N\mathbf{Z}$. Let θ be an element of the complex upper half plane such that $\mathbf{Z}[\theta]$ is the maximal order of* *an imaginary quadratic field K. Then the ray class field $\mathfrak{R}_N$ of K modulo N is generated by $\Lambda(\theta; Q_1, Q_2)$ and ζ over the Hilbert class field $K(j(\theta))$ of K.*

PROOF. The assertion is deduced from Theorems 1, 2 of [2] and Theorem 3.3. □

REMARK 4.6. Let k and ℓ be integers such that $0 < k \neq \ell < N/2$, $\mathrm{GCD}(k+\ell, N) = 1$. We consider a function

$$\Lambda^*_{k,\ell}(\tau) = \frac{\wp(\frac{k}{N}; L_\tau) - \wp(\frac{k+\ell}{N}; L_\tau)}{\wp(\frac{\ell}{N}; L_\tau) - \wp(\frac{k+\ell}{N}; L_\tau)}.$$

This is a modular function with respect to the group

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z}) \,\middle|\, a - 1 \equiv c \equiv 0 \mod N \right\}.$$

In Corollary 1 of [4] we show that $\Lambda^*_{k,\ell}$ and j generate the function field rational over $\mathbf{Q}(\zeta)$ with respect to $\Gamma_1(N)$. Let the notation be the same as in Theorem 4.5. From Corollary 3 and Theorem 4 of [4], we obtain that $\mathfrak{R}_N$ is generated by $\Lambda^*_{k,\ell}(\theta)$ and ζ over the Hilbert class field of K and that $\Lambda^*_{k,\ell}(\theta)$ is an algebraic integer under an additional assumption $\mathrm{GCD}(k(k+2\ell), N) = 1$.

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] 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.

[4] N. ISHII, Special values of generalized λ functions at imaginary quadratic points, Ramanujan J. **33** (2014), 121–130, DOI 10.1007/s11139-013-9463-5.

[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*, Addison-Wesley, London,1973.

[7] A. OGG, *Modular forms and Dirichlet Series*, Benjamin, 1969.

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

Present Address:
8–155 SHINOMIYA-KOGANEDUKA, YAMASHINA-KU,
KYOTO, 607–8022 JAPAN.
e-mail: Noburo.Ishii@ma2.seikyou.ne.jp