ARITHMETIC OF THE MODULAR FUNCTIONS $j_{1,2}$ AND $j_{1,3}$

CHANG HEON KIM AND JA KYUNG KOO
1. Introduction

Let $\mathcal{H}$ be the complex upper half plane and let $\Gamma_1(N)$ be a congruence subgroup of $SL_2(\mathbb{Z})$ whose elements are congruent to $\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \mod N \ (N = 1, 2, 3, \ldots)$. Since the group $\Gamma_1(N)$ acts on $\mathcal{H}$ by linear fractional transformations, we get the modular curve $X_1(N) = \Gamma_1(N) \backslash \mathcal{H}$, as the projective closure of smooth affine curve $\Gamma_1(N) \backslash \mathcal{H}$, with genus $g_{1, N}$. Since $g_{1, N} = 0$ only for the eleven cases $1 \leq N \leq 10$ and $N = 12$ ([6]), the function field $K(X_1(N))$ of the curve $X_1(N)$ is a rational function field over $\mathbb{C}$ for such $N$.

In this article we shall find the field generators $j_{1, 2}$ and $j_{1, 3}$ as the uniformizers of modular curves $X_1(N)$ when $N = 2$ and $3$, respectively. In §3 $j_{1, 2}$ is constructed by making use of the classical Jacobi theta functions $\theta_2$ and $\theta_4$. Meanwhile in §4 $j_{1, 3}$ is made by the Eisenstein series of weight 4. In §5 we shall estimate the normalized generators $N(j_{1, 2})$ and $N(j_{1, 3})$ which turn out to be the Thompson series of type 2B and 3B, respectively. And, when $\tau \in \mathcal{H} \cap \mathbb{Q}(\sqrt{-d})$ for a square free positive integer $d$, we shall show that $N(j_{1, N})(\tau) \ (N = 2, 3)$ becomes an algebraic integer.

Throughout the article we adopt the following notations:

(1) $\mathcal{H}^*$ the extended complex upper half plane
(2) $\Gamma(N) = \{ \gamma \in SL_2(\mathbb{Z}) \mid \gamma \equiv I \pmod N \}$
(3) $\Gamma_0(N)$ the Hecke subgroup $\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1) \mid c \equiv 0 \pmod N \}$
(4) $\Gamma$ the inhomogeneous group of $\Gamma(= \Gamma/ \pm I)$
(5) $q_h = e^{2\pi i z/h}$, $z \in \mathcal{H}$
(6) $M_k(\Gamma_1(N))$ the space of modular forms of weight $k$ with respect to the group $\Gamma_1(N)$
(7) \( f\left(\begin{array}{cc} a & b \\ c & d \end{array}\right) = f\left(\begin{array}{cc} a & b \\ c & d \end{array}\right) \cdot z \)

(8) \( f\left|_{\left(\begin{array}{cc} a & b \\ c & d \end{array}\right)x}\right. = (ad - bc)^{\frac{k}{2}} \cdot f\left(\begin{array}{cc} a & b \\ c & d \end{array}\right) \cdot (cz + d)^{-k} \)

(9) \( \nu_0(F) \) the sum of orders of zeros of a modular form (or function) \( F \)

2. Fundamental region of \( X_1(N) \)

Let \( \Gamma \) be a congruence subgroup of \( SL_2(\mathbb{Z}) \).

**Definition.** An (open) fundamental region \( R \) for \( \Gamma \) is an open subset of \( \mathbb{H}^* \) with the properties:

1. there do not exist \( \gamma \in \Gamma \) and \( w, z \in R \) for which \( w \neq z \) and \( w = \gamma z \),
2. for any \( z \in \mathbb{H}^* \), there exists \( \gamma \in \Gamma \) such that \( \gamma z \in \overline{R} \) the closure of \( R \).

We will develop some elementary results about fundamental regions, which will give us useful geometric informations about the modular curve \( X_1(N) \). Let \( \Gamma^1(N) \) be a congruence subgroup of \( SL_2(\mathbb{Z}) \) whose elements are congruent to \( \left(\begin{array}{cc} 1 & 0 \\ 0 & 1 \end{array}\right) \mod N \) \((N = 1, 2, 3, \ldots)\). We note that two groups \( \Gamma_1(N) \) and \( \Gamma^1(N) \) are conjugate:

\[
\Gamma^1(N) = \left(\begin{array}{cc} N & 0 \\ 0 & 1 \end{array}\right) \Gamma_1(N) \left(\begin{array}{cc} 1/N & 0 \\ 0 & 1 \end{array}\right).
\]

It turns out that the \( \Gamma^1 \) groups are more convenient than their \( \Gamma_1 \) counterparts in drawing pictures and making geometric computations. Now we will draw fundamental regions using Ferenbaugh’s idea ([4], §3). Suppose \( c, r \in \mathbb{R} \) with \( r > 0 \). Then we define the sets

\[
\begin{align*}
\text{arc}(c, r) &= \{z \in \mathbb{H}^* | |z - c| = r\} \\
\text{inside}(c, r) &= \{z \in \mathbb{H}^* | |z - c| < r\} \\
\text{outside}(c, r) &= \{z \in \mathbb{H}^* | |z - c| > r\}.
\end{align*}
\]

Let \( \gamma = \left(\begin{array}{cc} a & b \\ c & d \end{array}\right) \) be an element of \( \Gamma \), and assume \( c \neq 0 \). Then we define

\[
\begin{align*}
\text{arc}(\gamma) &= \text{arc}(a/c, 1/|c|) \\
\text{inside}(\gamma) &= \text{inside}(a/c, 1/|c|) \quad \text{and} \\
\text{outside}(\gamma) &= \text{outside}(a/c, 1/|c|).
\end{align*}
\]

If \( c = 0 \), \( \gamma \) is of the form \( z \mapsto z + n \) for some integer \( n \). We shall assume \( \gamma \) is not the identity, so \( n \neq 0 \). We then adopt the following conventions: for \( n > 0 \), we define

\[
\begin{align*}
\text{arc}(\gamma) &= \{z \in \mathbb{H}^* | \text{Re}(z) = \frac{n}{2}\} \\
\text{inside}(\gamma) &= \{z \in \mathbb{H}^* | \text{Re}(z) > \frac{n}{2}\} \\
\text{outside}(\gamma) &= \{z \in \mathbb{H}^* | \text{Re}(z) < \frac{n}{2}\}.
\end{align*}
\]
While for $n < 0$, we define “arc” in the same way and reverse the inequalities in the definitions of “inside” and “outside”. Then we have

**Proposition 1.** The element $\gamma \in \Gamma - \{I\}$ sends $\text{arc}(\gamma^{-1})$ to $\text{arc}(\gamma)$, $\text{inside}(\gamma^{-1})$ to $\text{outside}(\gamma)$ and $\text{outside}(\gamma^{-1})$ to $\text{inside}(\gamma)$.

*Proof.* [4], Proposition 3.1. 

**Theorem 2.** With definitions as above, a fundamental region $R$ for $\Gamma$ is given by

$$R = \bigcap_{\gamma \in \Gamma - \{I\}} \text{outside}(\gamma).$$

*Proof.* [4], Theorem 3.3. 

Now the following theorem allows us to get the generators of the group $\Gamma$.

**Theorem 3.** Let $\Gamma$ be a congruence subgroup of $\Gamma(1)$ of finite index and $R$ be a fundamental region for $\Gamma$. Then the sides of $R$ can be grouped into pairs $\lambda_i, \lambda'_i$ ($i = 1, 2, \ldots, s$) in such a way that $\lambda_i \subseteq \overline{R}$ and $\lambda'_i = \gamma_i \lambda_i$ where $\gamma_i \in \Gamma$ ($i = 1, 2, \ldots, s$). $\gamma_i$’s are called boundary substitutions of $R$. Furthermore, $\Gamma$ is generated by the boundary substitutions $\gamma_1, \ldots, \gamma_s$.

*Proof.* [13], Theorem 2.4.4 (or [7], Theorem 1). 

### 3. Modular function $j_{1,2}$

Let us take $\Gamma = \Gamma^1(2)$. Put

$$\gamma_1 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \gamma_2 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$ 

If $R_2$ is a fundamental region of $\Gamma^1(2)$, then by Theorem 2

$$R_2 = \bigcap_{i=1}^2 \text{outside}(\gamma_i^{\pm 1})$$

and its figure is as follows.

We denote by $S_\Gamma$ the set of inequivalent cusps of $\Gamma$. Then as in the above figure $S_{\Gamma^1(2)} = \{\infty, 0\}$. Furthermore it follows from Theorem 3 that $\Gamma^1(2)$ is generated by $\gamma_1$ and $\gamma_2$. Thus we obtain the following theorem by (1).
Theorem 4. (i) $S_{\Gamma_1(2)} = \{\infty, 0\}$. All cusps of $\Gamma_1(2)$ are regular ([11], [16]).

(ii) $\Gamma_1(2)$ is generated by $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$.

For later use we are in need of calculating the widths of the cusps of $\Gamma_1(2)$.

Lemma 5. Let $a/c \in \mathbb{P}^1(\mathbb{Q})$ be a cusp with $(a, c) = 1$. Then the width of $a/c$ in $X_1(N)$ is given by $N/(c, N)$ if $N \neq 4$.

Proof. [8], Lemma 3. □

We then have the following table of inequivalent cusps of $\Gamma_1(2)$:

<table>
<thead>
<tr>
<th>cusp</th>
<th>width</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\infty$</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>2</td>
</tr>
</tbody>
</table>

Now, we recall the Jacobi theta functions $\theta_2, \theta_3, \theta_4$ defined by

\[
\theta_2(z) = \sum_{n \in \mathbb{Z}} q_{2}^{(n+\frac{1}{2})^2}
\]

\[
\theta_3(z) = \sum_{n \in \mathbb{Z}} q_{2}^{n^2}
\]

\[
\theta_4(z) = \sum_{n \in \mathbb{Z}} (-1)^n q_{2}^{n^2}
\]
for \( z \in \mathbb{F} \). Here we list the following useful transformation formulas ([13] pp.218–219).

\[
\begin{align*}
\theta_2(z+1) &= e^{rac{i}{4} \pi i} \theta_2(z) \\
\theta_3(z+1) &= \theta_4(z) \\
\theta_4(z+1) &= \theta_3(z) \\
\theta_2 \left( -\frac{1}{z} \right) &= (-iz)^{\frac{1}{2}} \theta_4(z) \\
\theta_3 \left( -\frac{1}{z} \right) &= (-iz)^{\frac{1}{2}} \theta_3(z) \\
\theta_4 \left( -\frac{1}{z} \right) &= (-iz)^{\frac{1}{2}} \theta_2(z).
\end{align*}
\]

Put \( j_{1,2}(z) = \theta_2(z)^8/\theta_4(2z)^8 \). Then we obtain the following theorem.

**Theorem 6.** (i) \( \theta_2(z)^8, \theta_4(2z)^8 \in M_4(\Gamma_1(2)) \).

(ii) \( K(X_1(2)) = \mathbb{C}(j_{1,2}(z)) \) and \( j_{1,2}(\infty) = 0 \) (simple zero), \( j_{1,2}(0) = \infty \) (simple pole).

**Proof.** For the first part, we must check the invariance of slash operator and the cusp conditions. Let \( T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \) and \( S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \). Since \( T \) and \( ST^2S \) generate \( \Gamma_1(2) \) by Theorem 4-(ii), it is enough to check the invariance for these generators.

\[
\begin{align*}
\theta_2(z)^8|_{[T]_4} &= \theta_2(z+1)^8 \\
&= \left( e^{rac{i}{4} \pi i} \theta_2(z) \right)^8 \text{ by (2)} \\
&= \theta_2(z)^8 \\
\theta_2(z)^8|_{[S]_4} &= z^{-4} \theta_2 \left( -\frac{1}{z} \right)^8 \\
&= z^{-4} \left( (-iz)^{\frac{1}{2}} \theta_4(z) \right)^8 \text{ by (5)} \\
&= \theta_4(z)^8 \\
\theta_2(z)^8|_{[ST^2]_4} &= \theta_4(z)^8 |_{[T^2]_4} \\
&= \theta_4(z)^8 \text{ by (3) and (4)} \\
\theta_2(z)^8|_{[ST^2S]_4} &= \theta_4(z)^8 |_{[S]_4} \\
&= z^{-4} \left( (-iz)^{\frac{1}{2}} \theta_2(z) \right)^8 \text{ by (7)} \\
&= \theta_2(z)^8
\end{align*}
\]
\[ \theta_4(2z)^8 \mid |T_4| = \theta_4(2z + 2)^8 \]
\[ = \theta_4(2z)^8 \text{ by (3) and (4)} \]
\[ \theta_4(2z)^8 \mid |S_4| = z^{-4} \theta_4 \left( -\frac{2}{z} \right)^8 \]
\[ = z^{-4} \left\{ \left( -\frac{iz}{2} \right)^{\frac{1}{2}} \theta_2 \left( \frac{z}{2} \right) \right\}^8 \text{ by (7)} \]
\[ = \frac{1}{16} \theta_2 \left( \frac{z}{2} \right)^8 \]
\[ \theta_4(2z)^8 \mid |S^2| = \frac{1}{16} \theta_2 \left( \frac{z}{2} \right)^8 \mid |T_4|, \]
\[ = \frac{1}{16} \theta_2 \left( \frac{z}{2} \right)^8 \text{ by (2)} \]
\[ \theta_4(2z)^8 \mid |S^2S_4| = \frac{1}{16} \theta_2 \left( \frac{z}{2} \right)^8 \mid |S_4|, \]
\[ = \frac{1}{16} z^{-4} \{ (-2iz)^{\frac{1}{2}} \theta_4(2z) \}^8 \text{ by (5)} \]
\[ = \theta_4(2z)^8. \]

Now we’ll check the boundary conditions.

(i) \( s = \infty \):

Since \( \theta_2(z) = 2q_8(1 + q + q^3 + \cdots), \theta_2(z)^8 = 2^8 q(1 + q + q^3 + \cdots)^8 \). Hence \( \theta_2(z)^8 \) has a simple zero at \( s = \infty \). On the other hand, \( \theta_4(2z)^8 = \left( \sum_{n \in \mathbb{Z}} (-1)^n q^{n^2} \right)^8 = (1 - 2q + 2q^4 - 2q^9 + \cdots)^8 \). Thus \( \theta_4(2z)^8 \mid s = \infty = 1 \).

(ii) \( s = 0 \):

\[ \theta_2(z)^8 \mid s = 0 = \lim_{z \to i \infty} \theta_2(z)^8 \mid |S_4| \]
\[ = \lim_{z \to i \infty} \theta_4(z)^8 \text{ by (8)} \]
\[ = 1 \]

and

\[ \theta_4(2z)^8 \mid s = 0 = \lim_{z \to i \infty} \theta_4(2z)^8 \mid |S_4| \]
\[ = \lim_{z \to i \infty} \frac{1}{16} \theta_2 \left( \frac{z}{2} \right)^8 \text{ by (9)} \]
\[ = \lim_{z \to i \infty} \frac{1}{16} \cdot 2^8 q(1 + q + q^3 + \cdots)^8 \]
\[ = 0. \text{ (a simple zero)} \]

Now, we’ll prove the second part. From the well-known formula ([16], p.39) concerning the sum of orders of zeros of modular forms, it follows that

\[ \nu_0(\theta_2(z)^8) = \nu_0(\theta_4(2z)^8) = 1. \]
Hence $\theta_2(z)^8$ (resp. $\theta_4(2z)^8$) has no other zeros in $X_1(2)$ except at $s = \infty$ (resp. $s = 0$). Therefore $[K(X_1(4)): \mathbb{C}(j_{1,2}(z))] = \nu_0(j_{1,2}(z)) = 1$, and so (ii) follows.

4. Modular function $j_{1,3}$

Now let us take $\Gamma = \pm \Gamma_1(3)$, and put $\gamma_1 = \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix}$ and $\gamma_2 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$. Let $R_3$ be a fundamental region of $\Gamma_1(3)$. Then it is given by

$$R_3 = \bigcap_{i=1}^{2} \text{outside}(\gamma_i^{\pm 1})$$

with the following figure.

As is seen in the above figure $S_{\Gamma_1(3)} = \{\infty, 0\}$. Hence it follows from Theorem 3 that $\Gamma_1(3)$ is generated by $\gamma_1$ and $\gamma_2$. And we obtain the following theorem by (1).

**Theorem 7.**

(i) $S_{\Gamma_1(3)} = \{\infty, 0\}$. All cusps of $\Gamma_1(3)$ are regular ([11], [16]).

(ii) $\Gamma_1(3)$ is generated by $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ 3 & 1 \end{pmatrix}$.

By Lemma 5 we have the following table of inequivalent cusps of $\Gamma_1(3)$:

<table>
<thead>
<tr>
<th>Cusp</th>
<th>$\infty$</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Width</td>
<td>1</td>
<td>3</td>
</tr>
</tbody>
</table>
Let $E_4(z)$ be the normalized Eisenstein series of weight 4 defined by

$$E_4(z) = \frac{1}{2\zeta(4)} \sum_{m,n \in \mathbb{Z}, m,n \neq 0} \frac{1}{(mz+n)^4}, \; z \in \mathbb{H}$$

where the summation runs over pairs of integers $m, n$ not both zero, and $\zeta(s)$ denotes the Riemann zeta function for $s \in \mathbb{C}$. Then it has the following $q$-expansion ([9], p.111):

$$E_4(z) = 1 + 240 \sum_{n=0}^{\infty} \sigma_3(n) q^n, \; z \in \mathbb{H}.$$  \tag{10}

Put $j_{1,3}(z) = E_4(z)/E_4(3z)$.

**Theorem 8.** We have

(i) $j_{1,3}(z) \in K(X_1(3))$ and $j_{1,3}(\infty) = 1, \; j_{1,3}(0) = 81$.

(ii) $K(X_1(3)) = \mathbb{C}(j_{1,3}(z))$.

**Proof.** It is well known ([9], p.110 or [16], pp.32-33) that $E_4(z)$ is the modular form of weight 4 with respect to the full modular group $\Gamma(1)$. Hence $E_4$ satisfies $E_4(z+1) = E_4(z)$ and $E_4(z^{-1}) = z^4 E_4(z)$ for each $z \in \mathbb{H}$. We observe that

$$\left( \begin{array}{cc} 3 & 0 \\ 0 & 1 \end{array} \right)^{-1} \Gamma(1) \left( \begin{array}{cc} 3 & 0 \\ 0 & 1 \end{array} \right) \cap \Gamma(1) = \Gamma_0(3) = \pm \Gamma_1(3).$$

This implies that $E_4(z) \in M_4(\Gamma_1(3))$. Thus

$$j_{1,3}(z) = E_4(z)/E_4(3z) \in K(X_1(3)).$$

From (10) it follows that $j_{1,3}(\infty) = 1$. And

$$j_{1,3}(0) = \lim_{z \to i\infty} j_{1,3} \left( \begin{array}{cc} 0 & -1 \\ 1 & 0 \end{array} \right) = \lim_{z \to i\infty} j_{1,3} \left( \begin{array}{cc} -1/z \\ 1 \end{array} \right) = \frac{E_4(-1/z)}{E_4(-3/z)} = \left(\frac{z}{3}\right)^4 \frac{E_4(z)}{E_4(\frac{z}{3})} = \lim_{z \to i\infty} 81 \cdot \frac{1 + 240(q + 9q^2 + \cdots)}{1 + 240(q_3 + 9q_3^2 + \cdots)} = 81.$$

Now we consider (ii). From the zero formula we get that $\nu_0(F) = \frac{4}{3}$ for any $F \in M_4(\Gamma_1(3))$. And $\nu_0(E_4(z)) = \nu_0(E_4(3z)) = \frac{4}{3}$ so that

$$\nu_0(j_{1,3}) \leq \frac{4}{3}.$$  \tag{11}

Since $j_{1,3}$ is not a constant function, we have

$$[K(X_1(3)) : \mathbb{C}(j_{1,3})] = \nu_0(j_{1,3}),$$

which is an integer greater than or equal to 1. By (11) it must be 1. This proves (ii). \qed
5. Some remarks on Thompson series

For a modular function \( f \), we call \( f \) normalized if its \( q \)-series is

\[
\frac{1}{q} + 0 + a_1q + a_2q^2 + \cdots.
\]

**Lemma 9.** The normalized generator of a genus zero function field is unique.

**Proof.** [7], Lemma 8. □

Let \( \mathcal{F} \) be the set of functions \( f(z) \) satisfying the following conditions:

(i) \( f(z) \in K(X(\Gamma)) \) for some discrete subgroup \( \Gamma \) of \( SL_2(\mathbb{R}) \) that contains \( \Gamma_0(N) \) for some \( N \).

(ii) The genus of the curve \( X(\Gamma) \) is 0 and its function field \( K(X(\Gamma)) \) is equal to \( \mathbb{C} \).

(iii) In a neighborhood of \( \infty \), \( f(z) \) is expressed in the form

\[
f(z) = \frac{1}{q} + \sum_{n=0}^{\infty} a_n q^n, \quad a_n \in \mathbb{C}.
\]

We say that a pair \((G, \phi)\) is a “moonshine” for a finite group \( G \) if \( \phi \) is a function from \( G \) to \( \mathcal{F} \) and the mapping \( \sigma \rightarrow a_n(\sigma) \) from \( G \) to \( \mathbb{C} \) is a generalized character of \( G \) when \( \phi_\sigma(z) = \frac{1}{q} + a_0(\sigma) + \sum_{n=1}^{\infty} a_n(\sigma)q^n \) for \( \sigma \in G \). In particular, \( \phi_\sigma \) is a class function of \( G \).

Finding or constructing a “moonshine” \((G, \phi)\) for a given group \( G \), however, involves some nontrivial work. It is because that for each element \( \sigma \) of \( G \), we have to find a natural number \( N \) and a Fuchsian group \( \Gamma \) containing \( \Gamma_0(N) \) in such a way that its function field \( K(X(\Gamma)) \) is equal to \( \mathbb{C}(\phi_\sigma) \) and the coefficients \( a_n(\sigma) \) in the expansion of \( \phi_\sigma(z) \) at \( \infty \) induce generalized characters for all \( n \geq 1 \).

Let \( j \) be the modular invariant of \( \Gamma(1) \) whose \( q \)-series is

\[
j = q^{-1} + 744 + 196884q + \cdots = \sum_r c_r q^r.
\]

Then \( j - 744 \) is the normalized generator of \( \Gamma(1) \). Let \( M \) be the monster simple group of order approximately \( 8 \times 10^{53} \). Thompson proposed that the coefficients in the \( q \)-series for \( j - 744 \) be replaced by the representations of \( M \) so that we obtain a formal series

\[
H_{-1} q^{-1} + 0 + H_1 q + H_2 q^2 + \cdots
\]

in which the \( H_r \) are certain representations of \( M \) called **head representations**. \( H_r \) has degree \( c_r \) as in (12), for example, \( H_{-1} \) is the trivial representation (degree 1), while \( H_1 \) is the sum of this and the degree 196883 representation and \( H_2 \) is the sum of former two and the degree 21296876 representation ([18]). The following theorem conjectured by Thompson ([2]) and proved by Borcherds ([1]) shows that there exists a “moonshine” for the monster group \( M \).
Theorem 10. The series

\[ T_m = \frac{1}{q} + 0 + H_1(m)q + H_2(m)q^2 + \cdots \]

is the normalized generator of a genus zero function field arising from a group between \( \Gamma_0(N) \) and its normalizer in \( \text{PSL}_2(\mathbb{R}) \), where \( m \) is an element of \( M \) and \( H_r(m) \) is the character value of head representation \( H_r \) at \( m \).

We will construct such a normalized generator (or the Hauptmodul) of the function field \( K(X_1(N)) \) \((N = 2, 3)\) from the modular function \( j_{1,N} \) mentioned in Theorem 6 and Theorem 8.

\[
\frac{2^8}{j_{1,2}} = \frac{\theta_4(2z)^8}{\theta_2(z)^8} = \frac{2^8(1 - 2q + 2q^4 - 2q^9 + \cdots)^8}{(2q_8(1 + q + q^3 + \cdots))^8} = \frac{1}{q} - 24 + 276q - 2048q^2 + 11202q^3 - 49152q^4 + 184024q^5 + \cdots ,
\]

which is in \( q^{-1}\mathbb{Z}[[q]] \). Let \( N(j_{1,2}) = \frac{2^4}{j_{1,2}} + 24 \). In the case of the modular function \( j_{1,3} \), we consider

\[
\frac{240}{j_{1,3} - 1} = \frac{240}{E_4(3z)} = \frac{240(1 + 240(q^3 + 9q^6 + 28q^9 + 73q^{12} + \cdots))}{240(q + 9q^2 + 27q^3 + 73q^4 + 126q^5 + \cdots)} = \frac{1}{q} - 9 + 54q - 76q^2 - 243q^3 + 1188q^4 - 1384q^5 + \cdots ,
\]

which is also in \( q^{-1}\mathbb{Z}[[q]] \). Let \( N(j_{1,3}) = \frac{240}{j_{1,3} - 1} + 9 \). Then the above computations show that \( N(j_{1,2}) \) and \( N(j_{1,3}) \) are the normalized generators of \( K(X_1(2)) \) and \( K(X_1(3)) \), respectively. On the other hand by observing \( \Gamma_0(2) = \Gamma_1(2) \) and \( \Gamma_0(3) = \Gamma_1(3) \), we can get the normalized generators using \( \eta \)-functions (p.57 in [5] or Table 3 in [2]). Since the normalized generator is unique (Lemma 9) we get the following identities after adjusting the constant terms.

\[
\frac{2^8}{\theta_4(2z)^8} = \frac{\eta(z)^{24}}{\eta(2z)^{24}}
\]

and

\[
\frac{240}{E_4(3z)} = \frac{\eta(z)^{12}}{\eta(3z)^{12}} + 3.
\]

By Table 3 in [2] and Theorem 10, \( N(j_{1,2}) \) (resp. \( N(j_{1,3}) \)) corresponds to the Thompson series of type 2B (resp. type 3B). By Theorem 6-(ii) and 8-(ii) we have the following tables:
Table 3. Cusp values of $N(j_{1,2})$

<table>
<thead>
<tr>
<th>$s$</th>
<th>$\infty$</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>$N(j_{1,2})(s)$</td>
<td>$\infty$</td>
<td>24</td>
</tr>
</tbody>
</table>

Table 4. Cusp values of $N(j_{1,3})$

<table>
<thead>
<tr>
<th>$s$</th>
<th>$\infty$</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>$N(j_{1,3})(s)$</td>
<td>$\infty$</td>
<td>12</td>
</tr>
</tbody>
</table>

Lemma 11. Let $N$ be a positive integer such that the modular curve $X_1(N)$ is of genus 0. Let $t$ be an element of $K(X_1(N))$ for which (i) $K(X_1(N)) = \mathbb{C}(t)$ and (ii) $t$ has no poles except for a simple pole at one cusp $s$. Let $f \in K(X_1(N))$. If $f$ has a pole of order $n$ only at $s$, then $f$ can be written as a polynomial in $t$ of degree $n$.

Proof. Take $\gamma \in SL_2(\mathbb{Z})$ such that $\gamma \infty = s$. Let $h$ be the width of $s$. Then we have

$t|_\gamma = \frac{1}{c} \frac{1}{q_h} + \cdots$

and

$f|_\gamma = b_n \frac{1}{q_h^n} + \cdots$

for some $c \neq 0$ and $b_n \neq 0$. Thus

$(f - b_n(ct)^n)|_\gamma = \lambda_{n-1} \frac{1}{q_h^{n-1}} + \cdots$

for some $\lambda_{n-1}$. And

$(f - b_n(ct)^n - \lambda_{n-1}(ct)^{n-1})|_\gamma = \lambda_{n-2} \frac{1}{q_h^{n-2}} + \cdots$

for some $\lambda_{n-2}$. In this way we can choose $\lambda_i \in \mathbb{C}$ such that

$(f - b_n(ct)^n - \lambda_{n-1}(ct)^{n-1} - \cdots - \lambda_1(ct))|_\gamma \in \mathbb{C}[q_h]]$.

Let $g = f - b_n(ct)^n - \lambda_{n-1}(ct)^{n-1} - \cdots - \lambda_1(ct)$. Then $g$ has no poles in $\mathbb{H}^*$, and so $g$ must be a constant, say $\lambda_0$. Therefore we end up with $f = b_nct^n + \lambda_{n-1}ct^{n-1} + \cdots + \lambda_1ct + \lambda_0$, as desired. \qed

Theorem 12. Let $d$ be a square free positive integer and $t$ be the Hauptmodul $N(j_{1,N})$, $(N = 2, 3)$. For $\tau \in \mathbb{Q}(\sqrt{-d}) \cap \mathbb{H}$, $t(\tau)$ is an algebraic integer.

Proof. Let $j(z) = \frac{1}{q} + 744 + 196884q + \cdots$. It is well-known that $j(\tau)$ is an algebraic integer for $\tau \in \mathbb{Q}(\sqrt{-d}) \cap \mathbb{H}$ ([10], [16]). For algebraic proofs, see [3], [12], [15] and [17]. Now, we view $j$ as a function on the modular curve $X_1(N)$. Let $s$ be a cusp of $\Gamma_1(N)$ other than $\infty$, whose width is $h_s$. Then $j$ has a pole
of order \( h_s \) at the cusp \( s \). On the other hand, \( t(z) - t(s) \) has a simple zero at \( s \). Thus

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

has a pole only at \( \infty \) whose degree is 3 if \( N = 2 \), and 4 if \( N = 3 \). And so by Lemma 11, it is a monic polynomial in \( t \) of degree 3 or 4 according as \( N = 2 \) or 3, which we denote by \( f(t) \). With the aid of Table 1, we can compute the product part in the above more explicitly, that is,

\[ \prod_{s \in S_{\Gamma_1(N)} \setminus \{\infty\}} (t(z) - t(s))^{h_s} = \begin{cases} (t - 24)^2, & \text{if } N = 2 \\ (t - 12)^3, & \text{if } N = 3. \end{cases} \]

Since \( j \) and \( t \) have integer coefficients in the \( q \)-expansions, \( f(t) \) is a monic polynomial in \( \mathbb{Z}[t] \) of degree 3 or 4 according as \( N = 2 \) or 3. This claims that \( t(\tau) \) is integral over \( \mathbb{Z} \). Therefore \( t(\tau) \) is integral over \( \mathbb{Z} \) for \( \tau \in \mathbb{Q}(\sqrt{-d}) \cap \mathbb{H} \).

\[ \square \]

References


Chang Heon Kim  
Department of Mathematics  
Seoul Women's University  
Seoul 139-774, Korea  
E-mail address: chkim@swu.ac.kr

Ja Kyung Koo  
Korea Advanced Institute of Science and Technology  
Department of Mathematics  
Taejon 305-701, Korea  
E-mail address: jkko@math.kaist.ac.kr