ON THE RAMANUJAN'S CUBIC CONTINUED FRACTION AS MODULAR FUNCTION

BUMKYU CHO, JA KYUNG KOO AND YOON KYUNG PARK

Abstract. We first extend the results of Chan([4]) and Baruah([2]) on the modular equations of the Ramanujan's cubic continued fraction to all primes p by finding the affine models of modular curves $X(\Gamma)$ with $\Gamma = \Gamma_1(6) \cap \Gamma^0(3)$ and then derive the Kronecker's congruence relations for these modular equations. And, we further show that the singular values of $C(\tau)$ generate ray class fields modulo 6 over imaginary quadratic fields and find their class polynomials by working with $\frac{1}{C(\tau)}$ as algebraic integers.

1. Introduction

Let $\mathfrak{H}$ be the complex upper half plane and $\tau \in \mathfrak{H}$. We define the Rogers-Ramanujan continued fraction by

$$r(\tau) = \cfrac{q^{\frac{1}{5}}}{1 + \cfrac{q}{1 + \cfrac{q^2}{1 + \cfrac{q^3}{1 + \cdots}}}} = q^{\frac{1}{5}} \prod_{n=1}^{\infty} (1 - q^n)^{\left(\frac{n}{5}\right)}$$

where $q = e^{2\pi i \tau}$ and $\left(\frac{n}{5}\right)$ is the Legendre symbol.

In the Ramanujan's first letter to Hardy, he showed that $r(i) = \sqrt{\frac{5+\sqrt{5}}{2}} - \frac{\sqrt{5}+1}{2}$, $r\left(\frac{5+i}{2}\right) = \sqrt{\frac{5-\sqrt{5}}{2}} - \frac{\sqrt{5}-1}{2}$ and $r\left(\frac{\sqrt{-n}}{2}\right)$ can be exactly found if n is any positive rational quantity. Since $r(\tau)$ is a modular function, the existence of radical expressions is clear by class field theory. Strictly speaking $r(\tau)$ is a modular function for $\Gamma(5)$([10]) so that any singular value of $r(\tau)$ at imaginary quadratic argument is contained in some ray class field. Thus the splitting field of its minimal polynomial is abelian. In other words its Galois group is solvable and hence any singular value of $r(\tau)$ can be written by radicals. But finding the radical expressions explicitly is another problem which was settled down by Gee and Honsbeek who used, to this end, the Shimura reciprocity law([10]).

Besides, one of the other important subjects is the one about modular equations. Since the modular function field of level 5 has genus 0, there should be certain polynomials giving the relations between $r(\tau)$ and $r(n\tau)$ for all positive integers n. These are what we call the modular equations. Most of the followings were originally stated by Ramanujan and later on proved by several people.

2000 *Mathematics Subject Classification.* 11Y65, 11F11, 11R37, 11R04, 14H55.

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

n	mathematician (year)
2	Rogers (1920)
3	Rogers (1920)
4	Andrews, Berndt, Jacobsen, Lamphere (1992)
5	Rogers, Watson, Ramanathan (1984)
7	Yi (2001)
11	Rogers (1920)

These modular equations for $r(\tau)$ satisfy certain Kronecker's congruences in prime level. Moreover, for an element τ of an imaginary quadratic field the singular value $r(\tau)$ is a unit that can be expressed in terms of radicals over $\mathbb{Q}$. For more details, we refer to [8]. On the other hand, Cais and Conrad succeeded in generalizing the above results on modular equations to all primes p by means of geometric method, namely using the theory of arithmetic models of modular curves ([3]).

This paper is a continuation of our previous work([7]). Duke introduced in [8] the following continued fraction $C(\tau)$ defined by

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

which is now called the Ramanujan's cubic continued fraction as a holomorphic function on $\mathfrak{H}$. Like the case of Rogers-Ramanujan continued fraction there are some known results for modular equations with $v := C(\tau)$ and $u := C(n\tau)$ on a case-by-case basis.

n	mathematician (year)	equation
2	Chan (1995)	$v^2 + 2vu^2 - u = 0$
3	Chan (1995)	$4v^3u^2 + 2v^3u + v^3 - u + u^2 - u^3 = 0$
5	Baruah(2002)	$v^6 - vu + 5vu(v^3 + u^3)(1 - vu) + u^6$
		$-v^2u^2(16v^3u^3 - 20v^2u^2 + 20vu - 5) = 0$
7	Baruah(2002)	$v^8 - vu - 56v^3u^3(v^2 + u^2) + 7vu(v^3 + u^3)(1 - 8v^3u^3)$
		$+28v^2u^2(v^4 + u^4 + u^8 + v^4u^4(21 - 64v^3u^3) = 0$

Chan's results can be found in [4] and Baruah's results in [2], in which they used the theory of combinatorics. And the latter further presented the modular equation for the case $n = 11$ in the same paper which is too long to write it down so that we omit here. In general their existence was known to Klein long ago, but in our case there does not seem to have been a systematic construction given before for all primes p.

Unlike the arguments of Chan-Baruah and Cais-Conrad we first find in §3 the affine models of some modular curves from the theory of algebraic functions and then extend the above results to all primes p (Theorem 9), from which we rediscover Chan's results when $n = 2, 3$ (Theorem 8). And, we also provide a table of modular equations for $n = 5, 7, 11, 13, 17$ by means of our algorithm and the Maple program. We then further give an analytic proof of the Kronecker congruence relations for these modular equations (Theorem 10).

Since $C(\tau)$ is a Hauptmodul for $\Gamma_1(6)\cap\Gamma^0(3)$(Theorem 4), we show in §4 that the singular value of $C(\tau)$ generates the ray class field $K_{(6)}$ modulo 6 over an imaginary quadratic field K(Theorem 13) by means of certain new method of Cho and Koo ([6]). Although singular values of the Rogers-Ramanujan and Ramanujan-Göllnitz-Gordon continued fractions at imaginary quadratic arguments are known to be units ([8] or [7]), we can hardly say that in our case the Ramanujan's cubic continued fraction $C(\tau)$ is a unit or even an algebraic integer. For a counterexample, we have $C(\frac{3+\sqrt{-3}}{6}) = -\frac{1}{\sqrt[3]{4}}$([1]) (or $C(\frac{1+i}{2}) = \frac{1-\sqrt{3}}{2}$ ([4])). Hence, in the matter of estimating class polynomials we first prove that $\frac{1}{C(\tau)}$ instead becomes an algebraic integer (Theorem 16) and then by using this fact together with the idea of Gee([9]) we establish relevent class polynomials of $K_{(6)}$ whose coefficients seem to be relatively small when compared with others' works([5], [12] and [15]).

In §2 we provide necessary preliminaries about modular functions and Klein forms, and give some lemmas illustrating the cusps of congruence subgroups which will be used in §3.

2. Preliminaries

Before starting out the main results we would like to state some necessary definitions and properties from the theory of modular functions. Let $\Gamma(1) = SL_2(\mathbb{Z})$ be the full modular group. For any integer $N \geq 1$, we have congruent subgroups $\Gamma(N)$, $\Gamma_1(N)$, $\Gamma_0(N)$ and $\Gamma^0(N)$ of $\Gamma(1)$ consisting of matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ congruent modulo N to $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$, $\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$ and $\begin{pmatrix} * & 0 \\ * & * \end{pmatrix}$ respectively. And, let $\mathfrak{H} = \{\tau \in \mathbb{C} \mid \operatorname{Im} \tau > 0\}$ be the complex upper half plane and $\mathfrak{H}^* = \mathfrak{H} \cup \mathbb{Q} \cup \{\infty\}$.

Then a congruence subgroup Γ acts on $\mathfrak{H}^*$ by linear fractional transformations so that $\gamma(\tau) = (a\tau + b)/(c\tau + d)$ for $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$, and the quotient space $\Gamma\backslash\mathfrak{H}^*$ becomes a compact Riemann surface with the appropriate complex structure. By definition an element s of $\mathbb{Q} \cup \{\infty\}$ is called a cusp, and two cusps s_1, s_2 are equivalent under Γ if there exists $\gamma \in \Gamma$ such that $\gamma(s_1) = s_2$. Then the equivalence class of a cusp s or its representative s is called a cusp of Γ by abuse of terminology. Indeed, there exist at most finitely many inequivalent cusps of Γ. Let s be any cusp of Γ, and let $\rho \in SL_2(\mathbb{Z})$ be such that $\rho(s) = \infty$. We define the width of the cusp s in $\Gamma\backslash\mathfrak{H}^*$ by the smallest positive integer h satisfying $\rho^{-1}\begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}\rho \in \{\pm 1\} \cdot \Gamma$. Then the width depends only on the equivalence class of the cusp s under Γ and is independent of the choice of ρ.

By a modular function with respect to a congruence subgroup Γ we mean a $\mathbb{C}$-valued function $f(\tau)$ of $\mathfrak{H}$ satisfying the following three conditions.

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

The precise meaning of the last condition is as follows. For a cusp s for Γ, let h be the width for s and ρ be an element of $SL_2(\mathbb{Z})$ such that $\rho(s) = \infty$. Since $(f \circ \rho^{-1})(\tau + h) = (f \circ \rho^{-1}\begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}\rho)(\rho^{-1}\tau) = (f \circ \rho^{-1})(\tau)$, $f \circ \rho^{-1}$ has a Laurent series expansion in $q_h = e^{2\pi i \tau/h}$, namely for some integer n_0, $(f \circ \rho^{-1})(\tau) = \sum_{n \geq n_0} a_n q_h^n$ with $a_{n_0} \neq 0$. This integer n_0 is called the order of $f(\tau)$ at the cusp s and denoted by $ord_s f(\tau)$. If $ord_s f(\tau)$ is positive (respectively, negative), then we say that $f(\tau)$ has a zero (respectively, a pole) at s. If a modular function $f(\tau)$ is holomorphic on $\mathfrak{H}$ and $ord_s f(\tau)$ is greater than or equal to 0 for every cusp s, then we say that $f(\tau)$ is holomorphic on $\mathfrak{H}^*$. Since we may identify a modular function with respect to Γ with a meromorphic function on the compact Riemann surface $\Gamma\backslash\mathfrak{H}^*$, any holomorphic modular function with respect to some congruence subgroup Γ is a constant.

Let $A_0(\Gamma)$ be the field of all modular functions with respect to Γ, and $A_0(\Gamma)_{\mathbb{Q}}$ be the subfield of $A_0(\Gamma)$ in which the Fourier expansion of $f(\tau)$ has rational coefficients. Then we may identify $A_0(\Gamma)$ with the field $\mathbb{C}(\Gamma\backslash\mathfrak{H}^*)$ of all meromorphic functions of the compact Riemann surface $\Gamma\backslash\mathfrak{H}^*$, and if $f(\tau) \in A_0(\Gamma)$ is nonconstant, then the field extension degree $[A_0(\Gamma) : \mathbb{C}(f(\tau))]$ is finite and is equal to the total degree of poles of $f(\tau)$. Since we will consider the modular functions with neither zeros nor poles on $\mathfrak{H}$, the total degree of poles of $f(\tau)$ is $-\Sigma_s\, ord_s f(\tau)$ where the summation runs over all the inequivalent cusps s at which $f(\tau)$ has poles.

Next, we illustrate some facts about the Klein forms which will be used in the expression of $C(\tau)$. For a complete treatment, the reader may consult [14].

Let $\tau \in \mathfrak{H}$ and $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$. And let $a = (a_1\ a_2) \in \mathbb{R}^2 - \mathbb{Z}^2$. Here we use the same letter a by abuse of notation. Then the Klein form $\mathfrak{k}_a(\tau)$ satisfies the followings:

(**K0**) $\mathfrak{k}_{-a}(\tau) = -\mathfrak{k}_a(\tau)$.

(**K1**) $\mathfrak{k}_a(\gamma(\tau)) = (c\tau + d)^{-1}\mathfrak{k}_{a\gamma}(\tau)$.

(**K2**) For any $b = (b_1\ b_2) \in \mathbb{Z}^2$ we have $\mathfrak{k}_{a+b}(\tau) = \varepsilon(a, b)\mathfrak{k}_a(\tau)$, where $\varepsilon(a, b) = (-1)^{b_1b_2+b_1+b_2}$ $e^{\pi i(b_2a_1-b_1a_2)}$.

(**K3**) For $a = (\frac{r}{N}\ \frac{s}{N}) \in \frac{1}{N}\mathbb{Z}^2 - \mathbb{Z}^2$ and any $\gamma \in \Gamma(N)$ with an integer $N > 1$, $\mathfrak{k}_a(\gamma(\tau)) = \varepsilon_a(\gamma)\cdot(c\tau+d)^{-1}\cdot\mathfrak{k}_a(\tau)$ where $\varepsilon_a(\gamma) = -(-1)^{(\frac{a-1}{N}r+\frac{c}{N}s+1)(\frac{b}{N}r+\frac{d-1}{N}s+1)} \cdot e^{\pi i(br^2+(d-a)rs-cs^2)/N^2}$.

(**K4**) Let $\tau \in \mathfrak{H}$, $z = a_1\tau + a_2$ with $a = (a_1\ a_2) \in \mathbb{Q}^2 - \mathbb{Z}^2$, and further let $q = e^{2\pi i\tau}$, $q_z = e^{2\pi iz} = e^{2\pi ia_2}e^{2\pi ia_1\tau}$. Then $\mathfrak{k}_a(\tau) = -\frac{1}{2\pi i}\ e^{\pi ia_2(a_1-1)} \cdot q^{\frac{1}{2}a_1(a_1-1)} \cdot (1 - q_z) \cdot \prod_{n=1}^{\infty} \frac{(1-q^nq_z)(1-q^nq_z^{-1})}{(1-q^n)^2}$, and $ord_q\mathfrak{k}_a(\tau) = \frac{1}{2} < a_1 > (< a_1 > -1)$ where $< a_1 >$ denotes the number such that $0 \leq < a_1 > < 1$ and $a_1- < a_1 >\in \mathbb{Z}$.

(**K5**) Let $f(\tau) = \prod_a \mathfrak{k}_a^{m(a)}(\tau)$ be a finite product of Klein forms with $a = (\frac{r}{N}\ \frac{s}{N}) \in \frac{1}{N}\mathbb{Z}^2 - \mathbb{Z}^2$ for an integer $N > 1$, and let $k = -\sum_a m(a)$. Then $f(\tau)$ is a modular function with respect to $\Gamma(N)$ if and only if $k = 0$ and

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

Furthermore, we need the following three lemmas for later use which can be proved by using the standard theory of modular functions.

Let N, m be positive integers and $\Gamma = \Gamma_1(N)\cap\Gamma_0(mN)$. Note that if we let $\Gamma\backslash\Gamma(1)/\Gamma(1)_\infty = \{\Gamma\gamma_1\Gamma(1)_\infty, \cdots, \Gamma\gamma_g\Gamma(1)_\infty\}$, then $\{\gamma_1(\infty), \cdots, \gamma_g(\infty)\}$ is a set of all cusps of Γ which satisfies that $\gamma_i(\infty)$ and $\gamma_j(\infty)$ are not equivalent under Γ for any $i \neq j$. Let $M = \{(\bar{c}, \bar{d}) \in$

$\mathbb{Z}/mN\mathbb{Z} \times \mathbb{Z}/mN\mathbb{Z} \mid (\bar{c}, \bar{d}) = \bar{1}$, i.e., $(c, d, mN) = 1\}$. Further, let $\Delta = \{\overline{\pm(1+Nk)} \in (\mathbb{Z}/mN\mathbb{Z})^{\times} | k = 0, \cdots, m-1\}$ which is a subgroup of $(\mathbb{Z}/mN\mathbb{Z})^{\times}$. We define an equivalence relation $\sim$ on M by $(\overline{c_1}, \overline{d_1}) \sim (\overline{c_2}, \overline{d_2})$ if there exist $\bar{s} \in \Delta$ and $\bar{n} \in \mathbb{Z}/mN\mathbb{Z}$ such that $\overline{c_2} = \bar{s} \cdot \overline{c_1}$ and $\overline{d_2} = \bar{s} \cdot \overline{d_1} + \bar{n} \cdot \overline{c_1}$. Then $\sim$ is indeed an equivalence relation. And we further define a map $\phi : \Gamma \backslash \Gamma(1)/\Gamma(1)_{\infty} \to M/\sim$ by $\phi(\Gamma \begin{pmatrix} a & b \\ c & d \end{pmatrix} \Gamma(1)_{\infty}) = [(\bar{c}, \bar{d})]$. Here we see without difficulty that the map ϕ is well-defined and bijective. Thus we get the following lemma.

Lemma 1. *Let $a, c, a', c' \in \mathbb{Z}$ be such that $(a, c) = 1$ and $(a', c') = 1$. We understand that $\frac{\pm 1}{0} = \infty$. Then, with the notation Δ as above, $\frac{a}{c}$ and $\frac{a'}{c'}$ 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 $\begin{pmatrix} a' \\ c' \end{pmatrix} \equiv \begin{pmatrix} \bar{s}^{-1}a + nc \\ \bar{s}c \end{pmatrix}$ mod mN.*

Proof. Let $\Gamma = \Gamma_1(N) \cap \Gamma_0(mN)$. We take b, d, b', $d' \in \mathbb{Z}$ such that $\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \in \Gamma(1)$. Note that $\frac{a}{c}$ and $\frac{a'}{c'}$ are equivalent under $\Gamma \Leftrightarrow \Gamma \begin{pmatrix} a & b \\ c & d \end{pmatrix} \Gamma(1)_{\infty} = \Gamma \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \Gamma(1)_{\infty}$ $\Leftrightarrow [(\bar{c}, \bar{d})] = [(\overline{c'}, \overline{d'})] \Leftrightarrow$ there exist $\bar{s} \in \Delta$ and $\bar{n} \in \mathbb{Z}/mN\mathbb{Z}$ such that $\overline{c'} = \bar{s}\bar{c}$ and $\overline{d'} = \bar{s}\bar{d} + \bar{n}\bar{c}$. Since $ad - bc = a'd' - b'c' = 1$, the last statement is equivalent to the first one of the followings. Note that (there exist $\bar{s} \in \Delta$ and $\bar{n} \in \mathbb{Z}/mN\mathbb{Z}$ such that $\overline{c'} = \bar{s}\bar{c}$ and $\overline{(ad - bc)} \cdot \overline{d'} = \bar{s} \cdot \overline{(a'd' - b'c')} \cdot \bar{d} + \bar{n}\bar{c}) \Leftrightarrow$ (there exist $\bar{s} \in \Delta$ and $\bar{n} \in \mathbb{Z}/mN\mathbb{Z}$ such that $\overline{c'} = \bar{s}\bar{c}$ and $\bar{a}\overline{dd'} = \bar{s}\overline{a'}\,\overline{dd'} + \bar{n}\bar{c}) \Leftrightarrow$ (there exist $\bar{s} \in \Delta$ and $\bar{n} \in \mathbb{Z}/mN\mathbb{Z}$ such that $\overline{c'} = \bar{s}\bar{c}$ and $\bar{a} = \bar{s}\overline{a'} + \bar{n}\bar{c}$) by observing $(\overline{dd'}, \bar{c}) = \bar{1}$. This completes the proof. $\square$

For a positive divisor x of mN, let $\pi_x : (\mathbb{Z}/mN\mathbb{Z})^{\times} \to (\mathbb{Z}/x\mathbb{Z})^{\times}$ be the natural homomorphism. Observe that π_x is surjective. And for a positive divisor c of mN, let $\overline{s'_{c,1}}, \cdots, \overline{s'_{c,n_c}} \in (\mathbb{Z}/\frac{mN}{c}\mathbb{Z})^{\times}$ be all the distinct coset representatives of $\pi_{\frac{mN}{c}}(\Delta)$ in $(\mathbb{Z}/\frac{mN}{c}\mathbb{Z})^{\times}$ where $n_c = \frac{\varphi(\frac{mN}{c})}{|\pi_{\frac{mN}{c}}(\Delta)|}$. Here, φ is the Euler's φ-function. Then for any $\overline{s'_{c,i}}$ with $i = 1, \cdots, n_c$ we take $\overline{s_{c,i}} \in (\mathbb{Z}/mN\mathbb{Z})^{\times}$ such that $\pi_{\frac{mN}{c}}(\overline{s_{c,i}}) = \overline{s'_{c,i}}$. We further let $S_c = \{\overline{s_{c,1}}, \cdots, \overline{s_{c,n_c}} \in (\mathbb{Z}/mN\mathbb{Z})^{\times}\}$. For a positive divisor c of mN, let $\overline{a'_{c,1}}, \cdots, \overline{a'_{c,m_c}} \in (\mathbb{Z}/c\mathbb{Z})^{\times}$ be all the distinct coset representatives of $\pi_c(\Delta \cap \ker(\pi_{\frac{mN}{c}}))$ in $(\mathbb{Z}/c\mathbb{Z})^{\times}$, where $m_c = \frac{\varphi(c)}{|\pi_c(\Delta \cap \ker(\pi_{\frac{mN}{c}}))|} = \frac{\varphi(c)}{|\pi_{\frac{mN}{(c, \frac{mN}{c})}}(\Delta)|/|\pi_{\frac{mN}{c}}(\Delta)|}$. Then for any $\overline{a'_{c,j}}$ with $j = 1, \cdots, m_c$ we take $\overline{a_{c,j}} \in (\mathbb{Z}/mN\mathbb{Z})^{\times}$ such that $\pi_c(\overline{a_{c,j}}) = \overline{a'_{c,j}}$. With the notations as above, we finally let $A_c = \{a_{c,1}, \cdots, a_{c,m_c} \in \mathbb{Z}\}$ be a set such that $0 < a_{c,1}, \cdots, a_{c,m_c} \leq mN$, $(a_{c,j}, mN) = 1$ and $a_{c,j}$ is the representative of $\overline{a_{c,j}}$ for every $j = 1, \cdots, m_c$.

Lemma 2. *With the notations as above, let $S = \{(\bar{c} \cdot \overline{s_{c,i}}, \overline{a_{c,j}}) \in \mathbb{Z}/mN\mathbb{Z} \times \mathbb{Z}/mN\mathbb{Z} \ |0 < c|mN, \overline{s_{c,i}} \in S_c,\ a_{c,j} \in A_c\}$. For a given $(\bar{c} \cdot \overline{s_{c,i}},\ \overline{a_{c,j}}) \in S$, we can take x, $y \in \mathbb{Z}$ such that $(x, y) = 1$, $\bar{x} = \bar{c} \cdot \overline{s_{c,i}}$ and $\bar{y} = \overline{a_{c,j}}$ because $(c \cdot s_{c,i}, a_{c,j}, mN) = 1$. Then for such $x, y \in \mathbb{Z}$, $\frac{y}{x}$*

form a set of all the inequivalent cusps of $\Gamma_1(N)\cap\Gamma_0(mN)$ *and the number of such cusps is* $|S|=\sum_{\substack{c>0\\ c|mN}} n_c\cdot m_c=\sum_{\substack{c>0\\ c|mN}}\frac{\varphi(c)\varphi(\frac{mN}{c})}{|\pi_{\frac{mN}{(c,\frac{mN}{c})}}(\Delta)|}$.

Proof. Since there is a bijection between $\Gamma\backslash\Gamma(1)/\Gamma(1)_\infty$ and $M'/\sim$ where $M'=\{(\bar{c},\bar{a})\in\mathbb{Z}/mN\mathbb{Z}\times\mathbb{Z}/mN\mathbb{Z}\mid(\bar{c},\bar{a})=\bar{1}$, i.e., $(c,a,mN)=1\}$ and $(\overline{c_1},\overline{a_1})\sim(\overline{c_2},\overline{a_2})$ if there exist $\bar{s}\in\Delta$ and $\bar{n}\in\mathbb{Z}/mN\mathbb{Z}$ such that $\overline{c_2}=\bar{s}\cdot\overline{c_1}\in\mathbb{Z}/mN\mathbb{Z}$ and $\overline{a_2}=\bar{s}^{-1}\overline{a_1}+\bar{n}\overline{c_1}\in\mathbb{Z}/mN\mathbb{Z}$, it is enough to prove that the natural map $f:S\to M'/\sim$ is a bijection. We first prove the injectivity. Suppose that $[(\bar{c}\cdot\overline{s_{c,i}},\overline{a_{c,j}})]=[(\overline{c'}\cdot\overline{s_{c',i'}},\overline{a_{c',j'}})]$. Then there exist $\bar{s}\in\Delta$ and $\bar{n}\in\mathbb{Z}/mN\mathbb{Z}$ such that $\overline{c'}\cdot\overline{s_{c',i'}}=\bar{s}\cdot\bar{c}\cdot\overline{s_{c,i}}\in\mathbb{Z}/mN\mathbb{Z}$ and $\overline{a_{c',j'}}=\bar{s}^{-1}\overline{a_{c,j}}+\bar{n}\cdot\bar{c}\cdot\overline{s_{c,i}}\in\mathbb{Z}/mN\mathbb{Z}$. Since $\bar{s},\overline{s_{c,i}},\overline{s_{c',i'}}\in(\mathbb{Z}/mN\mathbb{Z})^\times$ and $c,c'\mid mN$, we obtain $c=c'$; hence $\pi_{\frac{mN}{c}}(\overline{s_{c,i'}})=\pi_{\frac{mN}{c}}(\bar{s})\cdot\pi_{\frac{mN}{c}}(\overline{s_{c,i}})\Rightarrow\overline{s'_{c,i'}}\in\pi_{\frac{mN}{c}}(\Delta)\overline{s'_{c,i}}\Rightarrow\overline{s'_{c,i'}}=\overline{s'_{c,i}}\Rightarrow i'=i\Rightarrow\pi_{\frac{mN}{c}}(\bar{s})=\bar{1}$, i.e., $\bar{s}\in\Delta\cap\ker(\pi_{\frac{mN}{c}})$. Thus $\overline{a_{c,j'}}=\pi_c(\bar{s}^{-1})\overline{a_{c,j}}\in(\mathbb{Z}/c\mathbb{Z})^\times$ implies $\overline{a_{c,j'}}\in\pi_c(\Delta\cap\ker(\pi_{\frac{mN}{c}}))\overline{a_{c,j}}$, from which we get $a_{c,j'}=a_{c,j}$. Now we prove the surjectivity. Let $[(\overline{c'},\overline{a'})]\in M'/\sim$. We take $c=(c',mN)$. Then $\overline{(\frac{c'}{c})}\in(\mathbb{Z}/\frac{mN}{c}\mathbb{Z})^\times$ implies $\overline{(\frac{c'}{c})}\in\pi_{\frac{mN}{c}}(\Delta)\overline{s'_{c,i}}=\pi_{\frac{mN}{c}}(\Delta)\pi_{\frac{mN}{c}}(\overline{s_{c,i}})$ for some i. Since $(\overline{c'},\overline{a'})=\bar{1}\in\mathbb{Z}/mN\mathbb{Z}$, we get $1=(c',a',mN)=(c,a')$, namely $\overline{a'}\in(\mathbb{Z}/c\mathbb{Z})^\times$, and hence $\overline{a'}\in\pi_c(\Delta\cap\ker(\pi_{\frac{mN}{c}}))\overline{a_{c,j}}$ for some j. We further claim that there exist $\bar{s}\in\Delta$ and $\bar{n}\in\mathbb{Z}/mN\mathbb{Z}$ such that $\overline{c'}=\bar{s}\cdot\bar{c}\cdot\overline{s_{c,i}}$ and $\overline{a'}=\bar{s}^{-1}\overline{a_{c,j}}+\bar{n}\cdot\bar{c}\cdot\overline{s_{c,i}}$. It is enough to prove that there exist $\bar{s}\in\Delta$ such that $\pi_{\frac{mN}{c}}(\bar{s})=\overline{(\frac{c'}{c})}\pi_{\frac{mN}{c}}(\overline{s_{c,i}})^{-1}\in\pi_{\frac{mN}{c}}(\Delta)\subset(\mathbb{Z}/\frac{mN}{c}\mathbb{Z})^\times$ and $\pi_c(\bar{s})=\overline{a'}^{-1}\overline{a_{c,j}}\in\pi_c(\Delta\cap\ker(\pi_{\frac{mN}{c}}))\subset(\mathbb{Z}/c\mathbb{Z})^\times$, which is equivalent to prove the following isomorphisms $\pi_{\frac{mN}{(c,\frac{mN}{c})}}(\Delta)/\pi_{\frac{mN}{(c,\frac{mN}{c})}}(\Delta\cap\ker(\pi_{\frac{mN}{c}}))\cong\pi_{\frac{mN}{c}}(\Delta)$ and $\pi_{\frac{mN}{(c,\frac{mN}{c})}}(\Delta\cap\ker(\pi_{\frac{mN}{c}}))\cong\pi_c(\Delta\cap\ker(\pi_{\frac{mN}{c}}))$ under the natural maps. Note that the kernel of the natural map $\pi_{\frac{mN}{(c,\frac{mN}{c})}}(\Delta)\to\pi_{\frac{mN}{c}}(\Delta)$ is equal to $\pi_{\frac{mN}{(c,\frac{mN}{c})}}(\Delta\cap\ker(\pi_{\frac{mN}{c}}))$. As for the second, let $\bar{s}\in\Delta\cap\ker(\pi_{\frac{mN}{c}})$ be such that $\pi_c(\bar{s})=\bar{1}\in(\mathbb{Z}/c\mathbb{Z})^\times$. Then $s\equiv1\bmod\frac{mN}{c}$ and $s\equiv1\bmod c$, which implies $s\equiv1\bmod\frac{mN}{(c,\frac{mN}{c})}$. This completes the proof. $\square$

Note that if $\Gamma=\Gamma_1(N)$ or $\Gamma_0(m)$ then Lemma 1 and Lemma 2 may be reduced to concise statements. In particular if $\Gamma=\Gamma_0(m)$, i.e., $N=1$ then $\Delta=(\mathbb{Z}/m\mathbb{Z})^\times$, and so $S_c=\{\bar{1}\in(\mathbb{Z}/m\mathbb{Z})^\times\}$ for any positive divisor c of m. Since $(c,a_{c,j})=1$ and $a_{c,j}=a_{c,j'}\Leftrightarrow a_{c,j}\equiv a_{c,j'}\bmod c$ and $a_{c,j}\equiv a_{c,j'}\bmod\frac{m}{c}\Leftrightarrow a_{c,j}\equiv a_{c,j'}\bmod(c,\frac{m}{c})$, we conclude by Lemma 2 that $\{\frac{a_{c,j}}{c}\in\mathbb{Q}\mid 0<c\,|\,m,\ 0<a_{c,j}\le m,\ (a_{c,j},m)=1$ and $a_{c,j}=a_{c,j'}\Leftrightarrow a_{c,j}\equiv a_{c,j'}\bmod(c,\frac{m}{c})\}$ is a set of all the inequivalent cusps of $\Gamma_0(m)$. Similarly if $\Gamma=\Gamma_1(N)$, i.e., $m=1$ then $\Delta=\{\overline{\pm1}\}\subset(\mathbb{Z}/N\mathbb{Z})^\times$; hence Lemma 1 can be restated as a simpler one.

Here we observe that Lemma 2 gives us a set of all the inequivalent cusps of $\Gamma_1(N)\cap\Gamma_0(mN)$. And we can figure out the width of each cusp by the following lemma.

Lemma 3. *Let* $\frac{a}{c}$ *be a cusp of* $\Gamma=\Gamma_1(N)\cap\Gamma_0(mN)$ *with* $a,\ c\in\mathbb{Z}$ *and* $(a,c)=1$. *We understand* $\frac{\pm1}{0}$ *as* ∞. *Then the width* h *of a cusp* $\frac{a}{c}$ *in* $\Gamma\backslash\mathfrak{H}^*$ *is given by*

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

Proof. First, we consider the case where N does not divide 4. We take $b, d \in \mathbb{Z}$ such that $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$. Observe that the width of the cusp $\frac{a}{c}$ in $\Gamma \backslash \mathfrak{H}^*$ is the smallest positive integer h such that $\begin{pmatrix} 1-ach & * \\ -c^2h & 1+ach \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} \in \{\pm 1\} \cdot (\Gamma_1(N) \cap \Gamma_0(mN))$. If $\begin{pmatrix} 1-ach & * \\ -c^2h & 1+ach \end{pmatrix} \in \{-1\} \cdot (\Gamma_1(N) \cap \Gamma_0(mN))$, then by taking the trace we have $2 \equiv -2 \bmod N$, which is a contradiction. So $\begin{pmatrix} 1-ach & * \\ -c^2h & 1+ach \end{pmatrix} \in \Gamma_1(N) \cap \Gamma_0(mN)$. Thus $h \in \frac{N}{(ac,N)}\mathbb{Z} \cap \frac{mN}{(c^2,mN)}\mathbb{Z} = \frac{mN}{(c,N)\cdot(m,\frac{c^2}{(c,N)})}\mathbb{Z}$. For the cases $N = 1, 2, 4$, we can verify the statement in a similar fashion. □

Now, we remark that arbitrary intersection $\Gamma = \Gamma_0(N_1) \cap \Gamma^0(N_2) \cap \Gamma_1(N_3) \cap \Gamma^1(N_4) \cap \Gamma(N_5)$ is in fact conjugate to the above form $\Gamma_1(N) \cap \Gamma_0(mN)$. More precisely, $\alpha^{-1}\Gamma\alpha = \Gamma_1(N) \cap \Gamma_0(mN)$ where $\alpha = \begin{pmatrix} lcm(N_2, N_4, N_5) & 0 \\ 0 & 1 \end{pmatrix}$, $N = lcm(N_3, N_4, N_5)$ and $m = lcm(N_1, N_3, N_5) \cdot lcm(N_2, N_4, N_5)/N$. Note that if we let $\{s_1, \cdots, s_g\}$ be a set of all the inequivalent cusps of some congruence subgroup Γ' and set $\Gamma' = \alpha^{-1}\Gamma\alpha$ for some α, then $\{\alpha(s_1), \cdots, \alpha(s_g)\}$ gives us a set of all the inequivalent cusps of Γ.

3. Ramanujan's cubic continued fraction $C(\tau)$

In this section, by using the lemmas introduced in §2 we establish certain properties of the Ramanujan's cubic continued fraction $C(\tau)$. Since $C(\tau)$ has an infinite product expression, we can show by routine calculations that it has the following finite product of Klein forms

$$C(\tau) = \zeta_{12}^5 \prod_{j=0}^{5} \frac{\mathfrak{k}_{\left(\frac{1}{6} \ \frac{j}{6}\right)}}{\mathfrak{k}_{\left(\frac{3}{6} \ \frac{j}{6}\right)}}(\tau)$$

, where $\zeta_{12} = \exp(\frac{2\pi i}{12})$.

Theorem 4. *Let $C(\tau)$ be the Ramanujan's cubic continued fraction as before. Then $C(\tau)$ is a Hauptmodul for $\Gamma_1(6) \cap \Gamma^0(3)$.*

Proof. Using (**K5**) we can check that the level of $C(\tau)$ is 6. By (**K1**) and (**K2**) or definition of $C(\tau)$ in §1, it is readily verified that $C \circ \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}(\tau) = C(\tau+1) = \zeta_3 C(\tau)$ where $\zeta_3 = \exp(\frac{2\pi i}{3})$; hence $C(\tau)^3$ is invariant under $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Since $\Gamma_1(6) =< \Gamma(6), \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} >$, we obtain that $C(\tau)^3 \in A_0(\Gamma_1(6))$. We first claim that $\mathbb{C}(C(\tau)^3) = A_0(\Gamma_1(6))$. It follows from Lemma 2 and 3 that there are four cusps 1, 1/2, 1/3, $1/6 \sim \infty$ of widths 6, 3, 2, 1 respectively. For a cusp $1/c$ of width $6/c$ with $c|6$, we get by applying (**K1**) and (**K4**) that $C^3 \circ \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix}(\tau)$ is of the form

$$(\text{some root of unity}) \cdot q_{6/c}^{r} + (\text{higher terms}),$$

where $r = \frac{9}{c}\sum_{j=0}^{5}(< \frac{1+cj}{6} > (< \frac{1+cj}{6} > -1) - < \frac{3+cj}{6} > (< \frac{3+cj}{6} > -1))$. An easy calculation shows that $r = 0,\ 0,\ -1,\ 1$ according as $c = 1,\ 2,\ 3,\ 6$. Therefore $C^3(\tau)$ has only a simple pole at $1/3$ and only a simple zero at ∞, which proves the claim. Let Γ' be a subgroup of $\Gamma(1)$ such that $\mathbb{C}(C(\tau)) = A_0(\Gamma')$, which is possible by the above claim. Then $[A_0(\Gamma') : A_0(\Gamma_1(6))] = 3$, i.e., $[\Gamma_1(6) : \Gamma'] = 3$. Note that $C(\tau)$ is invariant under the action of $\begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix}$ because $C \circ \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}(\tau) = \zeta_3 C(\tau)$. So $\Gamma' \supseteq < \Gamma(6), \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix} > = \Gamma_1(6) \cap \Gamma^0(3)$. Observing that $[\Gamma_1(6) : \Gamma_1(6) \cap \Gamma^0(3)] = 3$ we can conclude that $\Gamma' = \Gamma_1(6) \cap \Gamma^0(3)$. □

Since $C(\tau)$ has rational Fourier coefficients, the above theorem implies that $\mathbb{Q}(C(\tau)) = A_0(\Gamma_1(6) \cap \Gamma^0(3))_{\mathbb{Q}}$. Thus the following proposition indicates the existence of an affine plane model defined over $\mathbb{Q}$, which is called in our case the modular equation.

Proposition 5. *Let n be a positive integer. Then $\mathbb{Q}(C(\tau), C(n\tau)) = A_0(\Gamma_1(6) \cap \Gamma^0(3) \cap \Gamma_0(6n))_{\mathbb{Q}}$.*

Proof. Since $C(\tau)$ is a Hauptmodul for $\Gamma_1(6) \cap \Gamma^0(3)$, we see that for any $\alpha \in GL_2^+(\mathbb{Q})$, $C \circ \alpha = C$ implies $\alpha \in \mathbb{Q}^\times \cdot (\Gamma_1(6) \cap \Gamma^0(3))$. Let $\Gamma = \Gamma_1(6) \cap \Gamma^0(3)$ and $\beta = \begin{pmatrix} n & 0 \\ 0 & 1 \end{pmatrix}$. Note that $\Gamma \cap \Gamma_0(6n) = \Gamma_1(6) \cap \Gamma^0(3) \cap \Gamma_0(6n) = \Gamma \cap \beta^{-1}\Gamma\beta$, hence it is clear that $C(\tau), C(n\tau) \in A_0(\Gamma \cap \beta^{-1}\Gamma\beta)_{\mathbb{Q}}$. Thus it is enough to show that $\mathbb{Q}(C(\tau), C(n\tau)) \subset A_0(\Gamma \cap \beta^{-1}\Gamma\beta)_{\mathbb{Q}}$. Let Γ' be the subgroup of $SL_2(\mathbb{Z})$ such that $\mathbb{Q}(C(\tau), C(n\tau)) = A_0(\Gamma')_{\mathbb{Q}}$ and let γ be an element of Γ'. Since $C(\tau)$ is an Hauptmodul for $\Gamma_1(6) \cap \Gamma^0(3)$ and invariant under γ, we derive that $\gamma \in \Gamma$. Moreover, $C(n\tau)$ is invariant under γ and $C(\tau)$ is invariant under $\beta\gamma\beta^{-1}$, from which we have $\gamma \in \Gamma \cap \beta^{-1}\Gamma\beta$. Therefore, this completes the proof because it means that $\Gamma' \subset \Gamma \cap \beta^{-1}\Gamma\beta$, namely $A_0(\Gamma')_{\mathbb{Q}} \supset A_0(\Gamma \cap \beta^{-1}\Gamma\beta)_{\mathbb{Q}}$. □

In general, if we let $\mathbb{C}(f_1(\tau), f_2(\tau))$ be the field of all modular functions with respect to some congruence subgroup for which $f_1(\tau)$ and $f_2(\tau)$ are nonconstant, then $[\mathbb{C}(f_1(\tau), f_2(\tau)) : \mathbb{C}(f_i(\tau))]$ is equal to the total degree d_i of poles of $f_i(\tau)$ for $i = 1, 2$. So there exists a polynomial $\Phi(X, Y) \in \mathbb{C}[X, Y]$ such that $\Phi(f_1(\tau), Y)$ is an irreducible polynomial of $f_2(\tau)$ over $\mathbb{C}(f_1(\tau))$ with degree d_1, and similarly so is $\Phi(X, f_2(\tau))$ with degree d_2. Then Proposition 5 guarantees the existence of a polynomial $\Phi_n(X, Y) \in \mathbb{Q}[X, Y]$ such that $\Phi_n(C(\tau), C(n\tau)) = 0$ and $\Phi_n(X, Y)$ is irreducible both as a polynomial in X over $\mathbb{C}(Y)$ and as a polynomial in Y over $\mathbb{C}(X)$, for every positive integer n.

Let $\Gamma' = \Gamma_1(6) \cap \Gamma_0(18n)$. Then Γ' is conjugate to $\Gamma_1(6) \cap \Gamma^0(3) \cap \Gamma_0(6n)$, that is, $\begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix} \Gamma' \begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix}^{-1} = \Gamma_1(6) \cap \Gamma^0(3) \cap \Gamma_0(6n)$. And $\mathbb{Q}(C(3\tau), C(3n\tau)) = A_0(\Gamma')_{\mathbb{Q}}$. Since it is much easier to handle with Γ' than with the group $\Gamma_1(6) \cap \Gamma^0(3) \cap \Gamma_0(6n)$, we will concentrate on the modular equation of $C(3\tau)$ and $C(3n\tau)$, which gives rise to in return the modular equation of $C(\tau)$ and $C(n\tau)$. Now that it is also easier to handle with a Hauptmodul having a simple pole at ∞, we let $f(\tau) = \frac{1}{C(3\tau)}$ and $\Gamma = \Gamma_1(6) \cap \Gamma_0(18)$ hereafter and consider the modular equation $F_n(X, Y) \in \mathbb{Q}[X, Y]$ for $f(\tau)$ and $f(n\tau)$. Since $C(\tau)$ is a Hauptmodul for $\Gamma_1(6) \cap \Gamma^0(3)$, we see from the proof of Theorem 4 that $C(\tau)$ has a simple pole only at $1/3$ and a simple zero only at ∞. Thus for inequivalent cusps under Γ, $f(\tau)$ has a simple pole only at ∞ and a simple zero only at $\frac{1}{9}$.

Lemma 6. *Let $a, c, a', c' \in \mathbb{Z}$ and $f(\tau) = \frac{1}{C(3\tau)}$. Then we achieve the following assertions.*

(1) $f(\tau)$ has a pole at $\frac{a}{c} \in \mathbb{Q} \cup \{\infty\}$ with $(a,c)=1 \Leftrightarrow (a,c)=1$, $c \equiv 0$ mod 18.

(2) $f(n\tau)$ has a pole at $\frac{a'}{c'} \in \mathbb{Q} \cup \{\infty\} \Leftrightarrow$ there exist $a, c \in \mathbb{Z}$ such that $\frac{a}{c} = \frac{na'}{c'}$, $(a,c)=1$, $c \equiv 0$ mod 18.

(3) $f(\tau)$ has a zero at $\frac{a}{c} \in \mathbb{Q} \cup \{\infty\}$ with $(a,c)=1 \Leftrightarrow (a,c)=1$, $c \equiv 9$ mod 18.

(4) $f(n\tau)$ has a zero at $\frac{a'}{c'} \in \mathbb{Q} \cup \{\infty\} \Leftrightarrow$ there exist $a, c \in \mathbb{Z}$ such that $\frac{a}{c} = \frac{na'}{c'}$, $(a,c)=1$, $c \equiv 9$ mod 18.

Proof. Since $f(\tau)$ is a Hauptmodul for Γ with a simple pole only at ∞, $f(\tau)$ has a pole only at $\frac{a}{c} \in \mathbb{Q}\cup\{\infty\}$ such that $\frac{a}{c}$ is equivalent to ∞ under Γ. By Lemma 1 we get that $\frac{a}{c}$ is equivalent to ∞ under Γ if and only if there exist $\overline{s} \in \Delta = \{\overline{\pm 1}, \overline{\pm 7}, \overline{\pm 13} \in (\mathbb{Z}/18\mathbb{Z})^\times\} = (\mathbb{Z}/18\mathbb{Z})^\times$ and $n \in \mathbb{Z}$ such that $\begin{pmatrix} a \\ c \end{pmatrix} \equiv \begin{pmatrix} \overline{s}^{-1} \\ 0 \end{pmatrix}$ mod 18. So the first assertion follows. Furthermore, $f(\tau)$ has a zero at $\frac{a}{c}$ if and only if $\frac{a}{c}$ is equivalent to $\frac{1}{9}$ under Γ. Applying Lemma 1 we have $\begin{pmatrix} a \\ c \end{pmatrix} \equiv \begin{pmatrix} \overline{s}^{-1}+9n \\ 9 \end{pmatrix}$ mod 18. Hence we conclude the statement (3). Next, by using these we can derive the second and fourth assertions without difficulty. □

Let d_1 (respectively, d_n) be the total degree of poles of $f(\tau)$ (respectively, $f(n\tau)$). Then we may let $F_n(X,Y)$ be a polynomial $\sum_{\substack{0\le i\le d_n \\ 0\le j\le d_1}} C_{i,j}X^iY^j \in \mathbb{Q}[X,Y]$, which satisfies $F_n(f(\tau), f(n\tau)) = 0$. Ishida and Ishii([11]) showed the following theorem by means of the standard theory of algebraic functions, which will be useful in removing unnecessary coefficients $C_{i,j}$ from the polynomial $F_n(X,Y)$.

Theorem 7. *For any congruence subgroup Γ', let $f_1(\tau)$, $f_2(\tau)$ be nonconstants such that $\mathbb{C}(f_1(\tau), f_2(\tau)) = A_0(\Gamma')$ with the total degree D_k of poles of $f_k(\tau)$ for $k=1,2$, and let $F(X,Y) = \sum_{\substack{0\le i\le D_2 \\ 0\le j\le D_1}} C_{i,j}X^iY^j \in \mathbb{C}[X,Y]$ be such that $F(f_1(\tau), f_2(\tau)) = 0$. Let $S_{\Gamma'}$ be a set of all the inequivalent cusps of Γ', and $S_{k,0} = \{s \in S_{\Gamma'} \mid f_k(\tau)$ has zeros at $s\}$, and $S_{k,\infty} = \{s \in S_{\Gamma'} \mid f_k(\tau)$ has poles at $s\}$ for $k=1,2$. Further let $a = -\sum_{s\in S_{1,\infty}\cap S_{2,0}} ord_s f_1(\tau)$, and $b = \sum_{s\in S_{1,0}\cap S_{2,0}} ord_s f_1(\tau)$. Here we assume that a (respectively, b) is 0 if $S_{1,\infty}\cap S_{2,0}$ (respectively, $S_{1,0}\cap S_{2,0}$) is empty. Then we obtain the following assertions.*

(1) $C_{D_2,a} \neq 0$. If further $S_{1,\infty} \subset S_{2,\infty} \cup S_{2,0}$, then $C_{D_2,j} = 0$ for any $j \neq a$.

(2) $C_{0,b} \neq 0$. If further $S_{1,0} \subset S_{2,\infty} \cup S_{2,0}$, then $C_{0,j} = 0$ for any $j \neq b$.

(3) $C_{i,D_1} = 0$ for all i satisfying $0 \le i < |S_{1,0} \cap S_{2,\infty}|$ or $D_2 - |S_{1,\infty} \cap S_{2,\infty}| < i \le D_2$.

(4) $C_{i,0} = 0$ for all i satisfying $0 \le i < |S_{1,0} \cap S_{2,0}|$ or $D_2 - |S_{1,\infty} \cap S_{2,0}| < i \le D_2$.

If we interchange the roles of $f_1(\tau)$ and $f_2(\tau)$, then we may obtain further properties similar to (1)∼(4). Suppose further that there exist $r \in \mathbb{R}$ and $N, n_1, n_2 \in \mathbb{Z}$ with $N > 0$ such that $f_k(\tau+r) = \zeta_N^{n_k} f_k(\tau)$ for $k=1,2$, where $\zeta_N = e^{2\pi i/N}$. Then we obtain the following assertion.

(5) $n_1 i + n_2 j \not\equiv n_1 D_2 + n_2 a$ mod $N \Rightarrow C_{i,j} = 0$. Here note that $n_2 b \equiv n_1 D_2 + n_2 a$ mod N.

From now on using Theorem 7 we rediscover Chan's results on the modular equations when $p = 2$ and 3.

Theorem 8. *Let $C(\tau)$ be the Ramanujan's cubic continued fraction. Then*

(1) $\{C(\tau)\}^2 + 2C(\tau)\{C(2\tau)\}^2 - C(2\tau) = 0$

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

Proof. To prove (1) (respectively, (2)), we should find the modular equation $F_2(X,Y)$ (respectively, $F_3(X,Y)$) for $f(\tau)$ and $f(2\tau)$ (respectively, $f(3\tau)$), where $f(\tau) = \frac{1}{C(3\tau)}$.

Let us prove (1). By Proposition 5 we see that the congruence subgroup which we should consider is $\Gamma_1(6)\cap\Gamma_0(36)$; hence $\Delta_2 = \{\overline{\pm1}, \overline{\pm5}, \overline{\pm7}, \overline{\pm11}, \overline{\pm13}, \overline{\pm17} \in (\mathbb{Z}/36\mathbb{Z})^\times\} = (\mathbb{Z}/36\mathbb{Z})^\times$, where the notation Δ_2 is the subgroup in §2. We will first obtain d_1. By Lemma 2 and Lemma 6 we must consider S_{18}, A_{18}, S_{36} and A_{36}, which are easily derived as $S_{18} = S_{36} = \{\overline{1}\}$ and $A_{18} = A_{36} = \{1\}$, because n_{18}, m_{18}, n_{36} and m_{36} are 1. So all the cusps of $\Gamma_1(6)\cap\Gamma_0(36)$ at which $f(\tau)$ has poles are $1/18$ and $1/36$ by (1) of Lemma 6, where $1/36$ is equivalent to ∞ by Lemma 1. And we know by Lemma 3 the widths of $1/18$ and ∞ are 1 and 1, respectively. Since $f(\tau) = q^{-1} + O(1)$, we get that $ord_\infty f(\tau) = -1$. Now that $(f\circ\begin{pmatrix}1 & 0\\ 18 & 1\end{pmatrix})(\tau) = f(\tau) = q^{-1}+O(1)$ due to the fact $\begin{pmatrix}1 & 0\\ 18 & 1\end{pmatrix} \in \Gamma_1(6)\cap\Gamma_0(18)$, we claim that $ord_{1/18}f(\tau) = -1$. Thus the total degree d_1 of poles of $f(\tau)$ is 2. Next, we will estimate d_2. In like manner, by Lemma 2 and Lemma 6 we should consider S_{36} and A_{36}, which are already obtained in the above as $S_{36} = \{\overline{1}\}$ and $A_{36} = \{1\}$. And all the cusps of $\Gamma_1(6)\cap\Gamma_0(36)$ at which $f(2\tau)$ has poles is $1/36$ by (2) of Lemma 6. Since $1/36$ is equivalent to ∞ and the width of ∞ is 1, using $f(2\tau) = q^{-2} + O(1)$ we get that $ord_\infty f(2\tau) = -2$. So the total degree d_2 of poles of $f(2\tau)$ is 2. Hence, $F_2(X,Y)$ is of the form $\sum_{\substack{0\le i\le 2\\ 0\le j\le 2}} C_{i,j}X^iY^j \in \mathbb{Q}[X,Y]$.

Now, by utilizing Theorem 7 we can determine which coefficients $C_{i,j}$ should be eliminated. If we let $f_1(\tau) = f(\tau)$ and $f_2(\tau) = f(2\tau)$ in the theorem, we know that $S_{1,\infty} = \{\frac{1}{18}, \frac{1}{36}\}$, $S_{1,0} = \{\frac{1}{9}\}$, $S_{2,\infty} = \{\frac{1}{36}\}$ and $S_{2,0} = \{\frac{1}{9}, \frac{1}{18}\}$. Since $S_{1,\infty}\cap S_{2,0} = \frac{1}{18}$, we have $a = 1$. And, as for b, calculating $\mathrm{ord}_{\frac{1}{9}} f_1(\tau)$ we derive $b = 2$ because $(f\circ\begin{pmatrix}1 & 0\\ 9 & 1\end{pmatrix})(\tau) = 1/(C\circ\begin{pmatrix}3 & 0\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & 0\\ 9 & 1\end{pmatrix})(\tau) = 1/(C\circ\begin{pmatrix}1 & 0\\ 3 & 1\end{pmatrix})(3\tau) = q^{\frac{1}{2}} + \cdots$ and the width of $\frac{1}{9}$ is 4 in $(\Gamma_1(6)\cap\Gamma_0(36))\backslash\mathfrak{H}^*$. It follows from Theorem 7 (1) and (2) that $C_{2,1} \neq 0$ and $C_{2,2} = C_{2,1} = 0$ and $C_{0,2} \neq 0$ and $C_{0,1} = C_{0,0} = 0$. In order to use (5) of the theorem we calculate the followings in advance:

$$f_1(\tau+\frac{1}{3}) = f(\tau+\frac{1}{3}) = \frac{1}{C(3\tau+1)} = \zeta_3^{2} f(\tau) = \zeta_3^{2} f_1(\tau)$$
$$f_2(\tau+\frac{1}{3}) = f(2\tau+\frac{2}{3}) = \frac{1}{C(6\tau+2)} = \zeta_3 f(2\tau) = \zeta_3 f_2(\tau).$$

So we may assume that $N = 3$, $n_1 = 2$, $n_2 = 1$. Applying these to (5) of Theorem 7, $C_{2,2} = C_{1,2} = C_{1,1} = C_{0,1} = C_{2,0} = C_{0,0} = 0$. Hence, we are able to simplify our modular equation as $F_2(X,Y) = C_{2,1}X^2Y + C_{1,0}X + C_{0,2}Y^2$. Since $C_{0,2} \neq 0$, let it be 1.

Next, by replacing X(respectively, Y) by the q-expansion of $f(\tau)$ (respectively, $f(2\tau)$), we get that $C_{2,1} = -1$ and $C_{1,0} = 2$. Thus, $F_2(X,Y) = -X^2Y + 2X + Y^2$. Multiplying $F_2(\frac{1}{C(\tau)}, \frac{1}{C(2\tau)})$ by $C(\tau)^2C(2\tau)^2$ we achieve the first assertion.

In a similar way, by considering $\Gamma_1(6)\cap\Gamma_0(54)$ and $\Delta_3 = (\mathbb{Z}/54\mathbb{Z})^\times$ we can estimate the polynomial $F_3(X,Y) = \sum_{\substack{0\le i\le d_3\\ 0\le j\le d_1}} C_{i,j}X^iY^j$ such that $F_3(f(\tau), f(3\tau)) = 0$. In this case, since $S_{18} = S_{54} = \{\overline{1}\}$, $A_{18} = \{1,5\}$ and $A_{54} = \{1\}$, $f(\tau)$ has poles at $1/18$, $5/18$ and $1/54$

with width 1, 1 and 1 respectively by Lemma 3, in which 1/54 is equivalent to ∞ under $\Gamma_1(6)\cap\Gamma_0(54)$. And, we already know that $f(\tau)=q^{-1}+O(1)$ and $(f\circ\begin{pmatrix}1&0\\18&1\end{pmatrix})(\tau)=f(\tau)=q^{-1}+O(1)$. By the action of Klein forms (**K1**) $\sim$ (**K5**) we then see that $(f\circ\begin{pmatrix}5&-2\\18&-7\end{pmatrix})(\tau)=$ (some root of unity) $\cdot f(\tau)=$ (some root of unity) $\cdot\, q^{-1}+O(1)$. Considering the widths of cusps we have $ord_\infty f(\tau)=ord_{1/18}f(\tau)=ord_{5/18}f(\tau)=-1$. And, $d_1=3$. Likewise, $f(3\tau)$ has a pole only at $1/54\sim\infty$ and $f(3\tau)=q^{-3}+O(1)$. Hence, $ord_\infty f(3\tau)$ is -3. In other words, we deduce $d_3=3$.

We let $f_1(\tau)=f(\tau)$ and $f_2(\tau)=f(3\tau)$ in Theorem 7. Then $S_{1,\infty}=\{\frac{1}{18},\frac{5}{18},\frac{1}{54}\}$, $S_{1,0}=\{\frac{1}{9},\frac{2}{9},\frac{1}{27}\}$, $S_{2,\infty}=\{\frac{1}{54}\}$ and $S_{2,0}=\{\frac{1}{27}\}$. Since $S_{1,\infty}\cap S_{2,0}=\phi$, the number a in Theorem 7 is 0. By (1) of Theorem 7, we have $C_{3,0}\neq 0$. Interchanging the roles of $f_1(\tau)$ and $f_2(\tau)$ we get $C_{0,3}\neq 0$ and $C_{j,3}=0$ for any $j\neq 0$. Then by the same argument as above, substituting $\tau+\frac{1}{3}$ for τ in $f(\tau)$ and $f(3\tau)$ we obtain that $C_{1,0}=C_{1,1}=C_{1,2}=C_{1,3}=C_{2,0}=C_{2,1}=C_{2,2}=C_{2,3}=0$. So, we may write $F_3(X,Y)=C_{0,0}+C_{0,1}Y+C_{0,2}Y^2+C_{0,3}+C_{3,0}X^3+C_{3,1}X^3Y+C_{3,2}X^3Y^2$. Since $C_{0,3}\neq 0$, we let it be 1.

Now, by replacing X(respectively, Y) by the q-expansion of $f(\tau)$ (respectively, $f(3\tau)$), we conclude that $C_{0,0}=0$, $C_{0,1}=4$, $C_{0,2}=2$, $C_{3,0}=-1$, $C_{3,1}=1$ and $C_{3,2}=-1$. So, $F_3(X,Y)=4Y+2Y^2+Y^3-X^3+X^3Y-X^3Y^2$. If we multiply $F_3(\frac{1}{C(\tau)},\frac{1}{C(3\tau)})$ by $C(\tau)^3C(3\tau)^3$, our second assertion is established. $\square$

In order to extend the above results to all primes p we confine each prime p to the one relatively prime to 6 and find the relation between $f(\tau)$ and $f(p\tau)$.

Theorem 9. *Let p be a prime greater than 3. Then $F_p(X,Y)=\sum_{0\le i,j\le p+1}C_{i,j}X^iY^j\in\mathbb{Q}[X,Y]$ satisfies the following conditions.*

(1) $C_{p+1,0}\neq 0$ and $C_{p+1,1}=C_{p+1,2}=\cdots=C_{p+1,p+1}=0, C_{0,0}=0$

(2) If $p\equiv 1\mod 6$ and $i+j\equiv 0$ or $1\mod 3$, then $C_{i,j}=0$.

(3) If $p\equiv -1\mod 6$ and $i-j\equiv 1$ or $2\mod 3$, then $C_{i,j}=0$.

Proof. The congruence subgroup under consideration is $\Gamma'=\Gamma_1(6)\cap\Gamma_0(18p)$, and hence $\Delta=\{\overline{\pm(1+6k)}\in(\mathbb{Z}/18p\mathbb{Z})^\times|k=0,1,\cdots,3p-1\}$ where Δ is the subgroup as in §2. Since every integer relatively prime to 6 is congruent to ±1 modulo 6, we have to consider S_j and A_j only for $j\in\{9,18,9p,18p\}$ by Lemma 2 and 6. Since $n_j=1$ for all $j=9,18,9p$ and $18p$, $S_j=\{\overline{1}\}$. Thus all the inequivalent cusps under consideration are $\frac{1}{9},\frac{1}{18},\frac{1}{9p}$ and $\frac{1}{18p}$ with widths $2p$, p, 2 and 1, respectively by Lemma 3. And it follows from Lemma 1 that $\frac{1}{18p}$ is equivalent to ∞ . If we let $f_1(\tau)=f(\tau)$ and $f_2(\tau)=f(p\tau)$ in Theorem 7, then we know by Lemma 6 that $S_{1,\infty}=\{\frac{1}{18},\frac{1}{18p}\}$ and $S_{1,0}=\{\frac{1}{9},\frac{1}{9p}\}$. Further we obtain that $S_{2,\infty}=\{\frac{1}{18},\frac{1}{18p}\}$ and $S_{2,0}=\{\frac{1}{9},\frac{1}{9p}\}$. Now that $(f\circ\begin{pmatrix}1&0\\18&1\end{pmatrix})(\tau)=f(\tau)=q^{-1}+O(1)$ due to the fact that $\begin{pmatrix}1&0\\18&1\end{pmatrix}\in\Gamma$, we derive that $\mathrm{ord}_\infty f(\tau)=-1$ and $\mathrm{ord}_{\frac{1}{18}}f(\tau)=-p$. So the total degree d_1 of poles of $f(\tau)$ is $p+1$. Since $f(p\tau)=q^{-p}+O(1)$, we get $\mathrm{ord}_\infty f(p\tau)=-p$. In order to find $\mathrm{ord}_{\frac{1}{18}}f(p\tau)$, we first take $b,d\in\mathbb{Z}$ such that $\begin{pmatrix}1&b\\18&d\end{pmatrix}\in SL_2(\mathbb{Z})$. Since there exists $x \in \mathbb{Z}$ such that $d-6x \equiv 0 \mod p$, $\begin{pmatrix} 3p & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & b \\ 18 & d \end{pmatrix} = \begin{pmatrix} p & 3b-x \\ 6 & \frac{d-6x}{p} \end{pmatrix}\begin{pmatrix} 3 & x \\ 0 & p \end{pmatrix}$ where $\begin{pmatrix} p & 3b-x \\ 6 & \frac{d-6x}{p} \end{pmatrix} \in SL_2(\mathbb{Z})$. Thus the Fourier expansion of $f(p\tau)$ at $\frac{1}{18}$ can be derived from

$$(f \circ \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & b \\ 18 & d \end{pmatrix})(\tau) = 1/(C \circ \begin{pmatrix} 3p & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & b \\ 18 & d \end{pmatrix})(\tau) = (\frac{1}{C} \circ \begin{pmatrix} p & 3b-x \\ 6 & \frac{d-6x}{p} \end{pmatrix}\begin{pmatrix} 3 & x \\ 0 & p \end{pmatrix})(\tau)$$

by (**K1**) and (**K2**). We see by (**K4**) that the above is of the form

$$(\text{some root of unity}) \cdot q_p^k + \text{ higher order term},$$

where $k = 6(\frac{1}{2} < \frac{p}{2} > (< \frac{p}{2} > -1) - \frac{1}{2} < \frac{p}{6} > (< \frac{p}{6} > -1)) \times 3$ with the notation as in (**K4**). Considering $p \equiv \pm 1 \mod 6$ we have $k = -1$. Hence $\mathrm{ord}_{\frac{1}{18}} f(p\tau) = -1$. And the total degree d_p of poles of $f(p\tau)$ is $p+1$. Therefore $F_p(X, Y)$ is of the form $F_p(X,Y) = \sum_{0 \le i,j \le p+1} C_{i,j} X^i Y^j$. Since $S_{1,\infty} \cap S_{2,0}$ is empty, we claim that $a = 0$ in Theorem 7 and hence $C_{p+1,0} \neq 0$ and $C_{p+1,1} = C_{p+1,2} = \cdots = C_{p+1,p+1} = 0$. Interchanging the role of $f_1(\tau)$ and $f_2(\tau)$ we have $b = \mathrm{ord}_{\frac{1}{9}} f_2(\tau) + \mathrm{ord}_{\frac{1}{9p}} f_2(\tau) = p+1$ and $C_{0,0} = 0$. Then we can derive by Theorem 7 (5) all the other assertions. Next, we observe that $f_1(\tau + \frac{1}{3}) = f(\tau + \frac{1}{3}) = \frac{1}{C(3\tau+1)} = \zeta_3^2 f(\tau) = \zeta_3^2 f_1(\tau)$ and $f_2(\tau + \frac{1}{3}) = f(p(\tau + \frac{1}{3})) = \frac{1}{C(3p\tau+p)} = \zeta_3^{-p} f(p\tau)$ imply $f_2(\tau + \frac{1}{3}) = \zeta_3^2 f_2(\tau)$ (respectively, $\zeta_3 f_2(\tau)$) if $p \equiv 1 \mod 6$ (respectively, if $p \equiv -1 \mod 6$). Therefore, we establish that $i+j \equiv 0, 1 \mod 3 \Rightarrow C_{i,j} = 0$ (respectively, $i-j \equiv 1, 2 \mod 3 \Rightarrow C_{i,j} = 0$) if $p \equiv 1 \mod 6$ (respectively, if $p \equiv -1 \mod 6$). This completes the proof. □

Now we are ready to find the modular equation $\Phi_n(X,Y) = 0$ of $C(\tau)$ and $C(n\tau)$ for the case where n is a prime greater than 3. Using Theorem 9 and inserting enough terms of the Fourier expansions of $f(\tau)$ and $f(p\tau)$ into $F_p(X,Y)$ we can find $\Phi_p(X,Y) = 0$. Here we must deliberate the relation $\Phi_p(X,Y) = X^{p+1}Y^{p+1}F_p(\frac{1}{X}, \frac{1}{Y})$.

The following table shows that the coefficients of the modular equations are congruent to zero modulo p except for the ones of the terms v^{p+1}, w^{p+1}, vw and $v^p w^p$ in each case, which indicates the existence of Kronecker's congruences. Thus, we will work with the equation $\Phi_p(X,Y) = 0$ in order to find such congruences.

p	the modular equation of $v(:= C(\tau))$ and $w(:= C(p\tau))$
5	$v^6 - v^5w^5 - 5v^5(3w^5 + 2w^2) + 5v^4(4w^4 + w) - 20v^3w^3 - 5v^2(2w^5 - w^2) + 5vw^4 - vw + w^6 = 0$
7	$v^8 - v^7w^7 - 7v^7(9w^7 + 8w^4) + 28v^6w^2 - 56v^5w^3 - 7v^4(8w^7 - 3w^4 - w) - 56v^3w^5 + 28v^2w^6 + 7vw^4 - vw + w^8 = 0$
11	$v^{12} - v^{11}w^{11} - 11v^{11}(93w^{11} + 128w^8 + 32w^5 - 4w^2) - 22v^{10}(128w^{10} + 96w^7 - 34w^4 + w)$ $-44v^9(32w^9 + 28w^6 + w^3) - 11v^8(128w^{11} + 128w^8 + 28w^5 - 17w^2) - 22v^7(96w^{10} + 124w^7 - 7w^4 + w)$ $-154v^6(8w^9 + w^6 - w^3) - 22v^5(16w^{11} + 14w^8 + 31w^5 - 3w^2) + 11v^4(68w^{10} + 14w^7 - 8w^4 + w)$ $-22v^3(2w^9 - 7v^3w^6 + w^3) + 11v^2(4w^{11} + 17w^8 + 6w^5 - w^2) - 11v(2w^{10} + 2w^7 - w^4) - vw + w^{12} = 0$
13	$v^{14} - v^{13}w^{13} - 13v^{13}(315w^{13} + 512w^{10} + 192w^7 - 8w^4 - 2w) + 13v^{12}(1024w^{11} + 768w^8 - 240w^5 + 23w^2)$ $+52v^{11}(256w^{12} + 48w^9 - 186w^6 + 15w^3) - 13v^{10}(512w^{13} + 832w^{10} + 264w^7 - 132w^4 + w)$ $+26v^9(96w^{11} - 36w^8 - 194w^5 + 15w^2) + 39v^8(256w^{12} - 24w^9 - 172w^6 + 31w^3)$ $-39v^7(64w^{13} + 88w^{10} + 100w^7 - 11w^4 + w) - 39v^6(248w^{11} + 172w^8 - 3w^5 - 4w^2)$ $-13v^5(240w^{12} + 388w^9 - 9w^6 - 3w^3) + 13v^4(8w^{13} + 132w^{10} + 33w^7 - 13w^4 + w)$ $+13v^3(60w^{11} + 93w^8 + 3w^5 - 2w^2) + 13v^2(23w^{12} + 30w^9 + 12w^6 - 2w^3) + 13v(2w^{13} - w^{10} - 3w^7 + w^4) - vw + w^{14} = 0$
17	$v^{18} - v^{17}w^{17} - 17v^{17}(3855w^{17} + 8192w^{14} + 5120w^{11} + 640w^8 - 144w^5 - 2w^2)$ $+17v^{16}(16384w^{16} + 36864w^{13} + 12288w^{10} - 7488w^7 + 712w^4 - w)$ $-136v^{15}(3072w^{15} - 1024w^{12} - 2952w^9 + 1059w^6 - 79w^3)$ $-34v^{14}(4096w^{17} + 37888w^{14} + 25280w^{11} - 7512w^8 + 1001w^5 - 89w^2)$ $+17v^{13}(36864w^{16} + 33792w^{13} - 13120w^{10} - 9560w^7 + 1001w^4 + 9w)$ $+17v^{12}(8192w^{15} + 38016w^{12} + 17496w^9 - 10177w^6 + 1059w^3)$ $-34v^{11}(2560w^{17} + 25280w^{14} + 19328w^{11} - 3016w^8 + 1195w^5 - 117w^2)$ $+17v^{10}(12288w^{16} - 13120w^{13} - 26784w^{10} - 3016w^7 + 939w^4 + 5w)$ $+17v^9(23616w^{15} + 17496w^{12} - 11536w^9 - 2187w^6 + 369w^3)$ $-34v^8(320w^{17} - 7512w^{14} - 3016w^{11} + 3348w^8 - 205w^5 - 24w^2)$ $-17v^7(7488w^{16} + 9560w^{13} + 3016w^{10} + 2416w^7 - 395w^4 + 5w)$ $-17v^6(8472w^{15} + 10177w^{12} + 2187w^9 - 594w^6 + 16w^3)$ $+34v^5(72w^{17} - 1001w^{14} - 1195w^{11} + 205w^8 + 132w^5 - 18w^2)$ $+17v^4(712w^{16} + 1001w^{13} + 939w^{10} + 395w^7 - 74w^4 + w)$ $+17(632w^{15} + 1059w^{12} + 369w^9 - 16w^6 - 6w^3)$ $+17v^2(2w^{17} + 178w^{14} + 234w^{11} + 48w^8 - 18w^5 + w^2)$ $-17v(w^{16} - 9w^{13} - 5w^{10} + 5w^7 - w^4) - vw + w^{18} = 0$

As before, let $\Gamma = \Gamma_1(6) \cap \Gamma_0(18)$. For any integer a with $(a,6) = 1$, we fix $\sigma_a \in \Gamma(1)$ so that $\sigma_a \equiv \begin{pmatrix} a^{-1} & 0 \\ 0 & a \end{pmatrix}$ mod 18. Then for every positive integer a prime to 6 one has

$$\Gamma \begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix} \Gamma = \bigcup_{\substack{a>0 \\ a|n}} \bigcup_{0 \le b < \frac{n}{a}} \Gamma \sigma_a \begin{pmatrix} a & b \\ 0 & \frac{n}{a} \end{pmatrix},$$

in which the right hand side is a disjoint union. Indeed, first note that $|\Gamma \backslash \Gamma \begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix} \Gamma| = n \prod_{p|n}(1 + \frac{1}{p})$ and then use [16], Proposition 3.36.

Since σ_a depends only on a modulo 18, we fix σ_a as $\sigma_{\pm 1} = \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $\sigma_{\pm 5} = \pm \begin{pmatrix} 65 & 18 \\ 18 & 5 \end{pmatrix}$ and $\sigma_{\pm 7} = \pm \begin{pmatrix} -5 & 18 \\ 18 & -65 \end{pmatrix}$. Actually, since $\sigma_a \in (\pm 1) \cdot \Gamma$ for $a \in \{\pm 1, \pm 5, \pm 7\}$, we have $f \circ \sigma_a = f$.

For convenience, we let $\alpha_{a,b} = \sigma_a \begin{pmatrix} a & b \\ 0 & \frac{n}{a} \end{pmatrix}$ for such a, b. We now consider the following polynomial $\Psi_n(X, \tau)$ with the indeterminate X

$$\Psi_n(X, \tau) = \prod_{\substack{a>0 \\ a|n}} \prod_{\substack{0 \le b < \frac{n}{a} \\ (a,b,\frac{n}{a})=1}} (X - (f \circ \alpha_{a,b})(\tau)).$$

Note that $\deg \Psi_n(X, \tau) = n \prod_{p|n}(1 + \frac{1}{p})$. Since all the coefficients of $\Psi_n(X, \tau)$ are the elementary symmetric functions of the $f \circ \alpha_{a,b}$, they are invariant under Γ, i.e., $\Psi_n(X, \tau) \in \mathbb{C}(f(\tau))[X]$; hence we may write $\Psi_n(X, f(\tau))$ instead of $\Psi_n(X, \tau)$.

When $f(n\tau) = f_1(\tau)$ and $f(\tau) = f_2(\tau)$, we define $S_{j,\infty}$ to be the set of cusps at which $f_j(\tau)$ has pole and by $S_{j,0}$ we mean the set of cusps at which $f_j(\tau)$ has zero. And we recall from Theorem 7 that a is a nonnegative integer defined by

$$a = \begin{cases} 0 & , \text{if } S_{1,\infty} \cap S_{2,0} = \phi \\ -\sum_{s \in S_{1,\infty} \cap S_{2,0}} ord_s f_1(\tau) & , \text{otherwise.} \end{cases}$$

Then, in order to have a polynomial $F_n(X, f(\tau))$ in $\mathbb{C}[X, f(\tau)]$ which satisfies $F_n(f(\tau), f(n\tau)) = 0$, we should multiply $\Psi_n(X, f(\tau))$ by $f(\tau)^a$. However, $S_{1,\infty} \cap S_{2,0} = \phi$ due to the fact that $S_{1,\infty} = \{\frac{1}{18n}\}$ and $S_{2,\infty} = \{\frac{1}{18}, \cdots, \frac{1}{18n}\}$. Thus $a = 0$ so that we are to work with just $\Psi_n(X, f(\tau))$ as a polynomial of X and $f(\tau)$ to prove the following theorem.

Theorem 10. *With the notation as above, for any positive integer n with $(n,6) = 1$ we define $\Psi_n(X, Y)$ to be a polynomial such that $\Psi_n(f(\tau), f(n\tau)) = 0$. Then we get the following assertions.*

(1) $\Psi_n(X, Y) \in \mathbb{Z}[X, Y]$ and $\deg_X \Psi_n(X, Y) = \deg_Y \Psi_n(X, Y) = n \prod_{p|n}(1 + \frac{1}{p})$.

(2) $\Psi_n(X, Y)$ is irreducible both as a polynomial in X over $\mathbb{C}(Y)$ and as a polynomial in Y over $\mathbb{C}(X)$.

(3) $\Psi_n(X, Y) = \Psi_n(Y, X)$.

(4) If n is not a square, then $\Psi_n(X, X)$ is a polynomial of degree > 1 whose leading coefficient is ± 1.

(5) (Kronecker's congruence) Let p be an odd prime. Then

$$\Psi_p(X,Y) \equiv (X^p - Y)(X - Y^p) \mod p\mathbb{Z}[X,Y].$$

Proof. Since $f(\tau) = 1/C(3\tau)$, we let $f(\tau) = q^{-1} + \sum_{m=1}^{\infty} c_m q^m$ with $c_m \in \mathbb{Z}$. We further let $d = n\prod_{p|n}(1+\frac{1}{p})$ and let ψ_k be an automorphism of $\mathbb{Q}(\zeta_n)$ over $\mathbb{Q}$ defined by $\psi_k(\zeta_n) = \zeta_n^k$ for some integer k with $(k,n) = 1$. Then ψ_k induces an automorphism of $\mathbb{Q}(\zeta_n)((q^{\frac{1}{n}}))$ by the action on the coefficients. We denote the induced automorphism by the same notation ψ_k. Since $(f \circ \begin{pmatrix} a & b \\ 0 & \frac{n}{a} \end{pmatrix})(\tau) = f(\begin{pmatrix} a & b \\ 0 & \frac{n}{a} \end{pmatrix}\tau) = f(\frac{a^2}{n}\tau + \frac{ab}{n}) = \zeta_n^{-ab} q^{-\frac{a^2}{n}} + \sum_{m=1}^{\infty} c_m \zeta_n^{abm} q^{\frac{a^2 m}{n}}$, we obtain that $\psi_k((f \circ \begin{pmatrix} a & b \\ 0 & \frac{n}{a} \end{pmatrix})(\tau)) = \zeta_n^{-abk} q^{-\frac{a^2}{n}} + \sum_{m=1}^{\infty} c_m \zeta_n^{abkm} q^{\frac{a^2 m}{n}}$. Let b' be the unique integer such that $0 \le b' < \frac{n}{a}$ and $b' \equiv bk \bmod \frac{n}{a}$. Then $\psi_k(f \circ \begin{pmatrix} a & b \\ 0 & \frac{n}{a} \end{pmatrix}) = f \circ \begin{pmatrix} a & b' \\ 0 & \frac{n}{a} \end{pmatrix}$ because $\zeta_n^{abk} = \zeta_n^{ab'}$. And for all $a \in \{\pm 1, \pm 5, \pm 7\}$ we have $f \circ \sigma_a = f$, from which we get that $\psi_k(f \circ \alpha_{a,b}) = f \circ \alpha_{a,b'}$ and all the coefficients of $\Psi_n(X, f(\tau))$ are contained in $\mathbb{Q}((q^{\frac{1}{n}}))[X]$.

Note that $\Psi_n(f(\frac{\tau}{n}), f(\tau)) = 0$ yields $[\mathbb{C}(f(\frac{\tau}{n}), f(\tau)) : \mathbb{C}(f(\tau))] \le d$. Let $\mathfrak{F}$ be the field of all meromorphic functions on $\mathfrak{H}$ which contains $\mathbb{C}(f(\frac{\tau}{n}), f(\tau))$ as a subfield. We further observe that for any element γ of Γ the map $h(\tau) \mapsto h(\gamma(\tau))$ gives an embedding of $\mathbb{C}(f(\frac{\tau}{n}), f(\tau))$ into $\mathfrak{F}$, which is trivial on $\mathbb{C}(f(\tau))$. Also, note that for any $\alpha_{a,b}$ there exists $\gamma_{a,b} \in \Gamma$ such that $\begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix} \gamma_{a,b}\alpha_{a,b}^{-1} \in \Gamma$. Since $f(\alpha_{a,b}(\tau)) \ne f(\alpha_{a',b'}(\tau))$ for $\alpha_{a,b} \ne \alpha_{a',b'}$, there are at least d distinct embeddings of $\mathbb{C}(f(\frac{\tau}{n}), f(\tau))$ into $\mathfrak{F}$ over $\mathbb{C}(f(\tau))$ defined by $f(\frac{\tau}{n}) \mapsto f \circ \begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix} \circ \gamma_{a,b} = f(\alpha_{a,b}(\tau))$. Hence $[\mathbb{C}(f(\frac{\tau}{n}), f(\tau)) : \mathbb{C}(f(\tau))] = d$. This implies that $\Psi_n(X, f(\tau))$ is irreducible over $\mathbb{C}(f(\tau))$. Now that $\Psi_n(X, f(\tau))$ is an irreducible polynomial of $f(\frac{\tau}{n})$ over $\mathbb{C}(f(\tau))$ and $\Psi_n(f(\frac{\tau}{n}), Y)$ is also an irreducible polynomial of $f(\tau)$ over $\mathbb{C}(f(\frac{\tau}{n}))$, we derive the fact that $\Psi_n(X,Y)$ is irreducible both as a polynomial in X over $\mathbb{C}(Y)$ and as a polynomial in Y over $\mathbb{C}(X)$. On the other hand, since $\Psi_n(X, f(\tau)) \in \mathbb{Q}[X, f(\tau)]$ and all the Fourier coefficients of $\Psi_n(X, f(\tau))$ are algebraic integers, we conclude that $\Psi_n(X,Y) \in \mathbb{Z}[X,Y]$. It proves (1) and (2).

Now that $(X - (f \circ \alpha_{n,0})(\tau))$ is a factor of $\Phi_n(X, f(\tau))$ and $f \circ \alpha_{n,0} = f \circ \sigma_n \circ \begin{pmatrix} n & 0 \\ 0 & 1 \end{pmatrix} = f \circ \begin{pmatrix} n & 0 \\ 0 & 1 \end{pmatrix}$, we get $\Psi_n(f(n\tau), f(\tau)) = 0$, namely $\Psi_n(f(\tau), f(\frac{\tau}{n})) = 0$. Hence, $f(\frac{\tau}{n})$ is a root of the equation $\Psi_n(f(\tau), X) = 0$ and $\Psi_n(f(\tau), X) \in \mathbb{Z}[X, f(\tau)]$. Meanwhile, $f(\frac{\tau}{n})$ is also a root of $\Psi_n(X, f(\tau)) = 0$ and $\Psi_n(X, f(\tau))$ is irreducible over $\mathbb{C}(f(\frac{\tau}{n}))$. So there exists a polynomial $g(X, f(\tau)) \in \mathbb{Z}[X, f(\tau)]$ such that $\Psi_n(f(\tau), X) = g(X, f(\tau))\Psi_n(X, f(\tau))$. However, the identity

$$\Psi_n(f(\tau), X) = g(X, f(\tau)) \cdot g(f(\tau), X) \cdot \Psi_n(f(\tau), X)$$

implies $g(X, f(\tau)) = \pm 1$. If $g(X, f(\tau)) = -1$, $\Psi_n(f(\tau), f(\tau)) = -\Psi_n(f(\tau), f(\tau))$. Thus, $f(\tau)$ is a root of $\Psi_n(X, f(\tau)) = 0$, which is a contradiction to the irreducibility of $\Psi_n(X, f(\tau))$ over $\mathbb{C}(f(\tau))$. Therefore, (3) is proved.

As for the verification of (4), we assume that n is not a square. Then $f(\tau)-(f\circ\alpha_{a,b})(\tau) = q^{-1}-\zeta_n^{-ab}q^{-\frac{a^2}{n}}+O(q^{\frac{1}{n}})$. And, the coefficient of the lowest degree in $\Psi_n(f(\tau),f(\tau))$ is a unit. Since it is an integer and $\Psi_n(X,X)$ is a polynomial of degree >1, (4) is proved.

In order to justify the last assertion, let p be a prime greater than 3. For $g(\tau),h(\tau)\in\mathbb{Z}[\zeta_p]((q^{\frac{1}{n}}))$ and $\alpha\in\mathbb{Z}[\zeta_p]$, we know that $g(\tau)\equiv h(\tau) \bmod \alpha$ if $g(\tau)-h(\tau)\in\alpha\mathbb{Z}[\zeta_p]((q^{\frac{1}{p}}))$. On the other hand, since $f(\tau)=q^{-1}+\sum_{m=1}^{\infty}c_mq^m$ with $c_m\in\mathbb{Z}$, we deduce that

$$\begin{aligned} f(\alpha_{1,b}(\tau)) &= \zeta_p^{-b}q^{-\frac{1}{p}}+\sum_{m=1}^{\infty}c_m\zeta_p^{bm}q^{\frac{m}{p}} \\ &\equiv q^{-\frac{1}{p}}+\sum_{m=1}^{\infty}c_mq^{\frac{m}{p}} \mod (1-\zeta_p). \end{aligned}$$

Hence, $f(\alpha_{1,b}(\tau))\equiv f(\alpha_{1,0}(\tau)) \bmod (1-\zeta_p)$ for any $b=0,\cdots,p-1$. And, by making use of the relation $c_m^p\equiv c_m \bmod p$ we see that

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

So, $f(\alpha_{p,0}(\tau))\equiv f(\tau)^p \bmod (1-\zeta_p)$. In a similar way we get $f(\alpha_{1,0}(\tau))^p=(q^{-\frac{1}{p}}+\sum_{m=1}^{\infty}c_mq^{\frac{m}{p}})^p\equiv q^{-1}+\sum_{m=1}^{\infty}c_m^pq^m=f(\tau) \bmod (1-\zeta_p)$. Thus we achieve that

$$\begin{aligned} \Psi_p(X,f(\tau)) &= \prod_{0\le b<p}(X-f(\alpha_{1,b}(\tau)))\times(X-f(\alpha_{p,0}(\tau))) \\ &\equiv (X-f(\alpha_{1,0}(\tau))^p(X-f(\tau)^p)\equiv(X^p-f(\alpha_{1,0}(\tau))^p)(X-f(\tau)^p) \\ &\equiv (X^p-f(\tau))(X-f(\tau)^p) \mod (1-\zeta_p). \end{aligned}$$

Now, let $\Psi_p(X,f(\tau))-(X^p-f(\tau))(X-f(\tau)^p)$ be $\sum_\nu\psi_\nu(f(\tau))X^\nu\in(1-\zeta_p)\mathbb{Z}[X,f(\tau)]$, where $\psi_\nu(f(\tau))\in\mathbb{Z}[f(\tau)]$. Since all the Fourier coefficients of $\psi_\nu(f(\tau))$ are rational integers and divisible by $1-\zeta_p$, we obtain that $\psi_\nu(f(\tau))\in p\mathbb{Z}[f(\tau)]$. Therefore $\Psi_p(X,f(\tau))\equiv(X^p-f(\tau))(X-f(\tau)^p) \bmod p\mathbb{Z}[X,f(\tau)]$. □

4. Constructions of ray class fields and class polynomials

Let K be an imaginary quadratic field and N be a positive integer. Let $K_{(N)}$ be the ray class field modulo N over K and $\tau\in K\cap\mathfrak{H}$ be a root of the primitive equation $ax^2+bx+c=0$ such that $b^2-4ac=d_K$ where d_K is the discriminant of K. In this section we show that $C(\tau)$ generates $K_{(6)}$ over K and then find the class polynomial of $K_{(6)}$ by using the fact that $\frac{1}{C(\tau)}$ is an algebraic integer.

We first consider the principal congruence subgroup $\Gamma(N)$ of $SL_2(\mathbb{Z})$ as the kernel of the map $SL_2(\mathbb{Z})\to SL_2(\mathbb{Z}/N\mathbb{Z})$ obtained by reducing the entries modulo N. If h is a meromorphic function on the modular curve $X(N)=\Gamma(N)\backslash\mathfrak{H}^*$, its Laurent series expansion in the parameter $q^{\frac{1}{N}}=e^{\frac{2\pi i}{N}\tau}$ is called the Fourier expansion of h. Embedding the algebraic closure $\overline{\mathbb{Q}}$ of the rational numbers into $\mathbb{C}$ we see that $X(N)$ can be defined over $\mathbb{Q}(\zeta_N)$, and hence let F_N be its function field over $\mathbb{Q}(\zeta_N)$. Then one can have $F_1 = \mathbb{Q}(j)$ and define the automorphic function field $\mathfrak{F}$ as the union $\mathfrak{F} = \bigcup_{N\geq 1} F_N$. For a subfield $\mathfrak{F}'$ of $\mathfrak{F}$ and $z \in K$, the notation $K \cdot \mathfrak{F}'(z)$ in the following theorem means the compositum of K and the field $\mathfrak{F}'(z)$ which is generated over $\mathbb{Q}$ by $\{h(z)|h \in \mathfrak{F}'$ and h is defined and finite at $z\}$.

Theorem 11. *Let K be an imaginary quadratic field and $\tau \in K \cap \mathfrak{H}$ be a root of the primitive equation $aX^2 + bX + c = 0$ with $a, b, c \in \mathbb{Z}$ such that its discriminant is the field discriminant of K. Let x (respectively, y) be the least positive integer such that $x = (Nx, a)$ (respectively, $y = (Ny, c)$), and let*

$$\begin{aligned}
\mathfrak{F}^{(1)}_{min} &= \mathbb{Q}(j, j \circ \begin{pmatrix} Nx & 0 \\ 0 & 1 \end{pmatrix}, f_{\begin{pmatrix} 0 & \frac{1}{N} \end{pmatrix}}), \\
\mathfrak{F}^{(2)}_{min} &= \text{the field of all automorphic functions for } \Gamma_0(Nx) \cap \Gamma_1(N) \\
&\quad\ \text{with rational Fourier coefficients,} \\
\mathfrak{F}^{(3)}_{min} &= \text{the field of all automorphic functions for } \Gamma_0(Ny) \cap \Gamma^1(N) \\
&\quad\ \text{with rational Fourier coefficients,} \\
\mathfrak{F}^{(4)}_{min} &= \mathbb{Q}(j, j \circ \begin{pmatrix} 1 & 0 \\ 0 & Ny \end{pmatrix}, f_{\begin{pmatrix} 0 & \frac{1}{N} \end{pmatrix}} \circ \begin{pmatrix} 1 & 0 \\ 0 & Ny \end{pmatrix}), \\
\mathfrak{F}_{max} &= \text{the field of all automorphic functions for } \Gamma^0(Nc) \cap \Gamma_0(Na) \cap \Gamma(N) \\
&\quad\ \text{whose Fourier coefficients with respect to } e^{2\pi iz/Nc} \text{ belong to } \mathbb{Q}(\zeta_N).
\end{aligned}$$

Then for any field $\mathfrak{F}'$ in the hypothesis, $K \cdot \mathfrak{F}'(z)$ is the ray class field modulo N over K. Furthermore, if $\mathfrak{F}''$ is any intermediate field such that $\mathfrak{F}^{(i)}_{min} \subset \mathfrak{F}'' \subset \mathfrak{F}_{max}$ for some i $(1 \leq i \leq 4)$ or $F_N \subset \mathfrak{F}'' \subset \mathfrak{F}_{max}$, then $K \cdot \mathfrak{F}''(z)$ is also the ray class field modulo N over K.

Proof. Theorem 29 in [6]. □

Lemma 12. *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 let Γ' be any congruence subgroup containing $\Gamma(N)$ and contained in $\Gamma_1(N)$. Suppose that $(N, a) = 1$. Then the field generated over K by all the values $h(\tau)$, where $h \in A_0(\Gamma')_{\mathbb{Q}}$ is defined and finite at τ, is the ray class field modulo N over K.*

Proof. With the notations as in Theorem 11, if $(N, a) = 1$ then x in the theorem is equal to 1. Therefore the inclusions $\mathfrak{F}^{(2)}_{min} = A_0(\Gamma_1(N))_{\mathbb{Q}} \subset A_0(\Gamma')_{\mathbb{Q}} \subset A_0(\Gamma(N))_{\mathbb{Q}} \subset F_N \subset \mathfrak{F}_{max}$ imply the lemma. □

Theorem 13. *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 $b^2 - 4ac = d_K$. Then $K(C(\tau))$ is the ray class field modulo 6 over K if $(6, a) = 1$. In particular, if $\mathbb{Z}[\tau]$ is the ring of integers in K, then $K(C(\tau))$ is the ray class field modulo 6 over K.*

Proof. Since $C(\tau)$ is a Hauptmodul for $\Gamma_1(6) \cap \Gamma^0(3)$ with rational Fourier coefficients and $\Gamma(6) \subset \Gamma_1(6) \cap \Gamma^0(3) \subset \Gamma_1(6)$, we get the first assertion by Lemma 12. In particular, if $\mathbb{Z}[\tau]$ is the ring of integers in K, then $a = 1$ and hence we readily conclude the last statement. □

Next, we show that $\frac{1}{C(\tau)}$ is an algebraic integer for an imaginary quadratic argument τ, which helps us to approximate the coefficients of class polynomial.

Theorem 14. *Let K be an imaginary quadratic field with discriminant d_K and $t = \mathcal{N}(j_{1,N})$ be the normalized generator of $A_0(\Gamma_1(N))$. Let s be a cusp of $\Gamma_1(N)$ whose width is h_s and $S_{\Gamma_1(N)}$ is the set of inequivalent cusps of $\Gamma_1(N)\backslash\mathfrak{H}^*$. If $t \in q^{-1}\mathbb{Z}[[q]]$ and $\prod_{s\in S_{\Gamma_1(N)}-\{\infty\}}(t(z)-t(s))^{h_s}$ is a polynomial in $\mathbb{Z}[t]$, then $t(\tau)$ is an algebraic integer for $\tau \in K\cap\mathfrak{H}$.*

Here we call f the normalized generator of $A_0(\Gamma)$ for a congruence subgroup Γ associated to the genus zero modular curve $\Gamma\backslash\mathfrak{H}^*$, if its q-expansion starts with $q^{-1}+0+a_1q+a_2q^2+\cdots$.

Proof. See [13]. □

Lemma 15. *The normalized generator of $A_0(\Gamma_1(6))$ is $\frac{1}{C^3(\tau)} - 3$.*

Proof. Let $g(\tau) = \frac{1}{C^3(\tau)}$. It follows from Theorem 4 that $\mathbb{C}(C(\tau)) = A_0(\Gamma_1(6)\cap\Gamma^0(3))$. Since $\Gamma_1(6)\cap\Gamma^0(3)$ is a subgroup of $\Gamma_1(6)$ with index 3, for $\gamma \in \Gamma_1(6)\cap\Gamma^0(3)$ we deduce $g\circ\gamma = g$. Furthermore, using $C\circ\begin{pmatrix}1&1\\0&1\end{pmatrix}(\tau) = e^{\frac{2\pi i}{3}}C(\tau)$ we have $g\circ\begin{pmatrix}1&1\\0&1\end{pmatrix} = g$. But, $\Gamma_1(6)$ $=<\Gamma_1(6)\cap\Gamma^0(3), \begin{pmatrix}1&1\\0&1\end{pmatrix}>$, and so $\mathbb{C}(g(\tau)) \subset A_0(\Gamma_1(6))$. Observing $[A_0(\Gamma_1(6)) : \mathbb{C}(g(\tau))] = \frac{[\mathbb{C}(C(\tau)):\mathbb{C}(g(\tau))]}{[A_0(\Gamma_1(6)\cap\Gamma^0(3)):A_0(\Gamma_1(6))]} = \frac{[\mathbb{C}(C(\tau)):\mathbb{C}(g(\tau))]}{[\Gamma_1(6):\Gamma_1(6)\cap\Gamma^0(3)]} = 1$ we see that $g(\tau)$ is a generator of $A_0(\Gamma_1(6))$ with pole at ∞. And at ∞ we can easily find a q-expansion $g(\tau) = q^{-1}+3+a_1q+a_2q^2+\cdots$. Therefore, the normalized generator of $\Gamma_1(6)$ is $\frac{1}{C^3(\tau)} - 3$. □

Theorem 16. *Let K be an imaginary quadratic field with discriminant d_K and $\tau \in K\cap\mathfrak{H}$. Then $\frac{1}{C(\tau)}$ is an algebraic integer.*

Proof. We see by Lemma 15 that the normalized generator $t(\tau)$ is $\frac{1}{C^3(\tau)} - 3 \in q^{-1}\mathbb{Z}[[q]]$. And, before we go further we recall that h_s is the width of the cusp s and $\zeta_m = e^{\frac{2\pi i}{m}}$. Since $\overline{\Gamma_0(6)} = \overline{\Gamma_1(6)}$, we have $S_{\Gamma_1(6)} = \{\infty, 0, \frac{1}{2}, \frac{1}{3}\}$.

(i)

$$C\circ\begin{pmatrix}0&-1\\1&0\end{pmatrix}(\tau) = \zeta_{12}^5\prod_{j=0}^{5}\frac{\mathfrak{k}_{\left(\frac{1}{6}\ \ \frac{j}{6}\right)}}{\mathfrak{k}_{\left(\frac{3}{6}\ \ \frac{j}{6}\right)}}\begin{pmatrix}0&-1\\1&0\end{pmatrix}(\tau) = \zeta_{12}^5\prod_{j=0}^{5}\frac{\mathfrak{k}_{\left(\frac{j}{6}\ \ -\frac{1}{6}\right)}}{\mathfrak{k}_{\left(\frac{j}{6}\ \ -\frac{3}{6}\right)}}(\tau)$$

$= \zeta_{12}^5\prod_{j=0}^{5}\exp\pi i\{(-\frac{1}{6})(\frac{j}{6}-1) - (-\frac{3}{6})(\frac{j}{6}-1)\}\frac{1-\zeta_6^{-1}}{1-\zeta_6^{-3}}\times(1+O(q)) = \frac{1}{2}+O(q)$. So,

$$C(0) = \lim_{\tau\to\infty} C\circ\begin{pmatrix}0&-1\\1&0\end{pmatrix}(\tau) = \lim_{q\to0}\frac{1}{2}+O(q) = \frac{1}{2}.$$

Thus we get $t(0) = \frac{1}{C^3(0)} - 3 = 5$.

(ii)

$$C\circ\begin{pmatrix}1&0\\2&1\end{pmatrix}(\tau) = \zeta_{12}^5\prod_{j=0}^{5}\frac{\mathfrak{k}_{\left(\frac{1+2j}{6}\ \ \frac{j}{6}\right)}}{\mathfrak{k}_{\left(\frac{3+2j}{6}\ \ \frac{j}{6}\right)}}(\tau) = 1+O(q).$$

Then, $C(\frac{1}{2}) = \lim_{q\to0}(1+O(q)) = 1$ yields $t(\frac{1}{2}) = -2$.

(iii)

$$C \circ \begin{pmatrix} 1 & 0 \\ 3 & 1 \end{pmatrix}(\tau) = \zeta_{12}^5 \prod_{j=0}^{5} \frac{\mathfrak{k}_{\left(\frac{1+3j}{5} \ \frac{j}{6}\right)}}{\mathfrak{k}_{\left(\frac{3+3j}{6} \ \frac{j}{6}\right)}}(\tau).$$

We know by (**K5**) in §2 that $\mathrm{ord}_q C \circ \begin{pmatrix} 1 & 0 \\ 3 & 1 \end{pmatrix}(\tau) = -\frac{1}{6}$. In other words, $C(\tau)$ has a pole at $\frac{1}{3}$ and $t(\frac{1}{3}) = \frac{1}{C^3(\tau)} - 3 = -3$.

On the other hand, if follows from Lemma 3 that $h_0 = 6, h_{\frac{1}{2}} = 3$ and $h_{\frac{1}{3}} = 2$. Hence, the polynomial $\prod_{s \in S_{\Gamma_1(6)} - \{\infty\}}(t(z)-t(s))^{h_s}$ becomes $(t-5)^6(t+2)^3(t+3)^2$ so that it belongs to $\mathbb{Z}[t]$. Then we conclude by Theorem 14 that $\frac{1}{C^3(\tau)} - 3$ is an algebraic integer for $\tau \in K \cap \mathfrak{H}$. Therefore $\frac{1}{C(\tau)}$ is an algebraic integer, too. $\square$

We see from Theorem 13 that if an imaginary quadratic number θ generates the ring of integers in $K = \mathbb{Q}(\theta)$, then $K(C(\theta))$ is the ray class field modulo 6 over K. In this case to find its class polynomial we shall use the Shimura's reciprocity law by adopting the idea of Gee([9]).

We first consider the finite Galois extension $F_1 \subset F_N$. Let $\alpha_N \in SL_2(\mathbb{Z}/N\mathbb{Z})$ represent the $\Gamma(N)$-equivalence class of a linear fractional transformation $\alpha \in SL_2(\mathbb{Z})$ on $\mathfrak{H}^*$. For $h \in F_N$, the action $h^{\alpha_N} = h \circ \alpha$ is well defined and induces an isomorphism $SL_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1\} \cong \mathrm{Gal}(F_N/F_1(\zeta_N)) = \mathrm{Gal}(\mathbb{C} \cdot F_N/\mathbb{C} \cdot F_1)$. And for $d \in (\mathbb{Z}/N\mathbb{Z})^\times$, let σ_d denote the automorphism of $\mathbb{Q}(\zeta_N)$ given by $\zeta_N \mapsto \zeta_N^d$. Then the action of σ_d gives rise to a natural isomorphism $\mathrm{Gal}(F_1(\zeta_N)/F_1) \cong \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \cong (\mathbb{Z}/N\mathbb{Z})^\times$, which we can lift to F_N by changing $h = \sum_k c_k q^{\frac{k}{N}} \in F_N$ to $h^{\sigma_d} = \sum_k \sigma_d(c_k) q^{\frac{k}{N}}$. Thus $h \mapsto h^{\sigma_d}$ defines a group action of $(\mathbb{Z}/N\mathbb{Z})^\times$ on F_N whose invariant field $F_{N,\mathbb{Q}}$ is the subfield of F_N having Fourier coefficients in $\mathbb{Q}$. Here we have $F_{N,\mathbb{Q}} \cap F_1(\zeta_N) = F_1$.

Now, define the subgroup $G_N = \{\begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix} | d \in (\mathbb{Z}/N\mathbb{Z})^\times\}$ of $GL_2(\mathbb{Z}/N\mathbb{Z})$. Then the map $(\mathbb{Z}/N\mathbb{Z})^\times \simeq G_N$ gives an isomorphism $G_N \cong \mathrm{Gal}(F_N/F_{N,\mathbb{Q}})$. From this fact we get the following exact sequence

$$\{\pm 1\} \to GL_2(\mathbb{Z}/N\mathbb{Z}) \to \mathrm{Gal}(F_N/F_1) \to 1.$$

Passing to the projective limit we then have an exact sequence

$$1 \to \{\pm 1\} \to GL_2(\widehat{\mathbb{Z}}) \to \mathrm{Gal}(\mathfrak{F}/F_1) \to 1.$$

Let $K_p = \mathbb{Q}_p \otimes_{\mathbb{Q}} K$ and $\mathcal{O}_p = \mathbb{Z}_p \otimes_{\mathbb{Z}} \mathcal{O}$ for the ring of integer $\mathcal{O} = \mathbb{Z}[\theta]$ of K. By the main theorem of complex multiplication $j(\theta)$ generates the Hilbert class field over K and the maximal abelian extension K^{ab} is equal to $K(\mathfrak{F}(\theta))$. Moreover, the sequence

$$1 \to \mathcal{O}^\times \to \prod_p \mathcal{O}_p^\times \to \mathrm{Gal}(K^{ab}/K(j(\theta))) \to 1$$

is exact. Here the map $\prod_p \mathcal{O}_p^\times \to \mathrm{Gal}(K^{ab}/K(j(\theta)))$ is the Artin map $[\sim, K]$. In addition, the ray class field modulo N over K is $K(F_N(\theta))$ and the subgroup of $\prod_p \mathcal{O}_p^\times$ which acts trivially on $K(F_N(\theta))$ with respect to the Artin map is generated by $\mathcal{O}^\times$ and $\prod_p((1 + N\mathcal{O}_p) \cap \mathcal{O}_p^\times)$.

Let J_K^f be the finite idéles $\prod'_p K_p^\times$ of K. The restricted product is taken with respect to the subgroup $\mathcal{O}_p^\times \subset K_p^\times$. For every prime p we consider the map $(g_\theta)_p$ defined by $(g_\theta)_p : K_p^\times \to GL_2(\mathbb{Q}_p)$ as the injection satisfying $(g_\theta)_p(x_p)\begin{pmatrix}\theta\\1\end{pmatrix} = x_p\begin{pmatrix}\theta\\1\end{pmatrix}$. Since $\mathbb{Z}[\theta]$ is the ring of integers of K, θ has the minimal polynomial $X^2+BX+C \in \mathbb{Z}[X]$ which satisfies $\theta^2 + B\theta + C = 0$. Then for s_p and $t_p \in \mathbb{Q}_p$ we explicitly have

$$(g_\theta)_p : s_p\theta + t_p \mapsto \begin{pmatrix} t_p - B\cdot s_p & -C\cdot s_p \\ s_p & t_p \end{pmatrix}.$$

Therefore on J_K^f we get an injective map $g_\theta = \prod_p (g_\theta)_p : J_K^f \to \prod'_p GL_2(\mathbb{Q}_p)$. Here the restricted product is taken with respect to the subgroups $GL_2(\mathbb{Z}_p) \subset GL_2(\mathbb{Q}_p)$. Moreover, $g_\theta^{-1}(GL_2(\widehat{\mathbb{Z}})) = \prod_p \mathcal{O}_p^\times$. So we get the row exact diagram

$$\begin{array}{ccccccccc} 1 & \to & \mathcal{O}^\times & \to & \prod_p \mathcal{O}_p^\times & \xrightarrow{[\sim, K]} & \mathrm{Gal}(K^{ab}/K(j(\theta))) & \to & 1 \\ & & & & \downarrow g_\theta & & & & \\ 1 & \to & \{\pm 1\} & \to & GL_2(\widehat{\mathbb{Z}}) & \to & \mathrm{Gal}(\mathfrak{F}/F_1) & \to & 1. \end{array}$$

And by the Shimura reciprocity law, $h(\theta)^{[x^{-1},K]} = h^{(g_\theta(x))}(\theta)$ for $h \in \mathfrak{F}$ and $x \in \prod_p \mathcal{O}_p^\times$. For a positive integer N, $g_\theta^{-1}(Stab_{F_N}) = \prod_p((1+N\mathcal{O}_p)\cap \mathcal{O}_p^\times)$ where $Stab_{F_N}$ is the inverse image of $\mathrm{Gal}(\mathfrak{F}/F_N)$ in $GL_2(\widehat{\mathbb{Z}})$. Using the isomorphism $g_\theta^{-1}(Stab_{F_1})/g_\theta^{-1}(Stab_{F_N}) \simeq (\mathcal{O}/N\mathcal{O})^\times$ we define the reduction map $g_{\theta,N}$ of g_θ modulo N from $(\mathcal{O}/N\mathcal{O})^\times$ to $GL_2(\mathbb{Z}/N\mathbb{Z})$. Define $W_{N,\theta} = g_{\theta,N}((\mathcal{O}/N\mathcal{O})^\times) \subset GL_2(\mathbb{Z}/N\mathbb{Z})$. Precisely speaking, $W_{N,\theta}$ is a finite subgroup $\{\begin{pmatrix} t-Bs & -Cs \\ s & t\end{pmatrix} \in GL_2(\mathbb{Z}/N\mathbb{Z}) | t, s \in \mathbb{Z}/N\mathbb{Z}\}$.

Theorem 17. *Let K be an imaginary quadratic field of discriminant d_K and $\theta = \frac{\sqrt{d_K}}{2}$ (respectively, $\frac{3+\sqrt{d_K}}{2}$) if $d \equiv 0 \mod 4$ (respectively, $d \equiv 1 \mod 4$), and let $Q = [a,b,c]$ be a primitive positive definite quadratic form of discriminant d_K and τ_Q denote $\frac{-b+\sqrt{d_K}}{2} \in \mathfrak{H}$. Define $u = (u_p)_p \in \prod_p GL_2(\mathbb{Z}_p)$ as follows. (p runs over all rational primes.)*

<u>*Case 1 : $d \equiv 0$ mod 4*</u>

$$u_p = \begin{cases} \begin{pmatrix} a & \frac{b}{2} \\ 0 & 1 \end{pmatrix} & , \text{ if } p \nmid a, \\ \begin{pmatrix} -\frac{b}{2} & -c \\ 1 & 0 \end{pmatrix} & , \text{ if } p|a \text{ and } p \nmid c, \\ \begin{pmatrix} -a-\frac{b}{2} & -c-\frac{b}{2} \\ 1 & -1 \end{pmatrix} & , \text{ if } p|a \text{ and } p|c. \end{cases}$$

<u>*Case 2 : $d \equiv 1$ mod 4*</u>

$$u_p = \begin{cases} \begin{pmatrix} a & \frac{3+b}{2} \\ 0 & 1 \end{pmatrix} & , \text{ if } p \nmid a, \\ \begin{pmatrix} \frac{3-b}{2} & -c \\ 1 & 0 \end{pmatrix} & , \text{ if } p|a \text{ and } p \nmid c, \\ \begin{pmatrix} -a+\frac{3-b}{2} & -c-\frac{3+b}{2} \\ 1 & -1 \end{pmatrix} & , \text{ if } p|a \text{ and } p|c. \end{cases}$$

Then $h(\theta)^{[a,-b,c]} = h^u(\tau_Q)$ for any $h \in \mathcal{F}$ such that $h(\theta) \in K(j(\theta))$.

Proof. See [9]. □

With the notations as above, if $h \in F_p$ for a prime p, then $h(\theta)^{[a,-b,c]} = h^{u_p}(\tau_Q)$ because the action h^u depends only on the $p-$component. Here we observe that our continued fraction $C(\tau)$ is contained in F_6. Let $f(\tau) = \frac{1}{C(\tau)}$. Then $f(\theta)^{[a,-b,c]} = f^{(u_2,u_3,u_5,\cdots)}(\tau_Q) = f^{M_Q}(\tau_Q)$ where $M_Q \in M_2(\mathbb{Z}) \cap GL_2^+(\mathbb{Q})$ satisfies $M_Q \equiv u_p \mod 6$ for all primes p. Therefore, we may take $M_Q = 3u_2 - 2u_3 \in GL_2(\mathbb{Z}/6\mathbb{Z})$.

Let H be the Hilbert class field of K. Then there is a surjective homomorphism of $W_{N,\theta}$ onto $\mathrm{Gal}(K_{(N)}/H)$ defined by $\alpha \mapsto (h(\tau) \mapsto h^{\alpha^{-1}}(\theta))$. Let C be the kernel of this surjection. In fact, C is the image of $g_\theta(\mathcal{O}_K^\times)$ in $GL_2(\mathbb{Z}/N\mathbb{Z})$. Since $\mathrm{Gal}(K_{(N)}/K)/\mathrm{Gal}(K_{(N)}/H)$ is isomorphic to $\mathrm{Gal}(H/K) \cong C(d_K)$, where $C(d_K)$ is the form class group of discriminant d_K. Thus, the image of the homomorphism

$$C(d_K) \to \mathrm{Gal}(K_{(N)}/K)$$

$$[Q]^{-1} \mapsto (h(\theta) \mapsto h^{M_Q}(\theta))$$

gives all the coset representatives of $\mathrm{Gal}(K_{(N)}/H)$ in $\mathrm{Gal}(K_{(N)}/K)$. Hence, we obtain that $\{h^{\alpha \cdot M_Q} \mid \alpha \in W_{N,\theta}/C$ and Q is any reduced primitive quadratic form of discriminant $d_K\}$ is the set of all the conjugates of $h(\theta)$ over K.

Let $F(X) = \prod_{\alpha \in W_{6,\theta}/C,\ Q \in C(d_K)} (X - f^{\alpha \cdot M_Q}(\tau_Q)) \in K[X]$ be the minimal polynomial of $f(\theta)$ over K. Then, $F(X)$ is in $\mathbb{Z}[X]$. Indeed, since f has rational Fourier coefficients and $e^{\frac{2\pi i\theta}{3}} \in \mathbb{R}$ for θ defined in Theorem 17, $f(\theta)$ is always real. Observing $0 = F(f(\theta)) = \overline{F(f(\theta))} = \overline{F}(\overline{f(\theta)}) = \overline{F}(f(\theta))$ we see that $F(X) \in (K \cap \mathbb{R})[X] = \mathbb{Q}[X]$. Furthermore, $f(\theta)$ is an algebraic integer by Theorem 16 so that $F(X)$ is a polynomial with integral coefficients, that is, $F(X) \in \mathbb{Z}[X]$.

Now before closing this section we present an example with $K = \mathbb{Q}(\sqrt{-3})$ as follows.

Proposition 18. *Let $K = \mathbb{Q}(\sqrt{-3})$ be an imaginary quadratic field and $K_{(6)}$ be the ray class field of K modulo 6. And let $F(X)$ be the class polynomial of $K_{(6)}$. Then $F(X) = X^3 + 6X^2 + 4$.*

Proof. If $K = \mathbb{Q}(\sqrt{-3})$, then we have $\theta = \frac{3+\sqrt{-3}}{2}$ and $d_K = -3$. We may assume that a positive definite quadratic form Q is $[1,1,1]$ and $\tau_Q = \frac{-1+\sqrt{-3}}{2}$. Then as is well known it is the unique reduced primitive quadratic form of discriminant -3. It follows from Theorem

17 that $u_2 = u_3 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$, $M_Q = 3u_2 - 2u_3 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \in GL_2(\mathbb{Z}/6\mathbb{Z})$. And $B = -3, C = 3$ because $\theta^2 - 3\theta + 3 = 0$. Using these we get $W_{6,\theta}$ and C as follows.

$$\begin{aligned} W_{6,\theta} = \{ & \pm\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \pm\begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}, \pm\begin{pmatrix} 1 & 0 \\ 4 & 1 \end{pmatrix}, \pm\begin{pmatrix} 2 & 3 \\ 3 & 5 \end{pmatrix}, \\ & \pm\begin{pmatrix} 2 & 3 \\ 5 & 5 \end{pmatrix}, \pm\begin{pmatrix} 2 & 3 \\ 1 & 5 \end{pmatrix}, \pm\begin{pmatrix} 1 & 3 \\ 3 & 4 \end{pmatrix}, \pm\begin{pmatrix} 1 & 3 \\ 1 & 4 \end{pmatrix}, \pm\begin{pmatrix} 1 & 3 \\ 5 & 4 \end{pmatrix}\} \\ C = \{ & \pm\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \pm\begin{pmatrix} 1 & -3 \\ 1 & -2 \end{pmatrix}, \pm\begin{pmatrix} 2 & -3 \\ 1 & -1 \end{pmatrix}\}. \end{aligned}$$

So, $W_{6,\theta}/C$ has 3 distinct cosets $\left[\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right], \left[\begin{pmatrix} -2 & -3 \\ 1 & 1 \end{pmatrix}\right], \left[\begin{pmatrix} 1 & 0 \\ 4 & 1 \end{pmatrix}\right]$. Therefore $\{f^{\left(\begin{smallmatrix} 1 & 2 \\ 0 & 1 \end{smallmatrix}\right)}(\frac{-1+\sqrt{-3}}{2}), f^{\left(\begin{smallmatrix} -2 & -3 \\ 1 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & 2 \\ 0 & 1 \end{smallmatrix}\right)}(\frac{-1+\sqrt{-3}}{2}), f^{\left(\begin{smallmatrix} 1 & 0 \\ 4 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & 2 \\ 0 & 1 \end{smallmatrix}\right)}(\frac{-1+\sqrt{-3}}{2})\} = \{f(\frac{3+\sqrt{-3}}{2}), f(\frac{-2\theta-3}{\theta+1}), f(\frac{\theta}{4\theta+1})\}$ is the set of all the conjugates of $f(\theta)$ over K. Hence, through the approximation of these three values by using the fact $F(X) \in \mathbb{Z}[X]$ we get $F(X) = (X - f(\frac{3+\sqrt{-3}}{2}))(X - f(\frac{-2\theta-3}{\theta+1}))(X - f(\frac{\theta}{4\theta+1})) = X^3 + 6X^2 + 4$. □

By means of the same arguments we have the following class polynomials whose coefficients seem to be relatively small when compared with others' works, for examples, Morain([15]), Kaltofen-Yui([12]) and Chen-Yui([5]).

d_K	the class polynomial of $K_{(6)}$
-3	$X^3 + 6X^2 + 4$
-4	$X^4 - 8X^3 - 8X - 8$
-7	$X^4 + 16X^3 - 8X + 16$
-8	$X^4 - 20X^3 + 12X^2 + 16X - 8$
-11	$X^6 + 30X^5 - 72X^4 + 8X^3 + 120X^2 + 16$
-15	$X^6 + 60X^5 + 132X^4 + 56X^3 + 96X^2 + 96X + 64$
-19	$X^{12} + 96X^{11} + 232X^9 - 1440X^8 + 960X^6 + 4608X^5 + 256X^3 + 6144X^2 + 256$

References

1. C. Adiga, T. Kim, M.S. Mahadeva Naika and H.S. Madhusudhan, *On ramanujan's cubic continied fraction and explicit evaluations of theta-functions*, Indian J. Pure Appl. Math. 35(2004), no. 9, 1047-1062.
2. N. D. Baruah, *Modular equations for Ramanujan's cubic continued fraction*, J. Math. Anal. Appl. 268 (2002), 244-255.
3. B. Cais and B. Conrad, *Modular curves and Ramanujan's continued fraction*, J. Reine Angew. Math. 597 (2006), 27-104.
4. H. H. Chan, *On Ramanujan's cubic continued fraction*, Acta Arith. 73 (1995), no. 4, 343-355.
5. I. Chen and N. Yui, *Singular values of Thompson series*, Groups, difference sets, and the Monster, Ohio State Univ. Math. Res. Inst. Publ., 4(ed. K. Arasu, J. Dillon, K. Harada, S. Sehgal and R. Solomon), de Gruyter, Berlin, 1996, 255-326.
6. B. Cho and J. K. Koo, *Construction of class fields over imaginary quadratic fields*, submitted.
7. B. Cho, J. K. Koo and Y. K. Park, *Arithmetic of the Ramanujan-Göllnitz-Gordon continued fraction*, preprint.
8. W. Duke, *Continued fractions and modular functions*, Bull. Amer. Math. Soc. 42 (2005), no. 2, 137-162.
9. A. Gee, *Class invariants by Shimura's reciprocity law*, J. Theor. Nombres Bordeaux 11 (1999), no. 1, 45-72.

10. A. Gee and M. Honsbeek, *Singular values of the Rogers-Ramanujan continued fraction*, Ramanujan J. 11 (2006), no. 3, 267-284.
11. N. Ishida and N. Ishii, *The equations for modular function fields of principal congruence subgroups of prime level*, Manuscripta Math. 90 (1996), no. 3, 271-285.
12. E. Kaltofen and N. Yui, *Explicit construction of the Hilbert class fields of imaginary quadratic fields by integer lattice reduction*, Number theory, 149-202, Springer, New York, 1991.
13. C. H. Kim and J. K. Koo, *Super-replicable functions* $\mathcal{N}(j_{1,N})$ *and periodically vanishing property* , J. Korean Math. Soc. 44(2007), no. 2, 343-371.
14. D. Kubert and S. Lang, *Modular Units*, Springer-Verlag, New York-Berlin, 1981.
15. F. Morain, *Implementation of the Atkin-Goldwasser-Kilian primality testing algorithm*, draft, 1988.
16. G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Princeton University Press, 1971.

Department of Mathematical Sciences, Korea Advanced Institute of Science and Technology, 373-1 Guseong-dong, Yuseong-gu, Daejeon 305-701, Korea

Bumkyu Cho,
E-mail address: bam@math.kaist.ac.kr

Ja Kyung Koo,
E-mail address: jkkoo@math.kaist.ac.kr

Yoon Kyung Park,
E-mail address: ykpark@math.kaist.ac.kr