

Open Mathematics

Research Article

Yoonjin Lee and Yoon Kyung Park*

Modular equations of a continued fraction of order six

<https://doi.org/10.1515/math-2019-0003>

Received August 15, 2018; accepted January 3, 2019

Abstract: We study a continued fraction $X(\tau)$ of order six by using the modular function theory. We first prove the modularity of $X(\tau)$, and then we obtain the modular equation of $X(\tau)$ of level n for any positive integer n ; this includes the result of Vasuki et al. for $n = 2, 3, 5, 7$ and 11 . As examples, we present the explicit modular equation of level p for all primes p less than 19 . We also prove that the ray class field modulo 6 over an imaginary quadratic field K can be obtained by the value $X^2(\tau)$. Furthermore, we show that the value $1/X(\tau)$ is an algebraic integer, and we present an explicit procedure for evaluating the values of $X(\tau)$ for infinitely many τ 's in K .

Keywords: Ramanujan continued fraction, modular function, modular equation, ray class fields

MSC: 11Y65, 11F03, 11R37, 11R04, 14H55

1 Introduction

A continued fraction $X(\tau)$ of order six is defined as the quotient of mock theta functions

$$X(\tau) := q^{\frac{1}{4}} \left(\sum_{n=0}^{\infty} \frac{(-q; q^2)_n q^{n^2+2n}}{(q^4; q^4)_n} \right) / \left(\sum_{n=0}^{\infty} \frac{q^{n^2}}{(q^2; q^2)_n} \right)$$

where $\tau \in \mathfrak{H}$, \mathfrak{H} is the complex upper half plane, $q := e^{2\pi i \tau}$ and $(a; q)_n = \prod_{j=1}^n (1 - aq^{j-1})$. This was studied by Vasuki et al.[10], and they expressed $X(\tau)$ by an infinite product

$$X(\tau) = q^{\frac{1}{4}} \prod_{n=1}^{\infty} \frac{(1 - q^{6n-5})(1 - q^{6n-1})}{(1 - q^{6n-4})(1 - q^{6n-2})}.$$

Other types of Ramanujan continued fractions have been studied before. One of these is a continued fraction of order twelve $U(\tau)$, defined by

$$U(\tau) := \frac{q(1-q)}{1 - q^3 + \frac{q^3(1-q^2)(1-q^4)}{(1-q^3)(1+q^6) + \frac{q^3(1-q^8)(1-q^{10})}{(1-q^3)(1+q^{12}) + \dots}}.$$

Yoonjin Lee: Department of Mathematics, Ewha Womans University, 52, Seodaemun-gu, Seoul 03760, South Korea; E-mail: yoonjinl@ewha.ac.kr

***Corresponding Author: Yoon Kyung Park:** Department of Mathematics Education, Gongju National University of Education, 27, Ungjin-ro, Gongju-si, Chungcheongnam-do, 32553, South Korea; E-mail: ykpark@gjue.ac.kr

Mahadeva Naika et al. [8] found the infinite product form of $U(\tau)$:

$$U(\tau) = q \prod_{n=1}^{\infty} \frac{(1 - q^{12n-1})(1 - q^{12n-11})}{(1 - q^{12n-5})(1 - q^{12n-7})}$$

and the modular equations of levels 3 and 5 by theory of hypergeometric series. Moreover, they evaluated $U(\tau)$ at $\tau = i\sqrt{m}$ for several rational numbers m . For examples,

$$U\left(\frac{i}{2}\right) = \frac{\sqrt[4]{6\sqrt{3}-9}-1}{\sqrt[4]{6\sqrt{3}-9}+1},$$

$$U\left(\frac{\sqrt{-3}}{2}\right) = \frac{\sqrt[4]{-108+108\sqrt[3]{2}} - \sqrt[4]{12+12\sqrt[3]{2}}}{\sqrt[4]{-108+108\sqrt[3]{2}} + \sqrt[4]{12+12\sqrt[3]{2}}}$$

and

$$U\left(\frac{\sqrt{-5}}{2}\right) = \frac{\sqrt[4]{126\sqrt{5}+72\sqrt{15}-162\sqrt{3}-279}-1}{\sqrt[4]{126\sqrt{5}+72\sqrt{15}-162\sqrt{3}-279}+1}.$$

This follows from the fact that $U(\tau)$ is a generator of the function field on $\Gamma_1(12)$ and a singular value $U(\tau)$ is an algebraic unit for any imaginary quadratic quantity τ . This value $U(\tau)$ is also contained in some ray class field over an imaginary quadratic field; this is proved by the authors [7].

Vasuki et al. studied $X(\tau)$ using the identities of theta functions [10]. They obtained the modular equations of $X(\tau)$ of levels 2, 3, 5, 7 and 11 [10, Theorem 2.1-2.5]. However, there is no result on evaluating $X(\tau)$ at an imaginary quadratic number τ and generating a class field over an imaginary quadratic field.

The goal of this paper is to study a continued fraction $X(\tau)$ of order six by using the modular function theory. We first prove the modularity of $X(\tau)$ in Theorem 3.1, and then we find the modular equations of $X(\tau)$ of level n for any positive integer n in Theorem 3.2. Table 1 shows the exact modular equations of $X(\tau)$ of levels 2, 3, 5, 7, 11, 13, 17 and 19; this result includes the result of Vasuki et al. in [10, Theorems 2.1-2.5] for $n = 2, 3, 5, 7$ and 11. We show that the ray class field modulo 6 over an imaginary quadratic field K can be obtained by the value $X^2(\tau)$ (Theorem 4.1 and Corollary 4.5). We also show that the value $1/X(\tau)$ is an algebraic integer contained in a certain number field (Theorem 4.2). Furthermore, we find an explicit relation between $X(\tau)$ and $C(\tau)$, where $C(\tau)$, called *Ramanujan's cubic continued fraction*, will be defined in (4.1). We can evaluate the values $X(\theta)$ at infinitely many θ 's by using such a relation (Theorem 4.3). Examples of (2) and (3) of Theorem 4.3 are presented in Examples 4.8 and 4.10. We use MAPLE program to find the modular equations and examples.

2 Preliminaries

We begin with some definitions and properties regarding the theory of modular functions. Let $\Gamma(1) = \mathrm{SL}_2(\mathbb{Z})$ be the full modular group. For any positive integer N , the congruence subgroups $\Gamma(N)$, $\Gamma_1(N)$, $\Gamma^1(N)$, $\Gamma_0(N)$ and $\Gamma^0(N)$ of $\Gamma(1)$ consist of matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ congruent to $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 0 \\ * & 1 \end{pmatrix}$, $\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$ and $\begin{pmatrix} * & * \\ * & 0 \end{pmatrix}$ modulo N , respectively. Let $\mathfrak{H}^* = \mathfrak{H} \cup \mathbb{Q} \cup \{\infty\}$, where \mathfrak{H} is the complex upper half plane $\{\tau \in \mathbb{C} : \mathrm{Im}(\tau) > 0\}$.

A congruence subgroup Γ acts on \mathfrak{H}^* by $\gamma(\tau) = (a\tau + b)/(c\tau + d)$ for $\gamma \in \Gamma$. Then the quotient space $\Gamma \backslash \mathfrak{H}^*$ is a compact Riemann surface with an appropriate complex structure. One can identify γ with its action on \mathfrak{H}^* . We call an element $s \in \mathbb{Q} \cup \{\infty\}$ a *cusp*. If there exists $\gamma \in \Gamma$ such that $\gamma(s_1) = s_2$, then we say that two cusps s_1 and s_2 are *equivalent* under Γ . We also call the equivalence class of such s a *cusp*. We note that there exist at most finitely many inequivalent cusps of Γ . For any cusp s of Γ , there exists an element ρ of $\mathrm{SL}_2(\mathbb{Z})$ such that $\rho(s) = \infty$. Let h be the smallest positive integer satisfying

$$\rho^{-1} \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix} \rho \in \{\pm 1\} \cdot \Gamma, \quad (2.1)$$

and we call h the *width* of s . One can easily check that the width h of s depends only on the equivalence class of s under Γ , and it is independent of the choice of ρ .

We call a \mathbb{C} -valued function $f(\tau)$ a *modular function* on a congruence subgroup Γ if $f(\tau)$ satisfies the following three conditions:

1. $f(\tau)$ is meromorphic on \mathfrak{H} .
2. $f(\tau)$ is invariant under Γ , in other words, $(f \circ \gamma)(\tau) = f(\tau)$ for all $\gamma \in \Gamma$.
3. $f(\tau)$ is meromorphic at all cusps of Γ .

More precisely, the last condition means the following: for a cusp s of Γ , let h be the width of s and ρ be an element of $\mathrm{SL}_2(\mathbb{Z})$ such that $\rho(s) = \infty$ by (2.1). We thus have

$$(f \circ \rho^{-1})(\tau + h) = \left(f \circ \rho^{-1} \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix} \rho \right) (\rho^{-1}\tau) = (f \circ \rho^{-1})(\tau),$$

and so $f \circ \rho^{-1}$ has a Laurent series expansion in $q_h = e^{2\pi i \tau / h}$ and $(f \circ \rho^{-1})(\tau) = \sum_{n \geq n_0} a_n q_h^n$ with $a_{n_0} \neq 0$ for some integer n_0 . We call n_0 the *order* of $f(\tau)$ at the cusp s and write $n_0 = \mathrm{ord}_s f(\tau)$. We say that $f(\tau)$ has a zero (respectively, a pole) at s if $\mathrm{ord}_s f(\tau)$ is positive (respectively, negative). Moreover, a modular function $f(\tau)$ is holomorphic on \mathfrak{H}^* if $f(\tau)$ is holomorphic on \mathfrak{H} and $\mathrm{ord}_s f(\tau) \geq 0$ for all cusp s . We may identify a modular function on Γ with a meromorphic function on the compact Riemann surface $\Gamma \backslash \mathfrak{H}^*$. Any holomorphic modular function on Γ is constant.

Let $A_0(\Gamma)$ be the field of all modular functions on Γ , and let $A_0(\Gamma)_{\mathbb{Q}}$ be the subfield of $A_0(\Gamma)$ consisting of all modular functions $f(\tau)$ whose Fourier coefficients belong to \mathbb{Q} . One can identify $A_0(\Gamma)$ with the field $\mathbb{C}(\Gamma \backslash \mathfrak{H}^*)$ of all meromorphic functions on the compact Riemann surface $\Gamma \backslash \mathfrak{H}^*$. Note that if $f(\tau) \in A_0(\Gamma)$ is nonconstant, then the extension degree $[A_0(\Gamma) : \mathbb{C}(f(\tau))]$ is finite and it is the total degree of poles of $f(\tau)$. In this paper we consider the modular functions with neither zeros nor poles on \mathfrak{H} , and so the total degree of poles of $f(\tau)$ is $-\sum_s \mathrm{ord}_s f(\tau)$, where the summation runs over all the inequivalent cusps s at which $f(\tau)$ has poles.

The Klein form is a main tool for obtaining our main theorems. The *Weierstrass σ -function* is defined by

$$\sigma(z; L) := z \prod_{\omega \in L - \{0\}} \left(1 - \frac{z}{\omega} \right) e^{\frac{z}{\omega} + \frac{1}{2} \left(\frac{z}{\omega} \right)^2},$$

where L is a lattice in \mathbb{C} and $z \in \mathbb{C}$. The *Weierstrass ζ -function* is also defined by the logarithmic derivative of $\sigma(z; L)$ as follows:

$$\zeta(z; L) := \frac{\sigma'(z; L)}{\sigma(z; L)} = \frac{1}{z} + \sum_{\omega \in L - \{0\}} \left(\frac{1}{z - \omega} + \frac{1}{\omega} + \frac{z}{\omega^2} \right).$$

We notice that $\sigma(z; L)$ is holomorphic with only simple zeros at every lattice point $\omega \in L$ and $\zeta(z; L)$ is meromorphic with only simple poles at every lattice point $\omega \in L$. Moreover, it is easily checked that $\sigma(\lambda z; \lambda L) = \lambda \sigma(z; L)$ and $\zeta(\lambda z; \lambda L) = \lambda^{-1} \zeta(z; L)$ for any $\lambda \in \mathbb{C}^\times$. The *Weierstrass \wp -function* $\wp(z; L)$ is defined by

$$\wp(z; L) := -\zeta'(z; L) = \frac{1}{z^2} + \sum_{\omega \in L - \{0\}} \left(\frac{1}{(z - \omega)^2} - \frac{1}{\omega^2} \right).$$

Since $\wp(z + \omega; L) = \wp(z; L)$ and $\frac{d}{dz} [\zeta(z + \omega; L)] = 0$ for any $\omega \in L$, $\zeta(z + \omega; L) - \zeta(z; L)$ depends only on a lattice point $\omega \in L$ and not on $z \in \mathbb{C}$. Hence we may let

$$\eta(\omega; L) := \zeta(z + \omega; L) - \zeta(z; L)$$

for $\omega \in L$. Fixing the basis $\{\omega_1, \omega_2\}$ for $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$, define the *Weierstrass η -function* by

$$\eta(z; L) := a_1 \eta(\omega_1; L) + a_2 \eta(\omega_2; L)$$

for $z = a_1 \omega_1 + a_2 \omega_2 \in \mathbb{C}$ and $a_1, a_2 \in \mathbb{R}$. By using the fact that $\eta(z; L)$ does not depend on the choice of the basis $\{\omega_1, \omega_2\}$, $\eta(z; L)$ is well-defined and $\eta(rz; L) = r\eta(z; L)$ for any $r \in \mathbb{R}$.

Now we define the *Klein form* by

$$K(z; L) := e^{-\eta(z; L)z/2} \sigma(z; L)$$

and

$$K_{\mathfrak{a}}(\tau) = K(a_1\tau + a_2; \mathbb{Z}\tau + \mathbb{Z}),$$

where $\mathfrak{a} = (a_1, a_2) \in \mathbb{R}^2$. We note that $K_{\mathfrak{a}}(\tau)$ is holomorphic and nonvanishing on \mathfrak{H} if $\mathfrak{a} \in \mathbb{R}^2 - \mathbb{Z}^2$. Furthermore, $K_{\mathfrak{a}}(\tau)$ is homogeneous of degree 1, that is, $K(\lambda z; \lambda L) = \lambda K(z; L)$.

Let $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(\mathbb{Z})$ and $\mathfrak{a} = (a_1, a_2) \in \mathbb{R}^2$. The Klein form $K_{\mathfrak{a}}$ satisfies the following properties (K0)–(K5):

(K0) $K_{-\mathfrak{a}}(\tau) = -K_{\mathfrak{a}}(\tau)$.

(K1) $K_{\mathfrak{a}}(\gamma\tau) = (c\tau + d)^{-1} K_{\mathfrak{a}\gamma}(\tau)$.

(K2) For $\mathfrak{b} = (b_1, b_2) \in \mathbb{Z}^2$, we have that

$$K_{\mathfrak{a}+\mathfrak{b}}(\tau) = \varepsilon(\mathfrak{a}, \mathfrak{b}) K_{\mathfrak{a}}(\tau),$$

where $\varepsilon(\mathfrak{a}, \mathfrak{b}) = (-1)^{b_1 b_2 + b_1 + b_2} e^{\pi i (b_2 a_1 - b_1 a_2)}$.

(K3) For $\mathfrak{a} = (r/N, s/N) = (1/N)\mathbb{Z}^2 - \mathbb{Z}^2$ and $\gamma \in \Gamma(N)$ with an integer $N > 1$, we obtain that

$$K_{\mathfrak{a}}(\gamma\tau) = \varepsilon_{\mathfrak{a}}(\gamma)(c\tau + d)^{-1} K_{\mathfrak{a}}(\tau),$$

where $\varepsilon_{\mathfrak{a}}(\gamma) = -(-1)^{((a-1)r+cs+N)(br+(d-1)s+N)/N^2} e^{\pi i (br^2+(d-a)rs-cs^2)/N^2}$.

(K4) Let $\tau \in \mathfrak{H}$, $z = a_1\tau + a_2$ with $\mathfrak{a} = (a_1, a_2) \in \mathbb{Q}^2 - \mathbb{Z}^2$, and let $q = e^{2\pi i \tau}$ and $q_z = e^{2\pi i z} = e^{2\pi i a_2} e^{2\pi i a_1 \tau}$. Then

$$K_{\mathfrak{a}}(\tau) = -\frac{1}{2\pi i} e^{\pi i a_2 (a_1 - 1)} q^{a_1 (a_1 - 1)/2} (1 - q_z) \prod_{n=1}^{\infty} \frac{(1 - q^n q_z)(1 - q^n q_z^{-1})}{(1 - q^n)^2}$$

and $\text{ord}_q K_{\mathfrak{a}}(\tau) = \langle a_1 \rangle (\langle a_1 \rangle - 1)/2$, where $\langle a_1 \rangle$ is a rational number such that $0 \leq \langle a_1 \rangle < 1$ with $a_1 - \langle a_1 \rangle \in \mathbb{Z}$.

(K5) Let $f(\tau) = \prod_{\mathfrak{a}} K_{\mathfrak{a}}^{m(\mathfrak{a})}(\tau)$ be a finite product of Klein forms with $m(\mathfrak{a}) \in \mathbb{Z}$ and $\mathfrak{a} = (r/N, s/N) = (1/N)\mathbb{Z}^2 - \mathbb{Z}^2$ for an integer $N > 1$, and let $k = -\sum_{\mathfrak{a}} m(\mathfrak{a})$. Then $f(\tau)$ is a modular form of weight k on $\Gamma(N)$ if and only if

$$\begin{cases} \sum_{\mathfrak{a}} m(\mathfrak{a})r^2 \equiv \sum_{\mathfrak{a}} m(\mathfrak{a})s^2 \equiv \sum_{\mathfrak{a}} m(\mathfrak{a})rs \equiv 0 \pmod{N} & \text{if } N \text{ is odd,} \\ \sum_{\mathfrak{a}} m(\mathfrak{a})r^2 \equiv \sum_{\mathfrak{a}} m(\mathfrak{a})s^2 \equiv 0 \pmod{2N}, \sum_{\mathfrak{a}} m(\mathfrak{a})rs \equiv 0 \pmod{N} & \text{if } N \text{ is even.} \end{cases}$$

We can refer to [6] for more details on Klein forms.

Consider the modular function on $\Gamma = \Gamma_0(N_1) \cap \Gamma^0(N_2) \cap \Gamma_1(N_3) \cap \Gamma^1(N_4) \cap \Gamma(N_5)$. Let $N = \text{lcm}(N_3, N_4, N_5)$, $m = \text{lcm}(N_1, N_3, N_5) \text{lcm}(N_2, N_4, N_5)/N$ and $\beta = \begin{pmatrix} \text{lcm}(N_2, N_4, N_5) & 0 \\ 0 & 1 \end{pmatrix}$. Then $\beta^{-1}\Gamma\beta = \Gamma_1(N) \cap \Gamma_0(mN)$, which contains $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. For $f \in A_0(\Gamma)$ and $\gamma \in \Gamma$, we have $f \circ \beta \in A_0(\beta^{-1}\Gamma\beta) = A_0(\Gamma_1(N) \cap \Gamma_0(mN))$ because

$$(f \circ \beta) \circ (\beta^{-1}\gamma\beta) = f \circ \gamma\beta = f \circ \beta.$$

Since the width of ∞ is 1 on $\Gamma_1(N) \cap \Gamma_0(mN)$, $(f \circ \beta)(\tau)$ has the Fourier expansion $\sum_{n \in \mathbb{Z}} a_n q^n$. It means that $f \circ \beta$ is easier to treat than f .

The last thing that we need to discuss is some information on cusps of congruence subgroup $\Gamma_1(N) \cap \Gamma_0(mN)$. For positive integers N and m , let $\Gamma = \Gamma_1(N) \cap \Gamma_0(mN)$. When $\Gamma \backslash \Gamma(1)/\Gamma(1)_{\infty} = \{\Gamma\gamma_1\Gamma(1)_{\infty}, \dots, \Gamma\gamma_g\Gamma(1)_{\infty}\}$, the set $\{\gamma_1(\infty), \dots, \gamma_g(\infty)\}$ is a set of all inequivalent cusps of Γ such that $\gamma_i(\infty)$ and $\gamma_j(\infty)$ are not equivalent under Γ for any distinct i and j . Consider the set

$$M := \{(\bar{c}, \bar{d}) \in (\mathbb{Z}/mN\mathbb{Z})^2 : (\bar{c}, \bar{d}) = \bar{1}\}.$$

In fact, $(\bar{c}, \bar{d}) = \bar{1}$ if and only if $(c, d, mN) = 1$. Moreover, we define the subgroup Δ of $(\mathbb{Z}/mN\mathbb{Z})^{\times}$

$$\Delta := \{\overline{\pm(1 + Nk)} \in (\mathbb{Z}/mN\mathbb{Z})^{\times} : k = 0, \dots, m-1\}.$$

If there exists $\bar{s} \in \Delta$ and $\bar{n} \in \mathbb{Z}/mN\mathbb{Z}$ satisfying

$$\overline{c_2} = \bar{s} \cdot \overline{c_1} \text{ and } \overline{d_2} = \bar{s} \cdot \overline{d_1} + \bar{n} \cdot \overline{c_1},$$

we define an equivalence relation \sim on M by $(\overline{c_1}, \overline{d_1}) \sim (\overline{c_2}, \overline{d_2})$ for $(\overline{c_1}, \overline{d_1}), (\overline{c_2}, \overline{d_2}) \in M$. Hence, a map $\phi : \Gamma \backslash \Gamma(1) / \Gamma(1)_\infty \rightarrow M / \sim$ by $\phi(\Gamma(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix})) = [(\overline{c}, \overline{d})]$ is well-defined and bijective. Now we have the following lemma.

Lemma 2.1. Suppose that $a, c, a', c' \in \mathbb{Z}$ and $(a, c) = (a', c') = 1$. Consider $\pm 1/0$ as ∞ . Then with the notation Δ as before, a/c and a'/c' are equivalent under $\Gamma_1(N) \cap \Gamma_0(mN)$ if and only if there exist $\bar{s} \in \Delta \subset (\mathbb{Z}/mN\mathbb{Z})^\times$ and $n \in \mathbb{Z}$ such that $\begin{pmatrix} a' \\ c' \end{pmatrix} \equiv \begin{pmatrix} \bar{s}^{-1}a+nc \\ \bar{s}c \end{pmatrix} \pmod{mN}$.

For a positive divisor x of mN , let $\pi_x : (\mathbb{Z}/mN\mathbb{Z})^\times \rightarrow (\mathbb{Z}/x\mathbb{Z})^\times$ be the natural surjective homomorphism. For a positive divisor c of mN , let $\overline{s'_{c,1}}, \dots, \overline{s'_{c,n_c}} \in (\mathbb{Z}/(mN/c)\mathbb{Z})^\times$ be all the distinct coset representatives of $\pi_{mN/c}(\Delta)$ in $(\mathbb{Z}/(mN/c)\mathbb{Z})^\times$, where $n_c = \phi(mN/c)/|\pi_{mN/c}(\Delta)|$ and ϕ is the Euler's ϕ -function. Then we take $\overline{s_{c,i}} \in (\mathbb{Z}/mN\mathbb{Z})^\times$ such that $\pi_{mN/c}(\overline{s_{c,i}}) = \overline{s'_{c,i}}$ for any $i = 1, \dots, n_c$, and let

$$S_c := \{\overline{s_{c,1}}, \dots, \overline{s_{c,n_c}} \in (\mathbb{Z}/mN\mathbb{Z})^\times\}.$$

For a positive divisor c of mN , let $\overline{a'_{c,1}}, \dots, \overline{a'_{c,m_c}} \in (\mathbb{Z}/c\mathbb{Z})^\times$ be all distinct coset representatives of $\pi_c(\Delta \cap \ker(\pi_{mN/c})) \subset (\mathbb{Z}/c\mathbb{Z})^\times$, where $m_c = \phi(c)/|\pi_c(\Delta \cap \ker(\pi_{mN/c}))| = \phi(c) \cdot |\pi_{mN/c}(\Delta)|/|\pi_{c_0}(\Delta)|$ and $c_0 = mN/(c, mN/c)$. We take $\overline{a_{c,j}} \in (\mathbb{Z}/mN\mathbb{Z})^\times$ such that $\pi_c(\overline{a_{c,j}}) = \overline{a'_{c,j}}$ for any $j = 1, \dots, m_c$. Moreover, one can choose a representative $a_{c,j}$ of $\overline{a_{c,j}}$ such that $0 < a_{c,1}, \dots, a_{c,m_c} < mN$ and $(a_{c,j}, mN) = 1$, and let

$$A_c := \{a_{c,1}, \dots, a_{c,m_c}\}.$$

We then have a set of inequivalent cusps by using the sets S_c and A_c for $0 < c \mid mN$.

Lemma 2.2. With the notation as above, let

$$S := \left\{ (\overline{c} \cdot \overline{s_{c,i}}, \overline{a_{c,j}}) \in (\mathbb{Z}/mN\mathbb{Z})^2 : 0 < c \mid mN, \overline{s_{c,i}} \in S_c, a_{c,j} \in A_c \right\}.$$

For given $(\overline{c} \cdot \overline{s_{c,i}}, \overline{a_{c,j}}) \in S$, we can take $x, y \in \mathbb{Z}$ such that $(x, y) = 1$, $\bar{x} = \overline{c} \cdot \overline{s_{c,i}}$ and $\bar{y} = \overline{a_{c,j}}$ because $(c \cdot s_{c,i}, a_{c,j}, mN) = 1$. Then the set of y/x with such x and y is a set of all the inequivalent cusps of $\Gamma_1(N) \cap \Gamma_0(mN)$ and the number of such cusps is

$$|S| = \sum_{0 < c \mid mN} n_c \cdot m_c = \sum_{0 < c \mid mN} \frac{\phi(c)\phi(mN/c)}{|\pi_{c_0}(\Delta)|},$$

where $c_0 = mN/(c, mN/c)$.

The following lemma gives us the width of each cusp of $\Gamma_1(N) \cap \Gamma_0(mN)$.

Lemma 2.3. Consider $\pm 1/0$ as ∞ . Let a/c be a cusp of $\Gamma = \Gamma_1(N) \cap \Gamma_0(mN)$, where $a, c \in \mathbb{Z}$ and $(a, c) = 1$. Then the width h of a cusp a/c in $\Gamma \backslash \mathcal{H}^*$ is given by

$$h = \begin{cases} m/(c^2/4, m) & \text{if } N = 4, (m, 2) = 1 \text{ and } (c, 4) = 2, \\ mN/(c, N) \cdot (m, c^2/(c, N)) & \text{otherwise.} \end{cases}$$

The proofs of Lemmas 2.1, 2.2 and 2.3 are given in [3, Lemma 1-3].

3 A continued fraction $X(\tau)$ of order six

In this section we prove the existence of a modular equation of $X(\tau)$ (Theorem 3.2) for any level by showing the modularity of $X(\tau)$ (Theorem 3.1). The followings are parts of our main results.

Theorem 3.1. 1. The function field generated by $X^2(\tau)$ over \mathbb{C} is the field of modular functions on $\Gamma_1(6) \cap \Gamma^0(2)$.
 2. $X(\tau)$ is a modular function on $\langle \Gamma_1(12) \cap \Gamma^0(4), \begin{pmatrix} 1 & 0 \\ 6 & 1 \end{pmatrix}, \begin{pmatrix} -7 & -6 \\ 6 & 5 \end{pmatrix} \rangle$.

Theorem 3.2. For any positive integer n , one can find a modular equation $F_n(x, y)$ of $X(\tau)$ of level n .

We note that

$$X(\tau) = \zeta_{24}^5 \prod_{j=0}^5 \frac{K_{(1/6, j/6)}(\tau)}{K_{(2/6, j/6)}(\tau)}$$

as the finite product of Klein forms by (K4) with $\zeta_N = e^{2\pi i/N}$.

Proof of Theorem 3.1. (1)

Note that

$$\mathbb{C}(f(\tau)) = A_0(\Gamma) \iff \mathbb{C}(f(N\tau)) = A_0\left(\begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix}^{-1} \Gamma \begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix}\right),$$

where Γ is a congruence subgroup of genus zero, $f(\tau)$ is a modular function on Γ , and N is a positive integer. It is thus sufficient to prove that

$$\mathbb{C}(X^2(2\tau)) = A_0(\Gamma_0(12)). \quad (3.1)$$

By (K5), $X^2(\tau)$ is a modular function on $\Gamma(6)$. Since $X^2(\tau + 2) = X^2(\tau)$, $X^2(\tau)$ is a modular function on $\langle \Gamma(6), \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \rangle = \Gamma_1(6) \cap \Gamma^0(2)$. Furthermore, $X^2(2\tau)$ is a modular function on $\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}^{-1} \cdot (\Gamma_1(6) \cap \Gamma^0(2)) \cdot \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} = \Gamma_1(6) \cap \Gamma_0(12)$. In other words, $X^2(2\tau) \in A_0(\Gamma_1(6) \cap \Gamma_0(12)) = A_0(\Gamma_0(12))$ by using the fact that $(\Gamma_1(6) \cap \Gamma_0(12)) \cdot \{\pm I\} = \Gamma_0(12)$.

There are six inequivalent cusps on $\Gamma_0(12)$, and we observe the behaviour of $X^2(2\tau)$ at each cusp from the following table.

cusp s	∞	0	1/2	1/3	1/4	1/6
$\text{ord}_s X^2(2\tau)$	1	0	0	0	-1	0

We note that the degree $d = [A_0(\Gamma_0(12)) : \mathbb{C}(X^2(2\tau))]$ of the field extensions is the total degree of poles. Let $S_{\Gamma_0(12)} = \{\infty, 0, 1/2, 1/3, 1/4, 1/6\}$ be the set of inequivalent cusps on $\Gamma_0(12)$. Since

$$d = - \sum_{\substack{s \in S_{\Gamma_0(12)} \\ \text{ord}_s X^2(2\tau) < 0}} \text{ord}_s X^2(2\tau) = -\text{ord}_{1/4} X^2(2\tau) = 1,$$

we conclude that $A_0(\Gamma_0(12)) = \mathbb{C}(X^2(2\tau))$.

(2) By (K5), $X(\tau)$ is a modular function on $\Gamma(12)$. From (K1) and (K2), one can check that

$$X \circ \begin{pmatrix} 1 & 4 \\ 0 & 1 \end{pmatrix}(\tau) = X(\tau + 4) = X(\tau),$$

$$X \circ \begin{pmatrix} 1 & 0 \\ 6 & 1 \end{pmatrix}(\tau) = X(\tau)$$

and

$$X \circ \begin{pmatrix} -7 & -6 \\ 6 & 5 \end{pmatrix}(\tau) = X(\tau).$$

Hence $X(\tau)$ is a modular function on Γ' , where $\Gamma' := \langle \Gamma(12), \begin{pmatrix} 1 & 4 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 6 & 1 \end{pmatrix}, \begin{pmatrix} -7 & -6 \\ 6 & 5 \end{pmatrix} \rangle = \langle \Gamma_1(12) \cap \Gamma^0(4), \begin{pmatrix} 1 & 0 \\ 6 & 1 \end{pmatrix}, \begin{pmatrix} -7 & -6 \\ 6 & 5 \end{pmatrix} \rangle$.

□

Remark 3.3. Since

$$X \circ \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}^{-1} \gamma \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} = X \circ \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$$

for $\gamma \in \Gamma'$, we have that $X(2\tau)$ is invariant under the action of $\Gamma'' = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}^{-1} \Gamma' \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} = \langle \Gamma_1(12) \cap \Gamma^0(2), \begin{pmatrix} -7 & -3 \\ 12 & 5 \end{pmatrix} \rangle$. We denote $\bar{\Gamma} = \Gamma / \{\pm I\}$ (respectively, $\bar{\Gamma} = \Gamma$) if $-I \in \Gamma$ (respectively, if $-I \notin \Gamma$) for any $\Gamma \in SL_2(\mathbb{Z})$. Since $[\bar{\Gamma}_0(12) : \bar{\Gamma}_1(12) \cap \bar{\Gamma}^0(2)] = 4$ and $\Gamma_1(12) \cap \Gamma^0(2) \subset \Gamma'' \subset \Gamma_0(12)$, we obtain that $[\bar{\Gamma}_0(12) : \bar{\Gamma}''] = 2$.

Assume that there exists a congruence subgroup Γ_X such that $A_0(\Gamma_X) = \mathbb{C}(X(\tau))$, i.e., the genus of the field of modular functions is zero. Then the congruence subgroup Γ'_X corresponding to $X(2\tau)$ is also of genus zero. Moreover, $\Gamma'' \subset \Gamma'_X$ and $[\bar{\Gamma}_0(12) : \bar{\Gamma}'_X] = 2$ by Theorem 3.1 (1). Unfortunately, it does not guarantee that the genus of Γ'' is zero. That is the reason why we need to use $X^2(\tau)$ or $X^2(2\tau)$ instead of $X(\tau)$.

For convenience, we fix that

$$f(\tau) = \frac{1}{X^2(2\tau)}.$$

The following lemma shows the existence of an affine plain model, so-called *modular equation*.

Lemma 3.4. *Let n be a positive integer. Then we have*

$$\mathbb{Q}(f(\tau), f(n\tau)) = A_0(\Gamma_0(12n))_{\mathbb{Q}}.$$

Proof. By Theorem 3.1 (2), $\mathbb{Q}(f(\tau)) = A_0(\Gamma_0(12))_{\mathbb{Q}}$. Clearly, $f(\tau) \in A_0(\Gamma_0(12n))_{\mathbb{Q}}$ since $\Gamma_0(12) \supset \Gamma_0(12n)$. For $\beta = \begin{pmatrix} n & 0 \\ 0 & 1 \end{pmatrix}$, we get $\Gamma_0(12) \cap \beta^{-1}\Gamma_0(12)\beta = \Gamma_0(12n)$ and $f(n\tau) = (f \circ \beta)(\tau) \in A_0(\beta^{-1}\Gamma_0(12)\beta)_{\mathbb{Q}} \subset A_0(\Gamma_0(12n))_{\mathbb{Q}}$.

It is thus sufficient to show that $\mathbb{Q}(f(\tau), f(n\tau)) \supset A_0(\Gamma_0(12n))_{\mathbb{Q}}$. We take $M_i \in \Gamma_0(12)$ and write

$$\Gamma_0(12) = \cup_i (\Gamma_0(12n) \cdot M_i) \quad (3.2)$$

as a disjoint union.

We claim that all functions $f \circ \beta \circ M_i$ are distinct. Suppose that

$$f \circ \beta \circ M_i = f \circ \beta \circ M_{i'}$$

for i and i' with $i \neq i'$. Then $f \circ \beta M_{i'} M_i^{-1} \beta^{-1} = f$ and $\beta M_{i'} M_i^{-1} \beta^{-1} \in \mathbb{Q}^\times \cdot \Gamma_0(12)$. We get $M_{i'} M_i^{-1} \in \Gamma_0(12n)$ because $M_{i'} M_i^{-1} \in \beta^{-1}\Gamma_0(12)\beta$ and $M_i, M_{i'} \in \Gamma_0(12)$; but, this is a contradiction to (3.2). Consequently, $f(\tau)$ and $(f \circ \beta)(\tau) = f(n\tau)$ generate $A_0(\Gamma_0(12n))$. \square

By the table in the proof of Theorem 3.1 (2), $f(\tau)$ has a simple pole at ∞ and a simple zero at $1/4$ as a modular function on $\Gamma_0(12)$. Next, we investigate the behaviour of f at all cusps $s \in \mathbb{Q} \cup \{\infty\}$.

Lemma 3.5. *Let $a, c, a', c' \in \mathbb{Z}$ and $f(\tau) = 1/X^2(2\tau)$. Then we obtain the following assertions:*

1. $f(\tau)$ has a pole at $a/c \in \mathbb{Q} \cup \{\infty\}$ with $(a, c) = 1$ if and only if $(a, c) = 1$ and $c \equiv 0 \pmod{12}$.
2. $f(n\tau)$ has a pole at $a'/c' \in \mathbb{Q} \cup \{\infty\}$ if and only if there exist $a, c \in \mathbb{Z}$ such that $a/c = na'/c'$, $(a, c) = 1$ and $c \equiv 0 \pmod{12}$.
3. $f(\tau)$ has a zero at $a/c \in \mathbb{Q} \cup \{\infty\}$ if and only if $(a, c) = 1$ and $c \equiv \pm 4 \pmod{12}$.
4. $f(n\tau)$ has a pole at $a'/c' \in \mathbb{Q} \cup \{\infty\}$ if and only if there exist $a, c \in \mathbb{Z}$ such that $a/c = na'/c'$, $(a, c) = 1$ and $c \equiv \pm 4 \pmod{12}$.

Proof. We know that $f(\tau)$ has the only simple pole at $a/c \in \mathbb{Q} \cup \{\infty\}$ if and only if there exists $\bar{s} \in \Delta = (\mathbb{Z}/12\mathbb{Z})^\times$ with $\begin{pmatrix} a \\ c \end{pmatrix} \equiv \begin{pmatrix} \bar{s} \\ 0 \end{pmatrix} \pmod{12}$ by Lemma 2.1. This proves (1) and (2).

To prove (3) and (4), it is enough to find the condition for $a/c \in \mathbb{Q} \cup \{\infty\}$ to be equivalent to $1/4$ under $\Gamma_0(12)$. By using Lemma 2.1 again, $\begin{pmatrix} a \\ c \end{pmatrix} \equiv \begin{pmatrix} \bar{s}^{-1} + 4n \\ 4\bar{s} \end{pmatrix} \pmod{12}$ for $\bar{s} \in (\mathbb{Z}/12\mathbb{Z})^\times$ and $n \in \mathbb{Z}$. Hence, c should be congruent to $\pm 4 \pmod{12}$ and $(a, c) = 1$. \square

We denote d_1 (respectively, d_n) by the total degree of poles of $f(\tau)$ (respectively, $f(n\tau)$). Then there exists a polynomial $\mathcal{F}_n(x, y)$ such that

$$\mathcal{F}_n(x, y) = \sum_{\substack{0 \leq i \leq d_n \\ 0 \leq j \leq d_1}} C_{i,j} x^i y^j \in \mathbb{Q}[X, Y]$$

and $\mathcal{F}_n(f(\tau), f(n\tau)) = 0$. Ishida-Ishii [5] proved the following lemma using the theory of algebraic functions. This is useful when we check which coefficients $C_{i,j}$ of $\mathcal{F}_n(x, y)$ are zero.

Lemma 3.6. *For any congruence subgroup Γ , let $f_1(\tau)$ and $f_2(\tau)$ be nonconstant such that $\mathbb{C}(f_1(\tau), f_2(\tau)) = A_0(\Gamma)$ with the total degree D_j of poles of $f_j(\tau)$ for $j = 1, 2$, and let*

$$F(x, y) = \sum_{\substack{0 \leq i \leq D_2 \\ 0 \leq j \leq D_1}} C_{i,j} x^i y^j \in \mathbb{C}[x, y]$$

be such that $F(f_1(\tau), f_2(\tau)) = 0$. Let S_Γ be a set of all the inequivalent cusps of Γ , and let

$$S_{j,0} = \{s \in S_\Gamma : f_j(\tau) \text{ has zeros at } s\}$$

and

$$S_{j,\infty} = \{s \in S_\Gamma : f_j(\tau) \text{ has poles at } s\}$$

for $j = 1, 2$. Let

$$a = - \sum_{s \in S_{1,\infty} \cap S_{2,0}} \text{ord}_s f_1(\tau), \quad b = \sum_{s \in S_{1,0} \cap S_{2,\infty}} \text{ord}_s f_1(\tau).$$

We assume that a (respectively, b) is 0 if $S_{1,\infty} \cap S_{2,0}$ (respectively, $S_{1,0} \cap S_{2,\infty}$) is empty. Then we obtain the following assertions:

1. $C_{D_2,a} \neq 0$. In addition, if $S_{1,\infty} \subset S_{2,\infty} \cup S_{2,0}$, then $C_{D_2,j} = 0$ for any $j \neq a$.
2. $C_{0,b} \neq 0$. In addition, if $S_{1,0} \subset S_{2,\infty} \cup S_{2,0}$, then $C_{0,j} = 0$ for any $j \neq b$.
3. $C_{i,D_1} = 0$ for $0 \leq i < |S_{1,0} \cap S_{2,\infty}|$, $D_2 - |S_{1,\infty} \cap S_{2,\infty}| < i \leq D_2$.
4. $C_{i,0} = 0$ for $0 \leq i < |S_{1,0} \cap S_{2,0}|$, $D_2 - |S_{1,\infty} \cap S_{2,0}| < i \leq D_2$.

If we interchange the roles of $f_1(\tau)$ and $f_2(\tau)$, then we may have more properties similar to (1)-(4). Suppose that there exist $r \in \mathbb{R}$ and $N, n_1, n_2 \in \mathbb{Z}$ with $N > 0$ such that

$$f_j(\tau + r) = e^{2\pi i n_j / N} f_j(\tau)$$

for $j = 1, 2$. Then we get the following assertion:

5. If $n_1 i + n_2 j \not\equiv n_1 D_2 + n_2 a \pmod{N}$, then $C_{i,j} = 0$. Here note that $n_2 b \equiv n_1 D_2 + n_2 a \pmod{N}$.

Proof. See [5, Lemma 3 and 6]. □

Proof of Theorem 3.2. If $\mathbb{C}(f_1(\tau), f_2(\tau))$ is the field of all modular functions on some congruence subgroup for which $f_1(\tau)$ and $f_2(\tau)$ are nonconstant, then the extension degree $[\mathbb{C}(f_1(\tau), f_2(\tau)) : \mathbb{C}(f_j(\tau))]$ is equal to the total degree d_j of poles of f_j ($j = 1, 2$). Hence we get the polynomial $\Phi(x, y) \in \mathbb{C}[x, y]$ such that $\Phi(f_1(\tau), y)$ (respectively, $\Phi(x, f_2(\tau))$) is a minimal polynomial of $f_2(\tau)$ (respectively, $f_1(\tau)$) over $\mathbb{C}(f_1(\tau))$ (respectively, $\mathbb{C}(f_2(\tau))$). Let $f_1(\tau) = f(\tau)$ and $f_2(\tau) = f(n\tau)$. By Lemma 3.6, for any positive integer n we obtain a polynomial $\mathcal{F}_n(x, y) \in \mathbb{Q}[x, y]$ such that $\mathcal{F}_n(f(\tau), f(n\tau)) = 0$ with $\deg_x \mathcal{F}_n(x, y) = d_2$ and $\deg_y \mathcal{F}_n(x, y) = d_1$ since the q -expansion of $f(\tau)$ has only rational coefficients. Hence we get $\mathcal{F}_n(1/X^2(\tau), 1/X^2(n\tau)) = 0$ by substituting $f(\tau) = 1/X^2(2\tau)$. Let

$$\tilde{F}_n(x, y) = x^{2d_2} y^{2d_1} \mathcal{F}_n\left(\frac{1}{x^2}, \frac{1}{y^2}\right)$$

be a polynomial with $\tilde{F}_n(X(\tau), X(n\tau)) = 0$. By factorizing this, we can choose only one irreducible factor $F_n(x, y) \in \mathbb{Z}[x, y]$ satisfying $F_n(X(\tau), X(n\tau)) = 0$. In detail, by replacing x (respectively, y) by the q -expansion of $X(\tau)$ (respectively, $X(n\tau)$) in each irreducible factor of $\tilde{F}_n(x, y)$, one of the irreducible factors of $\tilde{F}_n(x, y)$ can be written as $O(q^N)$ for a suitable integer N ; then we denote such an irreducible factor by $F_n(x, y)$. Thus, $F_n(x, y)$ is the modular equation of $X(\tau)$ of level n for a positive integer n . □

Using Lemma 3.6, we obtain the modular equations of $f(\tau)$ of levels 2 and 3 as follows.

Theorem 3.7. *The modular equations of $X(\tau)$ of levels 2 and 3 are found as follows:*

1. (Modular equation of level 2)

$$X^4(\tau) = X^2(2\tau) \frac{1 - X^2(2\tau)}{1 + 3X^2(2\tau)},$$

2. (Modular equation of level 3)

$$X^3(\tau) - X(3\tau) + 3X(\tau)X^2(3\tau) - 3X^2(\tau)X^3(3\tau) = 0.$$

Proof. (1) By Lemma 3.4, $\mathbb{Q}(f(\tau), f(2\tau)) = A_0(\Gamma_0(24))_{\mathbb{Q}}$. We may write the set $S_{\Gamma_0(24)}$ of inequivalent cusps as

$$S_{\Gamma_0(24)} = \left\{ \infty, 0, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \frac{1}{6}, \frac{1}{8}, \frac{1}{12} \right\}.$$

By Lemma 3.5 and the property (K4) of the Klein form, with considering the width at each cusp,

$$\text{ord}_{1/4}f(\tau) = \text{ord}_{1/8}f(\tau) = 1 \text{ and } \text{ord}_{1/12}f(\tau) = \text{ord}_{\infty}f(\tau) = -1$$

and

$$\text{ord}_{1/8}f(2\tau) = 2 \text{ and } \text{ord}_{\infty}f(2\tau) = -2.$$

In other words, both of the total degrees of poles of $f(\tau)$ and $f(2\tau)$ are 2, and there exists a polynomial $\mathcal{F}_2(x, y)$ satisfying $\mathcal{F}_2(f(\tau), f(2\tau)) = 0$. Let

$$\mathcal{F}_2(X, Y) = \sum_{0 \leq i, j \leq 2} C_{i,j} X^i Y^j.$$

Since the set of poles of $f(\tau)$ and the set of zeros of $f(2\tau)$ are disjoint, we may assume that $C_{2,0} = 1$. By substituting $x = f(\tau)$ and $y = f(2\tau)$ to $\mathcal{F}_2(x, y)$,

$$\mathcal{F}_2(x, y) = x^2 - x^2y + y^2 + 3y$$

because all coefficients of q -expansion of $\mathcal{F}_2(f(\tau), f(2\tau))$ should be zero. Consider the polynomial $\tilde{F}_2(x, y) := x^4y^4\mathcal{F}_2(1/x^2, 1/y^2) = 3x^4y^2 + x^4 + y^4 - y^2$. Since $\tilde{F}_2(x, y)$ is irreducible, we get that

$$X^4(\tau) = \frac{X^2(2\tau)(1 - X^2(2\tau))}{1 + 3X^2(2\tau)}.$$

(2) Note that

$$\mathbb{Q}(f(\tau), f(3\tau)) = A_0(\Gamma_0(36))_{\mathbb{Q}}$$

and

$$S_{\Gamma_0(36)} = \left\{ \infty, 0, \frac{1}{2}, \frac{1}{3}, \frac{2}{3}, \frac{1}{4}, \frac{1}{6}, \frac{5}{6}, \frac{1}{9}, \frac{1}{12}, \frac{5}{12}, \frac{1}{18} \right\},$$

where $S_{\Gamma_0(36)}$ is the set of all inequivalent cusps of $\Gamma_0(36)$. For $s \in S_{\Gamma_0(36)}$,

$$\text{ord}_sf(\tau) = \begin{cases} -1 & \text{if } s \in \{1/12, 5/12, \infty\}, \\ \geq 0 & \text{otherwise} \end{cases}$$

and

$$\text{ord}_sf(3\tau) = \begin{cases} -3 & \text{if } s = \infty, \\ \geq 0 & \text{otherwise.} \end{cases}$$

So we may write the modular equation of $f(\tau)$ of level 3 as

$$\mathcal{F}_3(x, y) = \sum_{0 \leq i, j \leq 3} C_{i,j} x^i y^j.$$

Moreover, the only zero of $f(3\tau)$ is $1/12$, and there is no cusp s at which both $f(\tau)$ and $f(3\tau)$ vanish simultaneously. This means that we may assume that $C_{0,3} = 1$ by Lemma 3.6 (2). By substituting q -expansions of $f(\tau)$ and $f(3\tau)$ to X and Y in $\mathcal{F}_3(x, y)$, respectively, we get

$$\mathcal{F}_3(x, y) = y^3 - 9x + 6xy^2 + 3x^2y - x^3y^2$$

and

$$\begin{aligned}\tilde{F}_3(x, y) &:= x^6y^6 \times \mathcal{F}_3\left(\frac{1}{x^2}, \frac{1}{y^2}\right) \\ &= (x^3 + y + 3xy^2 + 3x^2y^3)(x^3 - y + 3xy^2 - 3x^2y^3).\end{aligned}\quad (3.3)$$

We note that $x^3 + y + 3xy^2 + 3x^2y^3 = 2q^{3/4} + \dots$ by substituting $x = X(\tau)$ and $y = X(3\tau)$, so we take the other factor of (3.3) as the modular equation of $X(\tau)$; thus,

$$F_3(x, y) = x^3 - y + 3xy^2 - 3x^2y^3$$

and

$$X^3(\tau) - X(3\tau) + 3X(\tau)X^2(3\tau) - 3X^2(\tau)X^3(3\tau) = 0.$$

□

The following theorem is useful for finding the modular equations of $f(\tau)$ and $X(\tau)$.

Theorem 3.8. *With the notation as above, let p be a prime ≥ 5 . Then the modular equation $\mathcal{F}_p(x, y) = \sum_{0 \leq i, j \leq p+1} C_{i,j} x^i y^j \in \mathbb{Q}[x, y]$ of $f(\tau) = 1/X^2(2\tau)$ satisfies the following conditions:*

1. $C_{p+1,0} \neq 0, C_{0,p+1} \neq 0$,
2. $C_{j,p+1} = 0, C_{p+1,j} = 0$ ($j = 1, \dots, p+1$),
3. $C_{j,0} = 0, C_{0,j} = 0$ ($j = 0, \dots, p$).

Proof. Assume that $p \geq 5$ is a prime. We may take the set $S_{\Gamma_0(12p)}$ of inequivalent cusps on $\Gamma_0(12p)$ as follows:

$$S_{\Gamma_0(12p)} = \left\{ \infty, 0, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \frac{1}{6}, \frac{1}{12}, \frac{1}{p}, \frac{1}{2p}, \frac{1}{3p}, \frac{1}{4p}, \frac{1}{6p} \right\}.$$

Consider ∞ and 0 as $1/12p$ and $1/1$ respectively. By Lemma 2.3, the width $h_{1/c}$ of the cusp $1/c$ is $12p/(12p, c^2)$ for a divisor c of $12p$. Hence

$$\text{ord}_{1/12} f(\tau) = -p, \text{ord}_{\infty} f(\tau) = -1, \text{ord}_{1/12} f(p\tau) = -1, \text{ and } \text{ord}_{\infty} f(p\tau) = -p.$$

So we obtain the modular equation $\mathcal{F}_p(x, y)$ of $f(\tau)$ of level p :

$$\mathcal{F}_p(x, y) = \sum_{0 \leq i, j \leq p+1} C_{i,j} x^i y^j.$$

Let $f_1(\tau) = f(\tau)$ and $f_2(\tau) = f(p\tau)$. Using the notation in Lemma 3.6,

$$a = 0 \text{ and } b = \sum_{s \in S_{1,0} \cap S_{2,0}} \text{ord} f_1(\tau) = p + 1$$

because $S_{1,0} = S_{2,0} = \{1/4, 1/4p\}$. Therefore, we get (1) because

$$C_{p+1,0} = C_{p+1,a} \neq 0 \text{ and } C_{0,p+1} = C_{0,b} \neq 0.$$

Moreover,

$$\begin{cases} C_{p+1,j} = 0 & \text{for } j \neq 0, \\ C_{0,j} = 0 & \text{for } j \neq p+1. \end{cases}$$

By switching the roles of $f(\tau)$ and $f(p\tau)$, let $f_1(\tau) = f(p\tau)$, $f_2(\tau) = f(\tau)$ and

$$F'_p(x, y) = \sum_{0 \leq i, j \leq p+1} C'_{i,j} x^i y^j$$

satisfying $F'_p(f(p\tau), f(\tau)) = 0$. By using Lemma 3.6 again, we get

$$\begin{cases} C_{j,p+1} = C'_{p+1,j} = 0 & \text{for } j \neq 0, \\ C_{j,0} = C'_{0,j} = 0 & \text{for } j \neq p+1. \end{cases}$$

□

In [10], Vasuki et al. computed the modular equations of $X(\tau)$ of levels 2, 3, 5, 7 and 11, where they used different methods for each level. They did not present the general method for getting the modular equation of higher levels. We can get the modular equation of any integer level. The following table, which can be computed by Theorem 3.2, shows the modular equations of levels 2, 3, 5, 7, 11, 13, 17 and 19.

Since $f(\tau)$ is a generator of a field of modular functions on congruence subgroup with genus zero, its modular equation has similar properties to the modular equation of the classical elliptic modular function $j(\tau)$. We state those properties in Theorem 3.9 after setting some notation.

Consider $\Gamma := \Gamma_0(12)$. For any integer a with $(a, 6) = 1$, we choose $\sigma_a \in \Gamma(1)$ such that $\sigma_a \equiv \begin{pmatrix} a^{-1} & 0 \\ 0 & a \end{pmatrix} \pmod{12}$. Clearly, $\sigma_a \in \Gamma_0(12)$. For instance, we may choose σ_a as

$$\sigma_{\pm 1} = \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ and } \sigma_{\pm 5} = \pm \begin{pmatrix} 5 & 12 \\ 12 & 29 \end{pmatrix}.$$

For every integer n with $(n, 6) = 1$, we can write

$$\Gamma \begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix} \Gamma = \bigcup_{0 < a|n} \bigcup_{\substack{0 \leq b < n/a \\ (a,b,n/a)=1}} \Gamma \sigma_a \begin{pmatrix} a & b \\ 0 & \frac{n}{a} \end{pmatrix}$$

as the disjoint union and $|\Gamma \backslash \Gamma \begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix} \Gamma| = n \prod_{p|n} (1 + 1/p)$ [9, Proposition 3.36].

Define the polynomial

$$\Phi_n(x, \tau) := \prod_{0 < a|n} \prod_{\substack{0 \leq b < n/a \\ (a,b,n/a)=1}} (x - (f \circ \alpha_{a,b})(\tau))$$

of degree $n \prod_{p|n} (1 + 1/p)$ with $\alpha_{a,b} := \sigma_a \begin{pmatrix} a & b \\ 0 & n/a \end{pmatrix}$. Each coefficient of the $\Phi_n(x, y)$ (in x) is an elementary symmetric function of $f \circ \alpha_{a,b}$ and invariant under Γ . It means that they are in $\mathbb{C}(f(\tau))$ and $\Phi_n(x, \tau) \in \mathbb{C}(f(\tau))[x]$ because $A_0(\Gamma) = \mathbb{C}(f(\tau))$. By abuse of notation we may write $\Phi_n(x, f(\tau))$ instead of $\Phi_n(x, \tau)$. By using $\alpha_{a,b} = \alpha_{n,0} = \sigma_n \begin{pmatrix} n & 0 \\ 0 & 1 \end{pmatrix}$, $(f \circ \alpha_{n,0})(\tau) = f(n\tau)$. Since $f \circ \alpha_{n,0}$ is a zero of $\Phi_n(x, f(\tau))$, $\Phi_n(f(n\tau), f(\tau)) = 0$. Let $f(n\tau) = f_1(\tau)$, $f(\tau) = f_2(\tau)$ and the set $S_{j,\infty}$ (respectively, $S_{j,0}$) be the set of cusps which are poles (respectively, zeros) of $f_j(\tau)$. With the same notation as Lemma 3.6, write $-a$ for the order $\text{ord}_s f_1(\tau)$ of f_1 at the cusp s in $S_{1,\infty} \cap S_{2,0}$. When we multiply $\Phi_n(x, f(\tau))$ by a suitable power of $f(\tau)$, we get a polynomial $F_n(x, f(\tau)) \in \mathbb{C}[x, f(\tau)]$ satisfying $F_n(f(n\tau), f(\tau)) = 0$. Since $f(\tau) = 1/X^2(2\tau)$ and $(n, 6) = 1$, a might be zero and we regard $\Phi_n(x, f(\tau))$ as a polynomial of x and $f(\tau)$. Hence we have the following theorem.

Theorem 3.9. *With the same notation as above, for any positive integer n such that $(n, 6) = 1$, let $f(\tau) = 1/X^2(2\tau)$ and $\Phi_n(x, y)$ be a polynomial with $\Phi_n(f(\tau), f(n\tau)) = 0$. Then we have the following assertions:*

1. $\Phi_n(x, y) \in \mathbb{Z}[x, y]$ and $\deg_x \Phi_n(x, y) = \deg_y \Phi_n(x, y) = n \prod_{p|n} (1 + 1/p)$.
2. $\Phi_n(x, y)$ is irreducible both as a polynomial in x over $\mathbb{C}(y)$ and as a polynomial in y over $\mathbb{C}(x)$.
3. $\Phi_n(x, y) = \Phi_n(y, x)$.
4. If n is not a square, $\Phi_n(x, x)$ is a polynomial of degree > 1 whose leading coefficient is ± 1 .
5. (Kronecker's congruence) Let p be an odd prime. Then

$$\Phi_p(x, y) \equiv (x^p - y)(x - y^p) \pmod{p\mathbb{Z}[x, y]}.$$

Table 1: The modular equation $F_p(x, y)$ of $X(\tau)$ of levels 2, 3, 5, 7, 11, 13, 17 and 19

p	The modular equation $F_p(x, y)$ of $X(\tau)$ of level p
2	$(x^4 - y^2)(1 - y^2) + 4x^4y^2$
3	$(x^3 - y) - 3xy^2(xy - 1)$
5	$(x^5 - y)(x + y^5) + 5xy(x^3y - xy^3 - 2x^4y^4 + x^4 + y^4)$
7	$(x^7 - y)(x + y^7)$ $+ 7xy(x^4 + 2x^5y + (-x^2 + 3x^6)y^2 + (1 - 3x^4)y^4 - 2xy^5 + (-4x^6 + 3x^2)y^6)$
11	$(x^{11} - y)(x - y^{11})$ $+ 11xy(x^4 - 2x^8 + 6x^9y + (-6x^{10} - 15x^6 + x^2)y^2 + 45x^7y^3 + (1 - 45x^8 - 28x^4)y^4$ $+ 84x^5y^5 + (27x^{10} - 84x^6 - 15x^2)y^6 + 45x^3y^7 + (-2 + 27x^8 - 45x^4)y^8 + 6xy^9$ $+ (-6x^2 - 22x^{10} + 27x^6)y^{10})$
13	$(x^{13} - y)(x - y^{13})$ $+ 13xy(x^4 - 3x^8 + x^{12} + (-x^3 - 2x^{11} + 10x^7)y + (2x^2 - 20x^6 - 10x^{10})y^2$ $+ (-x + 10x^5 + 68x^9)y^3 + (-27x^{12} - 13x^4 - 115x^8 + 1)y^4 + (10x^3 + 90x^{11} + 131x^7)y^5$ $+ (-20x^2 - 64x^6 - 180x^{10})y^6 + (131x^5 + 90x^9 + 10x)y^7 + (-115x^4 - 117x^8 + 81x^{12} - 3)y^8$ $+ (-81x^{11} + 90x^7 + 68x^3)y^9 + (-10x^2 + 162x^{10} - 180x^6)y^{10} + (-2x + 90x^5 - 81x^9)y^{11}$ $+ (-27x^4 + 81x^8 + 1 - 56x^{12})y^{12})$
17	$(x^{17} - y)(x + y^{17})$ $+ 17xy(-2x^{16} - 5x^8 + x^4 + 7x^{12} + (16x^{15} + 21x^7 - 28x^{11} - 2x^3)y$ $+ (14x^6 + 34x^{10} - 2x^2 - 14x^{14})y^2 + (2x - 35x^{13} + 168x^9 - 35x^5)y^3$ $+ (160x^8 + 30x^{12} - 30x^4 + 1 + 63x^{16})y^4 + (-378x^7 + 959x^{11} - 252x^{15} + 35x^3)y^5$ $+ (-210x^6 + 14x^2 + 306x^{10} + 306x^{14})y^6 + (1512x^{13} - 1583x^9 - 21x + 378x^5)y^7$ $+ (-405x^{16} + 160x^4 - 5 - 1190x^8 + 1440x^{12})y^8 + (1701x^{15} + 1583x^7 - 3402x^{11} - 168x^3)y^9$ $+ (306x^6 + 1134x^{14} + 34x^2 - 1890x^{10})y^{10} + (3402x^9 - 959x^5 + 28x - 2835x^{13})y^{11}$ $+ (1440x^8 + 729x^{16} - 2430x^{12} + 30x^4 + 7)y^{12} + (35x^3 - 1458x^{15} + 2835x^{11} - 1512x^7)y^{13}$ $+ (306x^6 + 1134x^{10} - 1458x^{14} - 14x^2)y^{14} + (252x^5 + 1458x^{13} - 1701x^9 - 16x)y^{15}$ $+ (729x^{12} - 386x^{16} - 2 + 63x^4 - 405x^8)y^{16})$
19	$(x^{19} - y)(x + y^{19})$ $- 19xy(6x^{16} - x^4 + 6x^8 - 12x^{12} + (5x^5 - 52x^9 - 26x^{17} + 65x^{13})y$ $+ (65x^{10} + 18x^{18} + 4x^2 - 42x^6 - 87x^{14})y^2 + (-135x^{15} - 20x^{11} + 2x^7)y^3$ $+ (-261x^{16} - 200x^8 + 33x^4 - 1 + 21x^{12})y^4 + (520x^9 + 585x^{17} - 5x - 1916x^{13})y^5$ $+ (591x^6 - 1512x^{10} + 63x^{14} - 42x^2 - 324x^{18})y^6 + (-180x^{15} - 1144x^{11} - 2x^3)y^7$ $+ (6 + 2091x^8 + 1755x^{16} - 4536x^{12} - 200x^4)y^8 + (-520x^5 - 4212x^{17} + 52x + 4680x^{13})y^9$ $+ (-5400x^{14} + 1458x^{18} + 6273x^{10} - 1512x^6 + 65x^2)y^{10} + (162x^{15} + 20x^3 + 1144x^7)y^{11}$ $+ (15957x^{12} - 12 - 10206x^{16} - 4536x^8 + 21x^4)y^{12} + (-4680x^9 + 1916x^5 - 65x + 3645x^{17})y^{13}$ $+ (63x^6 - 87x^2 - 2187x^{18} - 5400x^{10} + 8019x^{14})y^{14} + (-162x^{11} + 180x^7 + 135x^3)y^{15}$ $+ (-10206x^{12} + 6 + 8748x^{16} - 261x^4 + 1755x^8)y^{16} + (-585x^5 + 4212x^9 - 3645x^{13} + 26x)y^{17}$ $+ (1458x^{10} - 324x^6 - 2187x^{14} + 18x^2 + 1036x^{18})y^{18})$

Proof. Since $f(\tau) = q^{-1} + 2q + q^3 + \dots$, $f(\tau)$ has a Fourier expansion

$$f(\tau) = q^{-1} + \sum_{m=1}^{\infty} c_f(m)q^m \quad (c_f(m) \in \mathbb{Z}).$$

Let ψ_k be the automorphism of $\mathbb{Q}(\zeta_n)$ over \mathbb{Q} defined by $\psi_k(\zeta_n) = \zeta_n^k$ for an integer k with $(k, n) = 1$. Since

$$\left(f \circ \begin{pmatrix} a & b \\ 0 & n/a \end{pmatrix}\right)(\tau) = f\left(\frac{a^2\tau + ab}{n}\right) = \zeta_n^{-ab}q^{-a^2/n} + \sum_{m=1}^{\infty} c_f(m)\zeta_n^{abm}q^{a^2m/n},$$

ψ_k induces an automorphism $\hat{\psi}_k$ of $\mathbb{Q}(\zeta_n)((q^{1/n}))$ over $\mathbb{Q}(\zeta_n)$ such that

$$\hat{\psi}_k \left(f \circ \begin{pmatrix} a & b \\ 0 & n/a \end{pmatrix} (\tau) \right) = \zeta_n^{-abk} q^{-a^2/n} + \sum_{m=1}^{\infty} c_f(m) \zeta_n^{abkm} q^{a^2 m/n}.$$

When we take an integer b' such that $0 \leq b' < n/a$ and $b' \equiv bk \pmod{n/a}$, we get $ab' \equiv abk \pmod{n}$ and

$$\begin{aligned} \hat{\psi}_k(f \circ \alpha_{a,b}) &= \hat{\psi}_k \left(f \circ \sigma_a \begin{pmatrix} a & b \\ 0 & n/a \end{pmatrix} \right) = \hat{\psi}_k \left(f \circ \begin{pmatrix} a & b \\ 0 & n/a \end{pmatrix} \right) \\ &= f \circ \begin{pmatrix} a & b' \\ 0 & n/a \end{pmatrix} = f \circ \sigma_a \begin{pmatrix} a & b' \\ 0 & n/a \end{pmatrix} = f \circ \alpha_{a,b'}. \end{aligned}$$

This implies that $\hat{\psi}_k(\Phi_n(x, f(\tau))) = \Phi_n(x, f(\tau))$.

We note that the degree of $\Phi_n(x, f(\tau))$ in x is $n \prod_{p|n} (1 + 1/p)$, and let $d := n \prod_{p|n} (1 + 1/p)$. By using that $(f \circ \alpha_{1,0})(\tau) = f(\tau/n)$, $\Phi_n(f(\tau/n), f(\tau)) = 0$ and $[\mathbb{C}(f(\tau/n), f(\tau)) : \mathbb{C}(f(\tau))] \leq d$.

We have $\Gamma \alpha_{a,b} \subset \Gamma \begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix} \Gamma$, and so there exist $\gamma, \gamma', \gamma_{a,b} \in \Gamma$ such that $\gamma \begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix} \gamma_{a,b} = \gamma' \alpha_{a,b}$. Consider an embedding $\xi_{a,b}$ of $\mathbb{C}(f(\tau/n), f(\tau))$ to the field of all meromorphic functions on \mathfrak{H} containing $\mathbb{C}(f(\tau/n), f(\tau))$ over $\mathbb{C}(f(\tau))$ defined by

$$\xi_{a,b}(h) = h \circ \gamma_{a,b}.$$

So $\xi_{a,b}(f)(\tau) = f(\tau)$ and $\xi_{a,b}(f(\tau/n)) = (f \circ \alpha_{a,b})(\tau)$ because

$$\xi_{a,b}(f(\tau/n)) = \xi_{a,b} \left(f \circ \begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix} \right) (\tau) = \left(f \circ \begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix} \gamma_{a,b} \right) (\tau) = (f \circ \alpha_{a,b})(\tau).$$

In other words, $\alpha_{a,b} \neq \alpha_{a',b'}$ means that $f \circ \alpha_{a,b} \neq f \circ \alpha_{a',b'}$; hence, there exist distinct d embeddings $\xi_{a,b}$ of $\mathbb{C}(f(\tau/n), f(\tau))$ over $\mathbb{C}(f(\tau))$ and $[\mathbb{C}(f(\tau/n), f(\tau)) : \mathbb{C}(f(\tau))] = d$. Therefore, $\Phi_n(x, f(\tau))$ is irreducible over $\mathbb{C}(f(\tau))$.

Let $F(x, y)$ be the polynomial determined in Lemma 3.6. Let $f_1(\tau) = f(\tau)$, $f_2(\tau) = f(n\tau)$, d_j be the total degree of $f_j(\tau)$ for $j = 1, 2$ and

$$a = - \sum_{s \in S_{1,\infty} \cap S_{2,0}} \text{ord}_s f(\tau).$$

Then the polynomial $F(x, y)$ is written as

$$F(x, y) = C_{d_2, a} x^n + \sum_{\substack{0 \leq i \leq d_2 \\ 0 \leq j \leq d_1}} C_{i,j} x^i y^j.$$

We have the following relation:

$$F_n(x, f(\tau)) = C_{d_2, a} \cdot f(\tau)^a \Phi_n(x, f(\tau))$$

because $F(x, f(\tau))$ (respectively, $F(f(\tau/n), y)$) is the minimal polynomial of $f(\tau/n)$ (respectively, $f(\tau)$) over $\mathbb{C}(f(\tau))$ (respectively, $\mathbb{C}(f(\tau/n))$). As we mentioned before Theorem 3.9, $a = 0$. Moreover, both $F(x, y)$ and $\Phi_n(x, y)$ are in $\mathbb{Z}[x, y]$; thus (1) and (2) are proved.

(3) Note that $(f \circ \alpha_{n,0})(\tau) = f(n\tau)$. From that $\Phi_n(f(n\tau), f(\tau)) = 0$, $\Phi_n(f(\tau), f(\tau/n)) = 0$ and $f(\tau/n)$ is a root of $\Phi_n(f(\tau), x) = 0$. Since $\Phi_n(x, f(\tau)) \in \mathbb{Z}[x, f(\tau)]$ and $\Phi_n(x, f(\tau))$ is irreducible, we may assume that there is a polynomial $G(x, f(\tau))$ such that

$$\Phi_n(f(\tau), x) = G(x, f(\tau)) \Phi_n(x, f(\tau)).$$

By exchanging x with $f(\tau)$ and multiplying $G(x, f(\tau))$,

$$\Phi_n(f(\tau), x) = G(x, f(\tau)) \Phi_n(x, f(\tau)) = G(x, f(\tau)) G(f(\tau), x) \Phi_n(f(\tau), x);$$

so, we get $G := G(x, y) = \pm 1$.

We claim that $G = 1$. If $G = -1$, then $\Phi_n(f(\tau), x) = -\Phi_n(x, f(\tau)) = 0$. By substituting $x = f(\tau)$, we have $2\Phi_n(f(\tau), f(\tau)) = 0$, so $f(\tau)$ is a root of $\Phi_n(x, f(\tau)) = 0$. In other words, $x - f(\tau)$ divides $\Phi_n(x, f(\tau))$ as a polynomial. However, $\Phi_n(x, f(\tau))$ is irreducible over $\mathbb{C}(f(\tau))$ by (2), which is a contradiction. Hence, $G = 1$, and so $\Phi_n(f(\tau), x) = \Phi_n(x, f(\tau))$.

(4) We observe that each factor of $\Phi_n(f(\tau), f(\tau))$ is

$$f(\tau) - (f \circ \alpha_{a,b})(\tau) = q^{-1} - \zeta_n^{-ab} q^{-a^2/n} + O(q^{1/n}). \quad (3.4)$$

Assume that n is not a square. Let $c_{a,b}$ be the coefficient of the lowest term of (3.4). Then $c_{a,b}$ is 1 or $-\zeta_n^{-ab}$. Hence, the leading coefficient of $\Phi_n(f(\tau), f(\tau))$ is

$$\prod_{0 < a|n} \prod_{\substack{0 \leq b < n/a \\ (a,b,n/a)=1}} c_{a,b},$$

which is a unit. It is an integer by (1), thus (4) is proved.

(5) Assume that p is an odd prime. We write

$$g(\tau) \equiv h(\tau) \pmod{\alpha}$$

for $g(\tau), h(\tau) \in \mathbb{Z}[\zeta_p][[q^{1/p}]]$ satisfying

$$g(\tau) - h(\tau) \in \alpha \mathbb{Z}[\zeta_p][[q^{1/n}]].$$

Consider the Fourier expansion of $(f \circ \alpha_{a,b})(\tau) \pmod{1 - \zeta_p}$ as follows:

$$\begin{aligned} (f \circ \alpha_{1,b})(\tau) &= \zeta_p^{-b} q^{-1/p} + \sum_{m=1}^{\infty} c_f(m) \zeta_p^{bm} q^{m/p} \\ &\equiv q^{-1/p} + \sum_{m=1}^{\infty} c_f(m) q^{m/p} \pmod{1 - \zeta_p} \\ &= (f \circ \alpha_{1,0})(\tau), \end{aligned}$$

$$\begin{aligned} (f \circ \alpha_{p,0})(\tau) &= q^{-p} + \sum_{m=1}^{\infty} c_f(m) q^{pm} \\ &\equiv q^{-p} + \sum_{m=1}^{\infty} c_f(m)^p q^{pm} \pmod{p} \\ &\equiv f(\tau)^p \pmod{p}. \end{aligned}$$

On the other hand,

$$\begin{aligned} ((f \circ \alpha_{1,0})(\tau))^p &= \left(q^{-1/p} + \sum_{m=1}^{\infty} c_f(m) q^{m/p} \right)^p \\ &\equiv q^{-1} + \sum_{m=1}^{\infty} c_f(m) q^m \pmod{1 - \zeta_p} \\ &= f(\tau). \end{aligned}$$

Hence we get the following congruence equation

$$\Phi_p(x, f(\tau)) = \prod_{0 \leq b < p} (x - (f \circ \alpha_{1,b})(\tau)) (x - (f \circ \alpha_{p,0})(\tau))$$

$$\begin{aligned}
&\equiv (x - (f \circ \alpha_{1,0})(\tau))^p (x - f(\tau)^p) \pmod{1 - \zeta_p} \\
&\equiv (x^p - (f \circ \alpha_{1,0})(\tau)^p) (x - f(\tau)^p) \pmod{1 - \zeta_p} \\
&\equiv (x^p - f(\tau)) (x - f(\tau)^p) \pmod{1 - \zeta_p}.
\end{aligned}$$

This means that

$$\sum_i \beta_i X^i := \Phi_p(x, f(\tau)) - (x^p - f(\tau))(x - f(\tau)^p)$$

belongs to $(1 - \zeta_p)\mathbb{Z}[x, f(\tau)]$, where $\beta_i \in (1 - \zeta_p)\mathbb{Z}[f(\tau)]$. However, since we already know that $\Phi_p(x, y) - (x^p - y)(x - y^p)$ is contained in $\mathbb{Z}[x, y]$, we have $\sum_i \beta_i x^i \in \mathbb{Z}[x, f(\tau)]$, that is, $\beta_i \in \mathbb{Z}[f(\tau)]$. Hence, each β_i is a polynomial in $f(\tau)$ whose coefficient is divisible by $(1 - \zeta_p)$; thus, $\beta_i \in p\mathbb{Z}[f(\tau)]$. Therefore, the modular equation of $f(\tau)$ satisfies that

$$\Phi_p(x, y) - (x^p - y)(x - y^p) \in p\mathbb{Z}[x, y].$$

□

Remark 3.10. As we mentioned in Remark 3.3, we cannot conclude that $X(\tau)$ can generate the field of modular functions for certain congruence subgroup. But, in Table 1, we observe that the modular equations $F_n(x, y)$ of $X(\tau)$ satisfy the following congruence:

$$F_p(x, y) \equiv \begin{cases} (x^p - y)(x + y^p) & \text{if } p = 5, 7, 17, 19, \\ (x^p - y)(x - y^p) & \text{if } p = 11, 13. \end{cases}$$

Hence we conjecture that

$$F_p(x, y) \equiv \begin{cases} (x^p - y)(x - y^p) & \text{if } p \equiv \pm 1 \pmod{12}, \\ (x^p - y)(x + y^p) & \text{if } p \equiv \pm 5 \pmod{12}. \end{cases}$$

4 Ray class fields and evaluation of $X(\tau)$

In this section, we prove our remaining results. We first show that $X(\tau)$ generates the ray class field modulo 6 over K . We then prove that as a value, $1/X(\tau)$ is integral and $X(r\tau)$ can also be expressed in terms of radicals for any positive rational number r if $X(\tau)$ can be written in terms of radicals. We also present some examples at the end of this section.

Theorem 4.1. *Let K be an imaginary quadratic field with discriminant d_K and $\tau \in K \cap \mathfrak{H}$ be a root of the primitive equation $ax^2 + bx + c = 0$ such that $b^2 - 4ac = d_K$ and $(a, 6) = 1$, where $a, b, c \in \mathbb{Z}$. Then $K(X^2(\tau))$ is the ray class field modulo 6 over K .*

Theorem 4.2. *Let K be an imaginary quadratic field and $\tau \in K \cap \mathfrak{H}$. Then the value $1/X(\tau)$ is an algebraic integer.*

Theorem 4.3. *Suppose that $X(\tau)$ can be evaluated in terms of radicals. Then $X(r\tau)$ can also be expressed in terms of radicals for any positive rational number r .*

Let K be an imaginary quadratic field and d_K its discriminant. For a positive integer N , denote $K_{(N)}$ by the ray class field modulo N over K . In this section we first show that $X^2(\tau)$ generates the ray class field $K_{(6)}$ modulo 6 over K , where $\tau \in K \cap \mathfrak{H}$ is a root of the primitive equation $ax^2 + bx + c = 0$ such that $b^2 - 4ac = d_K$.

The following lemma gives us the ray class field generated by $X^2(\tau)$, and it is used for the proof of Theorem 4.1.

Lemma 4.4. Let K be an imaginary quadratic field with discriminant d_K , and let $\tau \in K \cap \mathfrak{H}$ be a root of the primitive equation $ax^2 + bx + c = 0$ in $\mathbb{Z}[x]$ such that $b^2 - 4ac = d_K$. Let Γ' be any congruence subgroup such that $\Gamma(N) \subset \Gamma' \subset \Gamma_1(N)$. Suppose that $(N, a) = 1$. Then the field generated over K by all the values $h(\tau)$ with $h \in A_0(\Gamma')_{\mathbb{Q}}$ is defined and finite at τ ; this field is the ray class field modulo N over K .

Proof. See [2, Corollary 5.2]. \square

Proof of Theorem 4.1. If Γ' is the congruence subgroup such that $\mathbb{Q}(X^2(\tau)) = A_0(\Gamma')_{\mathbb{Q}}$, then $\Gamma' = \Gamma_1(6) \cap \Gamma^0(2)$ and $\Gamma(6) \subset \Gamma' \subset \Gamma_1(6)$ by Theorem 3.1 (2). For an imaginary quadratic field K with discriminant d_K , consider $\tau \in K \cap \mathfrak{H}$ satisfying $a\tau^2 + b\tau + c = 0$, where $b^2 - 4ac = d_K$, $(a, 6) = 1$ and $a, b, c \in \mathbb{Z}$. Since X is defined and finite at this τ , $K(X^2(\tau))$ is the ray class field modulo 6 over K by Lemma 4.4. \square

Corollary 4.5. Let K be an imaginary quadratic field. If $\mathbb{Z}[\tau]$ is the integral closure of \mathbb{Z} in K , then $K(X^2(\tau))$ is the ray class field modulo 6 over K .

Proof. Assume that $\mathbb{Z}[\tau]$ is the ring of integers in K . If $a\tau^2 + b\tau + c = 0$, where $a, b, c \in \mathbb{Z}$ and $(a, b, c) = 1$, then a should be 1. Hence, $K(X^2(\tau))$ is the ray class field modulo 6 over K . \square

The *Hauptmodul* is the normalized generator of a genus zero function field with q -series $q^{-1} + O(q)$. Now, we focus on proving that $1/X(\tau)$ is an algebraic integer.

Lemma 4.6. The *Hauptmodul* of $A_0(\Gamma_1(6))$ is $1/X^4(\tau) - 4$.

Proof. Let $g(\tau) = 1/X^4(\tau)$. Since $g(\tau)$ is written as the product of Klein forms:

$$g(\tau) = \zeta_6 \prod_{j=0}^5 \frac{K_{(2/6, j/6)}^4}{K_{(1/6, j/6)}^4}(\tau) = q^{-1} \prod_{n=1}^{\infty} \frac{(1 - q^{6n-4})^4 (1 - q^{6n-2})^4}{(1 - q^{6n-5})^4 (1 - q^{6n-1})^4},$$

$g(\tau)$ is a modular function on $\Gamma(6)$ by (K5). Moreover, $g(\tau + 1) = g(\tau)$; this implies that $g(\tau) \in A_0(\Gamma_1(6))$. Note that there are four inequivalent cusps $\infty, 0, 1/2$ and $1/3$ with widths 1, 6, 3 and 2, respectively. By (K4), the orders of $g(\tau)$ at $\infty, 0, 1/2$ and $1/3$ are $-1, 0, 1$ and 0 , respectively. Hence, $g(\tau)$ generates the field $A_0(\Gamma_1(6))$, and it has q -expansion $q^{-1} + 4 + 6q + 4q^2 - 3q^3 + O(q^4)$. It implies that $g(\tau) - 4 = 1/X^4(\tau) - 4$ is the *Hauptmodul* of $\Gamma_1(6)$. \square

In [4], the cubic continued fraction $C(\tau)$ is defined as follows:

$$C(\tau) = \frac{q^{1/3}}{1 + \frac{q + q^2}{1 + \frac{q^2 + q^4}{1 + \dots}}}. \quad (4.1)$$

Then we get the following lemma.

Lemma 4.7. Let $X(\tau)$ and $C(\tau)$ be defined as before. Then

$$X^4(\tau) = \frac{C^3(\tau)}{1 + C^3(\tau)}.$$

Proof. In [4, Lemma 15], the *Hauptmodul* of $\Gamma_1(6)$ is $1/C^3(\tau) - 3$. By uniqueness of *Hauptmodul*, $1/C^3(\tau) = 1/X^4(\tau) - 1$, so the result follows. \square

Proof of Theorem 4.2. By [4, Theorem 16], $1/C(\tau)$ is an algebraic integer for $\tau \in K \cap \mathfrak{H}$. Hence we have that $1/X^4(\tau)$ and $1/X(\tau)$ are algebraic integers because $1/C^3(\tau) = 1/X^4(\tau) - 1$. \square

Proof of Theorem 4.3. For given $r \in \mathbb{Q}_{>0}$, we write r as $r = a/b$ for relatively prime integers a and b . For a prime factor p of r , let

$$\tau_0 = \begin{cases} p\tau & \text{if } p \mid a, \\ \tau/p & \text{if } p \mid b, \end{cases}$$

and take the modular equation $F_p(x, y)$ of $X(\tau)$ of level p in Table 1. Let

$$P(t) := \begin{cases} F_p(X(\tau), t) & \text{if } p \mid a, \\ F_p(t, X(\tau)) & \text{if } p \mid b. \end{cases}$$

By solving the equation $P(t) = 0$, we can get finitely many solutions s_1, \dots, s_l which are written in terms of radicals. For a sufficiently large N and $q_0 = e^{2\pi i \tau_0}$, we check the absolute values

$$abs_j := \left| q_0^{1/4} \prod_{n=1}^N \frac{(1 - q_0^{6n-5})(1 - q_0^{6n-1})}{(1 - q_0^{6n-4})(1 - q_0^{6n-2})} - s_j \right|$$

for $j = 1, \dots, l$. Then there is only one j' with extremely small $abs_{j'}$, and so we have $X(\tau_0) = s_{j'}$. We may repeat these steps until we get $X(r\tau)$. □

Example 4.8 (Evaluation of $X(i)$). One can obtain that

$$X(i) = \frac{\sqrt[4]{12 - \sqrt{3}}}{\sqrt{3}} \quad (4.2)$$

by going through the following procedure:

1. By [1, Theorem 3 (4.1)], $C((1+i)/2) = (1 - \sqrt{3})/2$.
2. Since $X^4(\tau) = C^3(\tau)/(1 + C^3(\tau))$, $X^4((1+i)/2) = (3 - 2\sqrt{3})/9$.
3. By comparing the approximation of $X((1+i)/2)$ with $i^s \cdot \sqrt[4]{(3 - 2\sqrt{3})/9}$ ($s = 0, 1, 2, 3$), we can see that

$$X\left(\frac{1+i}{2}\right) = -i \sqrt[4]{\frac{3 - 2\sqrt{3}}{9}} = -i \frac{\sqrt[4]{3 - 2\sqrt{3}}}{\sqrt{3}}.$$

4. Using the fact that the modular equation of level 2 is

$$x^4 + 3x^4y^2 - y^2 + y^4, \quad (4.3)$$

four zeros of (4.3) are

$$s_1 := \frac{\sqrt[4]{12 + \sqrt{3}}}{\sqrt{3}}, \quad s_2 := s_1, \quad s_3 := i \frac{\sqrt[4]{12 - \sqrt{3}}}{\sqrt{3}}, \quad s_4 := -s_3$$

when $x := X((1+i)/2)$.

5. Hence we find $X(1+i) = s_4$.
6. Actually, $X(i)$ should be $\epsilon^i \cdot X(1+i)$ ($s = 0, 1, 2, 3$). By comparing the approximation of $X(i)$ with $\epsilon^i \cdot s_4$ again, we get

$$X(i) = \frac{\sqrt[4]{12 - \sqrt{3}}}{\sqrt{3}}.$$

In detail, for $q_0 = e^{-2\pi i}$, let

$$abs_j := \left| q_0^{1/4} \prod_{n=1}^{100} \frac{(1 - q_0^{6n-5})(1 - q_0^{6n-1})}{(1 - q_0^{6n-4})(1 - q_0^{6n-2})} - \epsilon^j s_4 \right|.$$

Then $abs_1 = 0.5 \cdot 10^{-9}$.

Remark 4.9. One can use the value $C(i) = \frac{\sqrt{6\sqrt{3}-\sqrt{3}-1}}{4}$ for some steps. Then we get the value

$$X(i) = \frac{\sqrt{\sqrt[4]{27}\sqrt{2}-\sqrt{3}-1}}{\sqrt[4]{3}\sqrt{3} + \sqrt[4]{3}\sqrt{2} + \sqrt{3}},$$

which is equal to (4.2).

Example 4.10. Using the same method as Example 4.8, we obtain the following evaluations.

1.

$$X(\sqrt{-2}) = \sqrt{\frac{1-3\sqrt{3}+3\sqrt{2}}{3-3\sqrt{2}+3\sqrt{3}}},$$

2.

$$X(\sqrt{-5}) = \sqrt{\frac{3\sqrt{\xi_5}-1}{3+3\sqrt{\xi_5}}},$$

where $\xi_5 = -31 + 8\sqrt{15} + 14\sqrt{5} - 18\sqrt{3}$.

In [1, Theorems 3 and 5], we can find the values

$$C(\sqrt{-2}/2) = (\sqrt{6}-2)/2, \quad C((1+\sqrt{-5})/2) = (\sqrt{5}-3)(\sqrt{5}-\sqrt{3})/2,$$

and these are useful for finding the values $X(\sqrt{-2})$ and $X(\sqrt{-5})$.

Acknowledgement: The first-named author is supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MEST)(NRF-2017R1A2B2004574). The second-named author is supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-2017R1D1A1B03029519).

References

- [1] Chan H.H., On Ramanujan's cubic continued fraction, *Acta Arith.*, 1995, 73, no.4, 343–355.
- [2] Cho B., Koo J.K., Construction of class fields over imaginary quadratic fields and applications, *Quart. J. Math.* 2010, 61, 199–126.
- [3] Cho B., Koo J.K., Park Y.K., Arithmetic of the Ramanujan-Göllnitz-Gordon continued fraction, *J. Number Theory*, 2009, 129, 922–947.
- [4] Cho B., Koo J.K., Park Y.K., On Ramanujan's cubic continued fraction as a modular function, *Tohoku Math. J.*, 2010, 62 (4), 579–603.
- [5] Ishida N., Ishii N., The equations for modular function fields of principal congruence subgroups of prime level, *Manuscripta Math.*, 1996, 90, 271–285.
- [6] Kubert D., Lang S., *Modular Units*, Springer-Verlag, New York-Berlin, 1981.
- [7] Lee Y., Park Y.K., A continued fraction of order twelve as a modular function, *Math. Comp.*, 2018, 87, No. 312, 2011–2036.
- [8] Mahadeva Naika M.S., Dharmendra B.N., Shivashankar K., A continued fraction of order twelve, *Cent. Eur. J. Math.*, 2008, 6, 393–404.
- [9] Shimura G., Introduction to the arithmetic theory of automorphic functions, in: Kanô Memorial Lectures, no. 1, in: Publications of the Mathematical Society of Japan, vol. 11, Iwanami Shoten Publishers/Princeton University Press, Tokyo/Princeton, N. J., 1971, xiv+267.
- [10] Vasuki K.R., Bhaskar N., Sharath G., On a continued fraction of order six, *Ann. Univ. Ferrara Sez. VII Sci. Mat.*, 2010, 56, No. 1, 77–89.