Bull. Korean Math. Soc. **44** (2007), No. 1, pp. 47–59

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

Chang Heon Kim and Ja Kyung Koo

Abstract. We find the uniformizers of modular curves $X_1(N)$ $(N = 2, 3)$ and explore the relationship with Thompson series and number theoretic property.

1. Introduction

Let $\mathfrak{H}$ 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 $\mathfrak{H}$ by linear fractional transformations, we get the modular curve $X_1(N) = \Gamma_1(N)\backslash\mathfrak{H}^*$, as the projective closure of smooth affine curve $\Gamma_1(N)\backslash\mathfrak{H}$, with genus $g_{1,N}$. Since $g_{1,N} = 0$ only for the eleven cases $1 \le N \le 10$ 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 θ_2 and θ_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 $\tau \in \mathfrak{H} \cap \mathbb{Q}(\sqrt{-d})$ 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) $\mathfrak{H}^*$ the extended complex upper half plane
(2) $\Gamma(N) = \{\gamma \in SL_2(\mathbb{Z}) \mid \gamma \equiv I \mod N\}$
(3) $\Gamma_0(N)$ the Hecke subgroup $\{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma(1) \mid c \equiv 0 \mod N\}$
(4) $\overline{\Gamma}$ the inhomogeneous group of $\Gamma (= \Gamma/\pm I)$
(5) $q_h = e^{2\pi i z/h}$, $z \in \mathfrak{H}$
(6) $M_k(\Gamma_1(N))$ the space of modular forms of weight k with respect to the group $\Gamma_1(N)$

Received August 26, 2005.
2000 *Mathematics Subject Classification.* 11F03, 11F06, 11F11.
Key words and phrases. modular curve, uniformizer, normalized generator, Thompson series.

(7) $f|_{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)} = f(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \cdot z)$

(8) $f|_{[\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)]_k} = (ad - bc)^{\frac{k}{2}} \cdot f(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \cdot z) \cdot (cz + d)^{-k}$

(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 Γ be a congruence subgroup of $SL_2(\mathbb{Z})$.

Definition. An (*open*) *fundamental region* R for Γ is an open subset of $\mathfrak{H}^*$ 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 $z \in \mathfrak{H}^*$, 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 $\left(\begin{smallmatrix} 1 & 0 \\ * & 1 \end{smallmatrix}\right)$ mod N $(N = 1, 2, 3, \ldots)$. We note that two groups $\Gamma_1(N)$ and $\Gamma^1(N)$ are conjugate:

$$\Gamma^1(N) = \begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix} \Gamma_1(N) \begin{pmatrix} 1/N & 0 \\ 0 & 1 \end{pmatrix}. \tag{1}$$

It turns out that the Γ^1 groups are more convenient than their Γ_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

$$\begin{aligned} \operatorname{arc}(c, r) &= \{z \in \mathfrak{H}^* |\ |z - c| = r\} \\ \operatorname{inside}(c, r) &= \{z \in \mathfrak{H}^* |\ |z - c| < r\} \\ \operatorname{outside}(c, r) &= \{z \in \mathfrak{H}^* |\ |z - c| > r\}. \end{aligned}$$

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

$$\begin{aligned} \operatorname{arc}(\gamma) &= \operatorname{arc}(a/c, 1/|c|), \\ \operatorname{inside}(\gamma) &= \operatorname{inside}(a/c, 1/|c|) \quad \text{and} \\ \operatorname{outside}(\gamma) &= \operatorname{outside}(a/c, 1/|c|). \end{aligned}$$

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

$$\begin{aligned} \operatorname{arc}(\gamma) &= \left\{z \in \mathfrak{H}^* |\ \operatorname{Re}(z) = \frac{n}{2}\right\} \\ \operatorname{inside}(\gamma) &= \left\{z \in \mathfrak{H}^* |\ \operatorname{Re}(z) > \frac{n}{2}\right\} \\ \operatorname{outside}(\gamma) &= \left\{z \in \mathfrak{H}^* |\ \operatorname{Re}(z) < \frac{n}{2}\right\}. \end{aligned}$$

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* $\mathrm{arc}(\gamma^{-1})$ *to* $\mathrm{arc}(\gamma)$, $\mathrm{inside}(\gamma^{-1})$ *to* $\mathrm{outside}(\gamma)$ *and* $\mathrm{outside}(\gamma^{-1})$ *to* $\mathrm{inside}(\gamma)$.

Proof. [4], Proposition 3.1. □

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

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

Proof. [4], Theorem 3.3. □

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

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

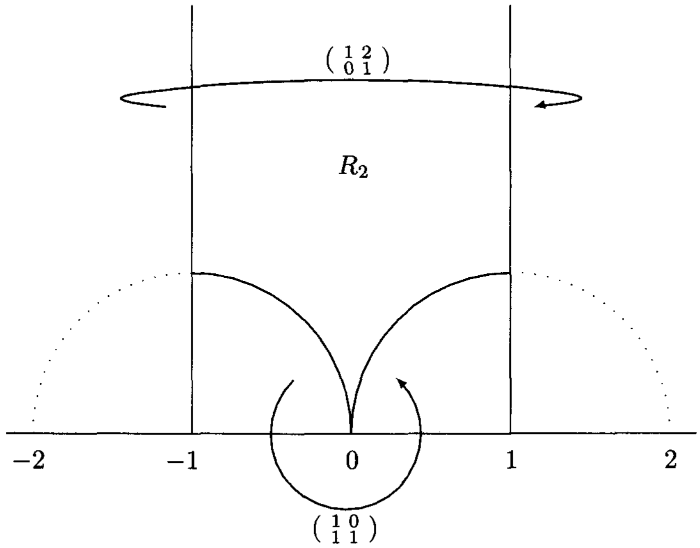
$$\gamma_1 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \gamma_2 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

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

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

and its figure is as follows.

We denote by S_Γ the set of inequivalent cusps of Γ. Then as in the above figure $S_{\Gamma^1(2)} = \{\infty, 0\}$. Furthermore it follows from Theorem 3 that $\overline{\Gamma}^1(2)$ is generated by γ_1 and γ_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) $\overline{\Gamma}_1(2)$ *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 1. Cusps of $\Gamma_1(2)$

cusp	∞	0
width	1	2

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 $z \in \mathfrak{H}$. Here we list the following useful transformation formulas ([13] pp.218–219).

$$\theta_2(z+1) = e^{\frac{1}{4}\pi i}\theta_2(z) \tag{2}$$

$$\theta_3(z+1) = \theta_4(z) \tag{3}$$

$$\theta_4(z+1) = \theta_3(z) \tag{4}$$

$$\theta_2\left(-\frac{1}{z}\right) = (-iz)^{\frac{1}{2}}\theta_4(z) \tag{5}$$

$$\theta_3\left(-\frac{1}{z}\right) = (-iz)^{\frac{1}{2}}\theta_3(z) \tag{6}$$

$$\theta_4\left(-\frac{1}{z}\right) = (-iz)^{\frac{1}{2}}\theta_2(z). \tag{7}$$

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 $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$. Since T and ST^2S generate $\overline{\Gamma}_1(2)$ by Theorem 4-(ii), it is enough to check the invariance for these generators.

$$\begin{aligned}
\theta_2(z)^8|_{[T]_4} &= \theta_2(z+1)^8 \\
&= (e^{\frac{\pi i}{4}}\theta_2(z))^8 \quad \text{by (2)} \\
&= \theta_2(z)^8 \\
\theta_2(z)^8|_{[S]_4} &= z^{-4}\theta_2\left(-\frac{1}{z}\right)^8 \\
&= z^{-4}\{(-iz)^{\frac{1}{2}}\,\theta_4\,(z)\}^8 \quad \text{by (5)} \\
&= \theta_4\,(z)^8 \\
\theta_2(z)^8|_{[ST^2]_4} &= \theta_4\,(z)^8\,|_{[T^2]_4} \\
&= \theta_4\,(z)^8 \quad \text{by (3) and (4)} \\
\theta_2(z)^8|_{[ST^2S]_4} &= \theta_4\,(z)^8\,|_{[S]_4} \\
&= z^{-4}\{(-iz)^{\frac{1}{2}}\theta_2(z)\}^8 \quad \text{by (7)} \\
&= \theta_2(z)^8
\end{aligned} \tag{8}$$

$$\begin{aligned}
\theta_4(2z)^8|_{[T]_4} &= \theta_4(2z+2)^8 \\
&= \theta_4(2z)^8 \quad \text{by (3) and (4)} \\
\theta_4(2z)^8|_{[S]_4} &= z^{-4}\theta_4\left(-\frac{2}{z}\right)^8 \\
&= z^{-4}\left\{\left(-\frac{iz}{2}\right)^{\frac{1}{2}}\theta_2\left(\frac{z}{2}\right)\right\}^8 \quad \text{by (7)} \qquad (9)\\
&= \frac{1}{16}\theta_2\left(\frac{z}{2}\right)^8 \\
\theta_4(2z)^8|_{[ST^2]_4} &= \frac{1}{16}\theta_2\left(\frac{z}{2}\right)^8|_{[T^2]_4} \\
&= \frac{1}{16}\theta_2\left(\frac{z}{2}\right)^8 \quad \text{by (2)} \\
\theta_4(2z)^8|_{[ST^2S]_4} &= \frac{1}{16}\theta_2\left(\frac{z}{2}\right)^8|_{[S]_4} \\
&= \frac{1}{16}z^{-4}\{(-2iz)^{\frac{1}{2}}\theta_4(2z)\}^8 \quad \text{by (5)} \\
&= \theta_4(2z)^8.
\end{aligned}$$

Now we'll check the boundary conditions.
(i) $s=\infty$:

Since $\theta_2(z) = 2q_8(1+q+q^3+\cdots)$, $\theta_2(z)^8 = 2^8q(1+q+q^3+\cdots)^8$. Hence $\theta_2(z)^8$ has a simple zero at $s=\infty$. On the other hand, $\theta_4(2z)^8 = (\sum_{n\in\mathbb{Z}}(-1)^nq^{n^2})^8 = (1-2q+2q^4-2q^9+\cdots)^8$. Thus $\theta_4(2z)^8|_{s=\infty}=1$.
(ii) $s=0$:

$$\begin{aligned}
\theta_2(z)^8|_{s=0} &= \lim_{z\to i\infty}\theta_2(z)^8|_{[S]_4} \\
&= \lim_{z\to i\infty}\theta_4(z)^8 \quad \text{by (8)} \\
&= 1
\end{aligned}$$

and

$$\begin{aligned}
\theta_4(2z)^8|_{s=0} &= \lim_{z\to i\infty}\theta_4(2z)^8|_{[S]_4} \\
&= \lim_{z\to i\infty}\frac{1}{16}\theta_2\left(\frac{z}{2}\right)^8 \quad \text{by (9)} \\
&= \lim_{z\to i\infty}\frac{1}{16}\cdot 2^8q(1+q+q^3+\cdots)^8 \\
&= 0. \quad \text{(a simple zero)}
\end{aligned}$$

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

$$\nu_0(\theta_2(z)^8) = \nu_0(\theta_4(2z)^8) = 1.$$

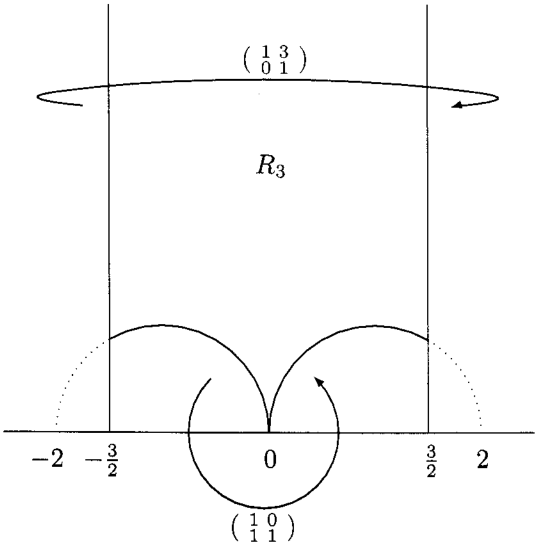
Hence $\theta_2(z)^8$ (resp. $\theta_4(2z)^8$) has no other zeros in $X_1(2)$ except at $s = \infty$ (resp. $s = 0$). Therefore $[K(X_1(4)) : \mathbb{C}(j_{1,2}(z))] = \nu_0(j_{1,2}(z)) = 1$, and so (ii) follows. □

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 $\overline{\Gamma}^1(3)$ is generated by γ_1 and γ_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) $\overline{\Gamma}_1(3)$ *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 2. Cusps of $\Gamma_1(3)$

cusp	∞	0
width	1	3

Let $E_4(z)$ be the normalized Eisenstein series of weight 4 defined by

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

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):

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

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 $E_4(-\frac{1}{z}) = z^4 E_4(z)$ for each $z \in \mathfrak{H}$. We observe that

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

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

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

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). □

5. Some remarks on Thompson series

For a modular function f, we call f *normalized* if its q-series is

$$\frac{1}{q} + 0 + a_1 q + a_2 q^2 + \cdots .$$

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

Proof. [7], Lemma 8. □

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

(i) $f(z) \in K(X(\Gamma))$ for some discrete subgroup Γ 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 $\mathbb{C}(f)$.

(iii) In a neighborhood of ∞, $f(z)$ 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, ϕ) is a "moonshine" for a finite group G if ϕ is a function from G to $\mathfrak{F}$ and the mapping $\sigma \to a_n(\sigma)$ 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, ϕ_σ is a class function of G.

Finding or constructing a "moonshine" (G, ϕ) for a given group G, however, involves some nontrivial work. It is because that for each element σ of G, we have to find a natural number N and a Fuchsian group Γ 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 ∞ induce generalized characters for all $n \geq 1$.

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

$$j = q^{-1} + 744 + 196884\, q + \cdots = \sum_r c_r\, q^r. \tag{12}$$

Then $j - 744$ is the normalized generator of $\Gamma(1)$. Let M be the monster simple group of order approximately 8×10^{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 $PSL_2(\mathbb{R})$, 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 $j_{1,N}$ $(N = 2, 3)$ mentioned in Theorem 6 and Theorem 8.

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

which is in $q^{-1}\mathbb{Z}[[q]]$. Let $N(j_{1,2}) = \frac{2^8}{j_{1,2}} + 24$. In the case of the modular function $j_{1,3}$, we consider

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

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 $\overline{\Gamma}_0(2) = \overline{\Gamma}_1(2)$ and $\overline{\Gamma}_0(3) = \overline{\Gamma}_1(3)$, we can get the normalized generators using η-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.

$$\frac{2^8\ \theta_4(2z)^8}{\theta_2(z)^8} = \frac{\eta(z)^{24}}{\eta(2z)^{24}}$$

and

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

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 $N(j_{1,2})$

s	∞	0
$N(j_{1,2})(s)$	∞	24

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

s	∞	0
$N(j_{1,3})(s)$	∞	12

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 λ_{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 λ_{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 $\mathfrak{H}^*$, and so g must be a constant, say λ_0. Therefore we end up with $f = b_nc^nt^n + \lambda_{n-1}c^{n-1}t^{n-1} + \cdots + \lambda_1ct + \lambda_0$, as desired. □

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

Proof. Let $j(z) = \dfrac{1}{q} + 744 + 196884q + \cdots$. It is well-known that $j(\tau)$ is an algebraic integer for $\tau \in \mathbb{Q}(\sqrt{-d}) \cap \mathfrak{H}$ ([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 ∞, 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

$$j \times \prod_{s \in S_{\Gamma_1(N)} \backslash \{\infty\}} (t(z) - t(s))^{h_s}$$

has a pole only at ∞ 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∼4, we can compute the product part in the above more explicitly, that is,

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

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 $\mathbb{Z}[j(\tau)]$. Therefore $t(\tau)$ is integral over $\mathbb{Z}$ for $\tau \in \mathbb{Q}(\sqrt{-d}) \cap \mathfrak{H}$. □

References

[1] R. E. Borcherds, *Monstrous moonshine and monstrous Lie superalgebras*, Invent. Math. **109** (1992), no. 2, 405–444.

[2] J. H. Conway and S. P. Norton, *Monstrous moonshine*, Bull. London Math. Soc. **11** (1979), no. 3, 308–339.

[3] M. Deuring, *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper*, Abh. Math. Sem. Hansischen Univ. **14** (1941), 197–272.

[4] C. R. Ferenbaugh, *The genus-zero problem for n|h-type groups*, Duke Math. J. **72** (1993), no. 1, 31–63.

[5] K. Harada, *Moonshine of Finite Groups*, Ohio State University, (Lecture Note).

[6] C. H. Kim and J. K. Koo, *On the genus of some modular curve of level N*, Bull. Austral. Math. Soc. **54** (1996), no. 2, 291–297.

[7] ———, *Arithmetic of the modular function $j_{1,4}$*, Acta Arith. **84** (1998), no. 2, 129–143.

[8] ———, *Arithmetic of the modular function $j_{1,8}$*, Ramanujan J. **4** (2000), no. 3, 317–338.

[9] N. Koblitz, *Introduction to Elliptic Curves and Modular Forms*, Graduate Texts in Mathematics, 97. Springer-Verlag, New York, 1984.

[10] S. Lang, *Elliptic Functions*, Graduate Texts in Mathematics, 112. Springer-Verlag, New York, 1987.

[11] T. Miyake, *Modular Forms*, Translated from the Japanese by Yoshitaka Maeda. Springer-Verlag, Berlin, 1989.

[12] A. Néron, *Modeles minimaux des variétés abéliennes sur les corps locaux et globaux*, Inst. Hautes Études Sci. Publ. Math. No. **21** (1964), 5–128.

[13] R. Rankin, *Modular Forms and Functions*, Cambridge University Press, Cambridge-New York-Melbourne, 1977.

[14] B. Schoeneberg, *Elliptic modular functions: an introduction*, Translated from the German by J. R. Smart and E. A. Schwandt. Die Grundlehren der mathematischen Wissenschaften, Band 203. Springer-Verlag, New York-Heidelberg, 1974.

[15] J.-P. Serre and J. Tate, *Good reduction of abelian varieties*, Ann. of Math. (2) **88** (1968), 492–517.

[16] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Publications of the Mathematical Society of Japan, No. 11. Iwanami Shoten, Publishers, Tokyo; Princeton University Press, Princeton, N.J., 1971.
[17] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, 151. Springer-Verlag, New York, 1994.
[18] J. G. Thompson, *Some numerology between the Fischer-Griess Monster and the elliptic modular function*, Bull. London Math. Soc. **11** (1979), no. 3, 352–353.

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: jkkoo@math.kaist.ac.kr