ACTA ARITHMETICA
LXXXIV.2 (1998)

Arithmetic of the modular function $j_{1,4}$

by

Chang Heon Kim and Ja Kyung Koo (Taejon)

We find a generator $j_{1,4}$ of the function field on the modular curve $X_1(4)$ by means of classical theta functions θ_2 and θ_3, and estimate the normalized generator $N(j_{1,4})$ which becomes the Thompson series of type $4C$. With these modular functions we investigate some number theoretic properties.

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 $\left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right)$ mod N ($N = 1, 2, \ldots$). 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 the 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 $N = 12$ ([9]), the function field $K(X_1(4))$ of the curve $X_1(4)$ is a rational function field over $\mathbb{C}$.

In this article we will first find the field generator $j_{1,4}$ in Section 3 by making use of the classical Jacobi theta functions θ_2 and θ_3. Furthermore, we will show that $\mathbb{Q}(j_{1,4}) = \mathbb{Q}(j, j(4z))$ ($j =$ the modular invariant of $SL_2(\mathbb{Z})$) is the field of all modular functions in $K(X_1(4))$ whose Fourier coefficients with respect to q $(= e^{2\pi iz}, z \in \mathfrak{H})$ are rational numbers. We will also find the relation between two modular functions $j_{1,4}$ and $j_4 = \theta_3(z/2)/\theta_4(z/2)$ ([8]). In Section 4 we will estimate the normalized generator $N(j_{1,4})$ of $K(X_1(4))$ as the type of the field which turns out to be the Thompson series of type $4C$, and will investigate the replication formulas for the coefficients of $N(j_{1,4})$. When $\tau \in \mathfrak{H} \cap \mathbb{Q}(\sqrt{-d})$ for a square-free positive integer d, we will show that $N(j_{1,4})(\tau)$ becomes an algebraic integer. Finally, in Section 5 we will construct some class fields over an imaginary quadratic field by applying Shimura theory and standard results of complex multiplication to our function $j_{1,4}$.

Throughout the article we adopt the following notations:

1991 *Mathematics Subject Classification*: 11F03, 11F11, 11F22, 11R04, 11R37, 14H55.

Supported by KOSEF research grant 95-K3-0101 (RCAA).

- $\mathfrak{H}^*$ the extended complex upper half plane,
- $\Gamma(N) = \{\gamma \in SL_2(\mathbb{Z}) \mid \gamma \equiv I \bmod N\}$,
- $\Gamma_0(N)$ the Hecke subgroup $\left\{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma(1) \mid c \equiv 0 \bmod N\right\}$,
- $\overline{\Gamma}$ the inhomogeneous group of Γ $(= \Gamma/\pm I)$,
- $q_h = e^{2\pi i z/h}$, $z \in \mathfrak{H}$,
- $M_k(\Gamma_1(N))$ the space of modular forms of weight k with respect to the group $\Gamma_1(N)$,
- $\mathbb{Z}_p$ the ring of p-adic integers,
- $\mathbb{Q}_p$ the field of p-adic numbers.

2. Generators of $\Gamma_1(4)$. Let Γ be a congruence subgroups of $\Gamma(1)$ $(= SL_2(\mathbb{Z}))$. A subset $\mathbb{F}$ of $\mathfrak{H}^*$ is called a *fundamental set* for the group $\overline{\Gamma}$ if it contains exactly one representative of each class of points of $\mathfrak{H}^*$ equivalent under $\overline{\Gamma}$. A set $\mathbb{F}$ is called a *fundamental region* if $\mathbb{F}$ contains a fundamental set and, for $z \in \mathbb{F}$ and $\gamma z \in \mathbb{F}$ with γ $(\neq I) \in \overline{\Gamma}$, z is a boundary point of $\mathbb{F}$.

Although the following theorem is well known, we present its proof for the sake of completeness.

THEOREM 1. *Let $\overline{\Gamma}$ be a congruence subgroup of $\overline{\Gamma}(1)$ of finite index and $\mathbb{F}$ be a fundamental region for $\overline{\Gamma}$. Then the sides of $\mathbb{F}$ can be grouped into pairs λ_j, λ_j' $(j = 1, \ldots, s)$ in such a way that $\lambda_j \subseteq \mathbb{F}$ and $\lambda_j' = \gamma_j \lambda_j$ where $\gamma_j \in \overline{\Gamma}$ $(j = 1, \ldots, s)$. γ_j's are called boundary substitutions of $\mathbb{F}$. Furthermore, $\overline{\Gamma}$ is generated by the boundary substitutions $\gamma_1, \ldots, \gamma_s$.*

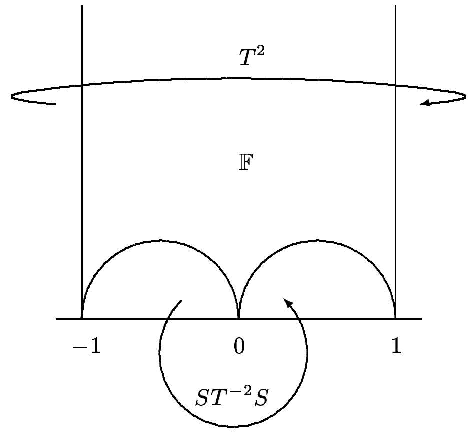
Proof. For the first part, see [16], p. 58. For any $\gamma \in \overline{\Gamma}$, suppose that there exists a sequence of images of $\mathbb{F}$, that is, $\mathbb{F}, S_1\mathbb{F}, S_2\mathbb{F}, \ldots, S_n\mathbb{F} = \gamma\mathbb{F}$ $(S_j \in \overline{\Gamma})$, each adjacent to its successor. Let $\mathbb{F} \cap S_1\mathbb{F} \supseteq \lambda_j'$. Since $\gamma_j \lambda_j = \lambda_j'$ and $\gamma_j\mathbb{F}$ is another fundamental region, $\gamma_j\mathbb{F} = S_1\mathbb{F}$, which yields that $S_1 = \gamma_j$. Then $\gamma_j\lambda_i, \gamma_j\lambda_i'$ $(i = 1, \ldots, s)$ form the sides of $S_1\mathbb{F}$ and $(\gamma_j\gamma_i\gamma_j^{-1})\gamma_j\lambda_i = \gamma_j\lambda_i'$, i.e., $\gamma_j\gamma_i\gamma_j^{-1}$ $(i = 1, \ldots, s)$ are boundary substitutions of $S_1\mathbb{F}$.

Now, we use induction on n to show that S_n $(= \gamma)$ is generated by $\gamma_1, \ldots, \gamma_s$ and boundary substitutions are also generated by them. The case $n = 1$ has been done. Denote the sides of $S_{n-1}\mathbb{F}$ by μ_i, μ_i' $(i = 1, \ldots, s)$. Let $L_i\mu_i = \mu_i'$ for $i = 1, \ldots, s$. Then, by induction hypothesis, S_{n-1} and L_i $(i = 1, \ldots, s)$ are generated by $\gamma_1, \ldots, \gamma_s$. If $S_{n-1}\mathbb{F} \cap S_n\mathbb{F} \supseteq \mu_j'$, then $L_j\mu_j = \mu_j'$ implies that $L_jS_{n-1}\mathbb{F} = S_n\mathbb{F}$, i.e., $S_n = L_jS_{n-1}$. Hence, it is generated by $\gamma_1, \ldots, \gamma_s$. Also, the set of all points in $\mathfrak{H}$ belonging to the region $S_n\mathbb{F}$ that can be reached by such sequences is open, and so is its complement in $\mathfrak{H}$ which must be empty by connectedness of $\mathfrak{H}$. This completes the proof of the theorem. ∎

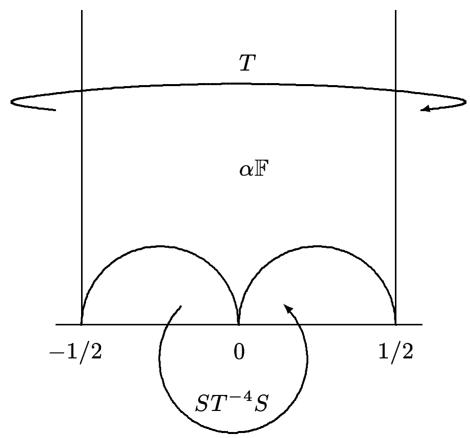
LEMMA 2. *Let $\alpha = \left(\begin{smallmatrix} 0 & -1 \\ 2 & 0 \end{smallmatrix}\right)$. Then $\pm\alpha\Gamma(2)\alpha^{-1} = \pm\Gamma_1(4)$.*

Proof. Straightforward. ∎

It is well known ([17], p. 84) that $\Gamma(2)$ has the following fundamental domain:



where $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$. Thus, by Lemma 2 we can come up with the fundamental domain $\alpha\mathbb{F}$ of $\Gamma_1(4)$ as follows:



Since T and $ST^{-4}S$ are in $\overline{\Gamma}_1(4)$, they generate the group $\overline{\Gamma}_1(4)$ by Theorem 1. There are 3 cusps $\infty, 0, \frac{1}{2}$ in $X_1(4)$ as seen in the above figure, whose widths are 1, 4 and 1, respectively. Here we observe that the first two are regular and the last one is irregular.

3. Hauptfunktionen of $K(X_1(4))$ as a quotient of Jacobi theta functions. First, we recall the Jacobi theta functions $\theta_2, \theta_3, \theta_4$ defined by

$$\theta_2(z) = \sum_{n\in\mathbb{Z}} q_2^{(n+1/2)^2}, \qquad \theta_3(z) = \sum_{n\in\mathbb{Z}} q_2^{n^2}, \qquad \theta_4(z) = \sum_{n\in\mathbb{Z}} (-1)^n q_2^{n^2}$$

for $z \in \mathfrak{H}$. Then we have the following transformation formulas ([16], pp. 218–219):

$$\theta_2(z+1) = e^{\pi i/4}\theta_2(z), \tag{1}$$
$$\theta_3(z+1) = \theta_4(z), \tag{2}$$
$$\theta_4(z+1) = \theta_3(z), \tag{3}$$
$$\theta_2(-1/z) = (-iz)^{1/2}\theta_4(z), \tag{4}$$
$$\theta_3(-1/z) = (-iz)^{1/2}\theta_3(z), \tag{5}$$
$$\theta_4(-1/z) = (-iz)^{1/2}\theta_2(z). \tag{6}$$

Put $j_{1,4}(z) = \theta_2(2z)^4/\theta_3(2z)^4$. Then we obtain the following theorem.

THEOREM 3. (i) $\theta_2(2z)^4, \theta_3(2z)^4 \in M_2(\Gamma_1(4))$.
(ii) $K(X_1(4)) = \mathbb{C}(j_{1,4}(z))$ *and* $j_{1,4}(\infty) = 0$ (*simple zero*), $j_{1,4}(0) = 1$, $j_{1,4}(1/2) = \infty$ (*simple pole*).

Proof. For the first part, we must check the invariance of the slash operator and the cusp conditions. Since T and $ST^{-4}S$ generate $\overline{\Gamma}_1(4)$, it is enough to check it for these generators.

$$\begin{aligned}
\theta_2(2z)^4|_{[T]_2} &= \theta_2(2z+2)^4 = (e^{\pi i/2}\theta_2(2z))^4 \quad \text{by (1)}\\
&= \theta_2(2z)^4,
\end{aligned}$$

$$\begin{aligned}
\theta_2(2z)^4|_{[S]_2} &= z^{-2}\theta_2(-2/z)^4 = z^{-2}\{(-iz/2)^{1/2}\theta_4(z/2)\}^4 \quad \text{by (4)}\\
&= -\tfrac{1}{4}\theta_4(z/2)^4,
\end{aligned} \tag{7}$$

$$\begin{aligned}
\theta_2(2z)^4|_{[ST^{-4}]_2} &= -\tfrac{1}{4}\theta_4(z/2)^4|_{[T^{-4}]_2} = -\tfrac{1}{4}\theta_4(z/2)^4 \quad \text{by (2) and (3)},\\
\theta_2(2z)^4|_{[ST^{-4}S]_2} &= -\tfrac{1}{4}\theta_4(z/2)^4|_{[S]_2} = -\tfrac{1}{4}z^{-2}\{(-2iz)^{1/2}\theta_2(2z)\}^4 \quad \text{by (6)}\\
&= \theta_2(2z)^4,\\
\theta_3(2z)^4|_{[T]_2} &= \theta_3(2z+2)^4 = \theta_3(2z)^4 \quad \text{by (2) and (3)},
\end{aligned}$$

$$\begin{aligned}
\theta_3(2z)^4|_{[S]_2} &= z^{-2}\theta_3(-2/z)^4 = z^{-2}\{(-iz/2)^{1/2}\theta_3(z/2)\}^4 \quad \text{by (5)}\\
&= -\tfrac{1}{4}\theta_3(z/2)^4,
\end{aligned} \tag{8}$$

$$\begin{aligned}
\theta_3(2z)^4|_{[ST^{-4}]_2} &= -\tfrac{1}{4}\theta_3(z/2)^4|_{[T^{-4}]_2}\\
&= -\tfrac{1}{4}\theta_3(z/2)^4 \quad \text{by (2) and (3)},\\
\theta_3(2z)^4|_{[ST^{-4}S]_2} &= -\tfrac{1}{4}\theta_3(z/2)^4|_{[S]_2} = -\tfrac{1}{4}z^{-2}\{(-2iz)^{1/2}\theta_3(2z)\}^4 \quad \text{by (5)}\\
&= \theta_3(2z)^4.
\end{aligned}$$

Now we check the boundary conditions.

(i) $s = \infty$: Since $\theta_2(z) = 2q_8(1 + q + q^3 + \ldots)$, we have

$$\theta_2(2z)^4 = 2^4 q(1 + q^2 + q^6 + q^{12} + \ldots)^4.$$

Hence $\theta_2(2z)^4$ has a simple zero at $s = \infty$. On the other hand, $\theta_3(2z)^4 = (\sum_{n\in\mathbb{Z}} q^{n^2})^4 = (1 + 2q + 2q^4 + 2q^9 + \ldots)^4$. Thus $\theta_3(2z)^4|_{s=\infty} = 1$.

(ii) $s = 0$:

$$\theta_2(2z)^4|_{s=0} = \lim_{z\to i\infty} \theta_2(2z)^4|_{[S]_2} = \lim_{z\to i\infty} -\tfrac{1}{4}\theta_4(z/2)^4 \quad \text{by (7)}$$
$$= -\tfrac{1}{4}$$

and

$$\theta_3(2z)^4|_{s=0} = \lim_{z\to i\infty} \theta_3(2z)^4|_{[S]_2} = \lim_{z\to i\infty} -\tfrac{1}{4}\theta_3(z/2)^4 \quad \text{by (8)}$$
$$= -\tfrac{1}{4}.$$

(iii) $s = 1/2$: Observe that $(ST^{-2}S)\infty = 1/2$.
Considering the identities

$$\theta_2(2z)^4|_{[S]_2} = -\tfrac{1}{4}\theta_4(z/2)^4 \quad \text{by (7)},$$
$$\theta_2(2z)^4|_{[ST^{-2}]_2} = -\tfrac{1}{4}\theta_4(z/2)^4|_{[T^{-2}]_2} = -\tfrac{1}{4}\theta_3(z/2)^4 \quad \text{by (3)},$$
$$\theta_2(2z)^4|_{[ST^{-2}S]_2} = -\tfrac{1}{4}\theta_3(z/2)^4|_{[S]_2} = -\tfrac{1}{4}z^{-2}\{(-2iz)^{1/2}\theta_3(2z)\}^4 \quad \text{by (5)}$$
$$= \theta_3(2z)^4,$$

we get

$$\theta_2(2z)^4|_{s=1/2} = \lim_{z\to i\infty} \theta_2(2z)^4|_{[ST^{-2}S]_2} = \lim_{z\to i\infty} \theta_3(2z)^4 = 1.$$

The facts that

$$\theta_3(2z)^4|_{[S]_2} = -\tfrac{1}{4}\theta_3(z/2)^4 \quad \text{by (8)},$$
$$\theta_3(2z)^4|_{[ST^{-2}]_2} = -\tfrac{1}{4}\theta_3(z/2)^4|_{[T^{-2}]_2} = -\tfrac{1}{4}\theta_4(z/2)^4 \quad \text{by (2)},$$
$$\theta_3(2z)^4|_{[ST^{-2}S]_2} = -\tfrac{1}{4}\theta_4(z/2)^4|_{[S]_2} = -\tfrac{1}{4}z^{-2}\{(-2iz)^{1/2}\theta_2(2z)\}^4 \quad \text{by (6)}$$
$$= \theta_2(2z)^4$$

imply

$$\theta_3(2z)^4|_{s=1/2} = \lim_{z\to i\infty} \theta_3(2z)^4|_{[ST^{-2}S]_2} = \lim_{z\to i\infty} \theta_2(2z)^4$$
$$= \lim_{z\to i\infty} 2^4 q(1+q^2+q^6+q^{12}+\ldots)^4$$
$$= 0 \quad \text{a simple zero.}$$

Now, we prove the second part. From the well-known formula ([19], p. 39) concerning the sum of orders of zeros of modular forms, it follows that $\nu_0(\theta_2(2z)^4) = \nu_0(\theta_3(2z)^4) = 1$. Hence $\theta_2(2z)^4$ (resp. $\theta_3(2z)^4$) has no other zeros in $X_1(4)$ except at $s = \infty$ (resp. $s = 1/2$). Therefore $[K(X_1(4)) : \mathbb{C}(j_{1,4}(z))] = \nu_0(j_{1,4}(z)) = 1$, and so (ii) follows. ∎

Let $K(X(\Gamma'))$ be the function field of the modular curve $X(\Gamma') = \Gamma' \backslash \mathfrak{H}^*$. Suppose that the genus of $X(\Gamma')$ is zero. Let h be the width of the cusp ∞. By F we mean the field of all modular functions in $K(X(\Gamma'))$ whose Fourier coefficients with respect to q_h belong to $\mathbb{Q}$.

Lemma 4. *Let $K(X(\Gamma')) = \mathbb{C}(J')$ for some $J' \in K(X(\Gamma'))$. If $J' \in F$, then $F = \mathbb{Q}(J')$.*

Proof. First, note that F and $\mathbb{C}$ are linearly disjoint over $\mathbb{Q}$. Indeed, let $\mu_1, \ldots, \mu_m$ be the elements of $\mathbb{C}$ which are linearly independent over $\mathbb{Q}$. Assume that $\sum_i \mu_i g_i = 0$ with g_i in F. Let $g_i = \sum_n c_{in} q_h^n$ with $c_{in} \in \mathbb{Q}$. Then $\sum_i \mu_i c_{in} = 0$ for every n, so that $c_{in} = 0$ for all i and n. Hence $g_1 = \ldots = g_m = 0$. We then have the field tower

$$\begin{tikzcd}[column sep=small]
& \mathbb{C}(J') \arrow[dl, dash] \arrow[dr, dash] & & F \\
\mathbb{C} & & \mathbb{Q}(J') \arrow[ur, dash] & \\
& \mathbb{Q} \arrow[ul, dash] \arrow[ur, dash] & &
\end{tikzcd}$$

From the tower, we see that F and $\mathbb{C}(J')$ are linearly disjoint over $\mathbb{Q}(J')$ by [12], p. 361. Hence,

$$1 \le [F : \mathbb{Q}(J')] \le [\mathbb{C}F : \mathbb{C}(J')] \le [K(X(\Gamma')) : K(X(\Gamma'))] = 1,$$

which yields that $F = \mathbb{Q}(J')$. ∎

Lemma 5. *If $\Gamma' = \Gamma_0(N)$, then F is equal to $\mathbb{Q}(j, j(Nz))$ where j is the modular invariant of $\Gamma(1)$.*

Proof. Let $X(\Gamma') = X_0(N)$. We recall that $K(X_0(N)) = \mathbb{C}(j, j(Nz))$ ([19], Proposition 2.10) and consider the field tower

$$\begin{tikzcd}[column sep=small]
& \mathbb{C}(j, j(Nz)) \arrow[dl, dash] \arrow[dr, dash] & & F \\
\mathbb{C} & & \mathbb{Q}(j, j(Nz)) \arrow[ur, dash] & \\
& \mathbb{Q} \arrow[ul, dash] \arrow[ur, dash] & &
\end{tikzcd}$$

Since F and $\mathbb{C}$ are linearly disjoint over $\mathbb{Q}$, we claim that F and $\mathbb{C}(j, j(Nz))$ are linearly disjoint over $\mathbb{Q}(j, j(Nz))$. Therefore

$$1 \le [F : \mathbb{Q}(j, j(Nz))] \le [\mathbb{C}X : \mathbb{C}(j, j(Nz))] \le [K(X_{\Gamma'}) : K(X_{\Gamma'})] = 1. \ \blacksquare$$

Consider the case $N = 4$. Since $j_{1,4}$ has rational Fourier coefficients, from Lemmas 4 and 5 we derive

Theorem 6. *$\mathbb{Q}(j, j(4z)) = \mathbb{Q}(j_{1,4})$ is the field of all modular functions in $K(X_1(4))$ whose Fourier coefficients with respect to q are rational numbers.*

Define $j_4(z) = \theta_3(z/2)/\theta_4(z/2)$. Let F_4 be the field of all modular functions of level 4 whose Fourier expansions with respect to q_4 have rational coefficients. Then by [19], Proposition 6.9, we know that $F_4 = \mathbb{Q}(j(z), j(4z), f_{1,0}(z))$ where $f_{1,0}(z)$ is a Fricke function. Also by [8], Theorem 18, we see that $F_4 = \mathbb{Q}(j_4)$. Since $j_{1,4}$ has rational Fourier coefficients, we have

$j_{1,4} \in F_4$. Hence we are able to express $j_{1,4}$ as a rational function of j_4. On the other hand, it is not difficult to derive that

$$\theta_2(2z) = \tfrac{1}{2}(\theta_3(z/2) - \theta_4(z/2)) \quad \text{and} \quad \theta_3(2z) = \tfrac{1}{2}(\theta_3(z/2) + \theta_4(z/2)).$$

From the above we get

THEOREM 7.

$$j_{1,4}(z) = \left(\frac{j_4(z) - 1}{j_4(z) + 1}\right)^4.$$

4. Some remarks on Thompson series. Let Γ be a Fuchsian group of the first kind and $f \in K(X(\Gamma))$. We call f *normalized* if its q series is $q^{-1} + 0 + a_1 q + a_2 q^2 + \ldots$

LEMMA 8. *The normalized generator of a genus zero function field is unique.*

Proof. Let Γ be a Fuchsian group such that the genus of the curve $\Gamma\backslash\mathfrak{H}^*$ is zero. Assume that $K(X(\Gamma)) = \mathbb{C}(J_1) = \mathbb{C}(J_2)$ where J_1 and J_2 are normalized. We can then write their Fourier expansions as

$$J_1 = q^{-1} + 0 + a_1 q + a_2 q^2 + \ldots \quad \text{and} \quad J_2 = q^{-1} + 0 + b_1 q + b_2 q^2 + \ldots$$

Observe that $1 = [K(X(\Gamma)) : \mathbb{C}(J_i)] = \nu_0(J_i) = \nu_\infty(J_i)$ for $i = 1, 2$. Hence, J_1 and J_2 have only one zero and one pole whose orders are simple. We see that the only poles of J_i occur at ∞. Then, $J_1 - J_2$ has no poles because the two series start with q^{-1}. So, it should be a constant. Since $J_1 - J_2 = (a_1 - b_1)q + \ldots$, this constant must be zero. This proves the lemma. ■

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:

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

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 $\phi_\sigma(z) = q^{-1} + a_0(\sigma) + \sum_{n=1}^{\infty} a_n(\sigma) q^n$ 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. This is because 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 the function field $K(X(\Gamma'))$ is equal to $\mathbb{C}(\phi_\sigma)$ and the coefficients $a_n(\sigma)$ of 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

$$j = q^{-1} + 744 + 196884q + \ldots = \sum_r c_r q^r. \tag{9}$$

Then $j - 744$ is the normalized generator of $\Gamma(1)$. Let M be the monster simple group of order approximately $8 \cdot 10^{53}$. 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

$$H_{-1}q^{-1} + 0 + H_1 q + H_2 q^2 + \ldots$$

in which the H_r are certain representations of M called *head representations*. H_r has degree c_r as in (9), 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 the former two and the degree 21296876 representation ([20]). The following theorem conjectured by Thompson and proved by Borcherds shows that there exists a moonshine for the monster group M.

THEOREM 9. *The series*

$$T_m = q^{-1} + 0 + H_1(m)q + H_2(m)q^2 + \ldots$$

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 the head representation H_r at m ([1], [3]).

Now we consider the case $\Gamma' = \Gamma_1(4)$. We will then construct the normalized generator from the modular function $j_{1,4}$ mentioned in Theorem 3. We have

$$\begin{aligned}\frac{16}{j_{1,4}(z)} &= \frac{16\theta_3(2z)^4}{\theta_2(2z)^4} \\ &= \frac{(1+2q+2q^4+2q^9+2q^{16}+\ldots)^4}{q(1+q^2+q^6+q^{12}+q^{20}+\ldots)^4} \\ &= q^{-1} + 8 + 20q - 62q^3 + 216q^5 - 641q^7 + 1636q^9 + \ldots,\end{aligned}$$

which is in $q^{-1}\mathbb{Z}[[q]]$ because $q(1+q^2+q^6+q^{12}+\ldots)^4 \in q\mathbb{Z}[[q]]^\times$. Let $N(j_{1,4}) = 16/j_{1,4} - 8$. Then by [3], Lemma 8, Table 4, and checking the coefficients of q^i, $i \leq 5$ ([1]) we have

THEOREM 10. *$N(j_{1,4})$ is the normalized generator of $K(X_1(4))$, which corresponds to the Thompson series of type $4C$.*

REMARK 11. Let $V = \bigoplus_{n\in\mathbb{Z}} V_n$ be the infinite-dimensional graded representation of the monster simple group constructed by Frenkel *et al.* ([6], [7]). For each element m of the monster, we write the Thompson series as

$$T_m = \sum_{n\in\mathbb{Z}} \mathrm{Tr}(m|V_n)q^n$$

where $\mathrm{Tr}(m|V_n)$ is the trace of m on the vector space V_n and q is a formal variable which can usually be thought of as a complex number with $|q| < 1$. Let m be the conjugacy class of order 4 and type C in Atlas notation [2], and set

$$N(j_{1,4}) = q^{-1} + \sum_{n\geq 1} H_n(m)q^n.$$

Since $N(j_{1,4})$ is the Thompson series of m by Theorem 10, the results of [1] show that the coefficients $H_n(m)$ are the traces $\mathrm{Tr}(m|V_n)$ and satisfy the relation

$$p^{-1}\exp\Big(-\sum_{i>0}\sum_{\substack{k>0\\ n\in\mathbb{Z}}} \mathrm{Tr}(m^i|V_{kn})p^{ki}q^{ni}/i\Big) = \sum_{k\in\mathbb{Z}} \mathrm{Tr}(m|V_k)p^k - \sum_{n\in\mathbb{Z}} \mathrm{Tr}(m|V_n)q^n$$

where p is also a formal variable which can be thought of as a complex number with $|p| < 1$. The above identities then imply that $N(j_{1,4})$ is completely replicable, and lead us to the recursion formulas (9.1) in [1], which later in this section turn out to be the same as ours (18) provided we put $H_n(m^2) = H_n^{(2)}$ (the coefficient of q^n of the 2-plicate of $N(j_{1,4})$).

Observe that $\overline{\Gamma}_1(4) = \overline{\Gamma}_0(4)$ as transformation groups, but the algorithm presented here is different from Conway–Norton's.

Following Norton's idea ([15], also see [1], [3] and [11]), we will state some replication formulas on the coefficients of $N(j_{1,4})$. Let N be a positive integer and S be a subset of Hall divisors of N. By $N + S$ we mean the subgroup of $PSL_2(\mathbb{R})$ generated by $\Gamma_0(N)$ and all Atkin–Lehner involutions $W_{Q,N}$ for $Q \in S$. We assume that the genus of the curve $X(N + S)$ is zero. Let $t = q^{-1} + \sum_{m\geq 1} H_m q^m$ be the normalized generator of the function field of $X(N+S)$ as a completely replicable function. Then for each $n \geq 1$, there exists a unique polynomial $X_n(t)$ in t such that $X_n(t) \equiv n^{-1}q^{-n} \bmod q\mathbb{C}[[q]]$. In particular, $X_1(t) = t$. Write $X_n(t) = n^{-1}q^{-n} + \sum_{m\geq 1} H_{m,n}q^m$. Let $p = e^{2\pi i y}$ for $y \in \mathfrak{H}$ and $q = e^{2\pi i z}$ as usual. We then understand $t(y)$ and $t(z)$ as $p^{-1} + \sum_{m\geq 1} H_m p^m$ and $q^{-1} + \sum_{m\geq 1} H_m q^m$, respectively. Observe that $X_n(t)$ can be viewed as the coefficient of p^n in $\log p^{-1} - \log(t(y) - t(z))$

([15], p. 185). To this end it suffices to show that

$$\frac{1}{n!}\cdot\frac{\partial^n}{\partial p^n}(-\log p-\log(t(y)-t(z)))|_{p=0}$$

is a polynomial in t, which is congruent to $n^{-1}q^{-n}$ mod $q\mathbb{C}[[q]]$. Since

$$\log p^{-1}-\sum_{n\geq 1}X_n(t)p^n=\log(t(y)-t(z)),$$

we get by taking exponential on both sides,

$$p^{-1}\exp\Big(-\sum_{n\geq 1}X_n(t)p^n\Big)=t(y)-t(z). \tag{10}$$

If we compare the coefficients of the terms p^2, p^3 and p^4 in (10), we have

$$\tfrac{1}{2}(t^2-2X_2(t))=H_1, \tag{11}$$

$$-\tfrac{1}{6}(t^3-6t\cdot X_2(t)+6X_3(t))=H_2, \tag{12}$$

$$\tfrac{1}{24}(t^4-12t^2\cdot X_2(t)+12X_2(t)^2+24t\cdot X_3(t)-24X_4(t))=H_3. \tag{13}$$

Let $t^{(2)}$ be the normalized generator of the function field of $X(N^{(2)}+S^{(2)})$ and define $t^{(2^l)}$ to be $(t^{(2^{l-1})})^{(2)}$, where $N^{(2)}=N/(2,N)$ and $S^{(2)}$ is the set of all Q in S which divide $N^{(2)}$. Write $t^{(s)}=q^{-1}+\sum_{m\geq 1}H_m^{(s)}q^m$. Also define the operator U_n such that for $f(z)=\sum_{l\in\mathbb{Z}}a_lq^l$,

$$f(z)|_{U_n}=n\sum_{l\in\mathbb{Z}}a_{nl}q^l.$$

Then Koike ([11]) proved the following formulas called 2-plication and 4-plication, respectively:

$$X_2(t)=\tfrac{1}{2}(t|_{U_2}+t^{(2)}(2\tau)), \tag{14}$$

$$X_4(t)=\tfrac{1}{4}(t|_{U_4}+t^{(2)}|_{U_2}(2\tau)+t^{(4)}(4\tau)). \tag{15}$$

Then by (11) and (14), it follows that

$$\tfrac{1}{2}t^2-\tfrac{1}{2}(t|_{U_2}+t^{(2)}(2\tau))=H_1. \tag{16}$$

Also by (11)–(15) we get

$$\tfrac{1}{4}(t|_{U_2})^2+\tfrac{1}{2}t|_{U_2}\cdot t^{(2)}(2\tau)-H_2t-\tfrac{1}{4}t|_{U_4}=H_3+\tfrac{1}{2}H_1^2-\tfrac{1}{2}H_1^{(2)}. \tag{17}$$

If we compare the coefficients of q^{2k} and q^{2k+1} $(k\geq 1)$ of both sides in (16) and (17) and carry out some routine calculation, we find that the coefficients of t and $t^{(2)}$ satisfy the following recursion formulas for $k\geq 1$:

$$
\begin{aligned}
H_{4k} &= H_{2k+1} + \frac{H_k^2 - H_k^{(2)}}{2} + \sum_{1\le j<k} H_j H_{2k-j},\\
H_{4k+1} &= H_{2k+3} - H_2 H_{2k} + \frac{H_{2k}^2 + H_{2k}^{(2)}}{2} + \frac{H_{k+1}^2 - H_{k+1}^{(2)}}{2}\\
&\quad + \sum_{1\le j\le k} H_j H_{2k-j+2}\\
&\quad + \sum_{1\le j<k} H_j^{(2)} H_{4k-4j} + \sum_{1\le j<2k} (-1)^j H_j H_{4k-j},\\
H_{4k+2} &= H_{2k+2} + \sum_{1\le j\le k} H_j H_{2k-j+1},\\
H_{4k+3} &= H_{2k+4} - H_2 H_{2k+1} - \frac{H_{2k+1}^2 - H_{2k+1}^{(2)}}{2}\\
&\quad + \sum_{1\le j\le k+1} H_j H_{2k-j+3}\\
&\quad + \sum_{1\le j\le k} H_j^{(2)} H_{4k-4j+2} + \sum_{1\le j\le 2k} (-1)^j H_j H_{4k-j+2}.
\end{aligned}
\tag{18}
$$

From the above formulas, we see that if $m = 4$ or $m > 5$ then H_m is determined by the coefficients H_i and $H_i^{(2)}$ for $1 \le i < m$, so if we know all the coefficients $H_m^{(s)}$ for $m = 1, 2, 3,$ and 5 together with $s = 2^l$ then we can work out all the coefficients H_m.

Now we take $N = 4$ and $S = \{1\}$. Then t is precisely $N(j_{1,4})$ and $t^{(2)}$ is the normalized generator of the function field of $X_0(2)$ and for $l \ge 2$, $t^{(2^l)}$ is the normalized generator of the function field of $X_0(1)$. Hence we summarize the above results as follows.

THEOREM 12. *If we know the* 12 *coefficients* H_1, H_2, H_3, H_5, $H_1^{(2)}$, $H_2^{(2)}$, $H_3^{(2)}$, $H_5^{(2)}$, $H_1^{(4)}$, $H_2^{(4)}$, $H_3^{(4)}$ *and* $H_5^{(4)}$, *then all the coefficients* H_m *of the modular function* $N(j_{1,4})$ *can be determined.*

Observe that actually we do know the above 12 coefficients:

$H_1 = 20,\ H_2 = 0,\ H_3 = -62,\ H_5 = 216$ by the definition of $N(j_{1,4})$,
$H_1^{(2)} = 276,\ H_2^{(2)} = -2048,\ H_3^{(2)} = 11202,\ H_5^{(2)} = 184024$ by [10],
$H_1^{(4)} = 196884,\ H_2^{(4)} = 21493760,\ H_3^{(4)} = 864299970,$
$H_5^{(4)} = 333202640600$ by [3].

Here, the modular function $j_{1,2}$ is defined by $j_{1,2}(z) = \theta_2(z)^8/\theta_4(2z)^8$ for $z \in \mathfrak{H}$.

It is worth finding when the modular function $N(j_{1,4})$ could be an algebraic integer. We close this section by showing the following number theoretic result.

THEOREM 13. *Let d be a square-free positive integer. For $\tau \in \mathbb{Q}(\sqrt{-d}) \cap \mathfrak{H}$, $N(j_{1,4})(\tau)$ is an algebraic integer.*

Proof. Let $j(z) = q^{-1} + 744 + 196884q + \ldots$ It is well known that $j(\tau)$ is an algebraic integer for $\tau \in \mathbb{Q}(\sqrt{-d}) \cap \mathfrak{H}$ ([13], [19]). For algebraic proofs, see [4], [14] and [18]. Let $J = j/1728$. Then we know that

$$J = \frac{4}{27} \cdot \frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2(\lambda - 1)^2} \quad \text{where} \quad \lambda = \frac{\theta_2(z)^4}{\theta_3(z)^4} = j_{1,4}\left(\frac{z}{2}\right)$$

([16], p. 228). Hence,

$$j(2\tau) = 2^8 \cdot \frac{(j_{1,4}(\tau)^2 - j_{1,4}(\tau) + 1)^3}{j_{1,4}(\tau)^2(j_{1,4}(\tau) - 1)^2} = \frac{(N^2 - 32N + 448)^3}{(N-24)^2(N-8)^2}$$

where $N = N(j_{1,4})(\tau)$. This implies that $N(j_{1,4})(\tau)$ is integral over $\mathbb{Z}[j(2\tau)]$. Therefore it is integral over $\mathbb{Z}$ for $\tau \in \mathbb{Q}(\sqrt{-d}) \cap \mathfrak{H}$. ∎

5. Explicit class fields generated by the modular function $j_{1,4}$.

Let Γ be a Fuchsian group of the first kind. Then $\Gamma\backslash\mathfrak{H}^*$ $(= X(\Gamma))$ is a compact Riemann surface. Hence, there exists a projective nonsingular algebraic curve V, defined over $\mathbb{C}$, biregularly isomorphic to $\Gamma\backslash\mathfrak{H}^*$. We specify a Γ-invariant holomorphic map φ of $\mathfrak{H}^*$ to V which gives a biregular isomorphism of $\Gamma\backslash\mathfrak{H}^*$ to V. In that situation, we call (V, φ) a *model* of $\Gamma\backslash\mathfrak{H}^*$. Now we assume that the genus of $\Gamma\backslash\mathfrak{H}^*$ is zero. Then its function field $K(X(\Gamma))$ is equal to $\mathbb{C}(J')$ for some $J' \in K(X(\Gamma))$.

LEMMA 14. *$(\mathbb{P}^1(\mathbb{C}), J')$ is a model of $\Gamma\backslash\mathfrak{H}^*$.*

Proof. First, we view J' as a meromorphic function on $\Gamma\backslash\mathfrak{H}^*$. By defining

$$J'(z) = \begin{cases} [1:0] & \text{if } z \text{ is a pole,} \\ [J'(z):1] & \text{otherwise,} \end{cases}$$

we get a holomorphic function of $\Gamma\backslash\mathfrak{H}^*$ to $\mathbb{P}^1$, as a map between compact Riemann surfaces. We denote it again by J'. Now for any $c_0 \in \mathbb{C}$, we consider $J' - c_0$. Since $K(X(\Gamma)) = \mathbb{C}(J') = \mathbb{C}(J' - c_0)$ and $[K(X(\Gamma)) : \mathbb{C}(J' - c_0)] = \nu_0(J' - c_0)$ where ν_0 is the sum of orders of zeros, we have $\nu_0(J' - c_0) = 1$. Therefore there exists a unique point $z_0 \in \Gamma\backslash\mathfrak{H}^*$ such that $J'(z_0) = c_0$. This implies the bijectivity of J'. Since any injective holomorphic mapping between two Riemann surfaces is biholomorphic ([5], Corollary 2.5), the assertion follows. ∎

Let $G_{\mathbb{A}}$ be the adelization of $G = GL_2(\mathbb{Q})$. Put

$$\begin{aligned} G_p &= GL_2(\mathbb{Q}_p) \quad (p \text{ a rational prime}), \\ G_\infty &= GL_2(\mathbb{R}), \\ G_{\infty+} &= \{x \in G_\infty \mid \det(x) > 0\}, \\ G_{\mathbb{Q}_+} &= \{x \in GL_2(\mathbb{Q}) \mid \det(x) > 0\}. \end{aligned}$$

We define the topology of $G_{\mathbb{A}}$ by taking $U = \prod_p GL_2(\mathbb{Z}_p) \times G_{\infty+}$ to be an open subgroup of $G_{\mathbb{A}}$. Let K be an imaginary quadratic field and ξ be an embedding of K into $M_2(\mathbb{Q})$. We call ξ *normalized* if it is defined by $a\binom{z}{1} = \xi(a)\binom{z}{1}$ for $a \in K$ where z is the fixed point of $\xi(K^\times)$ $(\subset G_{\mathbb{Q}_+})$ in $\mathfrak{H}$. Observe that the embedding ξ defines a continuous homomorphism of $K_{\mathbb{A}}^\times$ into $G_{\mathbb{A}+}$, which we denote again by ξ. Here $G_{\mathbb{A}+}$ is the group $G_0G_{\infty+}$ with G_0 the nonarchimedean part of $G_{\mathbb{A}}$, and $K_{\mathbb{A}}^\times$ is the idele group of K.

Let $\mathcal{Z}$ be the set of open subgroups S of $G_{\mathbb{A}+}$ containing $\mathbb{Q}^\times G_{\infty+}$ such that $S/\mathbb{Q}^\times G_{\infty+}$ is compact. For $S \in \mathcal{Z}$, we see that $\det(S)$ is open in $\mathbb{Q}_{\mathbb{A}}^\times$. Therefore the subgroup $\mathbb{Q}^\times \cdot \det(S)$ of $\mathbb{Q}_{\mathbb{A}}^\times$ corresponds to a finite abelian extension of $\mathbb{Q}$, which we write k_S. Put $\Gamma_S = S \cap G_{\mathbb{Q}_+}$ for $S \in \mathcal{Z}$. Then it is known ([19], Proposition 6.27) that $\Gamma_S/\mathbb{Q}^\times$ is a Fuchsian group of the first kind commensurable with $\Gamma(1)/\{\pm 1\}$. Let $U' = \{x = (x_p) \in U \mid x_p \in U'_p$ for all finite $p\}$ where $U'_p = \left\{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in GL_2(\mathbb{Z}_p) \,\middle|\, c \equiv 0 \bmod N\mathbb{Z}_p\right\}$. We then have

LEMMA 15. (i) $\mathbb{Q}^\times U' \in \mathcal{Z}$.
(ii) $k_S = \mathbb{Q}$, *if* $S = \mathbb{Q}^\times U'$.
(iii) $\Gamma_S = \mathbb{Q}^\times \Gamma_0(N)$ *if* $S = \mathbb{Q}^\times U'$.

Proof. First, we observe that $\mathbb{Q}^\times U'$ is an open subgroup of $\mathbb{Q}^\times U$. Hence, for (i), it is enough to show that $\mathbb{Q}^\times U/\mathbb{Q}^\times G_{\infty+}$ is compact. But we know that $\mathbb{Q}^\times U/\mathbb{Q}^\times G_{\infty+} = \prod GL_2(\mathbb{Z}_p)$ is compact. For (ii), note that $\mathbb{Q}$ corresponds to the norm group $\mathbb{Q}^\times \cdot \mathbb{Q}_{\mathbb{A}}^{\times\infty}$ with $\mathbb{Q}_{\mathbb{A}}^{\times\infty} = \mathbb{R}^\times \times \prod_p \mathbb{Z}_p^\times$. We claim that $\det U' = \mathbb{Q}_{\mathbb{A}}^{\times\infty}$. Indeed, it is obvious that $\det U' \subset \mathbb{Q}_{\mathbb{A}}^{\times\infty}$. Conversely, for any element $(\alpha_p) \in \mathbb{Q}_{\mathbb{A}}^{\times\infty}$, take $y_p = \left(\begin{smallmatrix} 1 & 0 \\ 0 & \alpha_p \end{smallmatrix}\right)$. Then $(y_p) \in U'$ and $\det(y_p) = (\det y_p) = (\alpha_p)$. Finally, if $S = \mathbb{Q}^\times U'$ then we come up with $\Gamma_S = \mathbb{Q}^\times U' \cap G_{\mathbb{Q}_+} = \mathbb{Q}^\times(U' \cap G_{\mathbb{Q}_+}) = \mathbb{Q}^\times \Gamma_0(N)$. ∎

REMARK 16. For $z \in K \cap \mathfrak{H}$, we consider a normalized embedding $\xi_z : K \to M_2(\mathbb{Q})$ defined by $a\binom{z}{1} = \xi_z(a)\binom{z}{1}$ for $a \in K$. Then z is the fixed point of $\xi_z(K^\times)$ in $\mathfrak{H}$. Let (V_S, φ_S) be a model of $\Gamma_S\backslash\mathfrak{H}^*$. By Lemma 15(iii), $\Gamma_S = \mathbb{Q}^\times\Gamma_0(4) = \mathbb{Q}^\times\Gamma_1(4)$ when $S = \mathbb{Q}^\times U'$ with $N = 4$. By Theorem 3 and Lemma 14, we can take $\varphi_S = j_{1,4}$ and $V_S = \mathbb{P}^1$. Now it follows from [19], Proposition 6.31(ii), that $j_{1,4}(z)$ belongs to $\mathbb{P}^1(K^{\mathrm{ab}})$ where K^{ab} is the maximal abelian extension of K. Furthermore, $\theta_i(z)$ has no zeros in $\mathfrak{H}$ for $i = 2, 3, 4$. Hence, $j_{1,4}(z)$ in fact is in K^{ab} for $z \in K \cap \mathfrak{H}$.

Theorem 17. *Let K be an imaginary quadratic field and let ξ_z be the normalized embedding for $z \in K \cap \mathfrak{H}$. Then $j_{1,4}(z) \in K^{\mathrm{ab}}$ and $K(j_{1,4}(z))$ is a class field of K corresponding to the subgroup $K^\times \cdot \xi_z^{-1}(\mathbb{Q}^\times U')$ of $K_{\mathbb{A}}^\times$.*

Proof. From Lemma 15(ii) and (iii), if $S = \mathbb{Q}^\times U'$ with $N = 4$ then $k_S = \mathbb{Q}$ and $\Gamma_S = \mathbb{Q}^\times \Gamma_1(4)$. Since $j_{1,4}$ gives a model of the curve $X_1(4)$, we can take $\varphi_S = j_{1,4}$. Now the assertion follows from [19], Proposition 6.33 and Remark 16. ∎

In view of standard results on complex multiplication, it is interesting to investigate whether the value $N(j_{1,4})(\alpha)$ is a generator for a certain full ray class field if α is the quotient of a basis of an ideal belonging to the maximal order in $\mathbb{Q}(\sqrt{-d})$. We first need a result on complex multiplication.

Theorem 18. *Let $\mathfrak{F}_N$ be the field of modular functions of level N rational over $\mathbb{Q}(e^{2\pi i/N})$, and let k be an imaginary quadratic field. Let $\mathfrak{O}_k$ be the maximal order of k and $\mathfrak{A}$ be an $\mathfrak{O}_k$-ideal such that $\mathfrak{A} = [z_1, z_2]$ and $z = z_1/z_2 \in \mathfrak{H}$. Then the field $k\mathfrak{F}_N(z)$ generated over k by all values $f(z)$ with $f \in \mathfrak{F}_N$ and f defined at z is the ray class field over k with conductor N.*

Proof. [13], Ch. 10, Corollary of Theorem 2. ∎

Remark 19. When $N = 2$, $\mathfrak{F}_2$ is the field of all modular functions of level 2 rational over $\mathbb{Q}$. On the other hand, it is a well-known fact that $K(X(\Gamma(2))) = \mathbb{C}(\lambda)$ where λ is the classical modular function of level 2. Then by Lemma 4, $\mathfrak{F}_2 = \mathbb{Q}(\lambda)$. Hence by Theorem 18, $k(\lambda(z))$ is the ray class field over k with conductor 2 where z is chosen as in the theorem.

Theorem 20. *Let k and $\mathfrak{O}_k$ be as in Theorem 18. Put $\mathfrak{O}_k = x\mathbb{Z}+\mathbb{Z}$ and $\mathfrak{A} = x\mathbb{Z}+2\mathbb{Z}$ for $x \in \mathfrak{H}$. If $N_{k/\mathbb{Q}}(x)$ is an even integer, then $\mathfrak{A}$ is an $\mathfrak{O}_k$-ideal and $N(j_{1,4})(x/2)$ generates a ray class field over k with conductor 2.*

Proof. Note that $\mathfrak{A}$ is an $\mathfrak{O}_k$-ideal if and only if $x \cdot \mathfrak{A} \subseteq \mathfrak{A}$. Since $x \cdot \mathfrak{A} = x^2\mathbb{Z} + 2x\mathbb{Z}$, $x \cdot \mathfrak{A} \subseteq \mathfrak{A}$ is equivalent to $x^2 \in \mathfrak{A}$. Let $x^2 - \mathrm{Tr}_{k/\mathbb{Q}}(x) \cdot x + N_{k/\mathbb{Q}}(x) = 0$ be the equation of x. Since $\mathrm{Tr}_{k/\mathbb{Q}}(x)$ and $N_{k/\mathbb{Q}}(x)$ are in $\mathbb{Z}$, we have $x^2 \in \mathfrak{A}$ if and only if $N_{k/\mathbb{Q}}(x) \in 2\mathbb{Z}$. Next, we observe that

$$\lambda(z) = \frac{\theta_2(z)^4}{\theta_3(z)^4} = j_{1,4}\left(\frac{z}{2}\right) \quad \text{and} \quad N(j_{1,4}) = \frac{16}{j_{1,4}} - 8.$$

Hence

$$k\left(N(j_{1,4})\left(\frac{x}{2}\right)\right) = k\left(j_{1,4}\left(\frac{x}{2}\right)\right) = k(\lambda(x))$$

is the ray class field with conductor 2 by Remark 19. ∎

Corollary 21. *With the notations of Theorem 20, $N(j_{1,4})(x/2)$ belongs to the maximal order in the ray class field $k(\lambda(x))$ over k with conductor 2.*

Proof. This is immediate from Theorems 13 and 20. ∎

References

[1] R. E. Borcherds, *Monstrous moonshine and monstrous Lie superalgebras*, Invent. Math. 109 (1992), 405–444.

[2] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson, *Atlas of Finite Groups*, Clarendon Press, 1985.

[3] J. H. Conway and S. P. Norton, *Monstrous moonshine*, Bull. London Math. Soc. 11 (1979), 308–339.

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

[5] O. Foster, *Lectures on Riemann Surfaces*, Springer, 1981.

[6] I. B. Frenkel, J. Lepowsky, and A. Meurman, *Vertex Operator Algebras and the Monster*, Academic Press, Boston, 1988.

[7] —, —, —, *A natural representation of the Fischer–Griess monster with the modular function J as character*, Proc. Nat. Acad. Sci. U.S.A. 81 (1984), 3256–3260.

[8] C. H. Kim and J. K. Koo, *On the modular function j_4 of level 4*, preprint.

[9] —, —, *On the genus of some modular curve of level N*, Bull. Austral. Math. Soc. 54 (1996), 291–297.

[10] —, —, *On the modular function $j_{1,2}$*, in preparation.

[11] M. Koike, *On replication formula and Hecke operators*, preprint, Nagoya University.

[12] S. Lang, *Algebra*, Addison-Wesley, 1993.

[13] —, *Elliptic Functions*, Springer, 1987.

[14] A. Néron, *Modèles minimaux des variétés abéliennes sur les corps locaux et globaux*, Publ. Math. I.H.E.S. 21 (1964), 5–128.

[15] S. P. Norton, *More on moonshine*, in: Computational Group Theory, Academic Press, London, 1984, 185–195.

[16] R. Rankin, *Modular Forms and Functions*, Cambridge Univ. Press, Cambridge, 1977.

[17] B. Schoeneberg, *Elliptic Modular Functions*, Springer, 1973.

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

[19] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Publ. Math. Soc. Japan 11, Tokyo, 1971.

[20] J. G. Thompson, *Some numerology between the Fischer–Griess monster and the elliptic modular function*, Bull. London Math. Soc. 11 (1979), 352–353.

Department of Mathematics
Korea Advanced Institute of Science and Technology
Taejon 305-701, Korea
E-mail: kch@math.kaist.ac.kr
jkkoo@math.kaist.ac.kr

Received on 6.12.1996
and in revised form on 1.4.1997 (3093)