MINIMAL EQUATIONS AND VALUES OF GENERALIZED LAMBDA FUNCTIONS

NOBURO ISHII

Abstract. In our preceding article, we defined a generalized lambda function \( \Lambda(\tau) \) and showed that \( \Lambda(\tau) \) and the modular invariant function \( j(\tau) \) generate the modular function field with respect to a principal congruence subgroup. In this article we shall study a minimal equation and values of \( \Lambda(\tau) \).

1. Introduction

For a positive integer \( N \), let \( \Gamma(N) \) be the principal congruence subgroup of level \( N \) of \( SL_2(\mathbb{Z}) \), thus,
\[
\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \left| \begin{array}{l}
a - 1 \equiv b \equiv c \equiv 0 \mod N \end{array} \right. \right\}.
\]
We denote by \( \Gamma(1) \) the group \( SL_2(\mathbb{Z}) \). Let \( \mathcal{H} \) be the complex upper half plane. In the following, for a fixed positive integer \( N \), we put \( \zeta = \exp(2\pi i / N) \) and \( q = \exp(2\pi i \tau / N) \) for \( \tau \in \mathcal{H} \). Further let \( K_N = \mathbb{Q}(\zeta) \) and \( O_N \) the maximal order \( \mathbb{Z}[\zeta] \) of \( K_N \). We denote by \( A(N) \) the modular function field with respect to \( \Gamma(N) \) consisted of all modular functions having \( q \)-expansions with coefficients in \( K_N \). For \( \tau \in \mathcal{H} \), let \( L_\tau \) be the lattice of \( \mathbb{C} \) generated by 1 and \( \tau \) and \( \wp(z; L_\tau) \) the Weierstrass \( \wp \)-function relative to the lattice \( L_\tau \). Let \( \mathcal{E}_r[N] \) be the subgroup of \( N \)-division points of \( \mathcal{E}_r = \mathbb{C}/L_\tau \) and \( \varphi_\tau \) the isomorphism of the group \( \mathbb{Z}/NZ \oplus \mathbb{Z}/NZ \) to \( \mathcal{E}_r[N] \) defined by \( \varphi_\tau((r, s)) \equiv (\tau r + s)/N \mod L_\tau \). In [4], for a basis \( \{Q_1, Q_2\} \) of \( \mathbb{Z}/NZ \oplus \mathbb{Z}/NZ \), we defined a generalized lambda function by
\[
\Lambda(\tau; Q_1, Q_2) = \frac{\varphi(\varphi_\tau(Q_1); L_\tau) - \varphi(\varphi_\tau(Q_1 + Q_2); L_\tau)}{\varphi(\varphi_\tau(Q_2); L_\tau) - \varphi(\varphi_\tau(Q_1 + Q_2); L_\tau)}
\]
and showed that \( \Lambda(\tau; Q_1, Q_2) \) and the modular invariant function \( j(\tau) \) generate \( A(N) \) over \( K_N \) if \( N \neq 6 \). For \( N = 2 \), the function \( \lambda = \Lambda(\tau; (0, 1), (1, 0)) \) is known as the elliptic modular lambda function. It is proved in [5] 18.6 that
\[
j = 2^8 (\lambda^2 - \lambda + 1)^3 / \lambda^2 (\lambda - 1)^2.
\]
From this, we obtain a minimal equation of \( \lambda \) over \( \mathbb{Q}(j) \):
\[
x^6 - 3x^5 + (6 - j/256)x^4 + (-7 + j/128)x^3 + (6 - j/256)x^2 - 3x + 1 = 0.
\]

Date: 20 April 2015.
This equation has a symmetric property concerning the coefficients, which means that the coefficient of $x^i$ is equal to that of $x^{6-i}$ for $i = 0, \cdots, 3$.

In this article we study a minimal equation of $\Lambda(\tau; Q_1, Q_2)$ over $K_N(j)$ and especially prove a similar property of coefficients. Furthermore we study values of that function. In the last section, for the cases that $N = 3, 4$, we give some equations among $\Lambda = \Lambda(\tau; (1, 0), (0, 1)), j, \lambda$ and eta products $\eta(\tau)/\eta(N\tau)$, and compute the values of $\Lambda(\tau)$ for some imaginary quadratic integers $\alpha$ such that $\mathbb{Z}[\alpha]$ is a maximal order of class number one.

We shall use the following notation throughout this article.

For a function $f(\tau)$ and $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1)$, $f[A]_2$ and $f \circ A$ represent

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

and $f \circ A = f \left( \frac{a\tau + b}{c\tau + d} \right)$.

The greatest common divisor of $a, b \in \mathbb{Z}$ is denoted by $\text{GCD}(a, b)$. For an integer $\ell$ prime to $N$, the automorphism of $K_N$ defined by $\zeta^{\sigma_\ell} = \zeta^\ell$ is denoted by $\sigma_\ell$. The automorphism $\sigma_\ell$ acts on a power series $f = \sum_m a_m q^m$ with $a_m \in K_N$ by $f^{\sigma_\ell} = \sum_m a_m^{\sigma_\ell} q^m$.

## 2. Auxiliary results

In this section, we summarize the results in [4] needed below. For the proof, see [3] and [4]. Let $N > 2$. For an integer $x$, let $\{x\}$ and $\mu(x)$ be the integers defined by the following conditions:

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

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

For a pair of integers $(r, s)$ such that $(r, s) \not\equiv (0, 0) \mod N$, consider a modular form of weight 2 with respect to $\Gamma(N)$

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

**Proposition 2.1.** The form $E(\tau; r, s)$ has the following properties.

(i) $E(\tau; r, s) = E(\tau; -r, -s)$ and $E(\tau; r + aN, s + bN) = E(\tau; r, s)$ for any integers $a$ and $b$.

(ii) $E(\tau; r, s)[A]_2 = E(\tau; ar + cs, br + ds)$ for $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1)$.

(iii) $E(\tau; r, s) = \begin{cases} 
\omega \frac{|1 - \omega|^2}{(1 - \omega)^2} + \sum_{m=1}^{\infty} \sum_{n=1}^{\infty} n(\omega^n + \omega^{-n} - 2)q^{mnN} & \text{if } \{r\} = 0, \\
\sum_{n=1}^{\infty} nu^n + \sum_{m=1}^{\infty} \sum_{n=1}^{\infty} n(u^n + u^{-n} - 2)q^{mnN} & \text{otherwise},
\end{cases}$
where $\omega = \zeta^{\mu(r)s}$ and $u = \omega q^{(r)}$.

(iv) $E(\tau; r, s)^{u\ell} = E(\tau; r, s\ell)$ for any integer $\ell$ prime to $N$.

**Proposition 2.2.** Let $(r_1, s_1)$ and $(r_2, s_2)$ be pairs of integers such that $(r_1, s_1), (r_2, s_2) \not\equiv (0, 0) \mod N$ and $(r_1, s_1) \not\equiv \pm (r_2, s_2) \mod N$. Put $\omega_1 = \zeta^{\mu(r)s_1}$. Assume that $\{r_1\} \leq \{r_2\}$. Then

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

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

$$\theta = \begin{cases} \omega_1 - \omega_2 & \text{if } \{r_1\} \not\equiv 0, N/2, \\ (\omega_1 - \omega_2)(1 - \omega_1\omega_2) & \text{if } \{r_1\} = N/2, \\ \omega_1\omega_2 & \text{if } \{r_1\} = 0. \end{cases}$$

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

$$\theta = \begin{cases} \omega_1 & \text{if } \{r_1\} \not\equiv 0, \\ \omega_1(1 - \omega_1) & \text{if } \{r_1\} = 0. \end{cases}$$

Further $E(\tau; r_1, s_1) - E(\tau; r_2, s_2)$ has neither zeros nor poles on $\mathcal{H}$.

If $Q_i = (r_i, s_i) \ (i = 1, 2)$, then by the definition

$$\Lambda(\tau; Q_1, Q_2) = \frac{E(\tau; r_1, s_1) - E(\tau; r_1 + r_2, s_1 + s_2)}{E(\tau; r_2, s_2) - E(\tau; r_1 + r_2, s_1 + s_2)}.$$

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. Furthermore put $\Lambda(\tau) = \Lambda_1(\tau)$.

**Theorem 2.3.** Let $\{Q_1, Q_2\}$ be a basis of the group $\mathbb{Z}/N\mathbb{Z} \oplus \mathbb{Z}/N\mathbb{Z}$.

(i) $\Lambda(\tau; Q_1, Q_2)$ has zeros and poles only at cusps of $\Gamma(N)$ and has a $q$-expansion with coefficients in $K_N$.

(ii) $(1 - \zeta)^3\Lambda(\tau; Q_1, Q_2)$ is integral over $O_N[j]$. Especially $\Lambda(\tau; Q_1, Q_2)$ is a unit of the integral closure of $(O_N)_L[j]$ in $A(N)$, where $(O_N)_L$ is the localization of $O_N$ with respect to the multiplicative set $L = \{(1 - \zeta)^n \mid n \in \mathbb{Z}, n \geq 0\}$. Further if $N$ is not a prime power, then $\Lambda(\tau; Q_1, Q_2)$ is a unit of the integral closure of $O_N[j]$ in $A(N)$.

(iii) If $N \neq 6$, then $\Lambda(N) = K_N(j, \Lambda(\tau; Q_1, Q_2))$.

(iv) There exist an integer $k$ prime to $N$ and a matrix $A \in \Gamma(1)$ such that

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

(v) Let $k$ be an integer prime to $N$ and $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1)$. Then

$$\Lambda_k \circ A = (\Lambda \circ A_k)^{\sigma_k},$$

where $A_k$ is a matrix of $\Gamma(1)$ such that $A_k \equiv \begin{pmatrix} a & bk^{-1} \\ ck & d \end{pmatrix} \mod N$. 
Proof. The assertions except the latter part of (ii) are proved in [4]. The latter part of (ii) is deduced from the facts that \(1/\Lambda(\tau, Q_1, Q_2) = \Lambda(\tau, Q_2, Q_1)\) and \((1 - \zeta)\) is a unit of \((O_N)_L\), and that \((1 - \zeta)\) is a unit of \(O_N\) if \(N\) is not a prime power. \(\square\)

3. Minimal equation of \(\Lambda\) over \(K_N(j)\)

Let us consider a polynomial of \(X\) with coefficients in \(A(1)\);

\[\mathfrak{F}(X) = \prod_{A \in \mathfrak{R}} (X - \Lambda \circ A),\]

where \(\mathfrak{R}\) is a transversal of the coset decomposition of \(\Gamma(1)\) by \(\pm \Gamma(N)\).

**Proposition 3.1.** Let \(N > 2\) and \(N \neq 6\). Then we have the following:

(i) \(\mathfrak{F}(X)\) is a polynomial in \(K_N[j][X]\). The degree of \(\mathfrak{F}(X)\) is equal to \(d_N = \frac{N^3}{2} \prod_{p|N} (1 - p^{-2})\), where \(p\) runs over all prime divisors of \(N\).

(ii) If \(\Lambda(\tau, Q_1, Q_2) = \Lambda_k \circ A\) with \(\text{GCD}(k, N) = 1\) and \(A \in \Gamma(1)\), then \(\mathfrak{F}(X)^{\sigma_k}\) is a minimal equation of \(\Lambda(\tau, Q_1, Q_2)\) over \(K_N(j)\).

**Proof.** For (i), see the proof of Theorem 4.4 in [4]. The degree \(d_N\) is obviously equal to the index \([\Gamma(1) : \pm \Gamma(N)]\) = \(\frac{N^3}{2} \prod_{p|N} (1 - p^{-2})\). See 1.6 of [9]. Since \(N \neq 6\), Theorem 2.3 (iii) implies that \(\mathfrak{F}(X)\) is a minimal equation of \(\Lambda \circ A\) over \(K_N(j)\) for any \(A \in \Gamma(1)\). Therefore Theorem 2.3 (iv) and (v) show that the equation \(\mathfrak{F}^{\sigma_k}(X) = 0\) is a minimal equation of \(\Lambda(\tau, Q_1, Q_2)\). \(\square\)

We shall pick out a transversal \(\mathfrak{R}\) as follows. By [7], inequivalent cusps of \(\Gamma(N)\) correspond bijectively to elements of the set \(\Sigma\) of pairs of integers \((a, c)\), where \(a, c \in \mathbb{Z}/N\mathbb{Z}\), \(\text{GCD}(a, c, N) = 1\) and \((a, c)\) and \((-a, -c)\) are identified. We decompose \(\Sigma\) into two disjoint subsets \(\Sigma_1\) and \(\Sigma_2\), where \(\Sigma_1 = \{(a, c), (c, a)\} | a \neq \pm c \mod N\} \) and \(\Sigma_2 = \{(a, c) | c \equiv \pm a \mod N\}\). For each element \((a, c) \in \Sigma\), we fix a matrix \(A \in \Gamma(1)\) corresponding to \((a, c)\) so that \(A \equiv (a \ c) \mod N\). If \((a, c) \in \Sigma_1\) and \(A = (\frac{1}{a} \ 0)\) is the corresponding matrix to \((a, c)\), we choose \(A' = (\frac{1}{a} \ -\frac{1}{c})\) as a matrix corresponding to \((a, c)\). We denote by \(\mathfrak{S}\) the set of the corresponding matrices as above. Further, let \(\mathfrak{S}_1\) be the subset of \(\mathfrak{S}\) consisting of pairs \(\{A, A'\}\) corresponding to the pairs \(\{(a, c), (c, a)\}\) in \(\Sigma_1\) and \(\mathfrak{S}_2\) the subset of consisting of matrices corresponding to the elements of \(\Sigma_2\). Let \(T = (\frac{3}{1}, 1)\). Then \(\mathfrak{R} = \{AT^i | A \in \mathfrak{S}, i \in \mathbb{Z}/N\mathbb{Z}\}\) is a transversal. For pairs of integers \((r_1, s_1)\) and \((r_2, s_2)\) such that \((r_1, s_1), (r_2, s_2) \neq (0, 0), (r_1, s_1) \neq \pm (r_2, s_2) \mod N\), we define

\[W(\tau; r_1, s_1, r_2, s_2) = \frac{E(\tau; r_1, s_1) - E(\tau; r_2, s_2)}{E(\tau; r_1, -s_1) - E(\tau; r_2, -s_2)}\]

The next lemma is used in the proof of Theorem 3.4.
Theorem 3.4. Let \((F(i)\). □ does not change the first column, (ii) and (iii) are immediate results of Proposition 2.2 implies (i). Since right multiplication of a matrix with

First, we shall prove that

Proof. This is deduced from Proposition 2.2.

Lemma 3.2. Assume that \(\{r_1\} \leq \{r_2\}\). Then the leading coefficient \(c\) of the \(q\)-expansion of \(W(\tau; r_1, s_1, r_2, s_2)\) is given as follows:

\[
c = \begin{cases} 
-\zeta^{\mu(r_1)s_1 + \mu(r_2)s_2} & \text{if } \{r_1\} = \{r_2\} \neq 0, N/2, \\
\zeta^{2\mu(r_1)s_1} & \text{if } \{r_2\} > \{r_1\} \neq 0, \\
1 & \text{otherwise.}
\end{cases}
\]

Proof. Let \(A \equiv \begin{pmatrix} a & * \\ c & d \end{pmatrix} \pmod{N}\), then

\[
\nu(A) = \min\{\{a\}, \{a + c\}\} - \min\{\{c\}, \{a + c\}\}.
\]

(iii) Let \(A \in T(1)\). Then \(\nu(AT^i) = 0\) for any \(i \in \mathbb{Z}\).

Proof. Let \(A \in T(1)\) and assume that \(A \equiv \begin{pmatrix} a & b \\ c & d \end{pmatrix} \pmod{N}\). Since by Proposition 2.2 (ii)

\[
\Lambda \circ A = \frac{E(\tau; a, b) - E(\tau, a + c, b + d)}{E(\tau; c, d) - E(\tau, a + c, b + d)},
\]

Proposition 2.2 implies (i). Since right multiplication of a matrix with \(T^i\) does not change the first column, (ii) and (iii) are immediate results of (i).

Let \(F(X, Y)\) be the polynomial such that \(F(X, j) = \mathfrak{f}(X)\). Let us write \(F(X, Y)\) in a polynomial of \(K_N[Y][X]\), thus,

\[
F(X, Y) = \sum_{i=0}^{d_N} P_i(Y)X^{d_N-i}.
\]

Theorem 3.4. Let \(P_i(Y)\) be as above. Then we have the following:

(i) \((1 - \zeta)^{d_N}P_i(Y) \in ON[Y]\).

(ii) \(P_{d_N-i}(Y) = \overline{P_i(Y)}\) for all \(i\), where \(\overline{P_i(Y)}\) is the complex conjugation of \(P_i(Y)\).

(iii) \(P_i(Y)\) has degree smaller than \(i/2\). In particular \(P_1(Y)\) and \(P_2(Y)\) are constants.

(iv) Let \(t_N\) be the number of inequivalent cusps of \(\Gamma(N)\) where \(\Lambda\) has no poles. Then \(\deg P_1(Y) \leq \deg P_{Nt_N}(Y)\) for any \(i\).

Proof. First, we shall prove that \(P_{d_N}(Y) = 1\). Proposition 3.3 implies that \(P_{d_N}(Y)\) has no poles. Therefore, \(P_{d_N}(Y)\) is a constant and equals to the product of leading coefficients of \(q\)-expansions of \(\Lambda \circ A\ (A \in \mathfrak{m})\), since \(d_N\) is even. Let us consider a partial product:

\[
\prod_{\Lambda \circ (AT^i) \Lambda \circ (A'T^{-i}) = 1} \prod_{i=0}^{N-1} \Lambda \circ (AT^i)\Lambda \circ (A'T^{-i}).
\]
In other cases, we have easily that
\[ \Lambda \circ (AT^i) \cdot \Lambda \circ (AT^{-i}) = W(\tau; a, ia + b, a + c, i(a + c) + b + d) \]
\[ \times W(\tau; c, -(ic + d), a + c, -(i(a + c) + b + d)). \]

Let \( \delta \) and \( \delta' \) be the leading coefficient of \( \prod_{i=0}^{N-1} W(\tau; a, ia + b, a + c, i(a + c) + b + d) \) and \( \prod_{i=0}^{N-1} W(\tau; c, -(ic + d), a + c, -(i(a + c) + b + d)) \) respectively. Let \( \{a\} = \{a + c\} \neq 0, N/2 \). Then by Lemma 3.2
\[ \delta = (-1)^N \zeta^{\mu(a)}(ai+b)+\mu(a+c)\Sigma_i(a+c)i+b+d = (-1)^N \zeta^{\Sigma_i(\mu(a)+\mu(a+c)(a+c))i} \]
\[ = (-1)^N \zeta^{((a)+(a+c))N(N-1)/2} = (-1)^N. \]

In other cases, we have easily that \( \delta = 1 \). Similarly, \( \delta' = (-1)^N \) if \( \{c\} = \{a + c\} \) and \( \delta' = 1 \) otherwise. Since \( \{a\} = \{a + c\} = \{c\} \) does not hold, the number of \( A \) with \( \{a\} = \{a + c\} \) or \( \{c\} = \{a + c\} \) is equal to \( 2\varphi(N) \), where \( \varphi(x) \) is Euler totient function. Therefore the leading coefficient of the partial product is 1. If \( A \in \mathcal{S}_2 \), then \( c \equiv a, -a \mod N \). Therefore \( \{a\} \neq 0, N/2 \) and \( \{a + c\} = 0 \) or \( \{2a\} \), and if \( N \neq 3 \), then \( \{a\} \neq \{a + c\} \). Proposition 2.2 gives immediately that the leading coefficient of \( \prod_{i=0}^{N-1} \Lambda \circ (AT^i) \) is 1. Hence \( P_{dN}(Y) = 1 \). For \( N = 3 \), a direct calculation in \( \S 6 \) (I) gives that \( P_{dN}(Y) = 1 \). Next we shall prove the assertion (ii). By Theorem 2.3 \( \Lambda^{-1} = \Lambda_{-1} \circ S \), where \( S = \left( \begin{array}{cc} 0 & 1 \\ -1 & 0 \end{array} \right) \). Therefore, \( X^{dN}F(1/X, j) = 0 \) is a minimal equation of \( \Lambda_{-1} \). Further by Theorem 2.3 (v), since \( \Lambda_{-1} = \Lambda_{-1} \), \( F(X, j)_{\sigma^{-1}} = 0 \) is a minimal equation of \( \Lambda_{-1} \). This shows that \( X^{dN}F(1/X, j) = F(X, j) \), and \( P_{dN-i}(Y) = P_{dN}(Y) \) for all \( i \). The assertion (iii) is deduced from the fact that \( \nu(A) > -N/2 \) for all \( A \in \Gamma(1) \) and the \( q \)-expansion of \( j \) has order \( -N \). The assertion (i) is a consequence of Theorem 2.3 (ii). For (iv), see Theorem 4.1 (ii) in \( \S 4 \). \( \square \)

4. Minimal equation of \( j \) over \( K_N(\Lambda) \)

In this section, we shall study some properties of the polynomial \( F(X, Y) \) of \( Y \) with coefficients in \( K_N[X] \). Because the following result can be proved by the almost same argument in section 3 of [2], we outline the proof. We denote by \( X(N) \) the modular curve associated with \( \Gamma(N) \) defined over \( K_N \).

**Theorem 4.1.** Let \( N > 2, \neq 6 \). Put
\[ F(X, Y) = Q_0(X)Y^{\ell_N} + Q_1(X)Y^{\ell_N-1} + \cdots + Q_{\ell_N}(X). \]

(i) \( F(\Lambda, Y) \) is a minimal equation of \( j \) over \( K_N(\Lambda) \). The degree \( \ell_N \) of \( F(X, Y) \) with respect to \( Y \) is equal to \([A(N): K_N(\Lambda)]\).

(ii) Let \( t_N \) be the number of cusps of \( X(N) \) where \( \Lambda \) has poles. Let \( \alpha_k (k = 1, \cdots, d_N-2t_N) \) be cusps of \( X(N) \) where \( \Lambda \) has neither poles nor zeros. Then \( \Lambda(\alpha_k) \in K_N \) and \( Q_0(X) = c(X^{t_N} \prod_k (X - \Lambda(\alpha_k))^N \) for a non-zero constant \( c \in K_N \).
(iii) $Q_{1}(X) = F(X, 0) = c_{1}H_{1}(X)^{3},$ where $H_{1}(X) = \prod_{k=1}^{d_{N}/3}(X - \Lambda(\rho_{k}))$ and $\rho_{k}$ are points on $X(N)$ lying over $\rho = (1 + \sqrt{-3})/2$, and $c_{1}$ is a non-zero constant. Further $H_{1}(0) \neq 0$.

(iv) $F(X, 1728) = c_{2}H_{2}(X)^{2}$, where $H_{2}(X) = \prod_{k=1}^{d_{N}/2}(X - \Lambda(\tau_{k}))$ and $\tau_{k}$ are points on $X(N)$ lying over $i$, and $c_{2}$ is a non-zero constant. Further $H_{2}(0) \neq 0$.

(v) For any complex number $c \neq 0, 1728$, $F(X, c) = 0$ has no multiple roots.

Proof. For (i), see the argument in the latter part of Lemma 3 of [2]. The ramification points of $X(N)/X(1)$ are $\infty, \rho = (1 + \sqrt{-3})/2$ and $i = \sqrt{-1}$ and the ramification index of these points are $N, 3$ and $2$ respectively. See 1.6 of [9]. We know that $j(\rho) = 0, j(i) = 1728$. We note that zero points of $\Lambda$ on $X(N)$ are only cusps and the number of zero points of $\Lambda$ on $X(N)$ is $t_{N}$ by Proposition 3.3. The remaining assertions are obtained from these facts by using the argument in section 3 of [2].

For a positive integer $M$ and a non-negative integer $a$, let

$$I(a, M) = \sum_{k} k,$$

where $k$ runs over all integers such that $0 < k < \frac{M - 3a}{2}, GCD(a, k, M) = 1$.

Proposition 4.2. Let $N > 2, \neq 6$. Then

$$\ell_{N} = I(0, N) + 2 \sum_{0 < a < N/3} I(a, N) + \delta(N).$$

Here $\delta(N) = 3I(0, N/3)$ if $N \equiv 0 \mod 3$ and $\delta(N) = \sum_{k' \equiv -N \mod 3} k'$, where $k'$ runs over integers such that $0 < k' < N/2, GCD(k', N) = 1$ and $k' \equiv -N \mod 3$, if $N \equiv 0 \mod 3$.

Proof. By (i) of Theorem 4.1,

$$\ell_{N} = [A(N) : K_{N}(A)] = - \sum_{\nu(A) < 0, A \in \mathcal{S}} \nu(A).$$

If $A \in \mathcal{S}$ corresponds to $(a, c) \in \Sigma$, then $\nu(A) < 0$ if and only if $\{a\} < \min(\{c\}, \{a + c\})$, and $\nu(A) = \{a\} - \min(\{c\}, \{a + c\})$. Assuming that $0 \leq a < N/2$ and $-N/2 < c \leq N/2$, we shall determine $(a, c) \in \Sigma$ of the condition: $a < \min(\{c\}, \{a + c\})$. For each $a$, we determine $c$ by considering an integer $k = \{c\} - a$. The condition that $a \{c\} \leq N/2$ implies that $0 < k \leq N/2 - a$. If $a = 0$, then $0 < k < N/2$, $GCD(k, N) = 1$ and $\nu(A) = -k$. Let $a > 0$. If $-N/2 < c < 0$, then $c = -(a + k)$. Since $\{a + c\} = k < a + k = \{c\} < N/2$, the condition shows that $a < k < (N - 2a)/2$ and $\nu(A) = a - k$. By substituting $t$ for $k - a$, we have

(1) $0 < t < \frac{N - 4a}{2}$, $GCD(a, t, N) = 1$, $\nu(A) = -t$. 


Let $0 \leq c \leq N/2$. Then $a + c = 2a + k$. If $k \leq (N - 4a)/2$, then $\{c\} < \{a + c\} = 2a + k \leq N/2$ and $\nu(A) = a - \{c\} = -k$. Let $k > (N - 4a)/2$. Then $\{a + c\} = N - (2a + k)$. If $k \leq (N - 3a)/2$, then $\{a + c\} \geq \{c\}$ and $\nu(A) = a - \{c\} = -k$. If $k > (N - 3a)/2$, then $\{c\} > \{a + c\}$. The condition that $\{a + c\} > a$ is equal to that $k < N - 3a$. In this case $\nu(A) = \{a + c\} - a = 3a + k - N$. Therefore putting them together,

\[
\begin{align*}
(2) & \quad 0 < k \leq \frac{N - 3a}{2}, \ GCD(a, k, N) = 1, \nu(A) = -k, \\
(3) & \quad \begin{cases}
\frac{N - 3a}{2} < k \leq \min(N - 3a - 1, \frac{N - 2a}{2}), \ GCD(a, k, N) = 1, \\
\nu(A) = 3a + k - N.
\end{cases}
\end{align*}
\]

In (3), by substituting $t$ for $N - 3a - k$,

\[
\max(1, \frac{N - 4a}{2}) \leq t < \frac{N - 3a}{2}, \nu(A) = -t.
\]

Therefore bringing together (1) and (4),

\[
0 < t < \frac{N - 3a}{2}, \ GCD(a, t, N) = 1, \nu(A) = -t.
\]

Hence

\[
\ell_N = I(0, N) + 2 \sum_{0 < a < N/3} I(a, N) + \delta(N),
\]

where $\delta(N) = \sum_a (N - 3a)/2$, and $a$ runs over all integers such that $0 < a < N/3, a \equiv N \mod 2$ and $\text{GCD}(a, (N - a)/2) = 1$. Let $t = (N - 3a)/2$. Then $\delta(N) = \sum_t t$, where $0 < t < N/2, \text{GCD}(t, N) = \text{GCD}(3, N), t \equiv -N \mod 3$. \hfill \Box

In general, it is not easy to express $\ell_N$ explicitly except the case that $N$ is a prime power.

**Proposition 4.3.** Let $\ell_N$ be the degree of $F(X, Y)$ with respect to $Y$ and $t_N$ the number of cusps of $X(N)$ where $\Lambda$ has a pole.

(i) Let $N = 2^m$, where $m$ is an integer greater than 1. Then

\[
t_N = \frac{3 \cdot 2^{2m-3} - 2^{m-1} - (-1)^m}{3}, \ \ell_N = \frac{2^{3m-4} - (-1)^m}{3}.
\]

(ii) Let $N = 3^m$, where $m$ is a positive integer. If $m = 1$, then $\ell_N = t_N = 1$. If $m \geq 2$, then

\[
t_N = 4 \cdot 3^{2m-3} - 2 \cdot 3^{m-2}, \ \ell_N = 2 \cdot 3^{3m-4}.
\]
Let \( N = p^m \), where \( p \) is a prime number greater than 3 and \( m \) is a positive integer. Then

\[
t_N = \frac{p^{2m} - p^{2m-2} - 2p^m + 2p^{m-1}}{6} + \begin{cases} 
0 & \text{if } p \equiv 1 \mod 3, \\
\frac{1}{3} & \text{if } p \equiv 2 \mod 3, m: \text{odd}, \\
-\frac{1}{3} & \text{if } p \equiv 2 \mod 3, m: \text{even},
\end{cases}
\]

and

\[
\ell_N = \frac{p^{3m} - p^{3m-2}}{36} + \begin{cases} 
\frac{p-1}{9} & \text{if } p \equiv 1 \mod 3, \\
\frac{p+1}{9} & \text{if } p \equiv 2 \mod 3, m: \text{odd}, \\
-\frac{p+1}{9} & \text{if } p \equiv 2 \mod 3, m: \text{even}.
\end{cases}
\]

**Proof.** Let \( N = p^n \) be a prime power. Since \( \gcd(a, k, N) \neq 1 \) if and if \( p \) divides \( a \) and \( b \) at the same time,

\[
\sum_{0 < a < N/3} I(a, N) = \sum_{0 < a < N/3} \left( \sum_{0 < k < \frac{N-3a}{2}} k - p \left( \sum_{0 < a < \frac{N}{3p}} \sum_{0 < k < \frac{(N/p)-3a}{2}} k \right) \right).
\]

The assertions can be obtained from this observation by easy but tedious calculation. We omit details. \( \square \)

Proposition 4.2 implies that \( N \) of \( \ell_N = 1 \) are 3 and 4. On the other hand, the genus of \( X(N) \) is 0 for \( N = 1, 2, 3, 4 \) and 5. Thus for \( N = 3, 4 \), \( \Lambda \) is a generator of \( A(N) \) over \( \mathbb{K}_N \). Since \( \ell_5 = 4 \), \( \Lambda \) is not a generator for \( N = 5 \).

In the cases \( N = 3, 4 \), \( j \) can be expressed in a rational function of \( \Lambda \), thus, \( j = -Q_1(\Lambda)/Q_0(\Lambda) \).

**Remark 4.4.** \( A(1) \) (resp. \( A(2), A(5) \)) is generated by \( j \) (resp. \( \lambda, X_2 \)), where \( X_2 \) is a product of Klein forms similarly defined in 2 for \( p = 5 \).

### 5. Values of \( \Lambda \)

In this section, we summarize the properties of the values of \( \Lambda \).

**Theorem 5.1.** For the value \( \Lambda(\alpha) \) at \( \alpha \in \mathfrak{F} \), we have the following:

(i) If \( \Lambda(\alpha) \) is algebraic, then \( \alpha \) is imaginary quadratic or transcendental.

(ii) If \( \alpha \) is algebraic but is not imaginary quadratic, then \( \Lambda(\alpha) \) is transcendental.

(iii) Let \( \alpha \) be an imaginary quadratic number. Then \( (1 - \zeta)^3 \Lambda(\alpha) \) and \( (1 - \zeta^3/\Lambda(\alpha)) \) are algebraic integers.

(iv) Let \( \alpha \) be an imaginary quadratic number and assume that \( \mathbb{Z}[\alpha] \) is the maximal order of the field \( K = \mathbb{Q}(\alpha) \). Then \( K(\zeta, j(\alpha), \Lambda(\alpha)) \) is the ray class field of \( K \) modulo \( N \) if \( N \neq 6 \).

(v) \( \Lambda(\alpha)^{-1} = \Lambda(\alpha/|\alpha|^2) \). If the absolute value of \( \alpha \) is 1, then the absolute value of \( \Lambda(\alpha) \) is 1.
Corollary 5.2. Let $\Lambda$ be a prime power, then $\Lambda(\mathcal{N})$ is the composition of the composite field of quadratic extensions $K \subset M$. Therefore, $\Lambda(\mathcal{N})$ is a unit. If $N$ is a prime power, then $\Lambda(\alpha)$ is a unit. If $N$ is a prime power, then $\Lambda(\nu)$ is a unit. If $\nu$ is a prime power, then $\Lambda(\nu)$ is a unit.

Remark 5.3. If $N$ is a prime power, then the value of $\Lambda$ is not necessarily integral at an imaginary quadratic number. For example, for $N = 3$, $\Lambda(1 + \sqrt{-3})$ has norm $3^{-3}$ and for $N = 4$, $\Lambda(\sqrt{-2})$ has norm $1/2$. See Example (I), (II) in the last section.

Proposition 5.4. Let $K$ be the imaginary quadratic number field of discriminant $D_K$ and $M$ the Hilbert class field of $K$. Let $N = \prod p_i^{e_i}$ be the prime decomposition of $N$. Put $K_i = \mathbb{Q}(\zeta_{p_i})$. Assume that $K \neq \mathbb{Q}(\sqrt{-1}, \sqrt{-3})$.

(i) If $K$ is contained in one of $K_i$, then
$$[\mathfrak{A}_N : M(\zeta_N)] = N \prod_i \left(1 - \left(\frac{D_K}{p_i}\right) p_i^{-1}\right).$$

(ii) If $K$ is not contained in any $K_i$, then
$$[\mathfrak{A}_N : M(\zeta_N)] = \begin{cases} 2^s N \prod_i \left(1 - \left(\frac{D_K}{p_i}\right) p_i^{-1}\right) & \text{if } K \subset K_N, \\ 2^{s-1} N \prod_i \left(1 - \left(\frac{D_K}{p_i}\right) p_i^{-1}\right) & \text{otherwise}. \end{cases}$$

Here the integer $s$ is defined as follows. Denoting by $r$ the number of odd prime factors of $GCD(D_K, N)$,
$$s = \begin{cases} r + 1 & \text{if } N \equiv 4 \pmod{8}, D_K \equiv 4 \pmod{8}, \\ r + 1 & \text{if } N \equiv 0 \pmod{8}, D_K \equiv 0 \pmod{2}, \\ r & \text{otherwise}. \end{cases}$$

Proof. Let $h_K$ be the class number of $K$. If $K \subset K_i$, then $M \cap K(\zeta_N) = K$. Therefore $[M(\zeta_N) : K] = \varphi(N)h_K/2$. Let $K \not\subset K_i$ for any $i$. Let $L$ be the composite field of quadratic extensions $K \left(\sqrt{(-1)^{\frac{p-1}{2}} p}\right)$ for all odd prime factors $p$ of $GCD(D_K, N)$. By using elementary algebraic number theory, in the cases that $N \equiv 4 \pmod{8}, D_K \equiv 4 \pmod{8}$ and that $N \equiv 0 \pmod{8}, D_K \equiv 0 \pmod{4}$, $M \cap K(\zeta_N) = L(\sqrt{m})$, where $m$ is an integer suitably chosen from $\{-2, -1, 2\}$. In other cases, $M \cap K(\zeta_N) = L$. Therefore
\[ [M \cap K(\zeta_N) : K] = 2^s. \] This shows that \([M(\zeta_N) : K] = \varphi(N)k_K/2^{s+1}\) or \(\varphi(N)k_K/2^s\) according to \(K \subset K_N\) or not. Since

\[
[\mathcal{R}_N : K] = \frac{h_K\varphi(N)}{2}N \prod_{p|N} \left(1 - \left(\frac{D_K}{p}\right)p^{-1}\right),
\]

we have our assertion.

**Corollary 5.5.** Let \(\alpha\) be an imaginary quadratic number and assume that \(\mathbb{Z}[\alpha]\) is the maximal order of the field \(K = \mathbb{Q}(\alpha)\). If \(K \neq \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3})\), then the degree of a minimal equation of \(\Lambda(\alpha)\) over \(K(j(\alpha), \zeta_N)\) is equal to \([\mathcal{R}_N : M(\zeta_N)]\) and it is given in Proposition 5.4.

6. **Examples in the case \(N = 3\) and \(4\)**

Let \(\eta(\tau)\) be the Dedekind eta function. Let \(g_N(\tau) = \eta(\tau)/\eta(N\tau)\). By [3], 
\[ g_N(\tau)_{N = 3,4} \] is a generator of the modular function field of the Hecke group \(\Gamma_0(N)\) for \(N = 3,4\). Let \(X = 0(N)\) be the modular curve associated with \(\Gamma_0(N)\). In this section, for \(N = 3,4\), we give some equations among \(j, \lambda, g_N\) and \(\Lambda\), and compute values of \(\Lambda\) for some imaginary quadratic integers \(\alpha\) such that \(\mathbb{Z}[\alpha]\) is the maximal order of class number one. These values \(\Lambda(\alpha)\) can be obtained from comparing their approximate values with solutions of \(F(X, j(\alpha)) = 0\). The values of \(j\) for such \(\alpha\) are listed in [1] §12 C.

(I) the case \(N = 3\). We have \(d_3 = 12\) and \(\zeta = \rho - 1\).

\[
F(X, 1728) = (X-i+\zeta)^2(X+i+\zeta)^2(X-1+i\zeta)^2(X-1-i\zeta)^2 \times (X-i-i\zeta)^2(X+i+i\zeta)^2.
\]

Since \(g_3^{12} \in A(3)\), \(g_3^{12}\) is a rational function of \(\Lambda\), thus,

\[
g_3^{12} = 81(1-\zeta)\frac{(\Lambda-1)(\Lambda+\zeta)}{\Lambda^3}.
\]

Since \(X(3)\) is totally ramified at the point \(\rho/(\rho+1)\) of \(X_0(3)\) of ramification index 3, this gives the following equation;

\[
(\Lambda g_3^4)^3 + (3\Lambda)^3 = (3(\Lambda + \zeta - 1))^3.
\]

The solutions of the equation \(X^3 + Y^3 = Z^3\) are given by using modular functions \(\Lambda\) and \(g_3\). The values of \(\Lambda\) at \(\alpha = i, \rho\) and \(\sqrt{-2}\) are;

\[
\Lambda(i) = i\rho, \ \Lambda(\rho) = -\rho, \ \Lambda(\sqrt{-2}) = (\sqrt{-3} - \sqrt{-2})\rho.
\]

We remark that the ray class field of \(\mathbb{Q}(\sqrt{-m})\) of conductor 3 is a quadratic extension of \(\mathbb{Q}(\sqrt{-m})\) if \(m \equiv -1 \mod 3\) and it is a cyclic extension of degree 4 otherwise. The values \(v(m)\) of \(\Lambda\) at \(\alpha = (1 + \sqrt{-m})/2\), where
\( m = 3, 7, 11, 19, 43, 67 \) and \( 163 \), are as follows.
The case \( m \equiv -1 \mod 3 \).

\[
v(11) = \sqrt{-3}(-1 + 2\sqrt{-11} - 3\sqrt{-3})/18.
\]

The case \( m \equiv 1 \mod 3 \).

\[
v(m) = \frac{1 + \Omega - \beta \sqrt{3\sqrt{-3}\Omega}}{2},
\]

where

\[
(\beta, \Omega) = \begin{cases} 
(1, (\sqrt{-3} - \sqrt{-7})/2) & \text{if } m = 7, \\
(2, 5\sqrt{-3} - 2\sqrt{-19}) & \text{if } m = 19, \\
(6, 53\sqrt{-3} - 14\sqrt{-43}) & \text{if } m = 43, \\
(14, 293\sqrt{-3} - 62\sqrt{-67}) & \text{if } m = 67, \\
(154, 35573\sqrt{-3} - 4826\sqrt{-163}) & \text{if } m = 163.
\end{cases}
\]

Those values of \( \Lambda \) are units except \( v(11) \). The norm of \( v(11) \) is \( 3^{-3} \).

(II) the case \( N = 4 \). We have \( d_4 = 24 \).

\[
 j = -2^6 \frac{(\Lambda^2 - (1 - 2i)\Lambda - i)(\Lambda^2 - (2 - i)\Lambda - i)(\Lambda^2 - \Lambda + 1)(\Lambda^2 + i\Lambda - 1))^3}{(\Lambda(\Lambda + i)(\Lambda - 1 + i)(\Lambda - \frac{1+i}{2})^4}.
\]

\[
 F(X, 1728) = (X^2 - 2(1 - i)X - i)^2(X^2 + i)^2(X^2 - (1 - i)X - \frac{1 + i}{2})^2 \\
\times (X^2 - (1 - i)X + \frac{1 - i}{2})^2(X^2 + 2iX - 1 - i)(X^2 - 2X + 1 - i)^2.
\]

Since \( \lambda, g_4^8 \in A(4) \), \( \lambda \) and \( g_4^8 \) are rational functions of \( \Lambda \), thus,

\[
 \lambda = 2i \left( \frac{\Lambda - (1 - i)/2}{\Lambda(\Lambda - 1 + i)} \right)^2,
\]

\[
 g_4^8 = -2^6(1 - i) \frac{(\Lambda + i)(\Lambda - 1)(\Lambda + (i - 1)/2)}{\Lambda^4}.
\]

Since \( X(4) \) is totally ramified at the cusp \( 1/2 \) of \( X_0(4) \) of ramification index \( 4 \), the following equation is deduced;

\[
 (\Lambda g_4^4)^4 + (2\Lambda)^4 = (2(\Lambda + 1 - i))^4.
\]

The values \( \Lambda(\alpha) \) at \( \alpha = i, \rho, \sqrt{-2} \) and \( (1 + \sqrt{-7})/2 \) are;

\[
 \Lambda(i) = (i - 1)/\sqrt{-2}, \, \Lambda(\rho) = i(\rho - 1),
\]

\[
 \Lambda(\sqrt{-2}) = (1 - i) \left( 1 - \sqrt{1 + \sqrt{2}} \right)/2,
\]

\[
 \Lambda((1 + \sqrt{-7})/2) = (1 - 3i + (1 + i)\sqrt{-7})/2.
\]

For \( m = 11, 19, 43, 67 \) and \( 163 \), the ray class field of \( \mathbb{Q}(\sqrt{-m}) \) of conductor \( 4 \) is an abelian extension of degree 3 over \( \mathbb{Q}(\sqrt{-m}, i) \) and the value \( \Lambda((1 + \sqrt{-m})/2) \) is a root of the following equation \( EQ(m) \) of degree 3.
The case $m \equiv 11 \mod 16$.

EQ(11):

$$X^3 - \frac{3 + 2i - \sqrt{-11}}{2}X^2 + \frac{7 + 2i + (2i - 1)\sqrt{-11}}{2}X - \frac{3(1 - i) + (1 + i)\sqrt{-11}}{2} = 0,$$

EQ(43):

$$X^3 - \frac{3 + 58i - 9\sqrt{-43}}{2}X^2 + \frac{119 + 58i + 9(2i - 1)\sqrt{-43}}{2}X - \frac{59(1 - i) + 9(1 + i)\sqrt{-43}}{2} = 0$$

The case $m \equiv 3 \mod 16$.

EQ($m$) : $X^3 + \Omega iX^2 + \overline{\Omega}X + i = 0,$

where

$$\Omega = \begin{cases} 
\frac{(3-8i-3\sqrt{-19})}{2} & \text{if } m = 19, \\
\frac{(3-216i-27\sqrt{-67})}{2} & \text{if } m = 67, \\
\frac{(3-8000i-627\sqrt{-163})}{2} & \text{if } m = 163. 
\end{cases}$$

Those values are units except $\Lambda(\sqrt{-2})$ and $\Lambda(\frac{1+i\sqrt{-7}}{2})$. The norm of $\Lambda(\sqrt{-2})$ (resp. $\Lambda(\frac{1+i\sqrt{-7}}{2})$) is $1/2$ (resp. $2^3$).

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] N.Ishida and N.Ishii, The equation for modular function fields of principal congruence subgroups of prime level, Manuscripta Math. 90 (1996), 271-285.

[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, Generalized lambda functions and modular function fields of principal congruence subgroups, Tokyo.J.Math. 37.1 (2014), 237-246.

[5] S.Lang, Elliptic Functions, Addison-Wesley, London, 1973.

[6] M.Newman, Construction and application of a class of modular functions (II), Proc.London Math.Soc.(3) 9 (1959), 373-387.

[7] A.Ogg, Rational points on certain modular elliptic curves, in: Proc.Sympos.Pure Math.24.Amer.Math.Soc.,1973,221-231.

[8] T.Schneider, Arithmetische Untersuchungen elliptischer Integrale, Math.Ann. 113 (1937). 1–13.

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

Current address: 8-155 Shinomiya-Koganezuka Yamashina-ku Kyoto, 607-8022 Japan
E-mail address: Noburo.Ishii@ma2.seikyou.ne.jp