Math. Z.
DOI 10.1007/s00209-008-0456-9

Mathematische Zeitschrift

On some arithmetic properties of Siegel functions

Ja Kyung Koo · Dong Hwa Shin

Received: 16 June 2008 / Accepted: 7 November 2008

Abstract We deal with several arithmetic properties of the Siegel functions which are modular units. By modifying the ideas in Kubert and Lang (Modular Units. Grundlehren der mathematischen Wissenschaften, vol 244. Spinger, Heidelberg, 1981), we establish certain criterion for determining a product of Siegel functions to be integral over $\mathbb{Z}[j]$. We also find generators of the function fields $\mathcal{K}(X_1(N))$ by examining the orders of Siegel functions at the cusps and apply them to evaluate the Ramanujan's cubic continued fraction systematically. Furthermore we construct ray class invariants over imaginary quadratic fields in terms of singular values of j and Siegel functions.

Keywords Modular units · Continued fractions · Class fields

Mathematics Subject Classification (2000) 11F11 · 11F20 · 11G16 · 11R37 · 11Y65

Contents

This work was supported by the SRC Program of KOSEF Research Grant R11-2007-035-01001-0.

J. K. Koo · D. H. Shin (✉)
Department of Mathematical Sciences, KAIST, Daejeon 373-1, South Korea
e-mail: shakur01@kaist.ac.kr

J. K. Koo
e-mail: jkkoo@math.kaist.ac.kr

Published online: 28 November 2008

1 Introduction

Let $\mathfrak{H}$ be the complex upper half plane and N be a positive integer. We let

$$\begin{aligned}
\mathfrak{H}^* &= \mathfrak{H} \cup \mathbb{P}^1(\mathbb{Q}) \\
\Gamma_0(N) &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \ : \ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod{N} \right\} \\
\Gamma_1(N) &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \ : \ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod{N} \right\} \\
\Gamma(N) &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \ : \ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{N} \right\}.
\end{aligned}$$

We are especially concerned with the following three modular curves

$$X_0(N) = \Gamma_0(N)\backslash\mathfrak{H}^*, \quad X_1(N) = \Gamma_1(N)\backslash\mathfrak{H}^* \quad \text{and} \quad X(N) = \Gamma(N)\backslash\mathfrak{H}^*$$

and their function fields

$$\mathcal{K}(X_0(N)), \quad \mathcal{K}(X_1(N)) \quad \text{and} \quad \mathcal{K}(X(N)),$$

respectively. For the sake of arithmetic applications we consider the modular curve $X(N)$ defined over the Nth cyclotomic field, and take the integral closure of $\mathbb{Q}[j]$ where j is the elliptic modular function. The units in this ring which are called the modular units are the objects we deal with in this paper. We are mainly interested in the following three problems.

The first is to replace the Fricke functions, which play the roles of classical generators of the modular function fields, by the Siegel functions. The order formulas at the cusps in this case enable us to find such generators. In Sects. 4–6 and 8, we shall examine some arithmetic properties of Siegel functions for this purpose.

The second problem concerns about the integrality over $\mathbb{Z}[j]$ for modular functions. In Sect. 3, we shall establish a criterion for determining a product of Siegel functions to be integral over $\mathbb{Z}[j]$. To this end, we intensively analyze the Fourier coefficients of Siegel functions. Although Kubert and Lang [13] have already provided a criterion, it seems to be scarcely known to experts so that we try to reveal and clarify it. If a function is integral over $\mathbb{Z}[j]$, its values evaluated at some points would become algebraic integers in many cases, for instance, at imaginary quadratic arguments. In Sect. 7, we explain why the reciprocals of the values of the Ramanunjan's cubic continued fraction [6] at imaginary quadratic arguments are algebraic integers.

The third problem is certain construction of ray class fields over imaginary quadratic fields by means of singular values of some analytic functions. Ramachandra presented in [18] a ray class invariant as algebraic unit, its constructions is, however, too abstract and complicated in practical use. In Sect. 9, we find relatively simple ray class invariants in terms of the special values of j and Siegel functions.

For generic theory of modular functions, we refer to [15,20]. Unlike the classical approach to modular functions and the class field theory depending mainly on elliptic functions and theory of complex multiplication, our results are based on the Galois theory and the Shimura's reciprocity law.

2 Preliminaries

For a positive integer N we denote by $\mathbb{Q}_N$ and $\mathcal{F}_N$ the Nth cyclotomic field $\mathbb{Q}_N$ with $\zeta_N = e^{\frac{2\pi i}{N}}$ and the field of modular functions of level N defined over $\mathbb{Q}_N$, respectively. Then we have $\mathcal{F}_1 = \mathbb{Q}(j)$ and $\mathcal{K}(X(1)) = \mathbb{C}(j)$ [15,20]. Furthermore we let

$$\begin{aligned} \mathcal{R}_N &= \text{the integral closure of } \mathbb{Z}[j] \text{ in } \mathcal{F}_N \\ \mathbb{Q}\mathcal{R}_N &= \text{the integral closure of } \mathbb{Q}[j] \text{ in } \mathcal{F}_N. \end{aligned}$$

Here, the elements of $(\mathbb{Q}\mathcal{R}_N)^*$ will be called the *modular units* of level N and those of $\mathcal{R}_N^*$ will be called the *modular units over* $\mathbb{Z}$ of level N. And we have the diagram:

$$\begin{array}{ccc} \mathcal{F}_N & \text{———————} & \mathbb{Q}\mathcal{R}_N \supset (\mathbb{Q}\mathcal{R}_N)^* : \text{group of modular units} \\ \Big| & & \Big| \\ \text{Galois} & & \text{integral} \\ \text{extension} & & \text{closure} \\ \Big| & & \Big| \\ \mathcal{F}_1 & \text{———————} & \mathbb{Q}[j] \end{array}$$

The points τ on the modular curve $X(N)$ such that $j(\tau) = \infty$ are called the *cusps*. We then recall the following assertion which interprets algebraic objects as geometric ones. For the sake of completeness we give a proof.

Lemma 2.1 *If $f \in \mathcal{F}_N$ has zeros and poles only at the cusps, then the norm $\mathbf{N}_{\mathcal{F}_N/\mathbb{Q}_N(j)}(f)$ is a constant. Hence, so is $\mathbf{N}_{\mathcal{F}_N/\mathcal{F}_1}(f)$.*

Proof As we shall summarize in Sect. 4, $\mathrm{Gal}(\mathcal{F}_N/\mathbb{Q}_N(j))$ has a representation by $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1_2\}$ and the action of each element in $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1_2\}$ is given by composition. Hence if a function $f \in \mathcal{F}_N$ has zeros and poles only at the cusps, so does $\mathbf{N}_{\mathcal{F}_N/\mathbb{Q}_N(j)}(f)$.

On the other hand, $\mathbf{N}_{\mathcal{F}_N/\mathbb{Q}_N(j)}(f) \in \mathbb{Q}_N(j)$ is a function on the Riemann sphere $X(1)$. So, if it is not a constant, it has zeros and poles at least at two distinct points on the sphere. But this means that $\mathbf{N}_{\mathcal{F}_N/\mathbb{Q}_N(j)}(f)$ should have a zero or a pole on $\mathfrak{H}$, which contradicts the first part of the proof. Therefore $\mathbf{N}_{\mathcal{F}_N/\mathbb{Q}_N(j)}(f)$ is a constant, and so is $\mathbf{N}_{\mathcal{F}_N/\mathcal{F}_1}(f)$. □

Theorem 2.2 *Let $f \in \mathcal{F}_N$. Then f is a modular unit if and only if it has zeros and poles only at the cusps.*

Proof Assume that f is a modular unit. Then f and $1/f$ satisfy integral equations over $\mathbb{Q}[j]$, that is,

$$\begin{aligned} f^n + a_{n-1}f^{n-1} + \cdots + a_0 &= 0 \\ \frac{1}{f^m} + b_{m-1}\frac{1}{f^{m-1}} + \cdots + b_0 &= 0 \end{aligned}$$

for some $a_{n-1}, \ldots, a_0, b_{m-1}, \ldots, b_0 \in \mathbb{Q}[j]$. Dividing the first equation by f^n and multiplying the second by f^m we achieve

$$1 + a_{n-1}\frac{1}{f} + \cdots + a_0\frac{1}{f^n} = 0 \tag{2.1}$$

$$1 + b_{m-1}f + \cdots + b_0 f^m = 0. \tag{2.2}$$

Suppose that f has a zero at some point $\tau_0 \in \mathfrak{H}$. By (2.2) we get

$$1 + b_{m-1}(\tau_0) f(\tau_0) + \cdots + b_0(\tau_0) f(\tau_0)^m = 0,$$

which gives a contradiction $1 = 0$. Next suppose that f has a pole at some point $\tau_\infty \in \mathfrak{H}$. Then by (2.1) we have

$$1 + a_{n-1}(\tau_\infty) \frac{1}{f(\tau_\infty)} + \cdots + a_0(\tau_\infty) \frac{1}{f(\tau_\infty)^n} = 0,$$

which again renders a contradiction $1 = 0$. Thus f does not have zeros and poles on $\mathfrak{H}$, namely f has zeros and poles only at the cusps.

Conversely, assume that f has zeros and poles only at the cusps. Since $\mathbb{Q}[j]$ is a Dedekind domain, so is $\mathbb{Q}\mathcal{R}_N$. Hence

$$\mathbb{Q}\mathcal{R}_N = \bigcap_{\mathfrak{P}} (\mathbb{Q}\mathcal{R}_N)_{\mathfrak{P}} \tag{2.3}$$

where the intersection is taken over all prime ideals $\mathfrak{P}$ of $\mathbb{Q}\mathcal{R}_N$(of height 1). On the other hand, since $\mathbf{N}_{\mathcal{F}_N/\mathcal{F}_1}(f)$ is a constant by Lemma 2.1, we have $f \in ((\mathbb{Q}\mathcal{R}_N)_{\mathfrak{P}})^*$ for all prime ideals $\mathfrak{P}$ so that $f \in (\mathbb{Q}\mathcal{R}_N)^*$. Therefore f is a modular unit. □

Now, we introduce the Siegel functions as modular units. For a lattice L in $\mathbb{C}$ the *Weierstrass $\wp$-function* is defined by

$$\wp(\tau;\ L) = \frac{1}{\tau^2} + \sum_{\omega \in L \setminus \{0\}} \left\{ \frac{1}{(\tau - \omega)^2} - \frac{1}{\omega^2} \right\} \quad (\tau \in \mathbb{C}).$$

And the *Weierstrass σ-function* is defined by

$$\sigma(\tau;\ L) = \tau \prod_{\omega \in L \setminus \{0\}} \left(1 - \frac{\tau}{\omega}\right) e^{\frac{\tau}{\omega} + \frac{1}{2}\left(\frac{\tau}{\omega}\right)^2} \quad (\tau \in \mathbb{C})$$

which is clearly an odd function. Taking the logarithmic derivative we come up with the *Weierstrass ζ-function*

$$\zeta(\tau;\ L) = \frac{\sigma'(\tau;\ L)}{\sigma(\tau;\ L)} = \frac{1}{\tau} + \sum_{\omega \in L \setminus \{0\}} \left(\frac{1}{\tau - \omega} + \frac{1}{\omega} + \frac{\tau}{\omega^2} \right) \quad (\tau \in \mathbb{C}).$$

Differentiating the function $\zeta(\tau + \omega;\ L) - \zeta(\tau;\ L)$ for $\omega \in L$ results in 0 because $\zeta'(\tau;\ L) = -\wp(\tau;\ L)$ and the $\wp$-function is periodic with respect to L. Hence there is a constant $\eta(\omega;\ L)$ such that $\zeta(\tau + \omega;\ L) = \zeta(\tau;\ L) + \eta(\omega;\ L)$.

For $r = (r_1, r_2) \in \mathbb{Q}^2 \setminus \mathbb{Z}^2$ we define the *Klein form* $\mathfrak{k}_r$ by

$$\mathfrak{k}_r(\tau) = e^{-\frac{1}{2}(r_1\eta_1 + r_2\eta_2)(r_1\tau + r_2)} \sigma(r_1\tau + r_2;\ [\tau,\ 1]) \quad (\tau \in \mathbb{C}) \tag{2.4}$$

where $\eta_1 = \eta(\tau;\ [\tau,\ 1])$ and $\eta_2 = \eta(1;\ [\tau,\ 1])$. Note that η_1 and η_2 satisfy the Legendre relation $\eta_2\tau - \eta_1 = 2\pi i$ [15]. The following proposition provides us the transformation formulas of the Klein forms.

Proposition 2.3 (1) *For $r \in \mathbb{Q}^2 \setminus \mathbb{Z}^2$ we have*

$$\mathfrak{k}_{-r} = -\mathfrak{k}_r.$$

(2) *For* $r \in \mathbb{Q}^2\backslash\mathbb{Z}^2$ *and* $\alpha = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ *we derive*

$$\mathfrak{k}_r \circ \alpha = (c\tau + d)^{-1}\mathfrak{k}_{r\alpha}.$$

(3) *For* $r = (r_1, r_2) \in \mathbb{Q}^2\backslash\mathbb{Z}^2$ *and* $s = (s_1, s_2) \in \mathbb{Z}^2$ *we get*

$$\mathfrak{k}_{r+s} = \varepsilon(r, s)\mathfrak{k}_r$$

where $\varepsilon(r, s) = (-1)^{s_1 s_2 + s_1 + s_2} e^{-\pi i(s_1 r_2 - s_2 r_1)}$.

Proof Since the Weierstrass σ-function is an odd function, we can verify (1) from (2.4). For (2) and (3), see [13]. □

Finally we define the *Siegel function* g_r for any $r \in \mathbb{Q}^2\backslash\mathbb{Z}^2$ by

$$g_r(\tau) = \mathfrak{k}_r(\tau)\eta^2(\tau) \quad (\tau \in \mathfrak{H}) \tag{2.5}$$

where η is the *Dedekind* η*-function* defined by

$$\eta(\tau) = \sqrt{2\pi}\zeta_8 q_\tau^{\frac{1}{24}} \prod_{n=1}^{\infty}(1 - q_\tau^n) \quad (q_\tau = e^{2\pi i\tau},\ \tau \in \mathfrak{H})$$

and η^2 has the transformation formulas

$$\eta^2 \circ S = \zeta_{12}^9 \tau\eta^2 \tag{2.6}$$

$$\eta^2 \circ T = \zeta_{12}\eta^2 \tag{2.7}$$

for $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ and $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. Thus it follows that $\Delta(\tau) = \eta^{24}(\tau)$ is a modular form for $\mathrm{SL}_2(\mathbb{Z})$ of weight 12. We then have the following transformation formulas.

Proposition 2.4 (1) *For* $r \in \mathbb{Q}^2\backslash\mathbb{Z}^2$ *we have*

$$g_{-r} = -g_r.$$

(2) *For* $r = (r_1, r_2) \in \mathbb{Q}^2\backslash\mathbb{Z}^2$ *we get*

$$\begin{aligned} g_r \circ S &= \zeta_{12}^9 g_{rS} = \zeta_{12}^9 g_{(r_2, -r_1)} \\ g_r \circ T &= \zeta_{12} g_{rT} = \zeta_{12} g_{(r_1, r_1 + r_2)}. \end{aligned}$$

(3) *For* $r = (r_1, r_2) \in \mathbb{Q}^2\backslash\mathbb{Z}^2$ *and* $s = (s_1, s_2) \in \mathbb{Z}^2$ *we have*

$$g_{r+s} = \varepsilon(r, s)g_r$$

where $\varepsilon(r, s)$ *is the root of unity given in Proposition* 2.3(3).

Proof We can readily verify the formulas by using Proposition 2.3, (2.6) and (2.7). □

We define a function $\langle\ \rangle$ on $\mathbb{R}$ whose value $\langle X\rangle$ takes the fractional part of X, namely $0 \le \langle X\rangle < 1$. Then, for $\alpha = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ with $c > 0$ we have the transformation formula

$$\eta^2\left(\frac{a\tau + b}{c\tau + d}\right) = e^{2\pi i\left(\frac{a+d}{12c} + \frac{1}{2} + \sum_{\mu(\mathrm{mod}\ c)} \mathbf{B}_1(\langle\frac{\mu}{c}\rangle)\mathbf{B}_1\left(\left\langle\frac{d\mu}{c}\right\rangle\right)\right)}(c\tau + d)\eta^2(\tau)$$

where $\mathbf{B}_1(X) = X - \frac{1}{2}$ is the first Bernoulli polynomial [3, (2.10)]. Thus it follows from Proposition 2.3(2) and the definition $g_r = \mathfrak{k}_r\eta^2$ that

$$g_r \circ \alpha = e^{2\pi i\left(\frac{a+d}{12c} + \frac{1}{2} + \sum_{\mu(\mathrm{mod}c)} \mathbf{B}_1(\langle\frac{\mu}{c}\rangle)\mathbf{B}_1\left(\left\langle\frac{d\mu}{c}\right\rangle\right)\right)} g_{r\alpha}$$

for $r \in \mathbb{Q}\backslash\mathbb{Z}^2$. When one is particularly interested in constructing class fields, he may efficiently use this formula.

In addition to these transformation formulas a Siegel function has a fairly simple order formula. Let $\mathbf{B}_2(X) = X^2 - X + \frac{1}{6}$ be the second Bernoulli polynomial. Using the q_τ-expansion formula of the Weierstrass σ-function we get the following expansion formula of a Siegel function g_r

$$g_{(r_1,r_2)}(\tau) = -q_\tau^{\frac{1}{2}\mathbf{B}_2(r_1)} e^{\pi i r_2(r_1-1)}(1-q_z)\prod_{n=1}^{\infty}(1-q_\tau^n q_z)(1-q_\tau^n q_z^{-1}) \tag{2.8}$$

where $q_z = e^{2\pi i z}$ with $z = r_1\tau + r_2$. By analyzing (2.8) we obtain

$$\mathrm{ord}_{q_\tau} g_{(r_1,r_2)} = \frac{1}{2}\mathbf{B}_2(\langle r_1\rangle) \tag{2.9}$$

[13, Chapter 2, Section 1].

For a given positive integer $N > 1$, Kubert and Lang provided a necessary and sufficient condition for a product of Siegel functions to be of level N. Here we give a sufficient condition as follows. We say that a family of integers $\{m(r)\}_{r=(r_1,r_2)\in\frac{1}{N}\mathbb{Z}^2\backslash\mathbb{Z}^2}$ with $m(r) = 0$ except finitely many r satisfies the *quadratic relation* modulo N if

$$\sum_r m(r)(Nr_1)^2 \equiv \sum_r m(r)(Nr_2)^2 \equiv 0 \pmod{\gcd(2, N)\cdot N}$$
$$\sum_r m(r)(Nr_1)(Nr_2) \equiv 0 \pmod{N}.$$

Theorem 2.5 *Let $\{m(r)\}_{r\in\frac{1}{N}\mathbb{Z}^2\backslash\mathbb{Z}^2}$ be a family of integers such that $m(r) = 0$ except finitely many r. Then a product of Siegel functions*

$$g = \prod_{r\in\frac{1}{N}\mathbb{Z}^2\backslash\mathbb{Z}^2} g_r^{m(r)}$$

belongs to $\mathcal{F}_N$, if $\{m(r)\}_r$ satisfies the quadratic relation modulo N and 12 divides $\gcd(12, N)\cdot\sum_r m(r)$.

Proof See [13, Chapter 3, Theorems 5.2 and 5.3]. □

In particular, g_r and g_r^{12N} lie in $\mathcal{F}_{12N^2}$ and $\mathcal{F}_N$, respectively, for $r \in \frac{1}{N}\mathbb{Z}^2\backslash\mathbb{Z}^2$.

We can easily check by (2.8) that a Siegel function has zeros and poles only at the cusps. Hence by Theorems 2.2 and 2.5, we conclude that a product of Siegel functions becomes a modular unit of some level. For a given level $N > 1$ the products of Siegel functions of level N generate the group of modular units of level N up to 2-torsions [13, Chapter 4].

3 Integrality over $\mathbb{Z}[j]$

A Siegel function and its inverse are integral over $\mathbb{Q}[j]$ because they are modular units. Kubert and Lang provided in [13] a criterion for determining a product of Siegel functions to be a unit over $\mathbb{Z}$. In this section, however, we shall investigate their criterion and further develop it to have more effective test for the integrality over $\mathbb{Z}[j]$.

Let $L = [\omega_1,\ \omega_2]$ be a lattice in $\mathbb{C}$ such that $\omega_1/\omega_2 \in \mathfrak{H}$. For a point $t \in \mathbb{C}\backslash L$ of finite period with respect to L, we can write t as

$$t = r_1\omega_1 + r_2\omega_2$$

for a unique $r = (r_1, r_2) \in \mathbb{Q}^2\backslash\mathbb{Z}^2$. We define a function

$$g\left(t;\ \begin{pmatrix}\omega_1\\ \omega_2\end{pmatrix}\right) = g_r\left(\frac{\omega_1}{\omega_2}\right), \tag{3.1}$$

which depends on the choice of ω_1 and ω_2. But if we raise g to the 12-th power, it becomes a function of t and L and so we just write it as $g^{12}(t;\ L)$. Furthermore $g^{12}(t;\ L)$ has weight 0, namely

$$g^{12}(\lambda t;\ \lambda L) = g^{12}(t;\ L) \tag{3.2}$$

for any $\lambda \in \mathbb{C}^*$.

Theorem 3.1 *Let $L' \supset L$ be two lattices in $\mathbb{C}$ and let c be the smallest positive integer such that $cL' \subset L$. Let*

$$t_1 = 0, \ldots, t_k$$

be a complete system of coset representatives of L'/L. If t is a complex number such that $t \notin L'$, $dt \in L$ for some positive integer d and $m = \mathrm{lcm}(c, d)$, then we have

$$g^{12m}(t;\ L') = \prod_{i=1}^{k} g^{12m}(t + t_i;\ L).$$

Proof See [13, Chapter 2 Theorem 4.1(ii)]. □

For a vector $r = (r_1, r_2) \in \mathbb{Q}^2\backslash\mathbb{Z}^2$, a positive integer N such that $Nr = (Nr_1, Nr_2)$ belongs to $\mathbb{Z}^2$ is called a *denominator* of r. In particular, the smallest denominator of r is called the *primitive denominator* of r. When the primitive denominator has at least two prime factors, we say that r or the primitive denominator is *composite*.

In what follows by the notation $\doteq$ we mean the equality = up to a root of unity. As a corollary of Theorem 3.1, we give a so-called distribution relation of Siegel functions.

Corollary 3.2 *Let p^n be a prime power and let $r = (r_1, r_2) \in \frac{1}{p^n}\mathbb{Z}^2\backslash\mathbb{Z}^2$. Then the Siegel function g_r can be written as a product*

$$g_r \doteq \prod_s g_s^{m(s)}$$

where all indices s with $m(s) \neq 0$ have the same primitive denominator p^n.

Proof If r already has the primitive denominator p^n, we are done. Suppose that r has the primitive denominator p^l with $l < n$. In the statement of Theorem 3.1 we set

$$L' = \frac{1}{p}[\tau,\ 1],\ L = [\tau,\ 1] \quad \text{and} \quad t = \frac{r_1\tau + r_2}{p}.$$

Then we have $k = [L' : L] = p^2$, $c = p$, $d = p^{l+1}$ and $m = p^{l+1}$. Taking

$$\frac{a\tau + b}{p} \quad \text{with} \quad 0 \le a,\ b < p$$

as a complete system of coset representatives of L/L' we get that

$$\begin{aligned} g_{(r_1,r_2)}^{12p^{l+1}}(\tau) &= g^{12p^{l+1}}(r_1\tau + r_2;\ [\tau,\ 1]) \\ &= g^{12p^{l+1}}\left(\frac{r_1\tau + r_2}{p};\ \frac{1}{p}[\tau,\ 1]\right) \quad \text{by (3.2)} \\ &= \prod_{0\le a,\ b<p} g^{12p^{l+1}}\left(\frac{r_1\tau + r_2}{p} + \frac{a\tau + b}{p};\ [\tau,\ 1]\right) \quad \text{by Theorem 3.1} \\ &= \prod_{0\le a,\ b<p} g^{12p^{l+1}}\left(\frac{r_1 + a}{p}\tau + \frac{r_2 + b}{p};\ [\tau,\ 1]\right) \\ &= \prod_{0\le a,\ b<p} g_{\left(\frac{r_1+a}{p},\frac{r_2+b}{p}\right)}^{12p^{l+1}}(\tau). \end{aligned}$$

Deleting the power $12p^{l+1}$ we establish

$$g_{(r_1,r_2)} \doteq \prod_{0\le a,\ b<p} g_{\left(\frac{r_1+a}{p},\frac{r_2+b}{p}\right)}.$$

Note that each index $(\frac{r_1+a}{p}, \frac{r_2+b}{p})$ in the above product has the primitive denominator p^{l+1}. Applying this procedure successively we can express g_r as a product of Siegel functions indexed with vectors of primitive denominator p^n. □

Let N be a given positive integer. For a modular unit f of level N, let

$$f = \sum_n c_n q_\tau^{\frac{n}{N}}$$

be its q_τ-expansion. We write

$$c_n(f) = c_n$$

for all $n \in \mathbb{Z}$ and, in particular,

$$c(f) = \text{the first non-zero coefficient.}$$

When we write

$$f = c(f) f^*,$$

we understand f^* as a q_τ-series with leading coefficient 1. For $f,\ f' \in (\mathbb{Q}\mathcal{R}_N)^*$ we have obvious identities

$$c(f \cdot f') = c(f) \cdot c(f') \tag{3.3}$$

$$(f \cdot f')^* = f^* \cdot f'^*. \tag{3.4}$$

Lemma 3.3 *Let f be a modular unit of level N. If $c_n(f \circ \alpha)$ are algebraic integers for all $n \in \mathbb{Z}$ and $\alpha \in \mathrm{SL}_2(\mathbb{Z})$, then f is integral over $\mathbb{Z}[j]$. If, in addition, $c(f \circ \alpha)$ are units for all $\alpha \in \mathrm{SL}_2(\mathbb{Z})$, then f is a unit over $\mathbb{Z}$.*

Proof See [13] Lemma 2.1. □

Remark 3.4 [13] Lemma 2.1 is a slightly weaker version of Lemma 3.3 which will be used in the matter of determining integrality over $\mathbb{Z}[j]$.

For $N > 1$ and $r = (r_1, r_2) \in \frac{1}{N}\mathbb{Q}^2\backslash\mathbb{Z}^2$, let us write

$$g_r = c(g_r)g_r^*$$
$$g_{(\langle r_1\rangle,\langle r_2\rangle)} = c(g_{(\langle r_1\rangle,\langle r_2\rangle)})g^*_{(\langle r_1\rangle,\langle r_2\rangle)}.$$

Since $g_r \doteq g_{(\langle r_1\rangle,\langle r_2\rangle)}$ by Proposition 2.4(3), we deduce

$$c(g_r) \doteq c(g_{(\langle r_1\rangle,\langle r_2\rangle)})$$
$$g_r^* = g^*_{(\langle r_1\rangle,\langle r_2\rangle)}.$$

Note that from the q_τ-expansion formula (2.8) we see that $g^*_{(\langle r_1\rangle,\langle r_2\rangle)}$ has in fact a q_τ-series all of whose coefficients are algebraic integers and has leading coefficient 1. Hence $c_n(g_r)$ are algebraic integers for all $n \in \mathbb{Z}$ if and only if $c(g_r)$ is an algebraic integer. The same argument holds for any conjugate of a Siegel function and any product of Siegel functions by Proposition 2.4(2), (3.3) and (3.4). Thus we have

Lemma 3.5 *Let g be a product of Siegel functions. Then g is integral over $\mathbb{Z}[j]$ if and only if $c(g\circ\alpha)$ are algebraic integers for all $\alpha \in \mathrm{SL}_2(\mathbb{Z})$.*

Proof First assume that g is integral over $\mathbb{Z}[j]$, then g satisfies an equation

$$g^m + a_{m-1}g^{m-1} + \cdots + a_0 = 0$$

for some $a_{m-1}, \ldots, a_0 \in \mathbb{Z}[j]$. Taking composition with any $\alpha \in \mathrm{SL}_2(\mathbb{Z})$ on both sides yields

$$(g\circ\alpha)^m + a_{m-1}(g\circ\alpha)^{m-1} + \cdots + a_0 = 0,$$

from which it follows that

$$\{c(g\circ\alpha)\}^m\left\{(g\circ\alpha)^*\right\}^m + a_{m-1}\{c(g\circ\alpha)\}^{m-1}\left\{(g\circ\alpha)^*\right\}^{m-1} + \cdots + a_0 = 0. \quad (3.5)$$

When the left side of (3.5) is regarded as a q_τ-series, each coefficient of the series should be zero. Note that the coefficients of q_τ-series of j and $(g\circ\alpha)^*$ are algebraic integers. Hence, when $t = \mathrm{ord}_{q_\tau}(g\circ\alpha)^*$, the coefficient of the term q_τ^{tm} in (3.5) is given by $\{c(g\circ\alpha)\}^m + b_{m-1}\{c(g\circ\alpha)\}^{m-1} + \cdots + b_0 = 0$ for some algebraic integers $b_{m-1}, \ldots, b_0$. This implies that $c(g\circ\alpha)$ is an algebraic integer.

Conversely, assume that $c(g\circ\alpha)$ are algebraic integers for all $\alpha \in \mathrm{SL}_2(\mathbb{Z})$. Then $c_n(g\circ\alpha)$ are algebraic integers for all $n \in \mathbb{Z}$. And, the assertion is a consequence of Lemma 3.3. □

Theorem 3.6 *Let $r \in \mathbb{Q}^2\backslash\mathbb{Z}^2$ have the primitive denominator $N > 1$.*

(1) *If N is composite, then g_r^{12N} is a modular unit over $\mathbb{Z}$ of level N. Hence g_r is a modular unit over $\mathbb{Z}$ of level $12N^2$.*
(2) *If $N = p^n$ is a prime power, then g_r^{12N} is a unit in $R_N[\frac{1}{p}]$. Thus g_r is a unit in $R_{12N^2}[\frac{1}{p}]$.*

Proof See [13] Chapter 2 Theorem 2.2. □

Let p^n be a prime power and suppose that $r = (r_1, r_2) \in \mathbb{Q}^2\backslash\mathbb{Z}^2$ has the primitive denominator p^n. Then the constant $c(g_r)$ has the property

$$c(g_r) \doteq c(g_{(\langle r_1\rangle,\langle r_2\rangle)}) \doteq \begin{cases} 1 & \text{if } \langle r_1\rangle \neq 0 \\ 1 - e^{2\pi i\langle r_2\rangle} = 1 - \zeta_{p^n}^{p^n\langle r_2\rangle} & \text{if } \langle r_1\rangle = 0 \end{cases}$$

from the q_τ-expansion formula (2.8). Hence

$$\operatorname{ord}_p(c(g_r)) = \begin{cases} 0 & \text{if } \langle r_1 \rangle \neq 0 \\ \operatorname{ord}_p\left(1 - \zeta_{p^n}^{p^n \langle r_2 \rangle}\right) = \frac{1}{\phi(p^n)} & \text{if } \langle r_1 \rangle = 0 \end{cases} \tag{3.6}$$

where ϕ is the Euler ϕ-function, and

$$\operatorname{ord}_{p'}(c(g_r)) = 0 \quad \text{for other primes } p'. \tag{3.7}$$

Lemma 3.7 *For a prime power p^n, consider a product of Siegel functions*

$$g_{(p)} = \prod_{r \in \frac{1}{p^n}\mathbb{Z}^2 \setminus \mathbb{Z}^2} g_r^{m(r)}.$$

Then $g_{(p)}$ is integral over $\mathbb{Z}[j]$ if and only if $\operatorname{ord}_p(c(g_{(p)} \circ \alpha)) \geq 0$ for all $\alpha \in \mathrm{SL}_2(\mathbb{Z})$.

Proof By (3.6) and (3.7), $c(g_{(p)} \circ \alpha)$ are algebraic integers if and only if $\operatorname{ord}_p(c(g_{(p)} \circ \alpha)) \geq 0$. Hence we get our assertion by Lemma 3.5. □

Lemma 3.8 *For a given product of Siegel functions*

$$g = \prod_{r \in \frac{1}{N}\mathbb{Z}^2 \setminus \mathbb{Z}^2} g_r^{m(r)},$$

decompose it into the form

$$g = g_{\mathrm{comp}} \prod_p g_{(p)}$$

where g_{comp} is the product taken over all composite r and $g_{(p)}$ for each prime p is the product taken over those r whose denominator is a power of p. Then g is integral over $\mathbb{Z}[j]$ if and only if $g_{(p)}$ are integral over $\mathbb{Z}[j]$ for all primes p.

Proof By Theorem 3.6, g_{comp} is a unit over $\mathbb{Z}$. Hence we deduce an assertion that

$$\begin{aligned} & g \text{ is integral over } \mathbb{Z}[j] \\ \iff & \prod_p g_{(p)} \text{ is integral over } \mathbb{Z}[j] \\ \iff & c\left(\prod_p g_{(p)} \circ \alpha\right) \text{ are algebraic integers for all } \alpha \in \mathrm{SL}_2(\mathbb{Z}) \quad \text{by Lemma 3.5} \\ \iff & \operatorname{ord}_p\left(c\left(\prod_p g_{(p)} \circ \alpha\right)\right) \geq 0 \text{ for all primes } p. \end{aligned}$$

On the other hand, for a fixed prime p we have by (3.7)

$$\operatorname{ord}_p\left(\prod_p c(g_{(p)})\right) = \operatorname{ord}_p(c(g_{(p)})).$$

Thus, we achieve that

$$\begin{aligned} & g \text{ is integral over } \mathbb{Z}[j] \\ \iff & \operatorname{ord}_p\left(c(g_{(p)})\right) \geq 0 \text{ for all primes } p \\ \iff & g_{(p)} \text{ are integral over } \mathbb{Z}[j] \text{ for all primes } p \text{ by Lemma 3.7.} \end{aligned}$$

□

Therefore we restrict ourselves to analyzing each $g_{(p)}$ separately. Let p^n be the maximal primitive denominator appearing in the indices of $g_{(p)}$ and $(\frac{1}{p^n}\mathbb{Z}^2/\mathbb{Z}^2)^*$ be the set of all primitive elements in the additive group $\frac{1}{p^n}\mathbb{Z}^2/\mathbb{Z}^2$. By Corollary 3.2 we may assume that all indices have the primitive denominator p^n. Moreover, by Proposition 2.4(1) and (3) we take $(\frac{1}{p^n}\mathbb{Z}^2/\mathbb{Z}^2)^*/\pm 1$ as the index set. And, note that the group $(\mathbb{Z}/p^n\mathbb{Z})^*$ naturally acts on $(\frac{1}{p^n}\mathbb{Z}^2/\mathbb{Z}^2)^*/\pm 1$ by multiplication.

Theorem 3.9 *Let*

$$g_{(p)} \doteq \prod_{r\in(\frac{1}{p^n}\mathbb{Z}^2/\mathbb{Z}^2)^*/\pm 1} g_r^{m(r)}.$$

Then $g_{(p)}$ is integral over $\mathbb{Z}[j]$ if and only if for each orbit of $(\mathbb{Z}/p^n\mathbb{Z})^*$ we get

$$\sum_{r\in orbit} m(r) \geq 0.$$

Proof By Lemma 3.7 we know that $g_{(p)}$ is integral over $\mathbb{Z}[j]$ if and only if $\mathrm{ord}_p(c(g_{(p)}\circ\alpha)) \geq 0$ for all $\alpha \in \mathrm{SL}_2(\mathbb{Z})$. It then follows from (3.6) that

$$\mathrm{ord}_p(c(g_{(p)})) \geq 0 \Longleftrightarrow \sum_{r\in\text{orbit containing } \left(0,\frac{1}{p^n}\right)} m(r) \geq 0.$$

Furthermore since $\mathrm{SL}_2(\mathbb{Z})$ permutes the orbits transitively, we conclude that

$$\mathrm{ord}_p\left(c(g_{(p)}\circ\alpha)\right) \geq 0 \quad \text{for all } \alpha \in \mathrm{SL}_2(\mathbb{Z}) \Longleftrightarrow \sum_{r\in\text{orbit}} m(r) \geq 0 \quad \text{for each orbit.}$$

□

Before closing this section we summarize the algorithm for determining whether a product of Siegel functions is integral over $\mathbb{Z}[j]$ or not as follows:

Step 1. For a product of Siegel functions

$$g = \prod_{r\in\frac{1}{N}\mathbb{Z}^2\setminus\mathbb{Z}^2} g_r^{m(r)},$$

decompose it into the form

$$g = g_{\mathrm{comp}} \prod_{p\,:\,\text{prime}} g_{(p)}.$$

Step 2. For each prime number p, let p^n be the maximal primitive denominator appearing in the indices of $g_{(p)}$. Using Corollary 3.2 we can write $g_{(p)}$ as

$$g_{(p)} \doteq \prod_{r\in\left(\frac{1}{p^n}\mathbb{Z}^2/\mathbb{Z}^2\right)^*/\pm 1} g_r^{m(r)}.$$

Step 3. For each orbit of $(\mathbb{Z}/p^n\mathbb{Z})^*$ in $(\frac{1}{p^n}\mathbb{Z}^2/\mathbb{Z}^2)^*/\pm 1$, check if

$$\sum_{r\in\text{orbit}} m(r) \geq 0.$$

Step 4. Then g is integral over $\mathbb{Z}[j]$ if and only if the third step is true for each prime p.

4 Field of modular functions of level N

For a congruence subgroup Γ we denote by $\mathcal{K}(X(\Gamma))$ the function field of the modular curve $X(\Gamma) = \Gamma\backslash\mathfrak{H}^*$. Let h be the width of the cusp ∞. For a subfield $\mathbb{Q}'$ of the maximal abelian extension $\mathbb{Q}_{ab}$ of $\mathbb{Q}$, let $\mathcal{K}'$ be the field of all modular functions in $\mathcal{K}(X(\Gamma))$ whose Fourier coefficients with respect to $q_\tau^{\frac{1}{h}} = e^{\frac{2\pi i\tau}{h}}$ belong to $\mathbb{Q}'$.

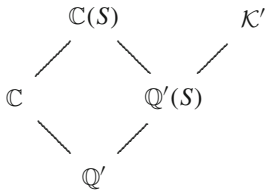
Lemma 4.1 *Let $\mathcal{K}(X(\Gamma)) = \mathbb{C}(S)$ for a subset S in $\mathcal{K}(X(\Gamma))$. If $S \subset \mathcal{K}'$, then $\mathcal{K}' = \mathbb{Q}'(S)$.*

Proof First note that $\mathbb{C}$ and $\mathcal{K}'$ are linearly disjoint over $\mathbb{Q}'$. Indeed, let $c_1, \ldots, c_m$ be the elements of $\mathbb{C}$ which are linearly independent over $\mathbb{Q}'$. Assume that $\sum_{k=1} c_k f_k = 0$ for some $f_1, \ldots, f_m \in \mathcal{K}'$. Writing $f_k = \sum_{n=-\infty}^{\infty} c_{kn} q_\tau^{\frac{n}{h}}$ with $c_{kn} \in \mathbb{Q}'$, we have

$$\sum_{k=1}^{m} c_k f_k = \sum_{k=1}^{m} c_k \sum_{n=-\infty}^{\infty} c_{kn} q_\tau^{\frac{n}{h}} = \sum_{n=-\infty}^{\infty} \left(\sum_{k=1}^{m} c_k c_{kn} \right) q_\tau^{\frac{n}{h}} = 0,$$

which yields $\sum_{k=1}^{m} c_k c_{kn} = 0$ for each $n \in \mathbb{Z}$. Since $c_1, \ldots, c_m$ are linearly independent over $\mathbb{Q}'$, we have $c_{kn} = 0$ for all k and n. Hence $f_1 = \cdots = f_m = 0$.

Now consider the field tower:



Since $\mathbb{C}(S)$ and $\mathcal{K}'$ are linearly disjoint over $\mathbb{Q}'(S)$ [14, VIII Proposition 3.1], we have

$$1 \le [\mathcal{K}' : \mathbb{Q}'(S)] \le [\mathbb{C}\mathcal{K}' : \mathbb{C}(S)] \le [\mathcal{K}(X(\Gamma)) : \mathcal{K}(X(\Gamma))],$$

which yields that $\mathcal{K}' = \mathbb{Q}'(S)$. □

Now we turn our interest to the study of modular function fields. Since the algebraic closure of $\mathbb{Q}$ in $\mathcal{F}_N$ is $\mathbb{Q}_N$, we have $\mathrm{Gal}\,(\mathcal{F}_N/\mathbb{Q}_N(j)) \cong \mathrm{Gal}\,(\mathcal{K}(X(N))/\mathcal{K}(X(1)))$. And, as is well-known $\mathrm{Gal}\,(\mathcal{K}(X(N))/\mathcal{K}(X(1)))$ has the representation

$$\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1_2\} \cong \Gamma_1/\pm\Gamma(N)$$

where each element of $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1_2\}$ acts on modular functions by composition. For the representation of $\mathrm{Gal}(\mathcal{F}_N/\mathcal{F}_1)$, we first note that

$$\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1_2\} = G_N \cdot \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1_2\} = \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1_2\} \cdot G_N \quad (4.1)$$

where

$$G_N = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix} \ : \ d \in (\mathbb{Z}/N\mathbb{Z})^* \right\}.$$

For an element $\left(\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix}\right) \in G_N$, let σ_d be the automorphism of $\mathbb{Q}_N$ defined by $\zeta_N^{\sigma_d} = \zeta_N^d$. This automorphism σ_d is naturally extended to $\mathcal{F}_N$ by

$$\sum_n c_n q_\tau^{\frac{n}{N}} \mapsto \sum_n c_n^{\sigma_d} q_\tau^{\frac{n}{N}}$$

where $\sum_n c_n q_\tau^{n/N}$ is the q_τ-expansion of a modular function. Then $\mathrm{Gal}(\mathcal{F}_N/\mathcal{F}_1)$ has the representation $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1_2\}$ from the decomposition (4.1) [15,20].

Next we exhibit generators of the function field $\mathcal{F}_N$ in terms of Siegel functions and explain the action of $\mathrm{Gal}(\mathcal{F}_N/\mathcal{F}_1)$ on them explicitly. Consider the *first Weber function* defined by

$$f_0(z;\ L) = -2^7 3^5 \frac{g_2(L)g_3(L)}{\Delta(L)} \wp(z;\ L) \quad (z \in \mathbb{C},\ L \text{ a lattice in } \mathbb{C})$$

where $g_2(L) = 60 \sum_{w \in L\setminus\{0\}} \frac{1}{w^4}$, $g_3(L) = 140 \sum_{w \in L\setminus\{0\}} \frac{1}{w^6}$ and $\Delta(L) = g_2^3(L) - 27 g_3^2(L)$. For $(a, b) \in \mathbb{Z}^2 \setminus N\mathbb{Z}^2$, we let

$$f_{\left(\frac{a}{N}, \frac{b}{N}\right)}(\tau) = f_0\left(\frac{a}{N}\tau + \frac{b}{N};\ [\tau, 1]\right).$$

Then we have

$$\mathcal{F}_N = \mathbb{Q}\left(j,\ f_{\left(\frac{a}{N}, \frac{b}{N}\right)}\right)_{\forall (a,b) \in \mathbb{Z}^2 \setminus N\mathbb{Z}^2}$$
$$\mathcal{K}(X(N)) = \mathbb{C}\mathcal{F}_N.$$

The action of $\alpha \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ is described by the rule

$$f^\alpha_{\left(\frac{a}{N}, \frac{b}{N}\right)} = f_{\left(\frac{a}{N}, \frac{b}{N}\right)\alpha}$$

[15,20]. We can then restate these fields in terms of Siegel functions as follows:

Theorem 4.2 *For $N > 1$, we have*

$$\mathcal{K}(X(N)) = \mathbb{C}\left(j,\ g^{12N}_{\left(\frac{a}{N}, \frac{b}{N}\right)}\right)_{\forall (a,b) \in \mathbb{Z}^2 \setminus N\mathbb{Z}^2} = \mathbb{C}\left(j,\ g^{12N}_{\left(\frac{1}{N}, 0\right)},\ g^{12N}_{\left(0, \frac{1}{N}\right)}\right)$$
$$\mathcal{F}_N = \mathbb{Q}_N\left(j,\ g^{12N}_{\left(\frac{1}{N}, 0\right)},\ g^{12N}_{\left(0, \frac{1}{N}\right)}\right).$$

Proof Put

$$E = \mathbb{C}\left(j,\ g^{12N}_{\left(\frac{a}{N}, \frac{b}{N}\right)}\right)_{\forall (a,b) \in \mathbb{Z}^2 \setminus N\mathbb{Z}^2}$$

which is a subfield of $\mathcal{K}(X(N))$ over $\mathcal{K}(X(1))$. We shall show that any element $\gamma \in \Gamma_1$ which acts trivially on E must lie in $\pm\Gamma(N)$. Then E should be all of $\mathcal{K}(X(N))$ by Galois theory. To this end, we consider the effect of γ on two functions $g^{12N}_{(\frac{1}{N}, 0)}$ and $g^{12N}_{(0, \frac{1}{N})}$. Letting $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ we have by Proposition 2.4(2)

$$\left(g^{12N}_{\left(\frac{1}{N}, 0\right)}\right)^\gamma = g^{12N}_{\left(\frac{1}{N}, 0\right)\gamma} = g^{12N}_{\left(\frac{a}{N}, \frac{b}{N}\right)}$$
$$\left(g^{12N}_{\left(0, \frac{1}{N}\right)}\right)^\gamma = g^{12N}_{\left(0, \frac{1}{N}\right)\gamma} = g^{12N}_{\left(\frac{c}{N}, \frac{d}{N}\right)}.$$

Since the action of γ is trivial, we establish

$$g^{12N}_{\left(\frac{a}{N},\frac{b}{N}\right)} = g^{12N}_{\left(\frac{1}{N},0\right)} \tag{4.2}$$

$$g^{12N}_{\left(\frac{c}{N},\frac{d}{N}\right)} = g^{12N}_{\left(0,\frac{1}{N}\right)}. \tag{4.3}$$

The action of $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ on both sides of (4.2) and (4.3) respectively yields

$$g^{12N}_{\left(-\frac{b}{N},\frac{a}{N}\right)} = g^{12N}_{\left(0,\frac{1}{N}\right)} \tag{4.4}$$

$$g^{12N}_{\left(-\frac{d}{N},\frac{c}{N}\right)} = g^{12N}_{\left(-\frac{1}{N},0\right)}. \tag{4.5}$$

Then by virtue of (2.9) we can compute the orders with respect to q_τ of both sides of (4.2)–(4.5), which read

$$12N \cdot \frac{1}{2}\mathbf{B}_2\left(\left\langle \frac{a}{N} \right\rangle\right) = 12N \cdot \frac{1}{2}\mathbf{B}_2\left(\left\langle \frac{1}{N} \right\rangle\right) \quad 12N \cdot \frac{1}{2}\mathbf{B}_2\left(\left\langle \frac{c}{N} \right\rangle\right) = 12N \cdot \frac{1}{2}\mathbf{B}_2(\langle 0 \rangle)$$

$$12N \cdot \frac{1}{2}\mathbf{B}_2\left(\left\langle -\frac{b}{N} \right\rangle\right) = 12N \cdot \frac{1}{2}\mathbf{B}_2(\langle 0 \rangle) \quad 12N \cdot \frac{1}{2}\mathbf{B}_2\left(\left\langle -\frac{d}{N} \right\rangle\right) = 12N \cdot \frac{1}{2}\mathbf{B}_2\left(\left\langle -\frac{1}{N} \right\rangle\right).$$

Together with the fact $\det(\gamma) = 1$ we have $a \equiv d \equiv \pm 1 \pmod{N}$ and $b \equiv c \equiv 0 \pmod{N}$. Hence γ lies in $\pm\Gamma(N)$, which proves $E = \mathcal{K}(X(N))$. In fact, our observation implies that $\mathcal{K}(X(N)) = \mathbb{C}\left(j, g^{12N}_{\left(\frac{1}{N},0\right)}, g^{12N}_{\left(0,\frac{1}{N}\right)}\right)$. Furthermore since j, $g^{12N}_{\left(\frac{1}{N},0\right)}$ and $g^{12N}_{\left(0,\frac{1}{N}\right)}$ have Fourier coefficients in $\mathbb{Q}_N$, we have $\mathcal{F}_N = \mathbb{Q}_N\left(j, g^{12N}_{\left(\frac{1}{N},0\right)}, g^{12N}_{\left(0,\frac{1}{N}\right)}\right)$ by Lemma 4.1. □

5 Modular functions for $\Gamma_0(N)$

In this section, we construct certain family of modular functions for the Hecke congruence group $\Gamma_0(N)$ as products of Siegel functions and find their orders, which will be used in constructing principal divisors of $X_0(p)$ supported only at the cusps and generators of some function fields $\mathcal{K}(X_0(pq))$.

Proposition 5.1 *For $N > 1$, we define a function*

$$g_N(\tau) = \prod_{n=1}^{N-1} g^{\frac{12}{\gcd(12,N-1)}}_{(0,\frac{n}{N})}(\tau).$$

Then it is modular for $\Gamma_0(N)$ and

$$\operatorname{ord}_{q_\tau} g_N = \frac{N-1}{\gcd(12, N-1)}.$$

Proof Using the indentity

$$\frac{1-X^N}{1-X} = (1-\zeta_N X)(1-\zeta_N^2 X)\cdots(1-\zeta_N^{N-1} X)$$

and by the q_τ-expansion formula (2.8), we can easily see that

$$\prod_{n=1}^{N-1} g_{(0,\frac{n}{N})}(\tau) = Ne^{\pi i \frac{N-1}{2}} \frac{\eta^2(N\tau)}{\eta^2(\tau)}. \tag{5.1}$$

Thus

$$g_N(\tau) = \left(N\frac{\eta^2(N\tau)}{\eta^2(\tau)}\right)^{\frac{12}{\gcd(12,N-1)}}.$$

Instead of referring certain theorem about Dedekind eta functions [17, Theorem 1.64], we shall directly verify the proposition by making use of the transformation formulas of Klein forms.

Let $\alpha = \left(\begin{smallmatrix} a & b \\ Nc & d \end{smallmatrix}\right)$ with $a, b, c, d \in \mathbb{Z}$ be an element of $\Gamma_0(N)$. Then by Proposition 2.3(2) and (3) we obtain that

$$\begin{aligned}
g_N \circ \alpha &= \left\{\prod_{n=1}^{N-1} (\mathfrak{k}_{(0,\frac{n}{N})} \circ \alpha)(\eta^2 \circ \alpha)\right\}^{\frac{12}{\gcd(12,N-1)}} && \text{by (2.5)} \\
&= \left\{\prod_{n=1}^{N-1} \mathfrak{k}_{(0,\frac{n}{N})\alpha}(Nc\tau + d)^{-1}(\eta^2 \circ \alpha)\right\}^{\frac{12}{\gcd(12,N-1)}} && \text{by Proposition 2.3(2)} \\
&= \left\{\prod_{n=1}^{N-1} \mathfrak{k}_{\left(cn,\frac{dn}{N}\right)}\right\}^{\frac{12}{\gcd(12,N-1)}} \left\{(Nc\tau + d)^{-12}(\eta^{24} \circ \alpha)\right\}^{\frac{N-1}{\gcd(12,N-1)}} \\
&= \left\{\prod_{n=1}^{N-1} \mathfrak{k}_{\left(0,\frac{dn}{N}\right)+(cn,0)}\right\}^{\frac{12}{\gcd(12,N-1)}} (\eta^{24})^{\frac{N-1}{\gcd(12,N-1)}} \\
&= \left\{\prod_{n=1}^{N-1} \mathfrak{k}_{\left(0,\frac{dn}{N}\right)}(-1)^{cn} e^{-\pi i \cdot \frac{cdn^2}{N}}\right\}^{\frac{12}{\gcd(12,N-1)}} (\eta^{24})^{\frac{N-1}{\gcd(12,N-1)}} && \text{by Proposition 2.3(3)} \\
&= \left\{\prod_{n=1}^{N-1} \mathfrak{k}_{\left(0,\frac{dn}{N}\right)} \cdot (-1)^{\frac{c(N-1)N}{2}} e^{-\pi i \cdot \frac{cd(N-1)(2N-1)}{6}}\right\}^{\frac{12}{\gcd(12,N-1)}} (\eta^{24})^{\frac{N-1}{\gcd(12,N-1)}} \\
&= \left\{\prod_{n=1}^{N-1} \mathfrak{k}_{(0,\frac{dn}{N})}\right\}^{\frac{12}{\gcd(12,N-1)}} (\eta^{24})^{\frac{N-1}{\gcd(12,N-1)}} \\
&= \left\{\prod_{n=1}^{N-1} \mathfrak{k}_{\left(0,\left\langle\frac{dn}{N}\right\rangle\right)+\left(0,\frac{dn}{N}-\left\langle\frac{dn}{N}\right\rangle\right)}\right\}^{\frac{12}{\gcd(12,N-1)}} (\eta^{24})^{\frac{N-1}{\gcd(12,N-1)}} \\
&= \left\{\prod_{n=1}^{N-1} \mathfrak{k}_{\left(0,\left\langle\frac{dn}{N}\right\rangle\right)}(-1)^{\frac{dn}{N}-\left\langle\frac{dn}{N}\right\rangle}\right\}^{\frac{12}{\gcd(12,N-1)}} (\eta^{24})^{\frac{N-1}{\gcd(12,N-1)}} && \text{by Proposition 2.3(3)} \\
&= \left\{\prod_{n=1}^{N-1} \mathfrak{k}_{(0,\langle\frac{n}{N}\rangle)} \cdot (-1)^{\sum_n \frac{dn}{N} - \sum_n \left\langle\frac{dn}{N}\right\rangle}\right\}^{\frac{12}{\gcd(12,N-1)}} (\eta^{24})^{\frac{N-1}{\gcd(12,N-1)}}
\end{aligned}$$

$$= \left\{ \prod_{n=1}^{N-1} \mathfrak{k}_{(0,\frac{n}{N})} \cdot (-1)^{\frac{(d-1)(N-1)}{2}} \right\}^{\frac{12}{\gcd(12,N-1)}} (\eta^{24})^{\frac{N-1}{\gcd(12,N-1)}}$$

$$= \left\{ \prod_{n=1}^{N-1} \mathfrak{k}_{(0,\frac{n}{N})} \right\}^{\frac{12}{\gcd(12,N-1)}} (\eta^{24})^{\frac{N-1}{\gcd(12,N-1)}}$$

$$= \left\{ \prod_{n=1}^{N-1} \mathfrak{k}_{(0,\frac{n}{N})} \eta^2 \right\}^{\frac{12}{\gcd(12,N-1)}} \overset{(2.5)}{=} \left\{ \prod_{n=1}^{N-1} g_{(0,\frac{n}{N})} \right\}^{\frac{12}{\gcd(12,N-1)}} = g_N.$$

Hence g is modular for $\Gamma_0(N)$. Furthermore, by (2.9) we get

$$\begin{aligned} \operatorname{ord}_{q_\tau} g_N &= \frac{12}{\gcd(12, N-1)} \sum_{n=1}^{N-1} \operatorname{ord}_{q_\tau} g_{(0,\frac{n}{N})} \\ &= \frac{12}{\gcd(12, N-1)} \sum_{n=1}^{N-1} \frac{1}{2} \mathbf{B}_2(0) \\ &= \frac{N-1}{\gcd(12, N-1)}. \end{aligned}$$

□

Atkin [1] showed that for any prime p the cusp ∞ is not a Weierstrass point on the modular curve $X_0(p) = \Gamma_0(p)\backslash\mathfrak{H}^*$. This means that for any positive integer n with $1 \le n \le$ genus $\mathfrak{g}_p$ of $X_0(p)$, there does not exist any function on $X_0(p)$ which has a pole of order n at ∞ and is holomorphic elsewhere. Using this fact we shall completely determine all principal divisors of $X_0(p)$ supported only at the cusps. Note that our method is totally different from that of Ogg [16] who relied on some facts from algebraic geometry.

For this purpose we first provide some distribution relations of Siegel functions.

Theorem 5.2 (1) *For an odd prime p, if a product*

$$\prod_{r \in (\frac{1}{p}\mathbb{Z}^2/\mathbb{Z}^2)^*/\pm 1} g_r^{m(r)}$$

is a constant, then all exponents $m(r)$ are the same.

(2) *Let l and p be odd primes. Suppose that a modular function g satisfies*

$$g^l \doteq \prod_{r \in (\frac{1}{p}\mathbb{Z}^2/\mathbb{Z}^2)^*/\pm 1} g_r^{m(r)}$$

for some family of integers $\{m(r)\}_r$. Then there exists a representation

$$g = \lambda \prod_{r \in (\frac{1}{p}\mathbb{Z}^2/\mathbb{Z}^2)^*/\pm 1} g_r^{m'(r)}$$

for some family of integers $\{m'(r)\}_r$ and some $\lambda \in \mathbb{C}$.

Proof See [13, Chapters 2 and 4]. □

Theorem 5.3 *For a prime $p \geq 5$, the smallest positive integer d_p for which $d_p((0) - (\infty))$ is a principal divisor of $X_0(p)$ is given as follows*:

$$d_p = \begin{cases} \frac{p-1}{12} = \mathfrak{g}_p + 1 & \text{if } p \equiv 1 \pmod{12} \\ \frac{p-1}{4} = 3\mathfrak{g}_p + 1 & \text{if } p \equiv 5 \pmod{12} \\ \frac{p-1}{6} = 2\mathfrak{g}_p + 1 & \text{if } p \equiv 7 \pmod{12} \\ \frac{p-1}{2} = 6\mathfrak{g}_p - 1 & \text{if } p \equiv 11 \pmod{12} \end{cases}$$

where $\mathfrak{g}_p$ is the genus of the curve $X_0(p)$ [17].

Proof Note that ∞ and 0 are all the inequivalent cusps on $X_0(p)$ of widths 1 and p, respectively [10]. And every principal divisor supported only at the cusps is a multiple of the divisor $d_p((0) - (\infty))$. Since the cusp ∞ is not a Weierstass point, it follows that $d_p \geq \mathfrak{g}_p + 1$.
$p \equiv 1 \pmod{12}$. Consider a function

$$g = g_p^{-1} = \prod_{n=1}^{p-1} g_{\left(0, \frac{n}{p}\right)}^{-1}.$$

By Proposition 5.1, g is an element of $\mathcal{K}(X_0(p))$ and

$$\operatorname{ord}_\infty g = -\frac{p-1}{\gcd(12, p-1)} = -\frac{p-1}{12} = -(\mathfrak{g}_p + 1).$$

Since d_p divides the order $-(\mathfrak{g}_p + 1)$ and $d_p \geq \mathfrak{g}_p + 1$, d_p should be equal to $\mathfrak{g}_p + 1$.
$p \equiv 5 \pmod{12}$. We also consider a function

$$g = g_p^{-1} = \prod_{n=1}^{p-1} g_{\left(0, \frac{n}{p}\right)}^{-3} \doteq \prod_{n=1}^{\frac{p-1}{2}} g_{\left(0, \frac{n}{p}\right)}^{-6}.$$

Then by Proposition 5.1 we have

$$\operatorname{ord}_\infty g = -\frac{p-1}{\gcd(12, p-1)} = -\frac{p-1}{4} = -(3\mathfrak{g}_p + 1).$$

Since d_p divides the order $-(3\mathfrak{g}_p + 1)$ and $d_p \geq \mathfrak{g}_p + 1$, we get $d_p = 3\mathfrak{g}_p + 1$ or $d_p = \frac{3\mathfrak{g}_p+1}{2}$.
Suppose that $d_p = \frac{3\mathfrak{g}_p+1}{2}$, then there exists a function $f \in \mathcal{K}(X_0(p))$ such that

$$\operatorname{div}(f) = \frac{3\mathfrak{g}_p + 1}{2}((0) - (\infty)).$$

On the other hand, $\operatorname{div}(f^2 g^{-1}) = 2\operatorname{div}(f) - \operatorname{div}(g) = 0$ implies that $f^2 g^{-1}$ is a constant. So we may assume that

$$f = \prod_{n=1}^{\frac{p-1}{2}} g_{\left(0, \frac{n}{p}\right)}^{-3}.$$

Note that $d_p = \frac{3\mathfrak{g}_p+1}{2} = \frac{p-1}{8}$ is an integer. Take an element $\alpha = \left(\begin{smallmatrix} a & b \\ p & 3 \end{smallmatrix}\right)$ with $a, b \in \mathbb{Z}$ of $\Gamma_0(p)$ and observe that

$$
\begin{aligned}
f \circ \alpha &= \left\{ \prod_{n=1}^{\frac{p-1}{2}} g_{\left(0,\frac{n}{p}\right)} \circ \alpha \right\}^{-3} = \left\{ \prod_{n=1}^{\frac{p-1}{2}} (\mathfrak{k}_{\left(0,\frac{n}{p}\right)} \circ \alpha)(\eta^2 \circ \alpha) \right\}^{-3} \quad \text{by (2.5)} \\
&= \left\{ \prod_{n=1}^{\frac{p-1}{2}} \mathfrak{k}_{\left(n,\frac{3n}{p}\right)} (p\tau+3)^{-1} (\eta^2 \circ \alpha) \right\}^{-3} \quad \text{by Proposition 2.3(2)} \\
&= \left\{ \prod_{n=1}^{\frac{p-1}{2}} \mathfrak{k}_{\left(n,\frac{3n}{p}\right)} \right\}^{-3} \left\{ (p\tau+3)^{-12} (\eta^{24} \circ \alpha) \right\}^{-\frac{p-1}{8}} \\
&= \left\{ \prod_{n=1}^{\frac{p-1}{2}} \mathfrak{k}_{\left(0,\frac{3n}{p}\right)+(n,0)} \right\}^{-3} (\eta^{24})^{-\frac{p-1}{8}} \\
&= \left\{ \prod_{n=1}^{\frac{p-1}{2}} \mathfrak{k}_{\left(0,\frac{3n}{p}\right)} \cdot (-1)^{\sum_{n=1}^{\frac{p-1}{2}} n} e^{-\pi i \sum_{n=1}^{\frac{p-1}{2}} \frac{3n^2}{p}} \right\}^{-3} (\eta^{24})^{-\frac{p-1}{8}} \quad \text{by Proposition 2.3(3)} \\
&= \left\{ \prod_{n=1}^{\frac{p-1}{2}} \mathfrak{k}_{\left(0,\frac{3n}{p}\right)} \right\}^{-3} (\eta^{24})^{-\frac{p-1}{8}} \\
&= \left\{ \prod_{n=1}^{\frac{p-1}{2}} \mathfrak{k}_{\left(0,\left\langle\frac{3n}{p}\right\rangle\right)+\left(0,\frac{3n}{p}-\left\langle\frac{3n}{p}\right\rangle\right)} \right\}^{-3} (\eta^{24})^{-\frac{p-1}{8}} \\
&= \left\{ \prod_{n=1}^{\frac{p-1}{2}} \mathfrak{k}_{\left(0,\left\langle\frac{3n}{p}\right\rangle\right)} \cdot (-1)^{\sum_{n=1}^{\frac{p-1}{2}} \left(\frac{3n}{p}-\left\langle\frac{3n}{p}\right\rangle\right)} \right\}^{-3} (\eta^{24})^{-\frac{p-1}{8}} \quad \text{by Proposition 2.3(3)} \\
&= \left\{ \prod_{n=1}^{\frac{p-1}{2}} \mathfrak{k}_{\left(0,\left\langle\frac{3n}{p}\right\rangle\right)} \cdot (-1)^{\sum_{n=\frac{p+1}{3}}^{\frac{p-1}{2}} 1} \right\}^{-3} (\eta^{24})^{-\frac{p-1}{8}} \\
&= \left\{ \prod_{n=1}^{\frac{p-1}{2}} \mathfrak{k}_{\left(0,\left\langle\frac{3n}{p}\right\rangle\right)} \eta^2 \right\}^{-3} (-1)^{-\frac{p+1}{2}} = \left\{ \prod_{n=1}^{\frac{p-1}{2}} g_{\left(0,\left\langle\frac{3n}{p}\right\rangle\right)} \right\}^{-3} (-1) \\
&= \left\{ \prod_{n=1}^{\frac{p-1}{2}} g_{\left(0,\frac{n}{p}\right)} \right\}^{-3} (-1) = -f.
\end{aligned}
$$

The last line is obtained by verifing $g_{(0,r_2)} = g_{(0,1-r_2)}$ for $r_2 \in \mathbb{Q} \setminus \mathbb{Z}$ from Proposition 2.4(1) and (3). This contradicts the fact $f \in \mathcal{K}(X_0(p))$. Therefore $d_p = 3\mathfrak{g}_p + 1$.

$p \equiv 7 \pmod{12}$. Considering a function

$$g = g_p^{-1} = \prod_{n=1}^{p-1} g_{\left(0,\frac{n}{p}\right)}^{-2}$$

and by Proposition 5.1 we see that

$$\mathrm{ord}_\infty g = -\frac{p-1}{\gcd(12,\, p-1)} = -\frac{p-1}{6} = -(2\mathfrak{g}_p + 1).$$

Since d_p divides the order $-(2\mathfrak{g}_p + 1)$ and $d_p \geq \mathfrak{g}_p + 1$, d_p equals $2\mathfrak{g}_p + 1$.
$p \equiv 11 \pmod{12}$. We consider a function

$$g = g_p^{-1} = \prod_{n=1}^{p-1} g_{\left(0,\frac{n}{p}\right)}^{-6} \doteq \prod_{n=1}^{\frac{p-1}{2}} g_{\left(0,\frac{n}{p}\right)}^{-12}.$$

Then by Proposition 5.1 we achieve

$$\mathrm{ord}_\infty g = -\frac{p-1}{\gcd(12,\, p-1)} = -\frac{p-1}{2} = -(6\mathfrak{g}_p - 1).$$

Since d_p divides the order $-(6\mathfrak{g}_p - 1)$ and $d_p \geq \mathfrak{g}_p + 1$, d_p is equal to $6\mathfrak{g}_p - 1$ or $\frac{6\mathfrak{g}_p - 1}{5}$. Assume that $d_p = \frac{6\mathfrak{g}_p - 1}{5}$, then there exists a function $f \in \mathcal{K}(X_0(p))$ such that

$$\mathrm{div}(f) = \frac{6\mathfrak{g}_p - 1}{5}((0) - (\infty)).$$

On the other hand, $\mathrm{div}(f^5 g^{-1}) = 5\mathrm{div}(f) - \mathrm{div}(g) = 0$ implies that $f^5 g^{-1}$ is a constant. So we may assume that $f^5 = g$. Then by Theorem 5.2(2), f has a representation

$$f = \lambda \prod_{r \in (\frac{1}{p}\mathbb{Z}^2/\mathbb{Z}^2)^*/\pm 1} g_r^{m'(r)}$$

for some family of integers $\{m'(r)\}_r$ and some $\lambda \in \mathbb{C}$. Decompose $f^5 g^{-1}$ into

$$f^5 g^{-1} = \lambda \prod_{n=1}^{\frac{p-1}{2}} g_{\left(0,\frac{n}{p}\right)}^{5m'\left(0,\frac{n}{p}\right)+12} \cdot \prod_{r \text{ not of the form } \left(0,\frac{n}{p}\right)} g_r^{5m'(r)} = \text{a constant}.$$

By Theorem 5.2(1) we know that all exponents should be the same, but it is obviously impossible because 5 cannot divide 12. Therefore $d_p = 6\mathfrak{g}_p - 1$. □

Remark 5.4 We note from Theorem 5.3 that d_p is in fact the numerator of $\frac{p-1}{12}$. For a given modular curve one can define the *cuspidal divisor class group* [13] as the additive group of divisors of degree 0 generated by the cusps modulo the subgroup of principal divisors obtained from the modular units. The order of this group is called the *cuspidal class number*. Then our number d_p in Theorem 5.3 is none other than the cuspidal class number of such modular curve when N is a prime number larger than 3. On the other hand, Takagi also computed in [22] the cuspidal class number of $X_0(N)$ with N square-free. In general the cuspidal divisor group can be identified with a group ring R of a finite group. He expressed in the paper certain family of divisors from the modified Siegel functions as multiples of a so-called Stickelberger element $\theta \in R \otimes \mathbb{Q}$. He also proved that the family becomes a set of

Table 1 The orders at the cusps on $X_0(pq)$

Cusps	Functions				
	g_p	g_q	g_{pq}	$\frac{g_pg_q}{g_{pq}^2}$	$\frac{g_q}{g_{pq}^2}$
∞	$\frac{p-1}{12}$	$\frac{q-1}{12}$	$\frac{pq-1}{12}$	$-\frac{2pq-p-q}{12}$	$-\frac{2pq-q-1}{12}$
0	$-\frac{q(p-1)}{12}$	$-\frac{p(q-1)}{12}$	$-\frac{pq-1}{12}$	$\frac{p+q-2}{12}$	$\frac{pq+p-2}{12}$
$\frac{1}{p}$	$\frac{q(p-1)}{12}$	$-\frac{q-1}{12}$	$-\frac{q-p}{12}$	$\frac{pq+1-2p}{12}$	$\frac{q+1-2p}{12}$
$\frac{1}{q}$	$-\frac{p-1}{12}$	$\frac{p(q-1)}{12}$	$\frac{q-p}{12}$	$\frac{pq+1-2q}{12}$	$\frac{pq+p-2q}{12}$

generators for the subgroup of divisors from the modular units, which made him possible to find the cuspidal class number. Observe that the subgroups of divisors from modular units is an ideal of the ring R and is an analogue of the Stickelberger ideal in the theory of cyclotomic fields.

Let p and q be two distinct primes such that both $p,\ q \equiv 1 \pmod{12}$. Consider the functions

$$g_p = \prod_{n=1}^{p-1} g_{\left(0,\frac{n}{p}\right)}, \quad g_q = \prod_{n=1}^{q-1} g_{(0,\frac{n}{q})}, \quad g_{pq} = \prod_{n=1}^{pq-1} g_{(0,\frac{n}{pq})}.$$

We see from Proposition 5.1 that g_p, g_q and g_{pq} are modular for $\Gamma_0(p)$, $\Gamma_0(q)$ and $\Gamma_0(pq)$, respectively. We shall view all of them as functions on the modular curve $X_0(pq) = \Gamma_0(pq)\backslash\mathfrak{H}^*$. Then the inequivalent cusps on $X_0(pq)$ are $\infty, 0, \frac{1}{p}, \frac{1}{q}$ of widths $1, pq, q, p$, respectively [10]. For a product of Siegel functions

$$g = \prod_{r \in \frac{1}{pq}\mathbb{Z}^2 \backslash \mathbb{Z}^2} g_r^{m(r)}$$

which lies in $\mathcal{K}(X_0(pq))$ we can estimate the order at each cusp s as follows. Let γ_s be an element of $\mathrm{SL}_2(\mathbb{Z})$ such that $\gamma_s(\infty) = s$. And, we take

$$\gamma_\infty = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \gamma_0 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad \gamma_p = \begin{pmatrix} 1 & 0 \\ p & 1 \end{pmatrix}, \quad \gamma_q = \begin{pmatrix} 1 & 0 \\ q & 1 \end{pmatrix}.$$

Then (2.9) and Proposition 2.4(2) enable us to compute the order of g at s as

$$\begin{aligned} \mathrm{ord}_s g &= \text{width at } s \cdot \mathrm{ord}_{q_\tau}(g \circ \gamma_s) \\ &= \text{width at } s \cdot \sum_r m(r\gamma_s)\frac{1}{2}\mathbf{B}_2(\langle (r\gamma_s)_1 \rangle) \end{aligned}$$

where $(r\gamma_s)_1$ is the first entry of the vector $r\gamma_s$. Here we summarize the orders of g_p, g_q, g_{pq} and the additional functions g_pg_q/g_{pq}^2 and g_q/g_{pq}^2 in Table 1.

Note that the genus $\mathfrak{g}_{pq}$ of $X_0(pq)$ is given by $\frac{(p+1)(q+1)}{12} - \frac{10}{3}$ [10]. Now we know from the Table 1 that g_pg_q/g_{pq}^2 satisfies

$$\mathrm{ord}_\infty \frac{g_pg_q}{g_{pq}^2} = -2\mathfrak{g}_{pq} + \frac{p+q-26}{4}$$

and is holomorphic elsewhere. And g_q/g_{pq}^2 satisfies

$$\mathrm{ord}_\infty \frac{g_q}{g_{pq}^2} = -2\mathfrak{g}_{pq} + \frac{2p+3q-77}{12}$$

and is holomorphic elsewhere if $q \geq 2p-1$. At this stage we hope that these two functions will play a certain role in examining whether the cusp ∞ is a Weierstrass point of $X_0(pq)$ or not. On the other hand, we also have the following interesting result from the Table 1.

Theorem 5.5 *Let p and q be primes such that both $p,\ q \equiv 1 \pmod{12}$ and $q \geq 2p-1$. If $\frac{p-1}{12}$ and $\frac{q-1}{12}$ are relatively prime, then $\mathcal{K}(X_0(pq)) = \mathbb{C}\left(g_p,\ g_q/g_{pq}^2\right)$.*

Proof For convenience, put $A = \frac{2pq-p-q}{12}$ and $B = \frac{2pq-q-1}{12}$, then $-A+B = \frac{p-1}{12}$ and $2qA+(1-2q)B = \frac{q-1}{12}$. And by assumption A and B are relatively prime. Then the Table 1 indicates that the total degrees of poles of g_pg_q/g_{pq}^2 and g_q/g_{pq}^2 are equal to A and B, respectively. Hence $[\mathcal{K}(X_0(pq)) : \mathbb{C}(g_pg_q/g_{pq}^2)] = A$ and $[\mathcal{K}(X_0(pq)) : \mathbb{C}(g_q/g_{pq}^2)] = B$, which implies that $[\mathcal{K}(X_0(pq)) : \mathbb{C}(g_pg_q/g_{pq}^2,\ g_q/g_{pq}^2)]$ should be 1. Therefore g_pg_q/g_{pq}^2 and g_q/g_{pq}^2(or, g_p and g_q/g_{pq}^2) are generators of $\mathcal{K}(X_0(pq))$.

In particular, when $p = 13$ and $q(\geq 25)$ is a prime $\equiv 1 \pmod{12}$, we see that g_{13} and g_q/g_{13q}^2 are generators of $\mathcal{K}(X_0(13q))$. □

6 Hauptmoduln of $\mathcal{K}(X_1(N))$

Since g_N is an element of $\mathcal{K}(X_0(N))$, it is an element of $\mathcal{K}(X_1(N))$ too. However it doesn't seem to be good enough as a generator of $\mathcal{K}(X_1(N))$, because $\mathcal{K}(X_1(N))$ is much bigger than $\mathcal{K}(X_0(N))$ in general. To find its relevant generators we need more machinery. We have only thought of Siegel functions of the form $g_{(0,*)}$ so far. From now on we shall consider Siegel functions $g_{(r_1,r_2)}$ with $r_1 \notin \mathbb{Z}$. Precisely speaking, we shall consider the functions

$$g_{(\frac{t}{N},0)}(N\tau)$$

with $t \not\equiv 0 \pmod{N}$.

Lemma 6.1 *For an integer $t \not\equiv 0 \mod N$,*

$$\prod_{n=0}^{N-1} g_{(\frac{t}{N},\frac{n}{N})}(\tau) = e^{\pi i \frac{N-1}{2}(\frac{t}{N}+1)} g_{(\frac{t}{N},0)}(N\tau).$$

Proof One can readily prove the lemma by using the identity

$$1 - X^N = (1-X)(1-\zeta_N X)\cdots(1-\zeta_N^{N-1}X)$$

and the q_τ-expansion formula (2.8). □

The following theorem gives us a sufficient condition for a product of $g_{(\frac{t}{N},0)}(N\tau)$'s to be an element of $\mathcal{K}(X_1(N))$.

Theorem 6.2 *A product*

$$g = \prod_{t=1}^{N-1} g_{(\frac{t}{N},0)}^{m(t)}(N\tau)$$

is an element of $\mathcal{K}(X_1(N))$ *if*

$$\sum_t m(t) \equiv 0 \pmod{12} \quad \textit{and} \quad \sum_t m(t)t^2 \equiv 0 \pmod{\gcd(2, N) \cdot N}.$$

Furthermore, for $\alpha = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ *we have*

$$\mathrm{ord}_{q_\tau} g \circ \alpha = \frac{\gcd(c, N)^2}{2N} \sum_{t=1}^{N-1} m(t) \mathbf{B}_2 \left(\left\langle \frac{at}{\gcd(c, N)} \right\rangle \right). \tag{6.1}$$

Proof Assume the hypothesis of the theorem. By Lemma 6.1,

$$g = \lambda \prod_{t=1}^{N-1} \left\{ \prod_{n=0}^{N-1} g_{\left(\frac{t}{N}, \frac{n}{N}\right)} \right\}^{m(t)}$$

for some root of unity λ. For notation, we set

$$g = \lambda \prod_{\substack{r=(r_1,r_2) \in \frac{1}{N}\mathbb{Z}^2 \setminus \mathbb{Z}^2 \\ 0 \le r_1, r_2 < 1}} g_r^{m'(r)}.$$

Then

$$\begin{aligned}
\sum_r m'(r)(Nr_1)^2 &= N \sum_t m(t)t^2 \\
\sum_r m'(r)(Nr_2)^2 &= \frac{(N-1)N(2N-1)}{6} \sum_t m(t) \\
\sum_r m'(r)(Nr_1)(Nr_2) &= N \sum_t m(t)t \\
\sum_r m'(r) &= N \sum_t m(t).
\end{aligned}$$

Hence by Theorem 2.5, g is modular of level N. Note that $\Gamma_1(N) = \langle \Gamma(N), \ T \rangle$ with $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and

$$\begin{aligned}
g \circ T &= \lambda \prod_{t=1}^{N-1} \left\{ \prod_{n=0}^{N-1} (\mathfrak{k}_{\left(\frac{t}{N}, \frac{n}{N}\right)} \circ T)(\eta^2 \circ T) \right\}^{m(t)} \quad \text{by (2.5)} \\
&= \lambda \left\{ \prod_{t=1}^{N-1} \prod_{n=0}^{N-1} \mathfrak{k}_{\left(\frac{t}{N}, \frac{t+n}{N}\right)}^{m(t)} \right\} (\eta^2 \circ T)^{N \sum_t m(t)} \quad \text{by Proposition 2.3(2)} \\
&= \lambda \left\{ \prod_{t=1}^{N-1} \prod_{n=0}^{N-1} \mathfrak{k}_{\left(\frac{t}{N}, \frac{t+n}{N}\right)}^{m(t)} \right\} (\eta^{24})^{\frac{N}{12} \sum_t m(t)},
\end{aligned}$$

and

$$\begin{aligned}
\prod_{t=1}^{N-1}\prod_{n=0}^{N-1}\mathfrak{k}_{\left(\frac{t}{N},\frac{t+n}{N}\right)}^{m(t)} &= \prod_{t=1}^{N-1}\left\{\prod_{n=0}^{N-1-t}\mathfrak{k}_{\left(\frac{t}{N},\frac{t+n}{N}\right)}\prod_{n=N-t}^{N-1}\mathfrak{k}_{\left(\frac{t}{N},\frac{t+n}{N}\right)}\right\}^{m(t)}\\
&= \prod_{t=1}^{N-1}\left\{\prod_{n=0}^{N-1-t}\mathfrak{k}_{\left(\frac{t}{N},\frac{t+n}{N}\right)}\prod_{n=N-t}^{N-1}\mathfrak{k}_{\left(\frac{t}{N},\frac{t+n}{N}-1\right)+(0,1)}\right\}^{m(t)}\\
&= \prod_{t=1}^{N-1}\left\{\prod_{n=0}^{N-1-t}\mathfrak{k}_{\left(\frac{t}{N},\frac{t+n}{N}\right)}\prod_{n=N-t}^{N-1}\mathfrak{k}_{\left(\frac{t}{N},\frac{t+n}{N}-1\right)}\left(-e^{\pi i\frac{t}{N}}\right)\right\}^{m(t)}\\
&\qquad\qquad\text{by Proposition 2.3(3)}\\
&= \left\{\prod_{t=1}^{N-1}\prod_{n=0}^{N-1}\mathfrak{k}_{\left(\frac{t}{N},\frac{n}{N}\right)}^{m(t)}\right\}(-1)^{\sum_t tm(t)}e^{\pi i\frac{1}{N}\sum_t t^2m(t)}.
\end{aligned}$$

Since $\sum_t tm(t)\equiv\sum_t t^2m(t)\pmod 2$, it follows from our assumption that

$$g\circ T = g\cdot(-1)^{\sum_t tm(t)}e^{\pi i\frac{1}{N}\sum_t t^2m(t)} = g.$$

Therefore g is an element of $\mathcal{K}(X_1(N))$. Moreover, for $\alpha=\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)\in\mathrm{SL}_2(\mathbb{Z})$ we deduce that

$$\begin{aligned}
\mathrm{ord}_{q_\tau} g\circ\alpha &= \sum_{t=1}^{N-1}m(t)\sum_{n=0}^{N-1}\mathrm{ord}_{q_\tau} g_{\left(\frac{t}{N},\frac{n}{N}\right)\beta}\quad\text{by Proposition 2.4(2)}\\
&= \sum_{t=1}^{N-1}m(t)\sum_{n=0}^{N-1}\mathrm{ord}_{q_\tau} g_{\left(\frac{at+cn}{N},\frac{bt+dn}{N}\right)}\\
&= \sum_{t=1}^{N-1}m(t)\sum_{n=0}^{N-1}\frac{1}{2}\mathbf{B}_2\left(\left\langle\frac{at+cn}{N}\right\rangle\right)\quad\text{by (2.9)}\\
&= \frac{\gcd(c,N)^2}{2N}\sum_{t=1}^{N-1}m(t)\mathbf{B}_2\left(\left\langle\frac{at}{\gcd(c,N)}\right\rangle\right).
\end{aligned}$$

The last equality is obtained from the following well-known lemma concerning the distribution relations of the Bernoulli polynomials. We only need that of the second Bernoulli polynomial. □

Lemma 6.3 *For any $y\in\mathbb{Q}/\mathbb{Z}$ and a positive integer D we have*

$$\sum_{Dx=y,\ x\in\mathbb{Q}/\mathbb{Z}}\mathbf{B}_n\left(\langle x\rangle\right) = D^{1-n}\mathbf{B}_n\left(\langle y\rangle\right).$$

Proof For the sake of completeness we give a proof. The nth Bernoulli polynomial $\mathbf{B}_n(X)$ is defined by

$$\frac{We^{WX}}{e^W-1} = \sum_{n=0}^{\infty}\mathbf{B}_n(X)\frac{W^n}{n!}.$$

Here we observe directly from the above definition of $\mathbf{B}_n(X)$ that

$$\sum_{n=0}^{\infty}\mathbf{B}_n\left(\langle y\rangle\right)\frac{W^n}{n!}=\frac{We^{W\langle y\rangle}}{e^W-1}=\sum_{k=0}^{D-1}\frac{We^{W(\langle y\rangle+k)}}{e^{DW}-1}=\sum_{k=0}^{D-1}\frac{1}{D}\frac{(DW)e^{(DW)\frac{\langle y\rangle+k}{D}}}{e^{DW}-1}$$
$$=\sum_{k=0}^{D-1}\sum_{n=0}^{\infty}\frac{1}{D}\mathbf{B}_n\left(\frac{\langle y\rangle+k}{D}\right)\frac{(DW)^n}{n!}$$
$$=\sum_{n=0}^{\infty}\sum_{k=0}^{D-1}D^{n-1}\mathbf{B}_n\left(\frac{\langle y\rangle+k}{D}\right)\frac{W^n}{n!}.$$

Thus we achieve

$$\mathbf{B}_n\left(\langle y\rangle\right)=D^{n-1}\sum_{k=0}^{D-1}\mathbf{B}_n\left(\frac{\langle y\rangle+k}{D}\right)=D^{n-1}\sum_{Dx=y,\ x\in\mathbb{Q}/\mathbb{Z}}\mathbf{B}_n\left(\langle x\rangle\right).$$

□

The genus zero condition and the inequivalent cusps on the modular curve $X_1(N)$ are given in the following theorem.

Theorem 6.4 *The genus of $X_1(N)$ is zero if and only if $1\le N\le 10$ or $N=12$. Let $N\neq 1,2,4$. All the inequivalent cusps on $X_1(N)$ are represented by the pairs of integers (u,v) satisfying*

$$\begin{cases}1\le v<\frac{N}{2},\quad 1\le u\le D,\quad \gcd(u,D)=1,\ \text{or}\\ v=\frac{N}{2},\ N,\quad 1\le u\le\frac{D}{2},\quad \gcd(u,D)=1,\end{cases}$$

where $D=\gcd(v,N)$. If $\gcd(u,v)\neq 1$, we replace (u,v) by other pair of integers (u',v') such that $u'\equiv u \pmod N$, $v'\equiv v \pmod N$ and $\gcd(u',v')=1$. Then all the inequivalent cusps on $X_1(N)$ are given by the quotients $\frac{u}{v}$.

Proof See [10]. □

Theorem 6.5 *Assume that $X_1(N)$ is of genus 0 and let a product*

$$g=\prod_{t=1}^{N-1}g_{(\frac{t}{N},0)}^{m(t)}(N\tau)$$

be a function in $\mathcal{K}(X_1(N))$. For each cusp $s=\frac{a}{c}\in\mathbb{Q}$ with $\gcd(a,c)=1$ which is inequivalent to ∞, g is a generator of $\mathcal{K}(X_1(N))$ if

$$\frac{N}{2}\sum_t m(t)\mathbf{B}_2\left(\frac{t}{N}\right)=-1\quad\text{and}\quad\sum_t m(t)\mathbf{B}_2\left(\left\langle\frac{at}{\gcd(c,N)}\right\rangle\right)\ge 0.$$

Proof Note that the width of ∞ on $X_1(N)$ is 1. From the order formula (6.1) in Theorem 6.2 we see that the hypothesis in this theorem renders the fact that g has simple pole at ∞ and is holomorphic elsewhere. Hence $X_1(N)$ is isomorphic to the projective line $\mathbb{P}^1_{\mathbb{C}}$ through the map $\tau\mapsto[1:g(\tau)]$ and $\mathcal{K}(X_1(N))=\mathbb{C}(g)$. □

Remark 6.6 This result is similar to that of Yang [23, Lemma 3] developed by making use of the generalized Dedekind eta function. But we believe that the Siegel functions are more systematic and convenient to use than the generalized Dedekind eta functions, especially in the matter of transformation formulas.

Table 2 Generators of $\mathcal{K}(X_1(N))$

N	G_N	$j_{1,N}$
2	$g_{\left(\frac{1}{2},0\right)}^{12}(2\tau)$	$\frac{\theta_2^8(\tau)}{\theta_4^8(2\tau)}$
3	$g_{\left(\frac{1}{3},0\right)}^{12}(3\tau)$	$\frac{E_4(\tau)}{E_4(3\tau)}$
4	$g_{\left(\frac{1}{4},0\right)}^{-8}(4\tau)g_{\left(\frac{2}{4},0\right)}^{8}(4\tau)$	$\frac{\theta_2^4(2\tau)}{\theta_3^4(2\tau)}$
5	$g_{\left(\frac{1}{5},0\right)}^{-5}(5\tau)g_{\left(\frac{2}{5},0\right)}^{5}(5\tau)$	$\frac{4\eta^5(\tau)/\eta(5\tau)+E_2^{(5)}(\tau)}{\eta^5(5\tau)/\eta(\tau)}$
6	$g_{\left(\frac{1}{6},0\right)}^{-3}(6\tau)g_{\left(\frac{3}{6},0\right)}^{3}(6\tau)$	$\frac{H_2^{(2)}(\tau)-H_2^{(2)}(3\tau)}{2H_2^{(2)}(\tau)-H_2^{(3)}(\tau)}$
7	$g_{\left(\frac{1}{7},0\right)}^{-3}(7\tau)g_{\left(\frac{2}{7},0\right)}2(7\tau)g_{\left(\frac{3}{7},0\right)}(7\tau)$	$\frac{\wp_{\left(\frac{1}{7},0\right)}(7\tau)-\wp_{\left(\frac{2}{7},0\right)}(7\tau)}{\wp_{\left(\frac{1}{7},0\right)}(7\tau)-\wp_{\left(\frac{4}{7},0\right)}(7\tau)}$
8	$g_{\left(\frac{1}{8},0\right)}^{-2}(8\tau)g_{\left(\frac{3}{8},0\right)}^{2}(8\tau)$	$\frac{\theta_3(2\tau)}{\theta_3(4\tau)}$
9	$g_{\left(\frac{1}{9},0\right)}^{-2}(9\tau)g_{\left(\frac{2}{9},0\right)}(9\tau)g_{\left(\frac{4}{9},0\right)}(9\tau)$	$\frac{\wp_{\left(\frac{1}{9},0\right)}(9\tau)-\wp_{\left(\frac{2}{9},0\right)}(9\tau)}{\wp_{\left(\frac{1}{9},0\right)}(9\tau)-\wp_{\left(\frac{4}{9},0\right)}(9\tau)}$
10	$g_{\left(\frac{1}{10},0\right)}^{-1}(10\tau)g_{\left(\frac{2}{10},0\right)}^{-1}(10\tau)g_{\left(\frac{3}{10},0\right)}(10\tau)g_{\left(\frac{4}{10},0\right)}(10\tau)$	$\frac{\wp_{\left(\frac{1}{10},0\right)}(10\tau)-\wp_{\left(\frac{2}{10},0\right)}(10\tau)}{\wp_{\left(\frac{1}{10},0\right)}(10\tau)-\wp_{\left(\frac{4}{10},0\right)}(10\tau)}$
12	$g_{\left(\frac{1}{12},0\right)}^{-1}(12\tau)g_{\left(\frac{5}{12},0\right)}(12\tau)$	$\frac{\theta_3(2\tau)}{\theta_3(6\tau)}$

As an application of Theorem 6.5 we can explicitly find generators of $\mathcal{K}(X_1(N))$ of genus zero as shown in the Table 2. We denote them by G_N for convenience. On the other hand, in the Table 3 we additionally introduce relations between G_N and the generators $j_{1,N}$ of $\mathcal{K}(X_1(N))$ which appeared in [12] ahead of Yang's [23]. As for $j_{1,N}$ we need the following definitions:

$$\theta_2(\tau)=\sum_{n\in\mathbb{Z}}e^{\pi i(n+\frac{1}{2})^2},\quad \theta_3(\tau)=\sum_{n\in\mathbb{Z}}e^{\pi i n^2},\quad \theta_4(\tau)=\sum_{n\in\mathbb{Z}}(-1)^n e^{\pi i n^2}$$

$$H_2(\tau)=2\zeta(2)-8\pi^2\sum_{n=1}^{\infty}\sigma_1(n)q_\tau^n$$

$$E_2(\tau)=\frac{1}{2\zeta(2)}H_2(\tau),\qquad E_4(\tau)=1+240\sum_{n=1}^{\infty}\sigma_3(n)q_\tau^n$$

$$H_2^{(p)}(\tau)=H_2(\tau)-pH_2(p\tau)\text{ for each prime }p$$

$$E_2^{(p)}(\tau)=E_2(\tau)-pE_2(p\tau)\text{ for each prime }p$$

$$\wp_{(r_1,r_2)}(\tau)=\wp(r_1\tau+r_2;\ [\tau,1])\text{ for }(r_1,r_2)\in\mathbb{Q}^2\backslash\mathbb{Z}^2.$$

Now, using our algorithm in Sect. 3 for integrality over $\mathbb{Z}[j]$ we induce the following results.

Table 3 Hauptmoduln of $\mathcal{K}(X_1(N))$

N	Hauptmoduln (unique normalized generators)
2	$G_2+24=\frac{256}{j_{1,2}}+24=\frac{1}{q_\tau}+276q_\tau-2048q_\tau^2+11202q_\tau^3-49152q_\tau^4+184024q_\tau^5+\cdots$
3	$G_3+12=\frac{240}{j_{1,3}-1}+9=\frac{1}{q_\tau}+54q_\tau-76q_\tau^2-243q_\tau^3+1188q\tau^4-1384q_\tau^5+\cdots$
4	$G_4-8=\frac{16}{j_{1,4}}-8=\frac{1}{q_\tau}+20q_\tau-62q_\tau^3+216q_\tau^5-641q_\tau^7+1636q_\tau^9+\cdots$
5	$G_5-5=-\frac{8}{j_{1,5}+44}-5=\frac{1}{q_\tau}+10q_\tau+5q_\tau^2-15q_\tau^3-24q_\tau^4+15q_\tau^5+\cdots$
6	$G_6-3=\frac{2}{j_{1,6}-1}-1=\frac{1}{q_\tau}+6q_\tau+4q_\tau^2-3q_\tau^3-12q_\tau^4-8q_\tau^5+\cdots$
7	$G_7-3=-\frac{1}{j_{1,7}-1}-3=\frac{1}{q_\tau}+4q_\tau+3q_\tau^2-5q_\tau^4-7q_\tau^5-2q_\tau^6+\cdots$
8	$G_8-2=\frac{2}{j_{1,8}-1}-1=\frac{1}{q_\tau}+3q_\tau+2q_\tau^2+q_\tau^3-2q_\tau^4-4q_\tau^5+\cdots$
9	$G_9-2=-\frac{1}{j_{1,9}-1}-2=\frac{1}{q_\tau}+2q_\tau+2q_\tau^2+q_\tau^3-q_\tau^4-2q_\tau^5+\cdots$
10	$G_{10}-1=-\frac{1}{j_{1,10}-1}-2=\frac{1}{q_\tau}+2q_\tau+q_\tau^2+q_\tau^3-q_\tau^5-2q_\tau^6+\cdots$
12	$G_{12}-1=\frac{2}{j_{1,12}-1}=\frac{1}{q_\tau}+q_\tau+q_\tau^2+q_\tau^3-q_\tau^6-q_\tau^7+\cdots$

Theorem 6.7 (1) *For $N=5,7,8,9,10$ and 12, G_N are units over $\mathbb{Z}$.*
(2) *For $N=2,3,4,6$, G_N are integral over $\mathbb{Z}[j]$, but G_N^{-1} are not.*

Proof (1) $N=5,7,8,9$. For such N the indices of Siegel functions appearing in G_N have the same primitive denominator N. We shall only prove the case $N=7$, because the other cases are similar. By Lemma 6.1 we get

$$G_7=g_{\left(\frac{1}{7},0\right)}^{-3}(7\tau)g_{\left(\frac{2}{7},0\right)}^{2}(7\tau)g_{\left(\frac{3}{7},0\right)}(7\tau)\doteq\prod_{n=0}^{6}g_{\left(\frac{1}{7},\frac{n}{7}\right)}^{-3}g_{\left(\frac{2}{7},\frac{n}{7}\right)}^{2}g_{\left(\frac{3}{7},\frac{n}{7}\right)}.$$

The action(multiplication) of $(\mathbb{Z}/7\mathbb{Z})^*$ groups the indices in the above product into

$$\left\{\left(\frac{1}{7},0\right),\left(\frac{2}{7},0\right),\left(\frac{3}{7},0\right)\right\},\left\{\left(\frac{1}{7},\frac{1}{7}\right),\left(\frac{2}{7},\frac{2}{7}\right),\left(\frac{3}{7},\frac{3}{7}\right)\right\},$$
$$\left\{\left(\frac{1}{7},\frac{2}{7}\right)\left(\frac{2}{7},\frac{4}{7}\right)\left(\frac{3}{7},\frac{6}{7}\right)\right\}$$
$$\left\{\left(\frac{1}{7},\frac{3}{7}\right),\left(\frac{2}{7},\frac{6}{7}\right),\left(\frac{3}{7},\frac{2}{7}\right)\right\},\left\{\left(\frac{1}{7},\frac{4}{7}\right),\left(\frac{2}{7},\frac{1}{7}\right),\left(\frac{3}{7},\frac{5}{7}\right)\right\},$$
$$\left\{\left(\frac{1}{7},\frac{5}{7}\right),\left(\frac{2}{7},\frac{3}{7}\right),\left(\frac{3}{7},\frac{1}{7}\right)\right\}$$
$$\left\{\left(\frac{1}{7},\frac{6}{7}\right),\left(\frac{2}{7},\frac{5}{7}\right),\left(\frac{3}{7},\frac{4}{7}\right)\right\}.$$

It can then be directly checked that the sum of exponents for each orbit is zero. Therefore our algorithm claims that G_7 is a unit over $\mathbb{Z}$.
$N=10$. By Lemma 6.1 we have

$$G_{10}\doteq\prod_{n=0}^{9}g_{\left(\frac{1}{10},\frac{n}{10}\right)}^{-1}g_{\left(\frac{2}{10},\frac{n}{10}\right)}^{-1}g_{\left(\frac{3}{10},\frac{n}{10}\right)}g_{\left(\frac{4}{10},\frac{n}{10}\right)}=(G_{10})_{\text{comp}}\prod_{n=0}^{4}g_{\left(\frac{1}{5},\frac{n}{5}\right)}^{-1}g_{\left(\frac{2}{5},\frac{n}{5}\right)}.$$

From the algorithm it suffices to show that $(G_{10})_{(5)} = \prod_{n=0}^{4} g_{\left(\frac{1}{5},\frac{n}{5}\right)}^{-1} g_{\left(\frac{2}{5},\frac{n}{5}\right)}$ is a unit over $\mathbb{Z}$.

The action of $(\mathbb{Z}/5\mathbb{Z})^*$ groups the indices in $(G_{10})_{(5)}$ into

$$\left\{\left(\frac{1}{5},\frac{1}{5}\right),\left(\frac{2}{5},\frac{2}{5}\right)\right\},\left\{\left(\frac{1}{5},\frac{2}{5}\right),\left(\frac{2}{5},\frac{4}{5}\right)\right\},\left\{\left(\frac{1}{5},\frac{3}{5}\right),\left(\frac{2}{5},\frac{1}{5}\right)\right\},\left\{\left(\frac{1}{5},\frac{4}{5}\right),\left(\frac{2}{5},\frac{3}{5}\right)\right\}.$$

And it can be readily checked that the sum of exponents for each orbit is zero. Hence G_{10} is a unit over $\mathbb{Z}$.

$N = 12$. By Lemma 6.1 we get

$$G_{12} \doteq \prod_{n=0}^{11} g_{\left(\frac{1}{12},\frac{n}{12}\right)}^{-1} g_{\left(\frac{5}{12},\frac{n}{12}\right)} = (G_{12})_{\mathrm{comp}}.$$

And G_{12} is a unit over $\mathbb{Z}$ with no more argument.

(2) $N = 2, 3$. By Lemma 6.1 we obtain

$$G_2 \doteq g_{\left(\frac{1}{2},0\right)}^{12} g_{\left(\frac{1}{2},\frac{1}{2}\right)}^{12}$$
$$G_3 \doteq g_{\left(\frac{1}{3},0\right)}^{12} g_{\left(\frac{1}{3},\frac{1}{3}\right)}^{12} g_{\left(\frac{1}{3},\frac{2}{3}\right)}^{12}.$$

Since all the exponents are positive, G_2 and G_3 are obviously integral over $\mathbb{Z}[j]$. But, their inverses G_2^{-1} and G_3^{-1} are not.

$N = 4$. By the proof of Corollary 3.2 and Proposition 2.4(1) and (3) we deduce that

$$G_4 \doteq \prod_{n=0}^{3} g_{\left(\frac{1}{4},\frac{n}{4}\right)}^{-8} g_{\left(\frac{2}{4},\frac{n}{4}\right)}^{8} \doteq g_{\left(\frac{1}{4},0\right)}^{8} g_{\left(\frac{1}{4},\frac{1}{4}\right)}^{8} g_{\left(\frac{1}{4},\frac{2}{4}\right)}^{8} g_{\left(\frac{1}{4},\frac{3}{4}\right)}^{8} g_{\left(\frac{2}{4},\frac{1}{4}\right)}^{16}.$$

Thus G_4 is integral over $\mathbb{Z}[j]$, but G_4^{-1} is not.

$N = 6$. By Lemma 6.1 we obtain that

$$G_6 \doteq \prod_{n=0}^{5} g_{\left(\frac{1}{6},\frac{n}{6}\right)}^{-3} g_{\left(\frac{3}{6},\frac{n}{6}\right)}^{3} = (G_6)_{\mathrm{comp}} g_{\left(\frac{1}{2},0\right)}^{3} g_{\left(\frac{1}{2},\frac{1}{2}\right)}^{3}.$$

Thereofore G_6 is also integral over $\mathbb{Z}[j]$, but G_6^{-1} is not. □

7 Application to the Ramanujan's cubic continued fraction

Next, we shall investigate how to evaluate special values of the Ramanujan's cubic continued fraction if we know the singular j-invariants. The Ramanujan's cubic continued fraction [19] as a holomorphic function on $\mathfrak{H}$ is defined by

$$C(\tau) = \cfrac{q_\tau^{\frac{1}{3}}}{1+\cfrac{q_\tau+q_\tau^2}{1+\cfrac{q_\tau^2+q_\tau^4}{1+\cfrac{q_\tau^3+q_\tau^6}{1+\cdots}}}} = q_\tau^{\frac{1}{3}} \prod_{n=1}^{\infty} \frac{(1-q_\tau^{6n-1})(1-q_\tau^{6n-5})}{(1-q_\tau^{6n-3})^2}.$$

Since

$$g_{(\frac{t}{N},0)}(N\tau) = -q_\tau^{\frac{N}{2}\mathbf{B}_2(\frac{t}{N})}\prod_{n=1}^{\infty}(1-q_\tau^{N(n-1)+t})(1-q_\tau^{Nn-t})$$

from the q_τ-expansion formula (2.8), C can be written as

$$C = g_{\left(\frac{1}{6},0\right)}(6\tau)g^{-1}_{\left(\frac{3}{6},0\right)}(6\tau).$$

Note that we have $C^{-3} = G_6$ by the Table 2, which implies that C^{-1} is integral over $\mathbb{Z}[j]$ by Theorem 6.7(2).

We shall first find some relation between j and G_3, and then find that of G_3 and G_6. From these relations we will be able to estimate the values of C at some points in $\mathfrak{H}$ whenever we know the singular j-invariants there. To begin with, observe the following q_τ-expansions

$$\begin{aligned} j &= \frac{1}{q_\tau} + 744 + 196884q_\tau + 21493760q_\tau^2 + 864299970q_\tau^3 + \cdots \\ G_3 &= \frac{1}{q_\tau} - 12 + 54q_\tau - 76q_\tau^2 - 243q_\tau^3 + 1188q_\tau^4 - 1384q_\tau^5 + \cdots \\ G_6 &= \frac{1}{q_\tau} + 3 + 6q_\tau + 4q_\tau^2 - 3q_\tau^3 - 12q_\tau^4 - 8q_\tau^5 + \cdots . \end{aligned}$$

Theorem 7.1

$$j = \frac{(G_3+27)(G_3+243)^3}{G_3^3} \tag{7.1}$$

$$G_3 = \frac{(G_6+1)(G_6-8)^2}{G_6^2}. \tag{7.2}$$

Proof Let us take a complete system of right coset representatives of $\overline{\Gamma}_1/\overline{\Gamma}_1(3)$ as follows:

$$\alpha_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \alpha_2 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \quad \alpha_3 = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \quad \alpha_4 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Then the minimal polynomial of G_3 over $\mathcal{K}(X(1)) = \mathbb{C}(j)$ is written as

$$f(X) = \prod_{n=1}^{4}(X - G_3 \circ \alpha_n).$$

Since G_3 is a modular unit, each $G_3 \circ \alpha_n$ is also a modular unit. Hence each coefficient of $f(X)$ is holomorphic on $\mathfrak{H}$, which yields that it is a polynomial in j [15, Chapter 5]. Now that

$$G_3 \doteq g^{12}_{\left(\frac{1}{3},0\right)}g^{12}_{\left(\frac{1}{3},\frac{1}{3}\right)}g^{12}_{\left(\frac{1}{3},\frac{2}{3}\right)} \quad \text{by Lemma 6.1,}$$

we derive from Proposition 2.4(2) and (2.9) that

$$\begin{aligned} \mathrm{ord}_{q_\tau}(G_3 \circ \alpha_1) &= \mathrm{ord}_{q_\tau}\left(g^{12}_{\left(\frac{1}{3},0\right)}g^{12}_{\left(\frac{1}{3},\frac{1}{3}\right)}g^{12}_{\left(\frac{1}{3},\frac{2}{3}\right)}\right) = -1 \\ \mathrm{ord}_{q_\tau}(G_3 \circ \alpha_2) &= \mathrm{ord}_{q_\tau}\left(g^{12}_{\left(\frac{1}{3},0\right)}g^{12}_{\left(\frac{2}{3},\frac{1}{3}\right)}g^{12}_{\left(1,\frac{2}{3}\right)}\right) = \frac{1}{3} \end{aligned}$$

$$\operatorname{ord}_{q_\tau}(G_3\circ\alpha_3)=\operatorname{ord}_{q_\tau}\left(g^{12}_{\left(\frac{1}{3},0\right)}g^{12}_{\left(1,\frac{1}{3}\right)}g^{12}_{\left(\frac{5}{3},\frac{2}{3}\right)}\right)=\frac{1}{3}$$
$$\operatorname{ord}_{q_\tau}(G_3\circ\alpha_4)=\operatorname{ord}_{q_\tau}\left(g^{12}_{\left(0,-\frac{1}{3}\right)}g^{12}_{\left(\frac{1}{3},-\frac{1}{3}\right)}g^{12}_{\left(\frac{2}{3},-\frac{1}{3}\right)}\right)=\frac{1}{3}.$$

This shows that the only nonconstant coefficient of $f(X)$ is that of X^3 which is a linear polynomial in j. Thus we can write

$$j=\frac{G_3^4+A_3G_3^3+A_2G_3^2+A_1G_3+A_0}{A_3'G_3^3}$$

for some $A_3, A_3', A_2, A_1, A_0\in\mathbb{C}$. Now comparing the q_τ-expansions of both sides we have the formula (7.1).

Observe that the inequivalent cusps of $X_1(6)$ are $\infty, 0, \frac{1}{2}, \frac{1}{3}$ by Theorem 6.4 and the elements of $\mathrm{SL}_2(\mathbb{Z})$

$$\gamma_0=\begin{pmatrix}0&-1\\1&0\end{pmatrix},\quad \gamma_{\frac{1}{2}}=\begin{pmatrix}1&0\\2&1\end{pmatrix},\quad \gamma_{\frac{1}{3}}=\begin{pmatrix}1&0\\3&1\end{pmatrix}$$

satisfy $\gamma_0(\infty)=0, \gamma_{\frac{1}{2}}(\infty)=\frac{1}{2}$ and $\gamma_{\frac{1}{3}}(\infty)=\frac{1}{3}$. And, again by Proposition 2.4(2) and (2.9) we have

$$\operatorname{ord}_{q_\tau}(G_3\circ\gamma_0)=\operatorname{ord}_{q_\tau}\left(g^{12}_{\left(0,-\frac{1}{3}\right)}g^{12}_{\left(\frac{1}{3},-\frac{1}{3}\right)}g^{12}_{\left(\frac{2}{3},-\frac{1}{3}\right)}\right)=\frac{1}{3}$$
$$\operatorname{ord}_{q_\tau}(G_3\circ\gamma_{\frac{1}{2}})=\operatorname{ord}_{q_\tau}\left(g^{12}_{\left(\frac{1}{3},0\right)}g^{12}_{\left(1,\frac{1}{3}\right)}g^{12}_{\left(\frac{5}{3},\frac{2}{3}\right)}\right)=\frac{1}{3}$$
$$\operatorname{ord}_{q_\tau}(G_3\circ\gamma_{\frac{1}{3}})=\operatorname{ord}_{q_\tau}\left(g^{12}_{\left(\frac{1}{3},0\right)}g^{12}_{\left(\frac{4}{3},\frac{1}{3}\right)}g^{12}_{\left(\frac{7}{3},\frac{2}{3}\right)}\right)=-1.$$

Similarly, since

$$G_6=g^{-3}_{\left(\frac{1}{6},0\right)}(6\tau)g^{3}_{\left(\frac{3}{6},0\right)}(6\tau)\doteq\prod_{n=0}^{5}g^{-3}_{\left(\frac{1}{6},\frac{n}{6}\right)}g^{3}_{\left(\frac{3}{6},\frac{n}{6}\right)}\quad\text{by Lemma 6.1,}$$

we deduce by Proposition 2.4(2) and (2.9) that

$$\operatorname{ord}_{q_\tau}(G_6\circ\gamma_0)=\operatorname{ord}_{q_\tau}\left(\prod_{n=0}^{5}g^{-3}_{\left(\frac{n}{6},-\frac{1}{6}\right)}g^{3}_{\left(\frac{n}{6},-\frac{3}{6}\right)}\right)=0$$
$$\operatorname{ord}_{q_\tau}(G_6\circ\gamma_{\frac{1}{2}})=\operatorname{ord}_{q_\tau}\left(\prod_{n=0}^{5}g^{-3}_{\left(\frac{1+2n}{6},\frac{n}{6}\right)}g^{3}_{\left(\frac{3+2n}{6},\frac{n}{6}\right)}\right)=0$$
$$\operatorname{ord}_{q_\tau}(G_6\circ\gamma_{\frac{1}{3}})=\operatorname{ord}_{q_\tau}\left(\prod_{n=0}^{5}g^{-3}_{\left(\frac{1+3n}{6},\frac{n}{6}\right)}g^{3}_{\left(\frac{3+3n}{6},\frac{n}{6}\right)}\right)=\frac{1}{2}.$$

Now we consider the function

$$G=G_3G_6^2-(G_6+1)(G_6-8)^2.$$

Since G_3 and G_6 are holomorphic on $\mathfrak{H}$, so is G. Now that ord_{q_τ} is a valuation, for $n = 1, 2, 3$ it holds that

$$\begin{aligned}\mathrm{ord}_{q_\tau}(G \circ \gamma_n) \geq \min \big\{&\mathrm{ord}_{q_\tau}(G_3 \circ \gamma_n) + 2\mathrm{ord}_{q_\tau}(G_6 \circ \gamma_n),\\ &\mathrm{ord}_{q_\tau}(G_6 \circ \gamma_n + 1) + 2\mathrm{ord}_{q_\tau}(G_6 \circ \gamma_n - 8)\big\}.\end{aligned}$$

Then from our computation of orders we achieve

$$\mathrm{ord}_{q_\tau}(G \circ \gamma_n) \geq 0$$

for all $n = 1, 2, 3$, which means that G is holomorphic on $X_1(6)$ except possibly for the point ∞. And, observe that the q_τ-expansion of G is of the form

$$\begin{aligned}G &= G_3 G_6^2 - (G_6 + 1)(G_6 - 8)^2\\ &= \left(\frac{1}{q_\tau} - 12 + 54q_\tau - 76q_\tau^2 - 243q_\tau^3 + \cdots\right)\left(\frac{1}{q_\tau} + 3 + 6q_\tau + 4q_\tau^2 - 3q_\tau^3 + \cdots\right)^2\\ &\quad - \left(\frac{1}{q_\tau} + 4 + 6q_\tau + 4q_\tau^2 - 3q_\tau^3 + \cdots\right)\left(\frac{1}{q_\tau} - 5 + 6q_\tau + 4q_\tau^2 - 3q_\tau^3 + \cdots\right)^2\\ &= O(q),\end{aligned}$$

which shows that $\mathrm{ord}_{q_\tau} G \geq 1$. Therefore G is holomorphic on the whole $X_1(6)$ and has a zero at ∞, which implies that $G = 0$ as a function on the Riemann sphere $X_1(6)$. Therefore we obtain the formula (7.2). □

Corollary 7.2

$$j = \frac{(4C^3 + 1)^3(4C^3 + 6C + 1)^3(16C^6 - 24C^4 + 8C^3 + 36C^2 - 6C + 1)^3}{C^3(C + 1)^3(C^2 - C + 1)^3(2C - 1)^6(4C^2 + 2C + 1)^6}.$$

Proof If we plug (7.2) into (7.1) and replace G_6 by C^{-3}, then we get the above relation between j and C. □

Corollary 7.3 *If we know the singular value $j(\tau_0)$ for some $\tau_0 \in \mathfrak{H}$, we can express $C(\tau_0)$ in terms of radicals. In particular, if $\tau_0 \in \mathfrak{H}$ is imaginary quadratic, then $C^{-1}(\tau_0)$ is an algebraic integer.*

Proof By (7.1) we can express $G_3(\tau_0)$ in terms of radicals. Then by (7.2) we can also write $G_6(\tau_0)$ in terms of radicals. Since $G_6 = C^{-3}$, we finally evaluate $C(\tau_0)$ exactly.

If $\tau_0 \in \mathfrak{H}$ is imaginary quadratic, $j(\tau_0)$ becomes an algebraic integer [15,20]. And $G_3 = C^{-3}$ is integral over $\mathbb{Z}[j]$ by Theorem 6.7(2); hence $C^{-1}(\tau_0)$ is an algebraic integer, too. □

Example 7.4 We exhibit several values $C(\tau_0)$ in the following table. The singular values $j(\tau_0)$ are taken from [8, (12.20)] (Table 4).

The first six values of $C(\tau_0)$ can be also found in [2,4], which were obtained by theta function identities. Recently, Cho et al. [6] pointed out that C^{-1} is a generator of the function field $\mathcal{K}(X(\Gamma_1(6) \cap \Gamma^0(3)))$ where $\Gamma^0(3) = \left\{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) : \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \equiv \left(\begin{smallmatrix} * & 0 \\ * & \end{smallmatrix}\right) \pmod 3\right\}$. Thus the special value $C^{-1}(\tau_0)$ for the maximal order $[\tau_0, 1]$ of an imaginary quadratic field becomes a ray class invariant of level 6. Further, if we use the Shimura's reciprocity law and some numerical approximations, we can come up with the class polynomial for each $C^{-1}(\tau_0)$ as in [6].

Table 4 Explicit values of the Ramanujan's cubic continued fraction

τ_0	$j(\tau_0)$	$C(\tau_0)$
$\frac{3+\sqrt{-3}}{2}$	0	$\frac{\sqrt[3]{2}-\sqrt[3]{4}}{2}$
$\frac{3+\sqrt{-3}}{6}$	0	$-\frac{1}{\sqrt[3]{4}}$
i	1728	$\frac{-1-\sqrt{3}+\left(7-4\sqrt{3}\right)\left(\sqrt{1008+582\sqrt{3}}\right)}{4}$
$\frac{3+i}{2}$	1728	$\frac{1-\sqrt{3}}{2}$
$\sqrt{-2}$	8000	$\frac{2-3\sqrt{2}+\sqrt{6}}{4}$
$\frac{\sqrt{-2}}{2}$	8000	$\frac{-2+\sqrt{6}}{2}$
$\sqrt{-3}$	54000	$\frac{-5\left(2+2\sqrt[3]{2}+\sqrt[3]{4}\right)+\left(-56+18\sqrt[3]{2}+21\sqrt[3]{4}\right)\sqrt{1641279+1302684\sqrt[3]{2}+1033941\sqrt[3]{4}}}{20}$
$\frac{\sqrt{-3}}{3}$	54000	$\frac{\sqrt[3]{-5+3\sqrt{3}}}{2}$

8 Generators of $\mathcal{K}(X_1(N))$ of arbitrary genus

Since the modular curve $X_1(N)$ is a compact Riemann surface, the function field $\mathcal{K}(X_1(N))$ can be generated over $\mathbb{C}$ by two functions. Unlike Ishida–Ishii's result [11] we will find such two generators of $\mathcal{K}(X_1(N))$ of arbitrary genus by means of Siegel functions when $N \geq 7$. As for the cases $N = 2, 3, 4, 5$ and 6, we refer to the Sect. 6.

Let $N \geq 2$. By Proposition 2.4 and the discussion following it, we have the formula

$$g_r^{12N} \circ \alpha = g_{r\alpha}^{12N} = g_{(\langle (r\alpha)_1 \rangle, \langle (r\alpha)_2 \rangle)}^{12N} \tag{8.1}$$

where $r \in \frac{1}{N}\mathbb{Z}^2 \backslash \mathbb{Z}^2$, $\alpha \in \mathrm{SL}_2(\mathbb{Z})$ and $r\alpha = ((r\alpha)_1, (r\alpha)_2)$. For $t \in \mathbb{Z} \backslash N\mathbb{Z}$ we recall the q_τ-expansion formula

$$g_{(\frac{t}{N},0)}(N\tau) = -q_\tau^{\frac{N}{2}\mathbf{B}_2(\frac{t}{N})} \prod_{n=1}^{\infty} (1 - q_\tau^{N(n-1)+t})(1 - q_\tau^{Nn-t}) \tag{8.2}$$

whose coefficients are all rational numbers by (2.8). By Lemma 6.1 we have a distribution relation

$$g_{(\frac{t}{N},0)}^{12N}(N\tau) = \prod_{n=0}^{N-1} g_{(\frac{t}{N},\frac{n}{N})}^{12N}. \tag{8.3}$$

Furthermore by Proposition 6.2, $g_{(\frac{t}{N},0)}^{12N}(N\tau)$ is a modular function for $\Gamma_1(N)$ and we have the order formula

$$\mathrm{ord}_{q_\tau}\left(g_{(\frac{t}{N},0)}^{12N}(N\tau) \circ \alpha\right) = \mathrm{ord}_{q_\tau}\left(g_{(\frac{t}{N},0)}^{12N}(N(\alpha(\tau)))\right) = 6\gcd(c, N)^2 \mathbf{B}_2\left(\left\langle \frac{at}{\gcd(c, N)} \right\rangle\right) \tag{8.4}$$

where $\alpha = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$. From (8.2) we can easily verify that

$$\prod_{t=1}^{N-1} g_{(\frac{t}{N},0)}^{12N}(N\tau) = \left(\frac{\Delta(\tau)}{\Delta(N\tau)}\right)^N, \tag{8.5}$$

which is a modular function for $\Gamma_0(N)$ by (5.1) and Proposition 5.1.

Theorem 8.1 *For $N \geq 7$ we have*

$$\mathcal{K}(X_1(N)) = \mathbb{C}\left(j,\ g^{12N}_{\left(\frac{1}{N},0\right)}(N\tau)\right).$$

Furthermore, $\mathbb{Q}\left(j,\ g^{12N}_{\left(\frac{1}{N},0\right)}(N\tau)\right)$ is the field of all modular functions in $\mathcal{K}(X_1(N))$ with rational Fourier coefficients.

Proof It is well-known that

$$\mathrm{Gal}\left(\mathcal{K}(X(N))/\mathcal{K}(X_1(N))\right) \cong \left\{\pm\begin{pmatrix}1 & b\\ 0 & 1\end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1_2\} \ :\ b \in \mathbb{Z}/N\mathbb{Z}\right\}$$

as a subgroup of $\mathrm{Gal}\left(\mathcal{K}(X(N))/\mathcal{K}(X(1))\right) \cong \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1_2\}$ whose action is given by composition [9].

Let $g = g^{12N}_{\left(\frac{1}{N},0\right)}(N\tau)$. Assume that $g \circ \alpha = g$ for some $\alpha = \left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$, then $\mathrm{ord}_{q_\tau}(g \circ \alpha) = \mathrm{ord}_{q_\tau}(g)$. Thus from the order formula (6.1) we derive

$$6\gcd(c, N)^2\mathbf{B}_2\left(\left\langle\frac{a}{\gcd(c, N)}\right\rangle\right) = 6N^2\mathbf{B}_2\left(\frac{1}{N}\right).$$

The shape of the graph of $Y = \mathbf{B}_2(X)$ in the interval $0 \leq X \leq 1$ shows that the maximum value of $\mathbf{B}_2(X)$ is $\frac{1}{6}$ at $X = 0, 1$. If $\gcd(c, N) \neq N$, we have the inequality

$$6 - 6N + N^2 = 6N^2\mathbf{B}_2\left(\frac{1}{N}\right) = 6\gcd(c, N)^2\mathbf{B}_2\left(\left\langle\frac{a}{\gcd(c, N)}\right\rangle\right) \leq 6 \cdot \left(\frac{N}{2}\right)^2 \cdot \frac{1}{6},$$

which is impossible for $N \geq 7$. Hence $\gcd(c, N) = N$, which yields $\mathbf{B}_2\left(\langle\frac{a}{N}\rangle\right) = \mathbf{B}_2\left(\frac{1}{N}\right)$. Furthermore, since $\alpha \in \mathrm{SL}_2(\mathbb{Z})$, we have $a \not\equiv 0 \pmod N$ so that $a \equiv \pm 1 \pmod N$ from the shape of the graph $\mathbf{B}_2(X)$. Lastly, since $\det(\alpha) = 1$, we obtain $a \equiv d \equiv \pm 1 \pmod N$. Hence $\alpha \equiv \pm\left(\begin{smallmatrix}1 & b\\ 0 & 1\end{smallmatrix}\right) \pmod N$, which implies that $\mathbb{C}(j, g^{12N}_{\left(\frac{1}{N},0\right)}(N\tau))$ is all of $\mathcal{K}(X_1(N))$. And, since j and $g^{12N}_{\left(\frac{1}{N},0\right)}(N\tau)$ have rational Fourier coefficients, we get the second assertion by Lemma 4.1. □

And, in particular, for a prime level p we will present generators in terms of only Siegel functions.

Proposition 8.2 *For an odd prime p all inequivalent cusps of the modular curve $X_1(p)$ are listed as follows*:

$$\begin{cases} \frac{1}{1}, \frac{1}{2}, \ldots, \frac{1}{(p-1)/2} & \text{of width } p\\ \frac{1}{p}, \frac{2}{p}, \ldots, \frac{(p-1)/2}{p} & \text{of width } 1. \end{cases}$$

Proof See [10]. □

Theorem 8.3 *For a prime $p \geq 11$ we have*

$$\mathcal{K}(X_1(p)) = \mathbb{C}\left(\left(p^{12}\frac{\Delta(p\tau)}{\Delta(\tau)}\right)^{5-p} g^{12p}_{\left(\frac{1}{p},0\right)}(p\tau),\ \left(p^{12}\frac{\Delta(p\tau)}{\Delta(\tau)}\right)^{5-p} g^{12p}_{\left(\frac{2}{p},0\right)}(p\tau)\right).$$

Table 5 The orders at the cusps on $X_1(p)$

Cusps	Functions		
	Δ_p	$G_{p,1}$	$G_{p,2}$
$\frac{1}{1}$	$1-p$	p	p
$\frac{1}{2}$	$1-p$	p	p
$\cdots$	$\cdots$	$\cdots$	$\cdots$
$\frac{1}{(p-1)/2}$	$1-p$	p	p
$\frac{1}{p}$	$p-1$	$6p^2\mathbf{B}_2\left(\frac{1}{p}\right)$	$6p^2\mathbf{B}_2\left(\frac{2}{p}\right)$
$\frac{2}{p}$	$p-1$	$6p^2\mathbf{B}_2\left(\frac{2}{p}\right)$	$6p^2\mathbf{B}_2\left(\frac{4}{p}\right)$
$\cdots$	$\cdots$	$\cdots$	$\cdots$
$\frac{(p-1)/2}{p}$	$p-1$	$6p^2\mathbf{B}_2\left(\frac{(p-1)/2}{p}\right)$	$6p^2\mathbf{B}_2\left(\frac{p-1}{p}\right)$

Hence $\mathbb{Q}\left(\left(p^{12}\frac{\Delta(p\tau)}{\Delta(\tau)}\right)^{5-p} g^{12p}_{\left(\frac{1}{p},0\right)}(p\tau),\ \left(p^{12}\frac{\Delta(p\tau)}{\Delta(\tau)}\right)^{5-p} g^{12p}_{\left(\frac{2}{p},0\right)}(p\tau)\right)$ *is the field of all modular functions in* $\mathcal{K}(X_1(p))$ *with rational Fourier coefficients by Lemma* 4.1.

Proof For convenience, we set

$$\Delta_p(\tau) = p^{12}\frac{\Delta(p\tau)}{\Delta(\tau)}, \quad G_{p,1}(\tau) = g^{12p}_{\left(\frac{1}{p},0\right)}(p\tau), \quad G_{p,2}(\tau) = g^{12p}_{\left(\frac{2}{p},0\right)}(p\tau).$$

Then

$$\Delta_p(\tau) = \prod_{n=1}^{p-1} g^{12}_{(0,\frac{n}{p})}(\tau)$$

as we see in (5.1), which is modular for $\Gamma_0(p)$. Observe Table 5 constructed from the order formula (2.9) for Δ_p and (8.4) for $G_{p,1}, G_{p,2}$.

Let us take a negative integer M satisfying the inequality

$$6p^2\mathbf{B}_2\left(\frac{2}{p}\right) \ < \ (-M)\cdot(p-1) \ < \ 6p^2\mathbf{B}_2\left(\frac{1}{p}\right).$$

We take $M = 5-p$. From the shape of the graph $Y = \mathbf{B}_2(X)$ in the interval $0 \le X \le 1$ we see that

$$M(p-1) + 6p^2\mathbf{B}_2\left(\frac{n}{p}\right) < 0 < M(p-1) + 6p^2\mathbf{B}_2\left(\frac{1}{p}\right)$$
$$M(p-1) + 6p^2\mathbf{B}_2\left(\frac{2m}{p}\right) < 0 < M(p-1) + 6p^2\mathbf{B}_2\left(\frac{p-1}{p}\right)$$

for all $n = 2, 3, \ldots, \frac{p-1}{2}$ and $m = 1, 2, \ldots, \frac{p-3}{2}$. Now we observe the orders and the signs of orders of the functions $\Delta_p^M G_{p,1}$ and $\Delta_p^M G_{p,2}$ by Table 5.

For a function $g \in \mathcal{K}(X_1(p))$, we denote by $\deg(g)$ the total degree of the poles of g. Note that $\deg(g)$ is equal to the total degree of the zeros of g, and the functions $\Delta_p^M G_{p,1}$, $\Delta_p^M G_{p,2}$

Table 6 The orders and the signs of orders at the cusps on $X_1(p)$

Cusps	Functions	
	$\Delta_p^M G_{p,1}$	$\Delta_p^M G_{p,2}$
$\frac{1}{1}$	$p^2-5p+5>0$	$p^2-5p+5>0$
$\frac{1}{2}$	$p^2-5p+5>0$	$p^2-5p+5>0$
$\cdots$	$+$	$+$
$\frac{1}{(p-1)/2}$	$p^2-5p+5>0$	$p^2-5p+5>0$
$\frac{1}{p}$	$1>0$	$-(p^2-6p+5)+6p^2\mathbf{B}_2\left(\frac{2}{p}\right)<0$
$\frac{2}{p}$	$-(p^2-6p+5)+6p^2\mathbf{B}_2\left(\frac{2}{p}\right)<0$	$-(p^2-6p+5)+6p^2\mathbf{B}_2\left(\frac{4}{p}\right)<0$
$\cdots$	$-$	$-$
$\frac{(p-1)/2}{p}$	$-(p^2-6p+5)+6p^2\mathbf{B}_2\left(\frac{(p-1)/2}{p}\right)<0$	$1>0$

Table 7 The orders and the signs of orders at the cusps on $X_1(p)$

Cusps	Function
	$(\Delta_p^M G_{p,1})^{-1}+q(\Delta_p^M G_{p,2})^{-1}$
$\frac{1}{1}$	$-(p^2-5p+5)<0$
$\frac{1}{2}$	$-(p^2-5p+5)<0$
$\cdots$	$-$
$\frac{1}{(p-1)/2}$	$-(p^2-5p+5)<0$
$\frac{1}{p}$	$-1<0$
$\frac{2}{p}$	$\min\left\{(p^2-6p+5)-6p^2\mathbf{B}_2\left(\frac{2}{p}\right),\ (p^2-6p+5)-6p^2\mathbf{B}_2\left(\frac{2}{p}\right)\right\}>0$
$\cdots$	$+$
$\frac{(p-1)/2}{p}$	$-1<0$

are modular units. Hence from the Table 6 we get

$$\deg(\Delta_p^M G_{p,1})=\frac{p-1}{2}\cdot(p^2-5p+5)+1$$

$$\deg(\Delta_p^M G_{p,2})=\frac{p-1}{2}\cdot(p^2-5p+5)+1.$$

Let us consider the function $(\Delta_p^M G_{p,1})^{-1}+q(\Delta_p^M G_{p,2})^{-1}$ for a suitably large positive integer q. Again from the Table 6 we obtain the Table 7.

Hence we deduce that

$$\deg\left((\Delta_p^M G_{p,1})^{-1}+q(\Delta_p^M G_{p,2})^{-1}\right)=\frac{p-1}{2}\cdot(p^2-5p+5)+2=\deg(\Delta_p^M G_{p,1})+1.$$

Therefore, $\gcd(\deg(\Delta_p^M G_{p,1}),\ \deg((\Delta_p^M G_{p,1})^{-1}+q(\Delta_p^M G_{p,2})^{-1}))=1$, which leads to the fact that $\mathcal{K}(X_1(p))=\mathbb{C}(\Delta_p^M G_{p,1},\ \Delta_p^M G_{p,2})$, as desired. □

9 Ray class fields of imaginary quadratic fields

Let $K \neq \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3})$ be an imaginary quadratic field with discriminant d_K. We denote by $K_{(1)}$ the Hilbert class field of K and $K_{(N)}$ the ray class field modulo N of K for an integer $N \geq 2$. Let $\mathcal{O}_K = \mathbb{Z}[\theta]$ with $\theta \in \mathfrak{H}$ be the ring of algebraic integers in K. By the main theorem of complex multiplication we know that $K_{(1)} = K(j(\theta))$ and $K_{(N)} = K\mathcal{F}_N(\theta)$, the field generated over K by all values $h(\theta)$ with $h \in \mathcal{F}_N$ defined and finite at θ. Setting $\mathrm{irr}(\theta, \mathbb{Q}) = X^2 + BX + C$ we take a group

$$W_{N,\theta} = \left\{ \begin{pmatrix} t - Bs & -Cs \\ s & t \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) \ : \ t, s \in \mathbb{Z}/N\mathbb{Z} \right\}.$$

Then by the Shimura's reciprocity law we have a surjection with kernel $\{\pm 1_2\}$ given by

$$\begin{aligned} W_{N,\theta} &\longrightarrow \mathrm{Gal}\left(K_{(N)}/K_{(1)}\right) \\ \alpha &\longmapsto \overline{\alpha} = \left(h(\theta) \mapsto h^{\alpha}(\theta)\right) \end{aligned}$$

where $h \in \mathcal{F}_N$ is defined and finite at θ [7].

Lemma 9.1 *For $N \geq 2$, let A and D be positive integers such that $AD = N$ and $D \geq 2$. Then $N\theta$ and $\frac{A\theta+B}{D}$ are not equivalent under $\mathrm{SL}_2(\mathbb{Z})$ for any integer B.*

Proof Take an integer B' such that $\mathrm{Re}(\theta + B') = 0$ or $\frac{1}{2}$. Since $\left(\begin{smallmatrix} 1 & NB' \\ 0 & 1 \end{smallmatrix}\right)(N\theta) = N(\theta + B')$ and $\frac{A\theta+B}{D} = \frac{A(\theta+B')+(B-AB')}{D}$, we may assume that $\mathrm{Re}(\theta) = 0$ or $\frac{1}{2}$ in the beginning. Suppose on the contrary that $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)(N\theta) = \frac{A\theta+B}{D}$ for some $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$. Then by using the identity in [21, Lemma 1.1] we have

$$\mathrm{Im}\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}(N\theta)\right) = \frac{N}{|cN\theta + d|^2}\mathrm{Im}(\theta) = \mathrm{Im}\left(\frac{A\theta + B}{D}\right) = \frac{A}{D}\mathrm{Im}(\theta),$$

which yields $ND = A|cN\theta + d|^2 = Ac^2N^2|\theta|^2 + 2AcdN\mathrm{Re}(\theta) + Ad^2$. Replacing N by AD and dividing the equation by A gives

$$D^2 = A^2D^2c^2|\theta|^2 + 2ADcd\mathrm{Re}(\theta) + d^2. \tag{9.1}$$

If $\mathrm{Re}(\theta) = 0$, then (9.1) is reduced to $D^2 = A^2D^2c^2|\theta|^2 + d^2$. Hence D divides d so that putting $d = De$ and dividing both sides by D^2 we get $1 = A^2c^2|\theta|^2 + e^2$. Since $|\theta|^2 \geq 2$, we have $c = 0$ and $e = \pm 1$; hence $\gcd(c, d) = D \geq 2$. But this contradicts $ad - bc = 1$.

If $\mathrm{Re}(\theta) = \frac{1}{2}$, then (9.1) becomes $D^2 = A^2D^2c^2|\theta|^2 + ADcd + d^2$. Thus D divides d^2, which implies that $d \neq \pm 1$ because $D \geq 2$. On the other hand, since $|\theta|^2 \geq 2$, we have $D^2 \geq 2A^2D^2c^2 + ADcd + d^2 = \left(\frac{7A^2c^2}{4}\right)D^2 + \left(\frac{ADc}{2} + d\right)^2$. This yields $c = 0$ so that $\gcd(c, d) = |d| > 1$. But it again contradicts $ad - bc = 1$.

Therefore $N\theta$ and $\frac{A\theta+B}{D}$ can not be equivalent under $\mathrm{SL}_2(\mathbb{Z})$. □

Lemma 9.2 *Let $N \geq 2$. If $j(N\theta) = j(N\tau) \circ \alpha(\theta) (= j(N(\alpha(\theta))))$ for some $\alpha = \left(\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$, then $z \equiv 0 \pmod{N}$, that is, $\alpha \in \Gamma_0(N)$.*

Proof Note that $j(N\tau) \circ \alpha(\theta) = j \circ \left(\begin{smallmatrix} Nx & Ny \\ z & w \end{smallmatrix}\right)(\theta)$. Since $\left(\begin{smallmatrix} Nx & Ny \\ z & w \end{smallmatrix}\right)$ is a primitive matrix of determinant N, we can decompose it into $\beta\left(\begin{smallmatrix} A & B \\ 0 & D \end{smallmatrix}\right)$ for some $\beta \in \mathrm{SL}_2(\mathbb{Z})$ and positive integers A, B, D such that $AD = N$. Then $j(N\theta) = j \circ \left(\begin{smallmatrix} Nx & Ny \\ z & w \end{smallmatrix}\right)(\theta) = j \circ \beta\left(\begin{smallmatrix} A & B \\ 0 & D \end{smallmatrix}\right)(\theta) = j \circ \left(\begin{smallmatrix} A & B \\ 0 & D \end{smallmatrix}\right)(\theta) = j(\frac{A\theta+B}{D})$, which yields that $N\theta$ and $\frac{A\theta+B}{D}$ are equivalent under $\mathrm{SL}_2(\mathbb{Z})$. Now Lemma 9.1 forces us to have $D = 1$ and $A = N$, from which we achieve $z \equiv 0 \pmod{N}$ due to the fact $\left(\begin{smallmatrix} Nx & Ny \\ z & w \end{smallmatrix}\right) = \beta\left(\begin{smallmatrix} A & B \\ 0 & D \end{smallmatrix}\right)$. □

Lemma 9.3 *If $N \geq 4$, we have the following inequalities*

$$\left| g_{\left(\frac{1}{N},0\right)}(N\theta) \right| < \left| g_{\left(\frac{x}{N},0\right)}(N\theta) \right|$$

for $1 < x \leq \left[\frac{N}{2}\right]$.

Proof Put $A = |q_\theta| = |e^{2\pi i\theta}|$ and observe that for $1 < x \leq \left[\frac{N}{2}\right]$

$$M = \left| \frac{g_{\left(\frac{1}{N},0\right)}(N\theta)}{g_{\left(\frac{x}{N},0\right)}(N\theta)} \right| = \left| \frac{q_\theta^{\frac{N}{2}\mathbf{B}_2\left(\frac{1}{N}\right)} \prod_{n=1}^{\infty}(1-q_\theta^{N(n-1)+1})(1-q_\theta^{Nn-1})}{q_\theta^{\frac{N}{2}\mathbf{B}_2\left(\frac{x}{N}\right)} \prod_{n=1}^{\infty}(1-q_\theta^{N(n-1)+x})(1-q_\theta^{Nn-x})} \right| \quad \text{by (8.2)}$$

$$\leq A^{\frac{N}{2}(\mathbf{B}_2(\frac{1}{N})-\mathbf{B}_2(\frac{x}{N}))} \frac{\prod_{n=1}^{\infty}(1+A^{N(n-1)+1})(1+A^{Nn-1})}{\prod_{n=1}^{\infty}(1-A^{N(n-1)+x})(1-A^{Nn-x})}.$$

Since $A = |e^{2\pi i\theta}| \leq e^{-\sqrt{7}\pi} < 0.00025$, we obviously derive

$$\frac{1}{1-A^X} < 1 + A^{X-1} \quad \text{for any } X \geq 1. \tag{9.2}$$

Furthermore we have the inequality

$$1 + X < e^X \quad \text{for } X > 0. \tag{9.3}$$

Hence we get by (9.2) that

$$M \leq A^{\frac{N}{2}(\mathbf{B}_2(\frac{1}{N})-\mathbf{B}_2(\frac{x}{N}))} \prod_{n=1}^{\infty}(1+A^{N(n-1)+1})(1+A^{Nn-1})(1+A^{N(n-1)+x-1})(1+A^{Nn-x-1})$$

$$\leq A^{\frac{N}{2}\left(\mathbf{B}_2\left(\frac{1}{N}\right)-\mathbf{B}_2\left(\frac{2}{N}\right)\right)} \prod_{n=1}^{\infty}(1+A^{N(n-1)+2-1})^4 \quad \text{by the fact } A \leq e^{-\sqrt{7}\pi}$$

$$\leq A^{\left(\frac{1}{2}-\frac{3}{2N}\right)e^{\frac{4A}{1-A^N}}} \leq A^{\left(\frac{1}{2}-\frac{3}{8}\right)e^{\frac{4A}{1-A^4}}} < 1 \quad \text{by (9.3) and the fact } A \leq e^{-\sqrt{7}\pi}.$$

This proves the lemma. □

Lemma 9.4 *Let $N \geq 2$ and $\alpha = \left(\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right) \in \Gamma_0(N)$. Then for $t \in \mathbb{Z}\backslash N\mathbb{Z}$ we have the transformation formula*

$$g^{12N}_{\left(\frac{t}{N},0\right)}(N\tau) \circ \alpha = g^{12N}_{\left(\langle\frac{tx}{N}\rangle,0\right)}(N\tau). \tag{9.4}$$

Therefore, for any integer m the functions

$$\sum_{\substack{1 \leq t \leq N-1 \\ \gcd(t,N)=1}} g^{12Nm}_{\left(\frac{t}{N},0\right)}(N\tau) \quad \text{and} \quad \prod_{\substack{1 \leq t \leq N-1 \\ \gcd(t,N)=1}} g^{12Nm}_{\left(\frac{t}{N},0\right)}(N\tau)$$

are modular functions for $\Gamma_0(N)$ with rational Fourier coefficients. Furthermore, if $\left| g^{12N}_{\left(\frac{1}{N},0\right)}(N\tau) \circ \alpha(\theta) \right| = \left| g^{12N}_{\left(\frac{1}{N},0\right)}(N\theta) \right|$, we get $x \equiv w \equiv \pm 1 \pmod N$.

Proof Observe by (8.1), (8.3) and the fact $\gcd(w, N) = 1$ that

$$g^{12N}_{\left(\frac{t}{N},0\right)}(N\tau) \circ \alpha = \prod_{n=0}^{N-1} g^{12N}_{\left(\frac{t}{N},\frac{n}{N}\right)} \circ \begin{pmatrix} x & y \\ z & w \end{pmatrix} = \prod_{n=0}^{N-1} g^{12N}_{\left(\langle\frac{tx}{N}\rangle,\left\langle\frac{ty+nw}{N}\right\rangle\right)} = g^{12N}_{\left(\langle\frac{tx}{N}\rangle,0\right)}(N\tau).$$

Then for any integer m we achieve

$$\sum_{\substack{1\le t\le N-1\\ \gcd(t,N)=1}} g^{12Nm}_{\left(\frac{t}{N},0\right)}(N\tau)\circ\alpha=\sum_{\substack{1\le t\le N-1\\ \gcd(t,N)=1}} g^{12Nm}_{\left(\langle\frac{tx}{N}\rangle,0\right)}(N\tau)=\sum_{\substack{1\le t\le N-1\\ \gcd(t,N)=1}} g^{12Nm}_{\left(\frac{t}{N},0\right)}(N\tau)$$

and

$$\prod_{\substack{1\le t\le N-1\\ \gcd(t,N)=1}} g^{12Nm}_{\left(\frac{t}{N},0\right)}(N\tau)\circ\alpha=\prod_{\substack{1\le t\le N-1\\ \gcd(t,N)=1}} g^{12Nm}_{\left(\langle\frac{tx}{N}\rangle,0\right)}(N\tau)=\prod_{\substack{1\le t\le N-1\\ \gcd(t,N)=1}} g^{12Nm}_{\left(\frac{t}{N},0\right)}(N\tau)$$

because x is prime to N. Thus the functions $\sum_{\substack{1\le t\le N-1\\ \gcd(t,N)=1}} g^{12Nm}_{\left(\frac{t}{N},0\right)}(N\tau)$ and $\prod_{\substack{1\le t\le N-1\\ \gcd(t,N)=1}} g^{12Nm}_{\left(\frac{t}{N},0\right)}(N\tau)$ are modular for $\Gamma_0(N)$ and have rational Fourier coefficients owing to the fact that each $g^{12Nm}_{\left(\frac{t}{N},0\right)}(N\tau)$ has rational Fourier coefficients.

Suppose $|g^{12N}_{\left(\frac{1}{N},0\right)}(N\tau)\circ\alpha(\theta)|=|g^{12N}_{\left(\frac{1}{N},0\right)}(N\theta)|$. Then by previous observation we have $|g^{12N}_{\left(\langle\frac{x}{N}\rangle,0\right)}(N\theta)|=|g^{12N}_{\left(\frac{1}{N},0\right)}(N\theta)|$. If $N=2$ or 3, we automatically get $x\equiv\pm1 \pmod N$. If $N\ge4$, by Lemma 9.3 we see that $x\equiv\pm1 \pmod N$. Moreover, since $\det(\alpha)=1$, we deduce $x\equiv w\equiv\pm1 \pmod N$. □

Theorem 9.5 *For $N\ge2$ we have*

$$K_{(N)}=K\left(j(N\theta),\ g^{12N}_{\left(\frac{1}{N},0\right)}(N\theta)\right).$$

Proof Let F be the field on the right side. Since the functions $j(N\tau)$ and $g^{12N}_{\left(\frac{1}{N},0\right)}(N\tau)$ belong to $\mathcal{F}_N$, F is a subfield of $K_{(N)}$. Moreover, since $j(N\theta)$ is a generator of the ring class field of the order $[N\theta,\ 1]$, F contains the Hilbert class field $K_{(1)}$.

Let $\alpha=\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)\in W_{N,\theta}$ induce $\overline{\alpha}\in\mathrm{Gal}\left(K_{(N)}/K_{(1)}\right)$ which is the identity on F. For the action of α on $\mathcal{F}_N$ we decompose α into $\alpha=\left(\begin{smallmatrix}1&0\\0&u\end{smallmatrix}\right)\left(\begin{smallmatrix}x&y\\z&w\end{smallmatrix}\right)$ for some $u\in(\mathbb{Z}/N\mathbb{Z})^*$ and $\left(\begin{smallmatrix}x&y\\z&w\end{smallmatrix}\right)\in\mathrm{SL}_2(\mathbb{Z})$(see Sect. 4). Since $j(N\tau)$ has rational Fourier coefficients, we get

$$j(N\theta)=j(N\theta)^{\overline{\alpha}}=j(N\tau)^{\alpha}(\theta)=j(N\tau)\circ\begin{pmatrix}x&y\\z&w\end{pmatrix}(\theta).$$

Then we have $z\equiv0 \pmod N$ by Lemma 9.2, from which we get $\gcd(x,N)=\gcd(w,N)=1$ because $\left(\begin{smallmatrix}x&y\\z&w\end{smallmatrix}\right)\in\mathrm{SL}_2(\mathbb{Z})$. And, the fact that $g^{12N}_{\left(\frac{1}{N},0\right)}(N\tau)$ has rational Fourier coefficients enables us to derive

$$g^{12N}_{\left(\frac{1}{N},0\right)}(N\theta)=\left(g^{12N}_{\left(\frac{1}{N},0\right)}(N\theta)\right)^{\overline{\alpha}}=\left(g^{12N}_{\left(\frac{1}{N},0\right)}(N\tau)\right)^{\alpha}(\theta)=g^{12N}_{\left(\frac{1}{N},0\right)}(N\tau)\circ\begin{pmatrix}x&y\\z&w\end{pmatrix}(\theta).$$

Then by Lemma 9.4 we obtain $x\equiv w\equiv\pm1 \pmod N$; hence $\alpha=\pm\left(\begin{smallmatrix}1&0\\0&u\end{smallmatrix}\right)\left(\begin{smallmatrix}1&*\\0&1\end{smallmatrix}\right)=\pm\left(\begin{smallmatrix}1&*\\0&u\end{smallmatrix}\right)$. On the other hand, since α is of the form $\left(\begin{smallmatrix}t-Bs&-Cs\\s&t\end{smallmatrix}\right)\in W_{N,\theta}$ for some $t,s\in\mathbb{Z}/N\mathbb{Z}$, we have $s=0$ and $t=\pm1$ in $\mathbb{Z}/N\mathbb{Z}$, namely $\alpha=\pm1_2\in\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. This shows that the field F is all of $K_{(N)}$. □

Corollary 9.6 *For $N\ge2$, let $\mathcal{F}_N^1$ be the field of all modular functions for $\Gamma_1(N)$ with rational Fourier coefficients. Then we get*

$$K_{(N)}=K\mathcal{F}_N^1(\theta).$$

Proof Since the functions $j(N\tau)$ and $g^{12N}_{\left(\frac{1}{N},0\right)}(N\tau)$ belong to $\mathcal{F}^1_N$, we have the inclusion $K_{(N)} \subset K\mathcal{F}^1_N(\theta)$. However, the fact $K_{(N)} = K\mathcal{F}_N(\theta)$ implies that $K_{(N)} = K\mathcal{F}^1_N(\theta)$. □

Remark 9.7 Cho and Koo also showed in [7] the above corollary purely by means of Shimura's canonical models.

Ramachandra has shown in [18] that ray class fields over imaginary quadratic fields can be generated by elliptic units. However, the generators constructed by him involve very complicated products of high powers of singular values of the Klein form and singular values of the discriminant Δ. From now on unlike Ramachandra's invariant we will construct a ray class invariant of $K_{(N)}$ somewhat in a simpler way.

Theorem 9.8 *For $N \geq 2$, let*

$$T_N(\tau) = \sum_{\substack{1 \leq t \leq N-1 \\ \gcd(t,N)=1}} g^{24N}_{\left(\frac{t}{N},0\right)}(\tau).$$

Then we have

$$K_{(N)} = K\left(j(N\theta)T_N^{-1}(N\theta)g^{24N}_{\left(\frac{1}{N},0\right)}(N\theta)\right).$$

Proof It follows from Lemma 9.4 that the function $T_N(N\tau)$ is a modular function for $\Gamma_0(N)$ with rational Fourier coefficients. By (8.2) we easily see that $g^{24N}_{\left(\frac{t}{N},0\right)}(N\theta)$ is a positive real number for any $t \in \mathbb{Z} \setminus N\mathbb{Z}$, from which we get $T_N(N\theta) \neq 0$.

Let $F = K(j(N\theta)T_N(N\theta)^{-1}g^{24N}_{\left(\frac{1}{N},0\right)}(N\theta))$. Then F is a subfield of the ray class field $K_{(N)}$ because the function $j(N\tau)T_N^{-1}(N\tau)g^{24N}_{\left(\frac{1}{N},0\right)}(N\tau)$ belongs to $\mathcal{F}_N$. For $1 \leq m \leq N-1$ with $\gcd(m,N) = 1$, decompose each $\left(\begin{smallmatrix} m & 0 \\ 0 & m \end{smallmatrix}\right)$ into $\left(\begin{smallmatrix} 1 & 0 \\ 0 & m^2 \end{smallmatrix}\right)\left(\begin{smallmatrix} m & 0 \\ 0 & m^{-1} \end{smallmatrix}\right)$ in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. Since $j(N\tau)T_N^{-1}(N\tau)$ is a modular function for $\Gamma_0(N)$ with rational Fourier coefficients, each $\left(\begin{smallmatrix} m & 0 \\ 0 & m \end{smallmatrix}\right)$ fixes it. Furthermore, since $g^{24N}_{\left(\frac{1}{N},0\right)}(N\tau)$ has also rational Fourier coefficients, $\left(\begin{smallmatrix} m & 0 \\ 0 & m \end{smallmatrix}\right)$ acts as composition of $\left(\begin{smallmatrix} m & 0 \\ 0 & m^{-1} \end{smallmatrix}\right)$ on it. Now that $\left(\begin{smallmatrix} m & 0 \\ 0 & m \end{smallmatrix}\right) \in W_{N,\theta}$, we derive

$$\begin{aligned}\left(j(N\theta)T_N^{-1}(N\theta)g^{24N}_{\left(\frac{1}{N},0\right)}(N\theta)\right)^{\overline{\left(\begin{smallmatrix} m & 0 \\ 0 & m \end{smallmatrix}\right)}} &= (j(N\tau)T_N^{-1}(N\tau))^{\left(\begin{smallmatrix} m & 0 \\ 0 & m \end{smallmatrix}\right)}(\theta)\left(g^{24N}_{\left(\frac{1}{N},0\right)}(N\tau)\right)^{\left(\begin{smallmatrix} m & 0 \\ 0 & m \end{smallmatrix}\right)}(\theta) \\ &= j(N\theta)T_N^{-1}(N\theta)\left(g^{24N}_{\left(\frac{1}{N},0\right)}(N\tau) \circ \left(\begin{smallmatrix} m & 0 \\ 0 & m^{-1} \end{smallmatrix}\right)(\theta)\right) \\ &= j(N\theta)T_N^{-1}(N\theta)g^{24N}_{\left(\frac{m}{N},0\right)}(N\theta) \quad \text{by Lemma 9.4.}\end{aligned}$$

On the other hand, since $K_{(N)}$ is an abelian extension of K, the intermediate field F is also an abelian extension of K. Hence F has the following element

$$\sum_{\substack{1 \leq m \leq N-1 \\ \gcd(m,N)=1}} j(N\theta)T_N^{-1}(N\theta)g^{24N}_{\left(\frac{m}{N},0\right)}(N\theta) = j(N\theta)T_N^{-1}(N\theta)\sum_{\substack{1 \leq m \leq N-1 \\ \gcd(m,N)=1}} g^{24N}_{\left(\frac{m}{N},0\right)}(N\theta) = j(N\theta).$$

Here we regard F as an intermediate field between $K_{(N)}$ and $K_{(1)}$ because $K(j(N\theta))$ contains $K_{(1)}$. Let an element $\alpha \in W_{N,\theta}$ induce $\overline{\alpha} \in \mathrm{Gal}\left(K_{(N)}/K_{(1)}\right)$ which is the identity on F.

Decompose α into $\alpha = \left(\begin{smallmatrix} 1 & 0 \\ 0 & u \end{smallmatrix}\right)\left(\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right)$ for some $u \in (\mathbb{Z}/N\mathbb{Z})^*$ and $\left(\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$. Owing to the fact that $j(N\tau)$ has rational Fourier coefficients we deduce

$$j(N\theta) = j(N\theta)^{\overline{\alpha}} = j(N\tau)^{\alpha}(\theta) = j(N\tau) \circ \begin{pmatrix} x & y \\ z & w \end{pmatrix}(\theta).$$

Then by Lemma 9.2 we achieve $z \equiv 0 \pmod{N}$, from which we obtain $\gcd(N, x) = \gcd(N, w) = 1$ because $\left(\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$. Since $j(N\tau)T_N^{-1}(N\tau)$ is a modular function for $\Gamma_0(N)$ with rational Fourier coefficients and $z \equiv 0 \pmod{N}$, it is fixed by α. Thus $\overline{\alpha}$ fixes the value $j(N\theta)T_N^{-1}(N\theta)$. Moreover, since $\overline{\alpha}$ fixes the value $j(N\theta)T_N^{-1}(N\theta)g^{24N}_{\left(\frac{1}{N},0\right)}(N\theta)$, $\overline{\alpha}$ fixes $g^{24N}_{\left(\frac{1}{N},0\right)}(N\theta)$. Since $g^{24N}_{\left(\frac{1}{N},0\right)}(N\tau)$ has rational Fourier coefficient, it follows that

$$g^{24N}_{\left(\frac{1}{N},0\right)}(N\theta) = \left(g^{24N}_{\left(\frac{1}{N},0\right)}(N\theta)\right)^{\overline{\alpha}} = \left(g^{24N}_{\left(\frac{1}{N},0\right)}(N\tau)\right)^{\alpha}(\theta) = g^{24N}_{\left(\frac{1}{N},0\right)}(N\tau) \circ \begin{pmatrix} x & y \\ z & w \end{pmatrix}(\theta).$$

And, by Lemma 9.4 we have $x \equiv w \equiv \pm 1 \pmod{N}$ so that $\alpha = \pm\left(\begin{smallmatrix} 1 & 0 \\ 0 & u \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right) = \pm\left(\begin{smallmatrix} 1 & * \\ 0 & u \end{smallmatrix}\right)$. On the other hand, since α is of the form $\left(\begin{smallmatrix} t-Bs & -Cs \\ s & t \end{smallmatrix}\right) \in W_{N,\theta}$ for some $t, s \in \mathbb{Z}/N\mathbb{Z}$, we get $s = 0$ and $t = \pm 1$ in $\mathbb{Z}/N\mathbb{Z}$, that is, $\alpha = \pm 1_2 \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. This concludes that the field F is equal to $K_{(N)}$. □

We will also construct a primitive generator as a ring or ray class invariant from a different point of view.

Lemma 9.9 *Let $N \geq 2$. For any nonzero integer m, the value $\left(j(N\theta) + \frac{1}{3}\right)^m$ generates the ring class field of the order $[N\theta,\ 1]$ over K.*

Proof Let $\mathcal{O}$ be the order $[N\theta,\ 1]$ and $K_{\mathcal{O}}$ be the ring class field of the order $\mathcal{O}$ with extension degree $h_{\mathcal{O}} = [K_{\mathcal{O}} : K]$. Then $K_{\mathcal{O}}$ is generated by an algebraic integer $j(\mathcal{O})$, and the conjugates of $j(\mathcal{O})$ are of the form $j(\mathfrak{a}_1), \ldots, j(\mathfrak{a}_{h_{\mathcal{O}}})$ where $\mathfrak{a}_k$ runs over all representatives in the ideal class group of proper fractional $\mathcal{O}$-ideals.

Let σ be a nontrivial element of $\mathrm{Gal}(K_{\mathcal{O}}/K)$. Then $\sigma(j(\mathcal{O})) = j(\mathfrak{a}')$ for some proper fractional $\mathcal{O}$-ideal $\mathfrak{a}'$ which is not principal. Suppose that σ induces the identity on $K((j(\mathcal{O})+\frac{1}{3})^m)$. Then $\sigma((j(\mathcal{O})+\frac{1}{3})^m) = (j(\mathcal{O})+\frac{1}{3})^m = (j(\mathfrak{a})+\frac{1}{3})^m$. Hence $j(\mathcal{O})+\frac{1}{3} = \zeta(j(\mathfrak{a}')+\frac{1}{3})$ for some mth root of unity ζ in $K_{\mathcal{O}}$. If $\zeta = 1$, we have $j(\mathcal{O}) = j(\mathfrak{a}')$, which is impossible. If $\zeta \neq 1$, we have $j(\mathcal{O}) - \zeta j(\mathfrak{a}') = \frac{-1+\zeta}{3}$. Since $j(\mathcal{O}) - \zeta j(\mathfrak{a}')$ is an algebraic integer in $K_{\mathcal{O}}$, its norm from $K_{\mathcal{O}}$ to $\mathbb{Q}$ should be an integer. Letting $\mathrm{Gal}(K_{\mathcal{O}}/\mathbb{Q}) = \{\sigma_1, \ldots, \sigma_{2h_{\mathcal{O}}}\}$, we have

$$0 < \left|\mathbf{N}_{K_{\mathcal{O}}/\mathbb{Q}}\left(\frac{-1+\zeta}{3}\right)\right| = \frac{\prod_{k=1}^{2h_{\mathcal{O}}} |-1+\sigma_k(\zeta)|}{3^{2h_{\mathcal{O}}}} \leq \frac{2^{2h_{\mathcal{O}}}}{3^{2h_{\mathcal{O}}}} < 1,$$

which contradicts the fact that the norm is an integer. Thus σ could not induce the identity on $K((j(\mathcal{O}) + \frac{1}{3})^m)$, which implies that $K((j(\mathcal{O}) + \frac{1}{3})^m)$ is in fact all of $K_{\mathcal{O}}$. □

Theorem 9.10 *For $N \geq 2$, let*

$$M_N(\tau) = \prod_{\substack{1 \leq t \leq N-1 \\ \gcd(t,\, N) = 1}} g^{12N}_{\left(\frac{t}{N},0\right)}(\tau).$$

Then we have

$$K_{(N)} = K\left(\left(j(N\theta) + \frac{1}{3}\right) M_N^{-1}(N\theta) g^{12N\phi(N)}_{\left(\frac{1}{N},0\right)}(N\theta)\right).$$

Proof We replace the term

$$\sum_{\substack{1 \le m \le N-1 \\ \gcd(m,N)=1}} j(N\theta) T_N^{-1}(N\theta) g_{\left(\frac{m}{N},0\right)}^{24N}(N\theta)$$

which appears in the proof of Theorem 9.8 by

$$\prod_{\substack{1 \le m \le N-1 \\ \gcd(m,N)=1}} \left(j(N\theta) + \frac{1}{3}\right) M_N^{-1}(N\theta) g_{\left(\frac{m}{N},0\right)}^{12N\phi(N)}(N\theta).$$

Then the proof is quite similar to that of Theorem 9.8 except for the use of Lemma 9.9. So we omit the remaining part. □

Lastly, for a prime $p \ge 11$ we also give a ray class invariant which is the singular value of a product of Siegel functions without using the elliptic modular function j. When $p = 7$, Cho et al. [5, Corollary 4.7] achieved such an invariant by means of singular value of a modified theta constant.

Theorem 9.11 *For a prime $p \ge 11$, let $\Phi_p(X, Y) = 0$ be an affine curve such that $\Phi_p(X, Y) \in \mathbb{Q}[X, Y]$ and $\Phi_p((p^{12}\frac{\Delta(p\tau)}{\Delta(\tau)})^{5-p} g_{(\frac{1}{p},0)}^{12p}(p\tau), (p^{12}\frac{\Delta(p\tau)}{\Delta(\tau)})^{5-p} g_{(\frac{2}{p},0)}^{12p}(p\tau)) = 0$. Suppose that the point $((p^{12}\frac{\Delta(p\theta)}{\Delta(\theta)})^{5-p} g_{(\frac{1}{p},0)}^{12p}(p\theta),\ (p^{12}\frac{\Delta(p\theta)}{\Delta(\theta)})^{5-p} g_{(\frac{2}{p},0)}^{12p}(p\theta))$ on the curve is nonsingular. Then we obtain*

$$K_{(p)} = K\left(\left(p^{12}\frac{\Delta(p\theta)}{\Delta(\theta)}\right)^{5-p} g_{\left(\frac{1}{p},0\right)}^{12p}(p\theta)\right).$$

Proof We shall use the same conventions as in the proof of Theorem 8.3. Since $\Delta_p^{5-p} G_{p,1}$ and $\Delta_p^{5-p} G_{p,2}$ are defined and finite on $\mathfrak{H}$, the field on the right side is contained in $K_{(p)} = K\mathcal{F}_p(\theta)$. For any function $h \in \mathbb{Q}(\Delta_p^{5-p} G_{p,1}, \Delta_p^{5-p} G_{p,2})$ which is defined and finite at θ there exist $f(X, Y),\ g(X, Y) \in \mathbb{Q}[X, Y]/(\Phi_p(X, Y))$ such that $h = \frac{f(\Delta_p^{5-p} G_{p,1}, \Delta_p^{5-p} G_{p,2})}{g(\Delta_p^{5-p} G_{p,1}, \Delta_p^{5-p} G_{p,2})}$ and $g(\Delta_p^{5-p}(\theta) G_{p,1}(\theta),\ \Delta_p^{5-p}(\theta) G_{p,2}(\theta)) \ne 0$ because we are assuming that the point $(\Delta_p^{5-p}(\theta) G_{p,1}(\theta), \Delta_p^{5-p}(\theta) G_{p,2}(\theta))$ of the curve is nonsingular. Hence $h(\theta) \in \mathbb{Q}(\Delta_p^{5-p}(\theta) G_{p,1}(\theta),\ \Delta_p^{5-p}(\theta) G_{p,2}(\theta))$, and by Corollary 9.6 we have

$$K_{(p)} = K\mathcal{F}_p^1(\theta) = K\left(\Delta_p^{5-p}(\theta) G_{p,1}(\theta),\ \Delta_p^{5-p}(\theta) G_{p,2}(\theta)\right).$$

Decompose $\left(\begin{smallmatrix} 2 & 0 \\ 0 & 2 \end{smallmatrix}\right) \in W_{p,\theta}$ into $\left(\begin{smallmatrix} 2 & 0 \\ 0 & 2 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 2^2 \end{smallmatrix}\right)\left(\begin{smallmatrix} 2 & 0 \\ 0 & 2^{-1} \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$. Now that $\Delta_p^{5-p} G_{p,1}$ has rational Fourier coefficients, $\left(\begin{smallmatrix} 2 & 0 \\ 0 & 2 \end{smallmatrix}\right)$ acts on the function as composition with $\left(\begin{smallmatrix} 2 & 0 \\ 0 & 2^{-1} \end{smallmatrix}\right)$. Moreover, since Δ_p is modular for $\Gamma_0(p)$, $\left(\begin{smallmatrix} 2 & 0 \\ 0 & 2^{-1} \end{smallmatrix}\right)$ fixes Δ_p. It then follows that

$$\begin{aligned}
\left(\Delta_p^{5-p}(\theta) G_{p,1}(\theta)\right)^{\overline{\left(\begin{smallmatrix} 2 & 0 \\ 0 & 2 \end{smallmatrix}\right)}} &= \left(\Delta_p^{5-p} G_{p,1}\right)^{\left(\begin{smallmatrix} 2 & 0 \\ 0 & 2 \end{smallmatrix}\right)}(\theta) \\
&= \left(\Delta_p^{5-p} G_{p,1}\right)^{\left(\begin{smallmatrix} 2 & 0 \\ 0 & 2^{-1} \end{smallmatrix}\right)}(\theta) \\
&= \Delta_p^{5-p}(\theta)\left(G_{p,1}\right)^{\left(\begin{smallmatrix} 2 & 0 \\ 0 & 2^{-1} \end{smallmatrix}\right)}(\theta) \\
&= \Delta_p^{5-p}(\theta) G_{p,2}(\theta) \quad \text{by Lemma 9.4,}
\end{aligned}$$

which shows that $\Delta_p^{5-p}(\theta)G_{p,1}(\theta)$ and $\Delta_p^{5-p}(\theta)G_{p,2}(\theta)$ are conjugates. Therefore, $K_{(p)}$ can be generated over K by only one generator $\Delta_p^{5-p}(\theta)G_{p,1}(\theta)$. □

References

1. Atkin, A.O.L.: Weierstrass points at cusps $\Gamma_0(n)$. Ann. Math. **85**(2), 42–45 (1967)
2. Adiga, C., Kim, T., Naika, M.S.M., Madhusudhan, H.S.: On Ramanujan's cubic continued fraction and explicit evaluations of theta-functions. Indian J. Pure Appl. Math. **35**(9), 1047–1062 (2004)
3. Bringmann, K., Ono, K.: The $f(q)$ mock theta function conjecture and partition ranks. Invent. Math. **165**(2), 243–266 (2006)
4. Chan, H.H.: On Ramanujan's cubic continued fraction. Acta Arith. **73**(4), 343–355 (1995)
5. Cho, B., Kim, N.M., Koo, J.K.: Affine models of the modular curves $X(p)$ and its application (submitted)
6. Cho, B., Koo, J.K., Park, Y.K.: On the Ramanujan's cubic continued fraction as modular function (submitted)
7. Cho, B., Koo, J.K.: Constructions of class fields over imaginary quadratic fields and applications. Quart. J. Math. (to appear)
8. Cox, D.A.: Primes of the form $x^2 + ny^2$: Fermat, Class Field, and Complex Multiplication. Wiley, London (1989)
9. Diamond, F., Shurman, J.: A First Course in Modular Forms. Springer, Heidelberg (2005)
10. Harada, K.: "Moonshine" of Finite Groups. The Ohio State University Lecure Notes
11. Ishida, N., Ishii, N.: The equation for the modular curve $X_1(N)$ derived from the equation for the modular curve $X(N)$. Tokyo J. Math. **22**, 167–175 (1999)
12. Kim, C.H., Koo, J.K.: Self-recursion formulas satisfied by Fourier coefficients of some modular functions. J. Pure Appl. Algebra **160**(1), 53–65 (2001)
13. Kubert, D., Lang, S.: Modular Units. Grundlehren der mathematischen Wissenschaften, vol. 244. Springer, Heidelberg (1981)
14. Lang, S.: Algebra, 3rd edn. Addison-Wesely, Reading (1993)
15. Lang, S.: Elliptic Functions, 2nd edn. Springer, Heidelberg (1987)
16. Ogg, A.P.: Rational points on certain elliptic modular curves. Analytic number theory. In: Proc. Sympos. Pure Math., vol. XXIV. St. Louis Univ., St. Louis, Mo., 1972, pp. 221–231. American Mathematical Society, Providence (1973)
17. Ono, K.: CBMS102, The Web of Modularity: Arithmetic of the Coefficients of Modular Forms and q-series. American Mathematical Society, Providence (2003)
18. Ramachandra, K.: Some applications of Kronecker's limit formula. Ann. Math. **80**(2), 104–148 (1964)
19. Ramanujan, S.: The Lost Notebook and Other Unpublished Papers. Narosa, New Delhi (1988)
20. Shimura, G.: Introduction to the Arithmetic Theory of Automorphic Functions. Iwanami Shoten and Princeton University Press, Berlin/Princeton (1971)
21. Silverman, J.H.: Advanced Topics in the Arithmetic of Elliptic Curves. Springer, Heidelberg (1994)
22. Takagi, T.: The cuspidal class number formula for the modular curves $X_0(M)$ with M square-free. J. Algebra **193**(1), 180–213 (1997)
23. Yang, Y.: Transformation formulas for generalized Dedekind eta functions. Bull. Lond. Math. Soc. **36**(5), 671–682 (2004)