ARITHMETIC OF THE RAMANUJAN-GÖLLNITZ-GORDON CONTINUED FRACTION

BUMKYU CHO, JA KYUNG KOO, AND YOON KYUNG PARK

Abstract. We extend the results of Chan-Huang ([4]) and Vasuki-Srivatsa Kumar ([14]) to all odd primes p on the modular equations of the Ramanujan-Göllnitz-Gordon continued fraction $v(\tau)$ by computing the affine models of modular curves $X(\Gamma)$ with $\Gamma = \Gamma_1(8) \cap \Gamma_0(16p)$. We then deduce the Kronecker congruence relations for these modular equations. And, by showing that $v(\tau)$ is a modular unit over $\mathbb{Z}$ we give a new proof of the fact that the singular values of $v(\tau)$ are units at all imaginary quadratic arguments and further obtain that they generate ray class fields modulo 8 over imaginary quadratic fields.

1. Introduction

The well known Rogers-Ramanujan continued fraction is a holomorphic function $r(\tau)$ on the complex upper half plane $\mathfrak{H}$ defined by

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

where $q = e^{2\pi i\tau}$ and $(\frac{n}{5})$ is the Legendre symbol. In his first letter to Hardy, dated 1913, Ramanujan gave its value at $\tau = i$ as a radical expression

$$r(i) = \cfrac{e^{-\frac{2\pi}{5}}}{1+\cfrac{e^{-2\pi}}{1+\cfrac{e^{-4\pi}}{1+\cfrac{e^{-6\pi}}{1+\cdots}}}} = \sqrt{\frac{5+\sqrt{5}}{2}} - \frac{\sqrt{5}+1}{2}.$$

He also gave some other values at $\tau = \frac{5+i}{2}$, $\sqrt{-5}$, $\frac{5+\sqrt{-5}}{2}$, $\frac{-1+\sqrt{-3}}{2}$ ([1], [7]). And he further stated that $r(\frac{\sqrt{-n}}{2})$ can be exactly found whenever n is any positive rational quantity. However, the existence of radical expressions is nowadays clear by the class

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.

field theory. Precisely speaking, since $r(\tau)$ becomes a modular function as a Hauptmodul for the principal congruence subgroup $\Gamma(5)$ ([8]), any singular value of $r(\tau)$ at imaginary quadratic argument is contained in some ray class field over an imaginary quadratic field, and so the splitting field of its minimal polynomial is abelian, namely its Galois group is solvable. Thus the minimal polynomial is solvable by radicals. But the problem is how to find such radical expressions explicitly. Gee and Honsbeek ([8]) recently treated and settled down this problem by using the Shimura reciprocity law, and asserted that their method can be applied to any other similar problems.

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.

n	mathematician (year)
2	Rogers (1920)
3	Rogers (1920)
4	Andrews, Berndt, Jacobsen, Lamphere (1992)
5	Rogers (1920), Watson (1929), Ramanathan (1984)
7	Yi (2001)
11	Rogers (1920)

Recently, the modular equations of the Rogers-Ramanujan continued fraction are deeply studied and settled down by Cais and Conrad ([3]), whose arguments rely on the theory of arithmetic models of modular curves. They further found the Kronecker congruence relations for the modular equations which is similar to the one of the elliptic modular function $j(\tau)$. We will consider the same problem with the Ramanujan-Göllnitz-Gordon continued fraction defined below, but unlike Cais and Conrad's approach we establish by finding affine models of some modular curves from the standard theory of algebraic functions (see [10]).

Now the Ramanujan-Göllnitz-Gordon continued fraction $v(\tau)$ is defined by

$$v(\tau) = V(q) = \cfrac{q^{\frac{1}{2}}}{1+q+\cfrac{q^2}{1+q^3+\cfrac{q^4}{1+q^5+\cfrac{q^6}{1+q^7+\cdots}}}} = q^{\frac{1}{2}}\prod_{n=1}^{\infty}\frac{(1-q^{8n-7})(1-q^{8n-1})}{(1-q^{8n-5})(1-q^{8n-3})}.$$

In this case its singular values at some imaginary quadratic arguments in terms of radicals were studied by Chan and Huang ([4]), but Gee and Honsbeek's method can also be applied to this situation. Therefore we will not go into this direction any further.

On the other hand there are some modular equations with $v := v(\tau)$ and $w := v(n\tau)$ on a case-by-case basis as follows.

n	mathematician (year)	equation
2	Chan-Huang (1997)	$v^2 = w\frac{1-w}{1+w}$
3	Chan-Huang (1997)	$3vw(1-vw)(v+w)+(v^3-w)(1+vw^3)=0$
4	Chan-Huang (1997)	$v=\sqrt{\sqrt{(\frac{2w(1-w)}{1+w^2})^2+\frac{w(1-w)}{1+w}}-\frac{2w(1-w)}{1+w^2}}$
5	Vasuki-Srivatsa Kumar (2006)	$v^5-w+5v^2w-10v^2w^3-10v^3w^4$ $+10v^3w^2-5v^4w^5+10v^4w^3+v^6w^5$ $-5v^5w^2+5vw^4-vw^6=0$
7	Vasuki-Srivatsa Kumar (2006)	$v^8-7v^7w-(vw)^7-7v^7w^3+7v^7w^5$ $+28v^6w^2+7v^5w^7-7v^5w-49(vw)^5-7v^5w^3$ $+70(vw)^4+7v^3w-7v^3w^7-7v^3w^5-49(vw)^3$ $+28v^2w^6-vw-7vw^7-7vw^5+7vw^3+w^8=0$

Vasuki and Srivatsa Kumar also estimated the modular equation of order 11 ([14]). For more backgrounds of $r(\tau)$ and $v(\tau)$ we refer to [1] and [7].

If we let $\Phi_n(X,Y)=0$ be the above modular equation of order n, namely, $\Phi_n(v,w)=0$ with $w=v(n\tau)$, then it is worth of noting that

$$\Phi_3(X,Y)\equiv(X^3-Y)(1+XY^3) \bmod 3$$

and

$$\Phi_5(X,Y)\equiv(X^5-Y)(1+XY^5) \bmod 5.$$

Moreover for the case $n=7$ we see that

$$\Phi_7(X,Y)\equiv(X^7-Y)(X-Y^7) \bmod 7.$$

One of our results is to show that these Kroneckerian models can be formulated as follows: for any odd prime p

$$\Phi_p(X,Y)\equiv\begin{cases}(X^p-Y)(1+XY^p) \bmod p & \text{if } p\equiv\pm3 \bmod 8\\ (X^p-Y)(X-Y^p) \bmod p & \text{if } p\equiv\pm1 \bmod 8.\end{cases}$$

We first extend in §3 the above known results systematically by providing an algorithm to all odd primes p (, namely $w=v(p\tau)$) on the modular equations of the Ramanujan-Göllnitz-Gordon continued fraction and then as remarked above we give an analytic proof of the Kronecker congruence relations for these modular equations (Theorem 10). Secondly, although it is known that any singular value of $v(\tau)$ at imaginary quadratic argument is a unit ([4] §5 or [7] §9), we provide a new proof in §4 by showing that $v(\tau)$ is a modular unit over $\mathbb{Z}$. Finally, since $v(\tau)$ is a modular function, its singular values may generate some class fields. To be more precise, now that $v(\tau)$ is a Hauptmodul for $\Gamma_1(8)\cap\Gamma^0(2)$ (Theorem 5), we obtain in Theorem 15 that with some conditions on an imaginary quadratic argument the singular value of $v(\tau)$ generates the ray class field modulo 8 over arbitrary imaginary quadratic field. Those our methods can also be applied to the Rogers-Ramanujan continued fraction $r(\tau)$ as will be remarked at the end of §4. In §2 we present some basic and necessary preliminaries about modular functions and Klein forms, and give several lemmas about the cusps of a congruence subgroup which will be used in §3.

2. Preliminaries

Let $\mathfrak{H} = \{\tau \in \mathbb{C} | \text{ Im } \tau > 0\}$ be the complex upper half plane, $\mathfrak{H}^* = \mathfrak{H} \cup \mathbb{Q} \cup \{\infty\}$ and let $\Gamma(N) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) | a \equiv d \equiv 1 \bmod N, b \equiv c \equiv 0 \bmod N\}$ be the *principal congruence subgroup* of level N for any positive integer N. Here we mainly utilize congruence subgroups such as $\Gamma_0(N)$, $\Gamma^0(N)$ and $\Gamma_1(N)$ where $\Gamma_0(N)$ (respectively, $\Gamma^0(N)$, $\Gamma_1(N)$) consists of all $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ such that $c \equiv 0 \bmod N$ (respectively, $b \equiv 0 \bmod N$, $a \equiv d \equiv 1 \bmod N$ and $c \equiv 0 \bmod N$). Further let $A_0(\Gamma)$ be the field of all modular functions with respect to Γ and $A_0(\Gamma, \mathbb{Q})$ be the field of all modular functions $f(\tau)$ with respect to Γ such that the Fourier expansion of $f(\tau)$ has rational coefficients.

¿From now on we briefly recall the Klein forms, which is mainly used in this paper. We refer to [11] for more details. For any lattice $L \subset \mathbb{C}$ and $z \in \mathbb{C}$, we define the *Weierstrass σ-function* by

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

which is holomorphic with only simple zeros at all points $z \in L$. We further define the *Weierstrass ζ-function* by the logarithmic derivative of the Weierstrass σ-function, i.e.,

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

which is meromorphic with only simple poles at all points $z \in L$. It is easy to see that the Weierstrass σ-function (respectively, the Weierstrass ζ-function) is homogeneous of degree 1 (respectively, -1), that is, $\sigma(\lambda z; \lambda L) = \lambda \sigma(z; L)$ (respectively, $\zeta(\lambda z; \lambda L) = \lambda^{-1} \zeta(z; L)$) for any $\lambda \in \mathbb{C}^\times$. Note that $\zeta'(z; L) = -\wp(z; L)$ where

$$\wp(z; L) = \frac{1}{z^2} + \sum_{\omega \in L - \{0\}} (\frac{1}{(z - \omega)^2} - \frac{1}{\omega^2})$$

is the *Weierstrass $\wp$-function*. Since the Weierstrass $\wp$-function is an elliptic function, namely $\wp(z + \omega; L) = \wp(z; L)$ for $\omega \in L$, we obtain that $\frac{d}{dz}(\zeta(z + \omega; L) - \zeta(z; L)) = 0$ for any $\omega \in L$. This means that $\zeta(z + \omega; L) - \zeta(z; L)$ depends only on $\omega \in L$, not on $z \in \mathbb{C}$. Thus we may define $\eta(\omega; L) = \zeta(z + \omega; L) - \zeta(z; L)$ for all $\omega \in L$. Let $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$. For $z = a_1\omega_1 + a_2\omega_2$ with $a_1, a_2 \in \mathbb{R}$ we define the *Weierstrass η-function* by

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

Then it is easy to see that the Weierstrass η-function $\eta(z; L)$ is well-defined, in other words it does not depend on the choice of the basis $\{\omega_1, \omega_2\}$ of L, and $\eta(z; L)$ is $\mathbb{R}$-linear so that $\eta(rz; L) = r\eta(z; L)$ for any $r \in \mathbb{R}$. Note that since the Weierstrass ζ-function is

homogeneous of degree -1, so is the Weierstrass η-function. We now define the *Klein form* by

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

Let $\mathbf{a}=(a_1\ a_2)\in\mathbb{R}^2$ and $\tau\in\mathfrak{H}$. We further define $K_{\mathbf{a}}(\tau)=K(a_1\tau+a_2;\mathbb{Z}\tau+\mathbb{Z})$ which is also called the *Klein form* by abuse of terminology. Here we observe that $K_{\mathbf{a}}(\tau)$ is holomorphic and nonvanishing on $\mathfrak{H}$ if $\mathbf{a}\in\mathbb{R}^2-\mathbb{Z}^2$ and that the Klein form is homogeneous of degree 1, i.e., $K(\lambda z;\lambda L)=\lambda K(z;L)$.

The Klein form satisfies the following well-known properties (see [11]). Let $\gamma=\begin{pmatrix}a & b\\ c & d\end{pmatrix}\in SL_2(\mathbb{Z})$ and $\mathbf{a}\in\mathbb{R}^2$.

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

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

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

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

(**K4**) Let $\tau\in\mathfrak{H}$, $z=a_1\tau+a_2$ with $\mathbf{a}=(a_1\ a_2)\in\mathbb{Q}^2-\mathbb{Z}^2$ 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

$$K_{\mathbf{a}}(\tau)=-\frac{1}{2\pi i}e^{\pi ia_2(a_1-1)}q^{\frac{1}{2}a_1(a_1-1)}(1-q_z)\prod_{n=1}^{\infty}\frac{(1-q^nq_z)(1-q^nq_z^{-1})}{(1-q^n)^2}$$

and $\mathrm{ord}_qK_{\mathbf{a}}(\tau)=\frac{1}{2}<a_1>(<a_1>-1)$ where $<a_1>$ denotes the rational number such that $0\le<a_1><1$ and $a_1-<a_1>\in\mathbb{Z}$.

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

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

We remark that if the condition $k=0$ is omitted in **K5**, then $f(\tau)$ becomes a modular form of weight k with respect to $\Gamma(N)$.

For later use we now consider the set of all inequivalent cusps of some congruence subgroup Γ which can be achieved from the standard methods in [13].

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 as follows. $(\overline{c_1}, \overline{d_1}) \sim (\overline{c_2}, \overline{d_2})$ 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 the map ϕ is well-defined and bijective, and so 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 $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \in \Gamma(1)$. Then we have

$$\begin{aligned} & \tfrac{a}{c} \text{ and } \tfrac{a'}{c'} \text{ are equivalent under } \Gamma \\ \iff & \Gamma \begin{pmatrix} a & b \\ c & d \end{pmatrix} \Gamma(1)_\infty = \Gamma \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \Gamma(1)_\infty \\ \iff & [(\bar{c}, \bar{d})] = [(\overline{c'}, \overline{d'})] \\ \iff & \exists\, \bar{s} \in \Delta,\ \bar{n} \in \mathbb{Z}/mN\mathbb{Z} \text{ s.t. } \overline{c'} = \bar{s}\bar{c},\ \overline{d'} = \bar{s}\bar{d} + \bar{n}\bar{c}. \end{aligned}$$

Since $ad - bc = a'd' - b'c' = 1$, the last statement is equivalent to the first one of the followings. Note that

$$\begin{aligned} & \exists\, \bar{s} \in \Delta,\ \bar{n} \in \mathbb{Z}/mN\mathbb{Z} \text{ s.t. } \overline{c'} = \bar{s}\bar{c},\ \overline{(ad-bc)} \cdot \overline{d'} = \bar{s} \cdot \overline{(a'd'-b'c')} \cdot \bar{d} + \bar{n}\bar{c} \\ \iff & \exists\, \bar{s} \in \Delta,\ \bar{n} \in \mathbb{Z}/mN\mathbb{Z} \text{ s.t. } \overline{c'} = \bar{s}\bar{c},\ \bar{a}\overline{dd'} = \bar{s}\overline{a'}\,\overline{dd'} + \bar{n}\bar{c} \\ \iff & \exists\, \bar{s} \in \Delta,\ \bar{n} \in \mathbb{Z}/mN\mathbb{Z} \text{ s.t. } \overline{c'} = \bar{s}\bar{c},\ \bar{a} = \bar{s}\overline{a'} + \bar{n}\bar{c} \end{aligned}$$

by observing $(\overline{dd'}, \bar{c}) = \bar{1}$. This completes the proof. □

For any 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 $n_c = \varphi(\frac{mN}{c})/|\pi_{\frac{mN}{c}}(\Delta)|$. 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 $\pi_{\frac{mN}{c}}(\overline{s_{c,i}}) = \overline{s'_{c,i}}$. With the notations as above, we let

$$S_c = \{s_{c,1}, \cdots, s_{c,n_c}\} \subset \mathbb{Z}$$

be such a set that $0 < s_{c,1}, \cdots, s_{c,n_c} \leq mN$, $(s_{c,i}, mN) = 1$ and $s_{c,i}$ is the representative of $\overline{s_{c,i}}$ for every $i = 1, \cdots, n_c$.

On the other hand, 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 $\pi_c(\Delta \cap \mathrm{Ker}(\pi_{\frac{mN}{c}}))$ in $(\mathbb{Z}/c\mathbb{Z})^\times$, where $m_c = \varphi(c)/|\pi_c(\Delta \cap \mathrm{Ker}(\pi_{\frac{mN}{c}}))| = \varphi(c)|\pi_{\frac{mN}{c}}(\Delta)|/|\pi_{\frac{mN}{(c,\frac{mN}{c})}}(\Delta)|$. 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 $\pi_c(\overline{a_{c,j}}) = \overline{a'_{c,j}}$. We further let

$$A_c = \{a_{c,1}, \cdots, a_{c,m_c}\} \subset \mathbb{Z}$$

be such that $0 < a_{c,1}, \cdots, a_{c,m_c} \le mN$, $(a_{c,j}, mN) = 1$ 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*

$$\begin{aligned} S \;=\; & \{(\bar{c}\cdot\overline{s_{c,i}}, \overline{a_{c,j}}) \in \mathbb{Z}/mN\mathbb{Z} \times \mathbb{Z}/mN\mathbb{Z} \mid s_{c,i} \in S_c,\ a_{c,j} \in A_c \\ & \text{for every positive divisor } c \text{ of } mN\}. \end{aligned}$$

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 $\bar{y} = \overline{a_{c,j}}$. 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

$$M' = \{(\bar{c}, \bar{a}) \in \mathbb{Z}/mN\mathbb{Z} \times \mathbb{Z}/mN\mathbb{Z} \mid (\bar{c}, \bar{a}) = \bar{1},\ \text{i.e., } (c, a, mN) = 1\}$$

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 of S into $M'/\sim$ 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 $c, c' \,|\, mN$, we obtain $c = c'$; hence

$$\begin{aligned} \pi_{\frac{mN}{c}}(\overline{s_{c,i'}}) = \pi_{\frac{mN}{c}}(\bar{s})\cdot\pi_{\frac{mN}{c}}(\overline{s_{c,i}}) \;&\Longrightarrow\; \overline{s'_{c,i'}} \in \pi_{\frac{mN}{c}}(\Delta)\overline{s'_{c,i}} \\ &\Longrightarrow\; \overline{s'_{c,i'}} = \overline{s'_{c,i}} \\ &\Longrightarrow\; i' = i \;\Longrightarrow\; \pi_{\frac{mN}{c}}(\bar{s}) = \bar{1}, \end{aligned}$$

in other words $\bar{s} \in \Delta \cap \mathrm{Ker}(\pi_{\frac{mN}{c}})$. Thus $\pi_c(\overline{a_{c,j'}}) = \pi_c(\bar{s}^{-1})\pi_c(\overline{a_{c,j}}) \in (\mathbb{Z}/c\mathbb{Z})^\times$ implies $\overline{a'_{c,j'}} \in \pi_c(\Delta \cap \mathrm{Ker}(\pi_{\frac{mN}{c}}))\overline{a'_{c,j}}$, from which we get $j' = j$, that is, $a_{c,j'} = a_{c,j}$.

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

$$\overline{\left(\frac{c'}{c}\right)} \in \pi_{\frac{mN}{c}}(\Delta)\overline{s'_{c,i}} = \pi_{\frac{mN}{c}}(\Delta)\pi_{\frac{mN}{c}}(\overline{s_{c,i}})$$

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 $\overline{a'} \in \pi_c(\Delta \cap \mathrm{Ker}(\pi_{\frac{mN}{c}}))\overline{a'_{c,j}}$ 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 suffices to show 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 $\pi_c(\bar{s}) = \overline{a'}^{-1}\overline{a'_{c,j}} \in \pi_c(\Delta \cap \mathrm{Ker}(\pi_{\frac{mN}{c}})) \subset (\mathbb{Z}/c\mathbb{Z})^\times$, which is equivalent to prove the following isomorphisms

$$\pi_{\frac{mN}{(c,\frac{mN}{c})}}(\Delta)/\pi_{\frac{mN}{(c,\frac{mN}{c})}}(\Delta \cap \mathrm{Ker}(\pi_{\frac{mN}{c}})) \cong \pi_{\frac{mN}{c}}(\Delta)$$
$$\pi_{\frac{mN}{(c,\frac{mN}{c})}}(\Delta \cap \mathrm{Ker}(\pi_{\frac{mN}{c}})) \cong \pi_c(\Delta \cap \mathrm{Ker}(\pi_{\frac{mN}{c}}))$$

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 $\pi_{\frac{mN}{(c,\frac{mN}{c})}}(\Delta \cap \mathrm{Ker}(\pi_{\frac{mN}{c}}))$. As for the second, let $\bar{s} \in \Delta \cap \mathrm{Ker}(\pi_{\frac{mN}{c}})$ be such that $\pi_c(\bar{s}) = \bar{1} \in (\mathbb{Z}/c\mathbb{Z})^\times$. Then $s \equiv 1 \bmod \frac{mN}{c}$ and $s \equiv 1 \bmod c$, which implies $s \equiv 1 \bmod \frac{mN}{(c,\frac{mN}{c})}$. This completes the proof. □

The above lemma 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 $\frac{\pm 1}{0}$ as ∞. Then the width h of the cusp $\frac{a}{c}$ in $\Gamma\backslash\mathfrak{H}^*$ is*

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

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

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \begin{pmatrix} 1 - ach & * \\ -c^2h & 1 + ach \end{pmatrix} \in \{\pm 1\} \cdot (\Gamma_1(N) \cap \Gamma_0(mN)).$$

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 we have

$$\begin{pmatrix} 1 - ach & * \\ -c^2h & 1 + ach \end{pmatrix} \in \Gamma_1(N) \cap \Gamma_0(mN).$$

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 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 $N = lcm(N_3, N_4, N_5)$ and

$$\alpha = \begin{pmatrix} lcm(N_2, N_4, N_5) & 0 \\ 0 & 1 \end{pmatrix}, \ m = lcm(N_1, N_3, N_5)lcm(N_2, N_4, N_5)/N.$$

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 rise to a set of all the inequivalent cusps of Γ.

If we restrict the congruence subgroup Γ to $\Gamma_0(N)$, $\Gamma_1(N)$ or $\Gamma(N)$, then the above lemmas may be reduced to simpler statements as follows.

Corollary 4. *Let $a, c, a', c' \in \mathbb{Z}$ be such that $(a, c) = 1$ and $(a', c') = 1$. We understand that $\frac{\pm 1}{0} = \infty$. Further we denote by S_Γ a set of all the inequivalent cusps of a congruence subgroup Γ. Then we have the following assertions.*

(1) $\frac{a}{c}$ and $\frac{a'}{c'}$ are equivalent under $\Gamma_0(m)$ if and only if there exists $\bar{s} \in (\mathbb{Z}/m\mathbb{Z})^\times$ 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 m. Furthermore we can take $S_{\Gamma_0(m)}$ as the following set

$$\begin{aligned} S_{\Gamma_0(m)} \ = \ \{\tfrac{a_{c,j}}{c} \in \mathbb{Q} \mid c > 0, \ c|m, \ 0 < a_{c,j} \le m, \ (a_{c,j}, m) = 1, \\ a_{c,j} = a_{c,j'} \Longleftrightarrow a_{c,j} \equiv a_{c,j'} \ mod \ (c, \tfrac{m}{c})\} \end{aligned}$$

and the width of the cusp $\frac{a}{c}$ in $\Gamma_0(m)\backslash\mathfrak{H}^*$ is $m/(m, c^2)$.

(2) $\frac{a}{c}$ and $\frac{a'}{c'}$ are equivalent under $\Gamma_1(N)$ if and only if there exists $n \in \mathbb{Z}$ such that $\begin{pmatrix} a' \\ c' \end{pmatrix} \equiv \pm \begin{pmatrix} a + nc \\ c \end{pmatrix}$ mod N. And we can take $S_{\Gamma_1(N)}$ to be the set

$$\begin{aligned} S_{\Gamma_1(N)} \ = \ \{\tfrac{y_{c,j}}{x_{c,i}} \in \mathbb{Q} \mid c > 0, \ c|N, \ 0 < s_{c,i}, a_{c,j} \le N, \ (s_{c,i}, N) = (a_{c,j}, N) = 1, \\ s_{c,i} = s_{c,i'} \Longleftrightarrow s_{c,i} \equiv \pm s_{c,i'} \ mod \ \tfrac{N}{c}, \\ a_{c,j} = a_{c,j'} \Longleftrightarrow a_{c,j} \equiv \pm a_{c,j'} \ mod \ c \ if \ c = \tfrac{N}{2} \ or \ N, \\ a_{c,j} = a_{c,j'} \Longleftrightarrow a_{c,j} \equiv a_{c,j'} \ mod \ c \ otherwise, \\ choose \ x_{c,i}, y_{c,j} \in \mathbb{Z} \ such \ that \ (x_{c,i}, y_{c,j}) = 1 \ and \\ x_{c,i} \equiv c \cdot s_{c,i} \ mod \ N \ and \ y_{c,j} \equiv a_{c,j} \ mod \ N\} \end{aligned}$$

and the width h of the cusp $\frac{a}{c}$ in $\Gamma_1(N)\backslash\mathfrak{H}^*$ is

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

(3) $\frac{a}{c}$ *and* $\frac{a'}{c'}$ *are equivalent under* $\Gamma(M)$ *if and only if* $\begin{pmatrix} a' \\ c' \end{pmatrix} \equiv \pm \begin{pmatrix} a \\ c \end{pmatrix}$ *mod* M. *Further, we can take* $S_{\Gamma(M)}$ *as the set*

$$\begin{aligned} S_{\Gamma(M)} \;=\; \{ & \tfrac{My_{c,j}}{x_{c,i}} \in \mathbb{Q} \mid c>0,\ c|M^2,\ 0<s_{c,i},a_{c,j}\le M^2,\ (s_{c,i},M)=(a_{c,j},M)=1, \\ & s_{c,i}=s_{c,i'} \Longleftrightarrow s_{c,i} \equiv \pm s_{c,i'} \ mod\ (M,\tfrac{M^2}{c}), \\ & a_{c,j}=a_{c,j'} \Longleftrightarrow a_{c,j} \equiv \pm a_{c,j'} \ mod\ (c,\tfrac{M^3}{c(M,\frac{M^2}{c})}) \ if\ (M,\tfrac{M^2}{c})=1 \ or\ 2, \\ & a_{c,j}=a_{c,j'} \Longleftrightarrow a_{c,j} \equiv a_{c,j'} \ mod\ (c,\tfrac{M^3}{c(M,\frac{M^2}{c})}) \ otherwise, \\ & choose\ x_{c,i},y_{c,j} \in \mathbb{Z}\ such\ that\ (x_{c,i},y_{c,j})=1\ and \\ & x_{c,i} \equiv c\cdot s_{c,i}\ mod\ M^2\ and\ y_{c,j} \equiv a_{c,j}\ mod\ M^2\} \end{aligned}$$

and the width of any cusp in $\Gamma(M)\backslash\mathfrak{H}^*$ *is* M.

Proof. Let $\Gamma=\Gamma_1(N)\cap\Gamma_0(mN)$. If $\Gamma=\Gamma_0(m)$, i.e., $N=1$, then $\Delta=(\mathbb{Z}/m\mathbb{Z})^\times$; hence $S_c=\{1\}\subset\mathbb{Z}$ for any positive divisor c of m. Since

$$a_{c,j}=a_{c,j'} \Longleftrightarrow a_{c,j} \equiv a_{c,j'} \bmod c$$

and

$$a_{c,j} \equiv a_{c,j'} \bmod \frac{m}{c} \Longleftrightarrow a_{c,j} \equiv a_{c,j'} \bmod (c,\frac{m}{c})$$

we obtain the assertion (1) by observing $(c,a_{c,j})=1$.

Now we consider the case $\Gamma=\Gamma_1(N)$, namely $m=1$. Since $\Delta=\{\overline{\pm 1}\}\subset(\mathbb{Z}/N\mathbb{Z})^\times$, we have

$$s_{c,i}=s_{c,i'} \Longleftrightarrow s_{c,i} \equiv \pm s_{c,i'} \bmod \frac{N}{c}.$$

Note that $\Delta\cap\ \mathrm{Ker}(\pi_{\frac{N}{c}})=\{\overline{\pm 1}\}$ if $c=\frac{N}{2}$ or N, and $\Delta\cap\ \mathrm{Ker}(\pi_{\frac{N}{c}})=\{\bar{1}\}$ otherwise. Hence we get the assertion (2).

To prove (3), we first observe that $\alpha^{-1}\Gamma(M)\alpha=\Gamma_1(M)\cap\Gamma_0(M^2)$ with $\alpha=\begin{pmatrix} M & 0 \\ 0 & 1 \end{pmatrix}$. Thus we consider the case $N=m=M$. Since $\Delta=\{\overline{\pm(1+Mk)} \mid k=0,\cdots,M-1\}\subset(\mathbb{Z}/M^2\mathbb{Z})^\times$, we have

$$s_{c,i}=s_{c,i'} \Longleftrightarrow s_{c,i} \equiv \pm s_{c,i'} \bmod (M,\frac{M^2}{c}).$$

Observe that we have

$$\Delta\cap\mathrm{Ker}(\pi_{\frac{M^2}{c}})=\overline{\{1+\frac{M^3}{c(M,\frac{M^2}{c})}k \mid k\in\mathbb{Z}\}\cup\{-1+Mr\frac{2}{(M,\frac{M^2}{c})}+\frac{M^3}{c(M,\frac{M^2}{c})}k \mid k\in\mathbb{Z}\}}$$

with an integer r satisfying $r\cdot\frac{M}{(M,\frac{M^2}{c})}\equiv 1 \bmod \frac{M^2}{c(M,\frac{M^2}{c})}$ if $(M,\frac{M^2}{c})=1$ or 2, and we have

$$\Delta\cap\mathrm{Ker}(\pi_{\frac{M^2}{c}})=\overline{\{1+\frac{M^3}{c(M,\frac{M^2}{c})}k \mid k\in\mathbb{Z}\}}$$

otherwise. Now that

$$\pi_c(\Delta \cap \mathrm{Ker}(\pi_{\frac{M^2}{c}})) = \begin{cases} \overline{\{\pm(1+\frac{M^3}{c(M,\frac{M^2}{c})}k) \mid k \in \mathbb{Z}\}} \subset (\mathbb{Z}/c\mathbb{Z})^\times & \text{if } (M, \frac{M^2}{c}) = 1 \text{ or } 2 \\ \overline{\{1+\frac{M^3}{c(M,\frac{M^2}{c})}k \mid k \in \mathbb{Z}\}} \subset (\mathbb{Z}/c\mathbb{Z})^\times & \text{otherwise,} \end{cases}$$

therefore we establish the assertion (3). This completes the proof. □

3. Modular equations and Kronecker's congruences

By definition, a Hauptmodul for some congruence subgroup Γ of genus zero is a modular function $f(\tau)$ with respect to Γ such that $A_0(\Gamma) = \mathbb{C}(f(\tau))$. First, we note that

$$v(\tau) = q^{\frac{1}{2}} \prod_{n=1}^{\infty} \frac{(1-q^{8n-7})(1-q^{8n-1})}{(1-q^{8n-5})(1-q^{8n-3})} = -\zeta_{16}^{-1} \prod_{j=0}^{7} \frac{K_{(1/8\ j/8)}(\tau)}{K_{(3/8\ j/8)}(\tau)}$$

by **K4** where $\zeta_n = e^{2\pi i/n}$, and so $v(\tau)$ is a modular function with respect to $\Gamma(8)$ by **K5**. Meanwhile, it was shown by Duke ([7]) that $v^2(\tau)$ is a Hauptmodul for $\Gamma_1(8)$.

Theorem 5. *The Ramanujan-Göllnitz-Gordon continued fraction $v(\tau)$ is a Hauptmodul for $\Gamma_1(8) \cap \Gamma^0(2)$.*

Proof. It is not hard to see that $v^2(\tau)$ is indeed a Hauptmodul for $\Gamma_1(8)$ because we know the transformation formulas of the Klein form (see [7]). If we let $\mathbb{C}(v(\tau)) = A_0(\Gamma)$ for some Γ, then $2 = [\mathbb{C}(v(\tau)) : \mathbb{C}(v^2(\tau))] = [\Gamma_1(8) : \Gamma]$. As stated above, since $v(\tau)$ is invariant under $\Gamma(8)$, Γ contains $\Gamma(8)$. Note that $\Gamma_1(8) \cap \Gamma^0(2) = <\Gamma(8), \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}>$ and $[\Gamma_1(8) : \Gamma_1(8) \cap \Gamma^0(2)] = 2$. So if $v \circ \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} = v$ holds, then $\Gamma_1(8) \cap \Gamma^0(2) \subset \Gamma \subset \Gamma_1(8)$; hence

$$\begin{aligned} 2 &= [\Gamma_1(8) : \Gamma_1(8) \cap \Gamma^0(2)] \\ &= [\Gamma_1(8) : \Gamma][\Gamma : \Gamma_1(8) \cap \Gamma^0(2)] \\ &= 2[\Gamma : \Gamma_1(8) \cap \Gamma^0(2)] \end{aligned}$$

implies $\Gamma = \Gamma_1(8) \cap \Gamma^0(2)$. Therefore it remains to verify that $v \circ \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} = v$. By using the transformation formulas **K1** and **K2** we obtain

$$v \circ \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} = -\zeta_{16}^{-1} \prod_{j=0}^{7} \frac{K_{(1/8\ (2+j)/8)}(\tau)}{K_{(3/8\ (6+j)/8)}(\tau)} = -\zeta_{16}^{-1} \frac{e^{\pi i/4} \cdot \prod_{j=0}^{7} K_{(1/8\ j/8)}(\tau)}{e^{9\pi i/4} \cdot \prod_{j=0}^{7} K_{(3/8\ j/8)}(\tau)} = v.$$

□

Since $v(\tau)$ clearly has rational Fourier coefficients, the above theorem implies that $\mathbb{Q}(v(\tau)) = A_0(\Gamma_1(8) \cap \Gamma^0(2), \mathbb{Q})$. And, from the following proposition we can further see the existence of an affine plane model defined over $\mathbb{Q}$, which is called in our case the modular equation.

Proposition 6. *Let n be a positive integer. Then we have*

$$\mathbb{Q}(v(\tau), v(n\tau)) = A_0(\Gamma_1(8) \cap \Gamma^0(2) \cap \Gamma_0(8n), \mathbb{Q}).$$

Proof. Since $v(\tau)$ is a Hauptmodul for $\Gamma_1(8) \cap \Gamma^0(2)$, we get that for $\alpha \in GL_2^+(\mathbb{Q})$, $v \circ \alpha = v$ yields $\alpha \in \mathbb{Q}^\times(\Gamma_1(8) \cap \Gamma^0(2))$. Let $\Gamma = \Gamma_1(8) \cap \Gamma^0(2)$ and $\beta = \begin{pmatrix} n & 0 \\ 0 & 1 \end{pmatrix}$. First, note that $\Gamma_1(8) \cap \Gamma^0(2) \cap \Gamma_0(8n) = \Gamma \cap \beta^{-1}\Gamma\beta$, hence it is clear that $v(\tau)$, $v(n\tau) \in A_0(\Gamma \cap \beta^{-1}\Gamma\beta, \mathbb{Q})$. Thus it is enough to show that $\mathbb{Q}(v(\tau), v(n\tau)) \supset A_0(\Gamma \cap \beta^{-1}\Gamma\beta, \mathbb{Q})$. Let Γ' be the subgroup of $SL_2(\mathbb{Z})$ such that $\mathbb{Q}(v(\tau), v(n\tau)) = A_0(\Gamma', \mathbb{Q})$, and let γ be any matrix in Γ'. Since $v(\tau)$ and $v(n\tau)$ are invariant under γ by the remark in the beginning of the proof, we establish that $\gamma \in \Gamma$ and $\beta\gamma\beta^{-1} \in \Gamma$, which implies $\gamma \in \Gamma \cap \beta^{-1}\Gamma\beta$. This completes the proof because it means that $\Gamma' \subset \Gamma \cap \beta^{-1}\Gamma\beta$, that is, $A_0(\Gamma', \mathbb{Q}) \supset A_0(\Gamma \cap \beta^{-1}\Gamma\beta, \mathbb{Q})$. □

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 where $f_1(\tau)$ and $f_2(\tau)$ are nonconstants, 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 $\Phi(X, Y) \in \mathbb{C}[X, Y]$ for which $\Phi(f_1(\tau), Y)$ is an irreducible polynomial of $f_2(\tau)$ over $\mathbb{C}(f_1(\tau))$ with degree D_1 and similarly so is $\Phi(X, f_2(\tau))$ over $\mathbb{C}(f_2(\tau))$ with degree D_2. Then Proposition 6 claims the existence of a polynomial $\Phi_n(X, Y) \in \mathbb{Q}[X, Y]$ with rational coefficients such that $\Phi_n(v(\tau), v(n\tau)) = 0$ 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 $\Gamma' = \Gamma_1(8) \cap \Gamma_0(16n)$. Then it is not hard to see that Γ' is conjugate to $\Gamma_1(8) \cap \Gamma^0(2) \cap \Gamma_0(8n)$, i.e.,

$$\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \Gamma' \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}^{-1} = \Gamma_1(8) \cap \Gamma^0(2) \cap \Gamma_0(8n)$$

and $\mathbb{Q}(v(2\tau), v(2n\tau)) = A_0(\Gamma', \mathbb{Q})$. Since it is rather easier to handle with Γ', we are going to concentrate on the modular equation of $v(2\tau)$ and $v(2n\tau)$, which is also the modular equation of $v(\tau)$ and $v(n\tau)$.

Now that it is more convenient to work with a Hauptmodul having the pole at ∞, we let $f(\tau) = 1/v(2\tau)$ and consider the modular equation $F_n(X, Y) = 0$ of $f(\tau)$ and $f(n\tau)$ with $F_n(X, Y) \in \mathbb{Q}[X, Y]$. Hereafter, we fix d_1 (respectively, d_n) to be the total degree of poles of the modular function $f(\tau)$ (respectively, $f(n\tau)$) with respect to $\Gamma' = \Gamma_1(8) \cap \Gamma_0(16n)$. Then we may let $F_n(X, Y) = \sum_{\substack{0 \le i \le d_n \\ 0 \le j \le d_1}} C_{i,j} X^i Y^j \in \mathbb{Q}[X, Y]$ so that it satisfies $F_n(f(\tau), f(n\tau)) = 0$.

Here we observe that $f(\tau)$ is a Hauptmodul for $\Gamma_1(8) \cap \Gamma_0(16)$ with a simple pole only at ∞ and a simple zero only at $3/16$, because $v(\tau)$ is a Hauptmodul for $\Gamma_1(8) \cap \Gamma^0(2)$ with a simple zero only at ∞ and a simple pole only at $3/8$.

In what follows, we fix the notation by

$$f(\tau) = \frac{1}{v(2\tau)}, \quad \Gamma = \Gamma_1(8) \cap \Gamma_0(16)$$

so that $f(\tau)$ is a Hauptmodul for Γ.

Lemma 7. *Let $a, c, a', c' \in \mathbb{Z}$ and $f(\tau) = 1/v(2\tau)$. Then we obtain the following assertions.*

(1) $f(\tau)$ has a pole at $\frac{a}{c} \in \mathbb{Q} \cup \{\infty\}$ with $(a, c) = 1$ if and only if $(a, c) = 1$, $c \equiv 0$ mod 16, $a \equiv \pm 1$ mod 8.

(2) $f(n\tau)$ has a pole at $\frac{a'}{c'} \in \mathbb{Q} \cup \{\infty\}$ if and only if there exist $a, c \in \mathbb{Z}$ such that $\frac{a}{c} = \frac{na'}{c'}$, $(a, c) = 1$, $c \equiv 0$ mod 16, $a \equiv \pm 1$ mod 8.

(3) $f(\tau)$ has a zero at $\frac{a}{c} \in \mathbb{Q} \cup \{\infty\}$ with $(a, c) = 1$ if and only if $(a, c) = 1$, $c \equiv 0$ mod 16, $a \equiv \pm 3$ mod 8.

(4) $f(n\tau)$ has a zero at $\frac{a'}{c'} \in \mathbb{Q} \cup \{\infty\}$ if and only if there exist $a, c \in \mathbb{Z}$ such that $\frac{a}{c} = \frac{na'}{c'}$, $(a, c) = 1$, $c \equiv 0$ mod 16, $a \equiv \pm 3$ mod 8.

Proof. It is enough to show (1) and (3), because (2) and (4) are the immediate consequences of (1) and (3). 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 know that

$$\begin{aligned} & \tfrac{a}{c} \text{ is equivalent to } \infty \text{ under } \Gamma \\ \iff \ & \exists\, \bar{s} \in \Delta = \{\pm 1, \pm 7 \in (\mathbb{Z}/16\mathbb{Z})^\times\},\ n \in \mathbb{Z} \text{ s.t. } \begin{pmatrix} a \\ c \end{pmatrix} \equiv \begin{pmatrix} \bar{s}^{-1} + 0 \\ 0 \end{pmatrix} \bmod 16. \end{aligned}$$

So we get the assertion (1). In a similar way we have the assertion (3) by observing that $f(\tau)$ has a simple zero at $3/16$. This completes the proof. □

We now introduce a method of finding modular equations by computing

$$F_2(X, Y) = \sum_{\substack{0 \le i \le d_2 \\ 0 \le j \le d_1}} C_{i,j} X^i Y^j$$

precisely. Then the congruence subgroup which we should consider is $\Gamma' = \Gamma_1(8) \cap \Gamma_0(32)$; hence

$$\Delta = \{\pm 1, \pm 9, \pm 17, \pm 25 \in (\mathbb{Z}/32\mathbb{Z})^\times\}$$

where the notation Δ is the subgroup illustrated as in §2. We will first obtain d_1. By the above lemma and Lemma 2 we should consider S_{16}, A_{16}, S_{32} and A_{32}, which are easily described as $S_{16} = S_{32} = \{1\}$, $A_{16} = A_{32} = \{1, 3\}$. So all the cusps of Γ' at which $f(\tau)$ has poles are $1/16$ and $1/32$ by (1) of Lemma 7, where $1/32$ is equivalent to ∞ by Lemma 1. And, all the cusps of Γ' at which $f(\tau)$ has zeros are $3/16$ and $3/32$ by (3) of Lemma 7. We see from Lemma 3 that the widths of $1/16$, ∞ in $\Gamma' \backslash \mathfrak{H}^*$ are 1 and 1, respectively. Since $f(\tau) = q^{-1} + O(1)$, we derive that $\mathrm{ord}_\infty f(\tau) = -1$. And, since $f \circ \begin{pmatrix} 1 & 0 \\ 16 & 1 \end{pmatrix} = f = q^{-1} + O(1)$ by observing that $\begin{pmatrix} 1 & 0 \\ 16 & 1 \end{pmatrix} \in \Gamma$, we conclude that $\mathrm{ord}_{1/16} f(\tau) = -1$. Hence the total degree d_1 of poles of $f(\tau)$ is 2. Next we will compute d_2. In like manner, by Lemma 7 and Lemma 2 we should consider S_{32} and A_{32}, which are already obtained as $S_{32} = \{1\}$, $A_{32} = \{1, 3\}$. Thus all the cusps of Γ' at which $f(2\tau)$ has poles is $1/32$ by (2) in the above lemma, where $1/32$ is equivalent to ∞ by Lemma 1. Meanwhile, we see that all the cusps of Γ' at which $f(2\tau)$ has zeros

is 3/32 by (4) of Lemma 7. As estimated in the above the width of ∞ in $\Gamma'\backslash\mathfrak{H}^*$ is 1. Since $f(2\tau) = q^{-2} + O(q^{-1})$, we have that $\mathrm{ord}_\infty f(2\tau) = -2$. So the total degree d_2 of poles of $f(2\tau)$ is 2. Therefore we have

$$F_2(X,Y) = \sum_{\substack{0\le i\le 2\\ 0\le j\le 2}} C_{i,j}X^iY^j.$$

In order to determine $F_2(X,Y)$ precisely, we are going to use the following theorem due to Ishida and Ishii ([9]) which can be derived from the standard theory of algebraic functions.

Theorem 8. *For any congruence subgroup Γ', let $f_1(\tau)$ and $f_2(\tau)$ 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 let

$$\begin{aligned} S_{k,0} &= \{s \in S_{\Gamma'} \mid f_k(\tau) \text{ has zeros at } s\}\\ S_{k,\infty} &= \{s \in S_{\Gamma'} \mid f_k(\tau) \text{ has poles at } s\} \end{aligned}$$

for $k = 1, 2$. Further let

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

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 $0 \le i < |S_{1,0}\cap S_{2,\infty}|$, $D_2 - |S_{1,\infty}\cap S_{2,\infty}| < i \le D_2$.

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

If we interchange the roles of $f_1(\tau)$ and $f_2(\tau)$, then we may have further properties similar to (1)$\sim$(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 get the following assertion.

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

Now we are ready to apply the above theorem to our situation. If we let $f_1(\tau) = f(\tau)$ and $f_2(\tau) = f(2\tau)$ in the above, then we achieve

$$\begin{aligned} S_{1,0} &= \{3/16, 3/32\}, & S_{1,\infty} &= \{1/16, \infty\},\\ S_{2,0} &= \{3/32\}, & S_{2,\infty} &= \{\infty\}. \end{aligned}$$

So we have

$$S_{1,\infty} \cap S_{2,0} = \phi \implies a = 0 \implies C_{2,0} \neq 0$$
$$S_{1,\infty} \cap S_{2,\infty} = \{\infty\} \implies C_{2,2} = 0$$
$$S_{1,0} \cap S_{2,0} = \{3/32\} \implies C_{0,0} = 0.$$

Since $f(\tau + 1/2) = -f(\tau)$ and $f(2(\tau + 1/2)) = f(2\tau)$, we also have that

$$i \not\equiv 0 \bmod 2 \implies C_{i,j} = 0$$

namely $C_{1,0} = C_{1,1} = C_{1,2} = 0$. Therefore we conclude that $F_2(X, Y) = C_{2,1}X^2Y + C_{2,0}X^2 + C_{0,2}Y^2 + C_{0,1}Y$.

Here we may determine all the coefficients of $F_2(X, Y)$ by inserting Fourier expansions of $f(\tau)$ and $f(2\tau)$. Since $v(\tau)$ is given by the q-product in §1 and $f(\tau) = \frac{1}{v(2\tau)}$, we obtain the Fourier expansions of $f(\tau)$ and $f(2\tau)$ by expanding each corresponding q-product as a series. Since $C_{2,0} \neq 0$, we may let $C_{2,0} = 1$ and by inserting enough terms of the Fourier expansions of $f(\tau)$ and $f(2\tau)$ we conclude that $C_{2,1} = -1$, $C_{0,2} = 1$, $C_{0,1} = 1$, and hence

$$F_2(X, Y) = -X^2Y + X^2 + Y^2 + Y,$$

from which we induce the relation

$$v^2(\tau) = \frac{v(2\tau)(1 - v(2\tau))}{1 + v(2\tau)}.$$

Note that this relation coincides with one of Chan and Huang's results.

Next, we consider the cases of all odd primes $n = p$ which also cover the results of Chan-Huang ([4]) and Vasuki-Srivatsa Kumar ([14]).

Theorem 9. *With the notations as above, let p be an odd prime. Then $F_p(X, Y) = \sum_{0 \leq i,j \leq p+1} C_{i,j}X^iY^j \in \mathbb{Q}[X, Y]$ satisfies the following conditions.*

(1) If $p \equiv \pm 1$ mod 8 then $C_{p+1,0} \neq 0$, $C_{0,0} = 0$ and

$$C_{p+1,1} = C_{p+1,2} = \cdots = C_{p+1,p+1} = 0$$
$$i + j \equiv 1 \bmod 2 \implies C_{i,j} = 0.$$

(2) If $p \equiv \pm 3$ mod 8 then $C_{p+1,p} \neq 0$ and

$$C_{p+1,0} = C_{p+1,1} = \cdots = C_{p+1,p-1} = C_{p+1,p+1} = 0$$
$$i + j \equiv 0 \bmod 2 \implies C_{i,j} = 0.$$

Proof. The congruence subgroup which we should consider is $\Gamma' = \Gamma_1(8) \cap \Gamma_0(16p)$, and hence

$$\Delta = \{\overline{\pm(1 + 8k)} \in (\mathbb{Z}/16p\mathbb{Z})^\times \mid k = 0, \cdots, 2p - 1\}$$

where Δ is the subgroup as in §2. Note that among the values $k = 0, \cdots, 2p - 1$, only two of them do not satisfy the condition $\overline{\pm(1 + 8k)} \in (\mathbb{Z}/16p\mathbb{Z})^\times$ because p is an odd prime. By Lemma 2 and 7 we have to consider S_{16}, A_{16}, S_{16p} and A_{16p}. And we know that $S_{16} = \{1\}$, for example, by observing that $\{1 + 8k \in (\mathbb{Z}/p\mathbb{Z})^\times \mid k = 0, \cdots, p - 1$ such that $1 + 8k \not\equiv 0 \bmod p\}$ is equal to the whole set $(\mathbb{Z}/p\mathbb{Z})^\times$. Further, we easily see that $S_{16p} = \{1\}$. Since $|\Delta| = 4(p - 1)$ and $|\pi_p(\Delta)| = p - 1$ as noted in the above, we

get $m_{16} = 2$ with the notation m_{16} as in §2. So we have that $A_{16} = \{1, 3\}$. Since m_{16p} is also equal to 2, we derive that

$$A_{16p} = \begin{cases} \{1,3\} & \text{if } p \neq 3 \\ \{1,5\} & \text{if } p = 3. \end{cases}$$

Thus all the inequivalent cusps under consideration are $\frac{1}{16}$, $\frac{3}{16}$, $\frac{1}{16p}$ and $\frac{3}{16p}$ (respectively, $\frac{1}{16}$, $\frac{3}{16}$, $\frac{1}{48}$ and $\frac{5}{48}$) if $p \neq 3$ (respectively, $p = 3$). Although we consider only the case $p \neq 3$ for convenience, all the statements below are true by replacing with appropriate cusps. Hence we concentrate on the cusps $\frac{1}{16}$, $\frac{3}{16}$, $\frac{1}{16p}$ and $\frac{3}{16p}$ at which the widths are p, p, 1 and 1, respectively by Lemma 3, and $\frac{1}{16p}$ is equivalent to ∞ by Lemma 1. If we let $f_1(\tau) = f(\tau)$ and $f_2(\tau) = f(p\tau)$ in Theorem 8, then by Lemma 7 we know that $S_{1,\infty} = \{\frac{1}{16}, \frac{1}{16p}\}$, $S_{1,0} = \{\frac{3}{16}, \frac{3}{16p}\}$. Further we obtain that

$$\begin{aligned} S_{2,\infty} = \{\tfrac{1}{16}, \tfrac{1}{16p}\},\ S_{2,0} = \{\tfrac{3}{16}, \tfrac{3}{16p}\} \quad & \text{if } p \equiv \pm 1 \bmod 8 \\ S_{2,\infty} = \{\tfrac{3}{16}, \tfrac{1}{16p}\},\ S_{2,0} = \{\tfrac{1}{16}, \tfrac{3}{16p}\} \quad & \text{if } p \equiv \pm 3 \bmod 8. \end{aligned}$$

Since $f \circ \begin{pmatrix} 1 & 0 \\ 16 & 1 \end{pmatrix} = f = q^{-1} + O(1)$ due to the fact that $\begin{pmatrix} 1 & 0 \\ 16 & 1 \end{pmatrix} \in \Gamma$, we derive that $\mathrm{ord}_\infty f(\tau) = -1$ and $\mathrm{ord}_{1/16} f(\tau) = -p$. So the total degree d_1 of poles of $f(\tau)$ is $p+1$. Since $f(p\tau) = q^{-p} + O(q^{-p+1})$, we get that $\mathrm{ord}_\infty f(p\tau) = -p$. Let $a = 1$ (respectively, $a = 3$) if $p \equiv \pm 1 \bmod 8$ (respectively, $p \equiv \pm 3 \bmod 8$). In order to find $\mathrm{ord}_{a/16} f(p\tau)$, we first take $b, d \in \mathbb{Z}$ such that $\begin{pmatrix} a & b \\ 16 & d \end{pmatrix} \in SL_2(\mathbb{Z})$. Then since there exists $x \in \mathbb{Z}$ such that $d - 8x \equiv 0 \bmod p$, we have

$$\begin{pmatrix} 2p & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ 16 & d \end{pmatrix} = \begin{pmatrix} pa & 2b - ax \\ 8 & \frac{d-8x}{p} \end{pmatrix} \begin{pmatrix} 2 & x \\ 0 & p \end{pmatrix}$$

where $\begin{pmatrix} pa & 2b - ax \\ 8 & \frac{d-8x}{p} \end{pmatrix} \in SL_2(\mathbb{Z})$. Thus the Fourier expansion of $f(p\tau)$ at $a/16$ can be derived from

$$\begin{aligned} 1/v \circ \begin{pmatrix} 2p & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ 16 & d \end{pmatrix} &= 1/v \circ \begin{pmatrix} pa & 2b - ax \\ 8 & \frac{d-8x}{p} \end{pmatrix} \begin{pmatrix} 2 & x \\ 0 & p \end{pmatrix} \\ &= (\text{some root of unity}) \cdot \textstyle\prod_{j=0}^{7} \frac{K_{(pa/8\ *)}(2\tau/p + x/p)}{K_{(3pa/8\ *)}(2\tau/p + x/p)} \end{aligned}$$

by **K1** and **K2**. By **K4** we see that the above is of the form

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

where $k = 8(< \frac{3pa}{8} > (< \frac{3pa}{8} > -1) - < \frac{pa}{8} > (< \frac{pa}{8} > -1))$ with the notation $< >$ as in **K4**. By plugging $p \equiv \pm 1 \bmod 8$ and $p \equiv \pm 3 \bmod 8$, respectively, into the above we come up with that $k = -1$ whether $p \equiv \pm 1 \bmod 8$ or not. Thus if $p \equiv \pm 1 \bmod 8$ then $\mathrm{ord}_{1/16} f(p\tau) = -1$, and if $p \equiv \pm 3 \bmod 8$ then $\mathrm{ord}_{3/16} f(p\tau) = -1$. And the total degree d_p of poles of $f(p\tau)$ is $p+1$. Therefore $F_p(X, Y)$ is of the form

$$F_p(X, Y) = \sum_{0 \leq i,j \leq p+1} C_{i,j} X^i Y^j.$$

Since $S_{1,\infty} \cap S_{2,0}$ is empty (respectively, $\{\frac{1}{16}\}$) if $p \equiv \pm 1 \bmod 8$ (respectively, $p \equiv \pm 3 \bmod 8$), we claim that $a = 0$ (respectively, $a = p$); and hence $C_{p+1,0} \neq 0$ (respectively, $C_{p+1,p} \neq 0$). Similarly, by Theorem 8 we derive all the other assertions. For example, by observing $f(\tau + \frac{1}{2}) = -f(\tau)$ and $f(p(\tau + \frac{1}{2})) = -f(p\tau)$ we get that

$$\begin{aligned} i + j \equiv 1 \bmod 2 &\implies C_{i,j} = 0 \quad \text{if } p \equiv \pm 1 \bmod 8 \\ i + j \equiv 0 \bmod 2 &\implies C_{i,j} = 0 \quad \text{if } p \equiv \pm 3 \bmod 8. \end{aligned}$$

This completes the proof. □

Now we are able to estimate the modular equation $\Phi_p(X, Y) = 0$ of $v(\tau)$ and $v(p\tau)$ by inserting enough terms of the Fourier expansions of $f(\tau)$ and $f(p\tau)$ into $F_p(X, Y)$ in Theorem 9 and observing $\Phi_p(X, Y) = X^{p+1}\, Y^{p+1}\, F_p(\frac{1}{X}, \frac{1}{Y})$. For instance, we have the following table which recovers the results of Chan-Huang and Vasuki-Srivatsa Kumar in §1. It is obvious that one may apply our method to find higher order modular equations $\Phi_p(X, Y) = 0$ for $p \geq 13$.

p	the modular equation of $v(:= v(\tau))$ and $w(:= v(p\tau))$
3	$v^4w^3 - v^3(3w^2 - 1) - 3v^2(w^3 - w) - v(w^4 - 3w^2) - w = 0$
5	$v^6w^5 - v^5(5w^2 - 1) - 5v^4(w^5 - 2w^3) - 10v^3(w^4 - w^2)$ $-5v^2(2w^3 - w) - v(w^6 - 5w^4) - w = 0$
7	$v^8 - v^7(w^7 - 7w^5 + 7w^3 + 7w) + 28v^6w^2$ $+7v^5(w^7 - 7w^5 - w^3 - w) + 70v^4w^4 - 7v^3(w^7 + w^5 + 7w^3 - w)$ $+28v^2w^6 - v(7w^7 + 7w^5 - 7w^3 + w) + w^8 = 0$
11	$v^{12}w^{11} + v^{11}(11w^{10} - 33w^8 - 11w^6 + 33w^4 - 11w^2 + 1)$ $-11v^{10}(w^{11} - 6w^9 + 6w^7 - 6w^3 + w)$ $-11v^9(6w^{10} - 21w^8 - 5w^6 + 36w^4 - 6w^2)$ $+33v^8(w^{11} - 12w^9 + 16w^7 + 6w^5 - 7w^3 + w)$ $-66v^7(3w^8 + 6w^6 - 8w^4 + w^2)$ $-11v^6(w^{11} - 5w^9 + 36w^7 - 36w^5 + 5w^3 - w)$ $+66v^5(w^{10} - 8w^8 + 6w^6 + 3w^4)$ $-33v^4(w^{11} - 7w^9 + 6w^7 + 16w^5 - 12w^3 + w)$ $-11v^3(6w^{10} - 36w^8 + 5w^6 + 21w^4 - 6w^2)$ $+11v^2(w^{11} - 6w^9 + 6w^5 - 6w^3 + w)$ $-v(w^{12} - 11w^{10} + 33w^8 - 11w^6 - 33w^4 + 11w^2) - w = 0$

¿From now on, in order to find the Kronecker congruence relations for the modular equations of $v(\tau)$ and $v(n\tau)$ we let $\Gamma = \Gamma_1(8) \cap \Gamma_0(16)$ as before and further let n be a positive integer with $(n, 2) = 1$. For any integer a with $(a, 2) = 1$, we fix $\sigma_a \in SL_2(\mathbb{Z})$ such that $\sigma_a \equiv \begin{pmatrix} a^{-1} & 0 \\ 0 & a \end{pmatrix} \bmod 16$. Then we have

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

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 use [13], Proposition 3.36.

Since σ_a depends only on a modulo 16, we fix σ_a as

$$\sigma_{\pm1}=\pm\begin{pmatrix}1&0\\0&1\end{pmatrix},\qquad \sigma_{\pm3}=\pm\begin{pmatrix}27&32\\16&19\end{pmatrix},$$
$$\sigma_{\pm5}=\pm\begin{pmatrix}-19&32\\16&-27\end{pmatrix},\quad \sigma_{\pm7}=\pm\begin{pmatrix}-41&32\\32&-25\end{pmatrix}.$$

It follows from the transformation formulas **K0∼K2** that

$$f\circ\sigma_{\pm1}=f\circ\sigma_{\pm7}=f,\quad f\circ\sigma_{\pm3}=f\circ\sigma_{\pm5}=-\frac{1}{f}.$$

For convenience, 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 $\deg_X\Psi_n(X,\tau)=n\prod_{p|n}(1+\frac{1}{p})$. 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., $\Psi_n(X,\tau)\in\mathbb{C}(f(\tau))[X]$, and we may write $\Psi_n(X,f(\tau))$ instead of $\Psi_n(X,\tau)$.

With the notations as in Theorem 8, we let $f_1(\tau)=f(\tau)$ and $f_2(\tau)=f(n\tau)$. Since $(n,2)=1$, we have $S_{1,\infty}\cup S_{1,0}=S_{2,\infty}\cup S_{2,0}$ by Lemma 7.

Theorem 10. *With the notations as above, for a positive integer n with $(n,2)=1$ we define*

$$F_n(X,f(\tau))=f(\tau)^a\Psi_n(X,f(\tau)),$$

that is, $F_n(X,Y)=Y^a\Psi_n(X,Y)$ with the nonnegative integer

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

Here we assume that $a=0$ if $S_{1,\infty}\cap S_{2,0}$ is empty. Then we obtain the following assertions.

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

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

(3) Let $d=n\prod_{p|n}(1+\frac{1}{p})$. If $n\equiv\pm1$ mod 8, then

$$F_n(X,Y)=F_n(Y,X).$$

If $n\equiv\pm3$ mod 8, then

$$F_n(X,Y)=Y^dF_n(-\frac{1}{Y},X).$$

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

(5) (Kronecker's congruences) Let p be an odd prime. If $p \equiv \pm 1$ mod 8, then

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

If $p \equiv \pm 3$ mod 8, then

$$F_p(X,Y) \equiv (X^p - Y)(XY^p + 1) \text{ mod } p\mathbb{Z}[X,Y].$$

Proof. Since $f(\tau) = \frac{1}{v(2\tau)}$, we may let $f(\tau) = \frac{1}{q} + \sum_{m=1}^{\infty} c_m q^m$ with $c_m \in \mathbb{Z}$. We further let $d = n\prod_{p|n}(1+\frac{1}{p})$ and let $\psi \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ be such that $\psi(\zeta_n) = \zeta_n^k$ for some integer k with $(k,n) = 1$. Then ψ induces an automorphism of $\mathbb{Q}(\zeta_n)((q^{\frac{1}{n}}))$ through the action on the coefficients. We denote the induced automorphism by the same notation ψ. Since

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

we get that

$$\psi(f \circ \begin{pmatrix} a & b \\ 0 & \frac{n}{a} \end{pmatrix}) = \frac{\zeta_n^{-abk}}{(q^{\frac{1}{n}})^{a^2}} + \sum_{m=1}^{\infty} c_m \zeta_n^{abkm} (q^{\frac{1}{n}})^{a^2 m}.$$

Let b' be the unique integer such that $0 \le b' < \frac{n}{a}$ and $b' \equiv bk \bmod \frac{n}{a}$. Then

$$\psi(f \circ \begin{pmatrix} a & b \\ 0 & \frac{n}{a} \end{pmatrix}) = f \circ \begin{pmatrix} a & b' \\ 0 & \frac{n}{a} \end{pmatrix}$$

because $\zeta_n^{abk} = \zeta_n^{ab'}$. Since $f \circ \sigma_a = f$ or $-\frac{1}{f}$, we have $\psi(f \circ \alpha_{a,b}) = f \circ \alpha_{a,b'}$, and so all the coefficients of $\Psi_n(X, f(\tau))$ are contained in $\mathbb{Q}((q^{\frac{1}{n}}))$. Hence by observing the fact $\Psi_n(X, f(\tau)) \in \mathbb{C}(f(\tau))[X]$ we see that $\Psi_n(X, f(\tau)) \in \mathbb{Q}(f(\tau))[X]$.

Meanwhile, $\Psi_n(f(\frac{\tau}{n}), f(\tau)) = 0$ implies that $[\mathbb{C}(f(\frac{\tau}{n}), f(\tau)) : \mathbb{C}(f(\tau))] \le d$. 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. Note that for $\gamma \in \Gamma$ the map $h(\tau) \mapsto h(\gamma(\tau))$ is an embedding of $\mathbb{C}(f(\frac{\tau}{n}), f(\tau))$ into $\mathfrak{F}$, which is the identity on $\mathbb{C}(f(\tau))$. Also, observe 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 $f(\alpha_{a,b}(\tau)) \ne f(\alpha_{a',b'}(\tau))$ if $\alpha_{a,b} \ne \alpha_{a',b'}$, 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

$$f(\frac{\tau}{n}) \mapsto f \circ \begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix} \circ \gamma_{a,b} = f(\alpha_{a,b}(\tau)).$$

Thus

$$[\mathbb{C}(f(\frac{\tau}{n}), f(\tau)) : \mathbb{C}(f(\tau))] = d,$$

which yields that $\Psi_n(X, f(\tau))$ is irreducible over $\mathbb{C}(f(\tau))$.

With the notations as in Theorem 8, if we let

$$a = -\sum_{s\in S_{1,\infty}\cap S_{2,0}} \mathrm{ord}_s f(\tau), \qquad b = \sum_{s\in S_{1,0}\cap S_{2,0}} \mathrm{ord}_s f(\tau),$$
$$a' = -\sum_{s\in S_{2,\infty}\cap S_{1,0}} \mathrm{ord}_s f(n\tau), \quad b' = \sum_{s\in S_{2,0}\cap S_{1,0}} \mathrm{ord}_s f(n\tau),$$

then $F(X,Y)$ in Theorem 8 is of the form

$$C_{d_n,a}X^{d_n}Y^a + C_{0,b}Y^b + C_{a',d_1}X^{a'}Y^{d_1} + C_{b',0}X^{b'} + \sum_{\substack{0<i<d_n\\ 0<j<d_1}} C_{i,j}X^iY^j.$$

Since $F(X, f(\tau))$ is an irreducible polynomial of $f(\frac{\tau}{n})$ over $\mathbb{C}(f(\tau))$ and $F(f(\frac{\tau}{n}), Y)$ is also an irreducible polynomial of $f(\tau)$ over $\mathbb{C}(f(\frac{\tau}{n}))$, we know that

$$f(\tau)^a\Psi_n(X, f(\tau)) = \frac{F(X, f(\tau))}{C_{d_n,a}}$$

and $F_n(X,Y)$ is a polynomial in X and Y which is irreducible both as a polynomial in X over $\mathbb{C}(Y)$ and as a polynomial in Y over $\mathbb{C}(X)$. Since $f(\tau)^a\Psi_n(X, f(\tau)) \in \mathbb{Q}[X, f(\tau)]$ and all the Fourier coefficients of the coefficients of $\Psi_n(X, f(\tau))$ are algebraic integers, we conclude that $f(\tau)^a\Psi_n(X, f(\tau)) \in \mathbb{Z}[X, f(\tau)]$, namely $F_n(X,Y) \in \mathbb{Z}[X,Y]$.

We first consider the case $n \equiv \pm 1 \bmod 8$. Since $\Psi_n(f(n\tau), f(\tau)) = 0$, i.e., $\Psi_n(f(\tau), f(\frac{\tau}{n}))$ $= 0$, $f(\frac{\tau}{n})$ is a root of the polynomial $F_n(f(\tau), X) \in \mathbb{Z}[X, f(\tau)]$. Now that $f(\frac{\tau}{n})$ is a root of the irreducible polynomial $F_n(X, f(\tau))$, we derive that

$$F_n(f(\tau), X) = g(X, f(\tau))F_n(X, f(\tau))$$

for some polynomial $g(X, f(\tau)) \in \mathbb{Z}[X, f(\tau)]$ by the Gauss lemma on the irreducibility of polynomials. Thus

$$F_n(f(\tau), X) = g(X, f(\tau))g(f(\tau), X)F_n(f(\tau), X)$$

implies $g(X, f(\tau)) = \pm 1$. If $g(X, f(\tau)) = -1$, then $F_n(f(\tau), f(\tau)) = -F_n(f(\tau), f(\tau))$; hence $f(\tau)$ is a root of $F_n(X, f(\tau))$, which is a contradiction to the irreducibility of $F_n(X, f(\tau))$ over $\mathbb{C}(f(\tau))$. Therefore we have

$$F_n(X, f(\tau)) = F_n(f(\tau), X).$$

Next, we consider the case $n \equiv \pm 3 \bmod 8$. Since $\Psi_n(-\frac{1}{f(n\tau)}, f(\tau)) = 0$, namely $\Psi_n(-\frac{1}{f(\tau)}, f(\frac{\tau}{n})) = 0$, $f(\frac{\tau}{n})$ is a root of the polynomial $f(\tau)^d\, F_n(-\frac{1}{f(\tau)}, X) \in \mathbb{Z}[X, f(\tau)]$. So

$$f(\tau)^d F_n(-\frac{1}{f(\tau)}, X) = g(X, f(\tau))F_n(X, f(\tau))$$

for some polynomial $g(X, f(\tau)) \in \mathbb{Z}[X, f(\tau)]$ again by the Gauss lemma. Note that

$$d = \deg_X F_n(X,Y) = \deg_Y F_n(X,Y) + \deg_Y g(X,Y)$$

and

$$\deg_Y F_n(X,Y) = \deg_X F_n(X,Y) + \deg_X g(X,Y),$$

and so $g(X,Y)$ is a constant and

$$\deg_X F_n(X,Y) = \deg_Y F_n(X,Y) = d.$$

Since $F_n(X,Y)$ is a primitive polynomial, we have $g(X,Y) = \pm 1$. By considering the coefficients of the equation $Y^d F_n(-\frac{1}{Y}, X) = g(X,Y)F_n(X,Y)$ we also get that the coefficient of $X^{d-a}Y^d$ in $F_n(X,Y)$ is equal to $(-1)^a g(X,Y)$. Since $\Psi_n(X, f(\tau))$ is equal to

$$\prod_{\substack{a>0, a|n \\ a\equiv\pm 1\,(8)}} \prod_{\substack{0\le b<\frac{n}{a} \\ (a,b,\frac{n}{a})=1}} (X - \zeta_n^{-ab} q^{-\frac{a^2}{n}} + \cdots) \prod_{\substack{a>0, a|n \\ a\equiv\pm 3\,(8)}} \prod_{\substack{0\le b<\frac{n}{a} \\ (a,b,\frac{n}{a})=1}} (X + \zeta_n^{ab} q^{\frac{a^2}{n}} + \cdots),$$

we see that the coefficient of $X^{d-a}Y^d$ in $F_n(X,Y)$ is equal to

$$\prod_{\substack{a>0, a|n \\ a\equiv\pm 1\,(8)}} \prod_{\substack{0\le b<\frac{n}{a} \\ (a,b,\frac{n}{a})=1}} (-\zeta_n^{-ab}).$$

For convenience, we denote the above products by $\prod\prod$, in other words, the first product runs over $a > 0$, $a|n$, $a \equiv \pm 1\,(8)$ and the second product runs over $0 \le b < \frac{n}{a}$, $(a, b, \frac{n}{a}) = 1$. Observe that $\prod\prod(-1) = (-1)^a$ by considering the degree with respect to X, and so $g(X,Y) = \prod\prod \zeta_n^{-ab}$. Hence we immediately obtain that $g(X,Y) = 1$ by the following elementary lemma (see [3], Lemma 6.7): If $m > 0$ is an odd integer and $k|m$, then $\prod_{\substack{0\le b<m \\ (b,k)=1}} \zeta_m^{-b} = 1$.

Now we consider the case where n is not a square. Then

$$f(\tau) - f(\alpha_{a,b}(\tau)) = \begin{cases} \frac{1}{q} - \frac{\zeta_n^{-ab}}{q^{\frac{a^2}{n}}} + O(q^{\frac{1}{n}}) & \text{if } a \equiv \pm 1 \bmod 8 \\ \frac{1}{q} + O(q^{\frac{1}{n}}) & \text{if } a \equiv \pm 3 \bmod 8. \end{cases}$$

Therefore the coefficient of the lowest degree in $F_n(f(\tau), f(\tau))$ is a unit. Since it must be an integer, $F_n(X,X)$ is a polynomial of degree > 1 with leading coefficient ± 1.

Let p be an odd prime. For any $g(\tau)$, $h(\tau) \in \mathbb{Z}[\zeta_p]((q^{\frac{1}{p}}))$ and $\alpha \in \mathbb{Z}[\zeta_p]$, we write

$$g(\tau) \equiv h(\tau) \bmod \alpha$$

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

First, we consider the case $p \equiv \pm 1 \bmod 8$. Since

$$f(\tau) = \frac{1}{q} + \sum_{m=1}^{\infty} c_m q^m \quad (c_m \in \mathbb{Z}),$$

we have that

$$f(\alpha_{1,b}(\tau)) = \frac{\zeta_p^{-b}}{q^{\frac{1}{p}}} + \sum_{m=1}^{\infty} c_m \zeta_p^{bm} (q^{\frac{1}{p}})^m \equiv \frac{1}{q^{\frac{1}{p}}} + \sum_{m=1}^{\infty} c_m (q^{\frac{1}{p}})^m \bmod 1 - \zeta_p,$$

that is,

$$f(\alpha_{1,b}(\tau)) \equiv f(\alpha_{1,0}(\tau)) \bmod 1 - \zeta_p$$

for any $b = 0, \cdots, p-1$. And, since

$$f(\alpha_{p,0}(\tau)) = \frac{1}{q^p} + \sum_{m=1}^{\infty} c_m q^{pm}$$

and $c_m^p \equiv c_m \bmod p$, we establish that $f(\alpha_{p,0}(\tau)) \equiv f(\tau)^p \bmod p$, i.e.,

$$f(\alpha_{p,0}(\tau)) \equiv f(\tau)^p \bmod 1-\zeta_p.$$

Here we note that

$$f(\tau) \equiv f(\alpha_{1,0}(\tau))^p \bmod 1-\zeta_p.$$

Since $a = -\sum_{s\in S_{1,\infty}\cap S_{2,0}} \mathrm{ord}_s f(\tau) = 0$ by Theorem 9, the above congruences yield that

$$\begin{aligned} F_p(X, f(\tau)) &= f(\tau)^a \Psi_p(X, f(\tau)) \;=\; \Psi_p(X, f(\tau)) \\ &= \textstyle\prod_{a=1,p} \prod_{0\le b<\frac{p}{a}} (X - f(\alpha_{a,b}(\tau))) \\ &\equiv (X - f(\alpha_{1,0}(\tau)))^p (X - f(\tau)^p) \\ &\equiv (X^p - f(\alpha_{1,0}(\tau))^p)(X - f(\tau)^p) \\ &\equiv (X^p - f(\tau))(X - f(\tau)^p) \bmod 1-\zeta_p. \end{aligned}$$

Let $F_p(X, f(\tau)) - (X^p - f(\tau))(X - f(\tau)^p) = \sum_\nu \psi_\nu(f(\tau)) X^\nu$, 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 see that $\psi_\nu(f(\tau)) \in p\mathbb{Z}[f(\tau)]$. So

$$F_p(X, f(\tau)) \equiv (X^p - f(\tau))(X - f(\tau)^p) \bmod p\mathbb{Z}[X, f(\tau)]$$

when $p \equiv \pm 1 \bmod 8$ as desired.

Lastly, we consider the case $p \equiv \pm 3 \bmod 8$. By the same arguments as in the case $p \equiv \pm 1 \bmod 8$, we achieve that

$$f(\alpha_{1,b}(\tau)) \equiv f(\alpha_{1,0}(\tau)) \bmod 1-\zeta_p$$

for any $b = 0, \cdots, p-1$ and

$$f(\tau) \equiv f(\alpha_{1,0}(\tau))^p \bmod 1-\zeta_p.$$

Since $f(\alpha_{p,0}(\tau)) = -\frac{1}{f(p\tau)}$ and $f(p\tau) \equiv f(\tau)^p \bmod p$, we get that $f(\alpha_{p,0}(\tau)) \equiv -\frac{1}{f(\tau)^p} \bmod p$, i.e.,

$$f(\alpha_{p,0}(\tau)) \equiv -\frac{1}{f(\tau)^p} \bmod 1-\zeta_p.$$

Now that $a = -\sum_{s\in S_{1,\infty}\cap S_{2,0}} \mathrm{ord}_s f(\tau) = p$ by Theorem 9 again, we claim that

$$\begin{aligned} F_p(X, f(\tau)) &= f(\tau)^a \Psi_p(X, f(\tau)) = f(\tau)^p \Psi_p(X, f(\tau)) \\ &= f(\tau)^p \textstyle\prod_{a=1,p} \prod_{0\le b<\frac{p}{a}} (X - f(\alpha_{a,b}(\tau))) \\ &\equiv f(\tau)^p (X - f(\alpha_{1,0}(\tau)))^p (X + \tfrac{1}{f(\tau)^p}) \\ &\equiv (X^p - f(\alpha_{1,0}(\tau))^p)(X f(\tau)^p + 1) \\ &\equiv (X^p - f(\tau))(X f(\tau)^p + 1) \bmod 1-\zeta_p. \end{aligned}$$

Then by the same arguments as in the case $p \equiv \pm 1 \bmod 8$ we conclude that

$$F_p(X, f(\tau)) \equiv (X^p - f(\tau))(X f(\tau)^p + 1) \bmod p\mathbb{Z}[X, f(\tau)].$$

This completes the proof. □

With the notations as in Theorem 10 we remark that $F_n(X,Y)=0$ is the modular equation of $f(\tau)$ and $f(n\tau)$ such that the coefficient of X^dY^a in $F_n(X,Y)$ is 1. Since $\deg_X F_n(X,Y)=\deg_Y F_n(X,Y)=d$, Theorem 10 can be rewritten as the modular equation $\Phi_n(X,Y)=0$ of $v(\tau)$ and $v(n\tau)$ by observing $\Phi_n(X,Y)=X^d\ Y^d\ F_n(\frac{1}{X},\frac{1}{Y})$.

4. Units and application

Let $j(\tau)$ be the classical elliptic modular function. By definition a modular unit over $\mathbb{Z}$ is a modular function $f(\tau)$ of some level N rational over $\mathbb{Q}(\zeta_N)$ such that $f(\tau)$ and $1/f(\tau)$ are integral over $\mathbb{Z}[j(\tau)]$.

Lemma 11. *Let $h(\tau)$ be a modular function of some level N rational over $\mathbb{Q}(\zeta_N)$ for which $h(\tau)$ has neither zeros nor poles on $\mathfrak{H}$. If for every $\gamma\in SL_2(\mathbb{Z})$ the Fourier expansion of $h\circ\gamma$ has algebraic integer coefficients and the coefficient of the term of lowest degree is a unit, then $h(\tau)$ is a modular unit over $\mathbb{Z}$.*

Proof. We refer the reader to [11] Chapter 2, Lemma 2.1, which can also be proved by the theory of Shimura reciprocity law (see [13]). □

Let $h(\tau)$ be a modular unit over $\mathbb{Z}$ and K be an imaginary quadratic field. Since it is well known that $j(\tau)$ is an algebraic integer for every $\tau\in K-\mathbb{Q}$, we can derive that for such τ, $h(\tau)$ is an algebraic integer which is a unit. By observing this fact we derive the following theorem.

Theorem 12. *Let $v(\tau)$ be the Ramanujan-Göllnitz-Gordon continued fraction and K be an imaginary quadratic field. Then $v(\tau)$ are units for all $\tau\in K-\mathbb{Q}$.*

Proof. As stated in the above, it is enough to prove that $v(\tau)$ is a modular unit over $\mathbb{Z}$. Let $\gamma=\begin{pmatrix}a & b\\ c & d\end{pmatrix}\in SL_2(\mathbb{Z})$. Since $v(\tau)=-\zeta_{16}^{-1}\prod_{j=0}^{7}\frac{K_{(1/8\ \ j/8)}(\tau)}{K_{(3/8\ \ j/8)}(\tau)}$, we obtain that

$$v(\gamma(\tau))=-\zeta_{16}^{-1}\prod_{j=0}^{7}\frac{K_{((a+jc)/8\ \ (b+jd)/8)}(\tau)}{K_{((3a+jc)/8\ \ (3b+jd)/8)}(\tau)}$$

by **K1**. If we replace the Klein forms by the q-products in **K4** and expand the products as a series, then the series is the Fourier expansion of $v(\gamma(\tau))$. Since we want to prove that $v(\gamma(\tau))$ has algebraic integer Fourier coefficients and the lowest coefficient is a unit, we may assume that

$$0\le (a+jc)/8,\ (3a+jc)/8<1$$

by **K2**. If we assume these, then the only term we should consider in **K4** is $1-q_z$. First, we treat the case where c is even. Since a is odd, $(a+jc)/8$ cannot be an integer for any $j=0,\cdots,7$. Similarly $(3a+jc)/8$ cannot be an integer for any $j=0,\cdots,7$. So $1-q_z$ cannot be complex numbers, namely it has algebraic integer coefficients with the lowest coefficient 1, and the series expansion of $v(\gamma(\tau))$ has the desired properties. Now we consider the case of c odd. Since $c\in(\mathbb{Z}/8\mathbb{Z})^\times$, there exist unique $j_1,j_2\in\{0,\cdots,7\}$ such that

$$a+j_1c\equiv 0 \bmod 8,\quad 3a+j_2c\equiv 0 \bmod 8.$$

Hence for such j_1, j_2 (respectively, j_2),

$$1 - q_z = \begin{cases} 1 - \zeta_8^{b+j_1 d} & \text{if } j_1 \text{ arises} \\ 1 - \zeta_8^{3b+j_2 d} & \text{if } j_2 \text{ arises.} \end{cases}$$

Thus $v(\gamma(\tau))$ has the desired properties if $\frac{1-\zeta_8^{b+j_1 d}}{1-\zeta_8^{3b+j_2 d}}$ is a unit. First, note that

$$(2, b + j_1 d) = (2, 3b + j_2 d) = 1$$

because $(\frac{1}{8} \ \frac{j_1}{8}) = (\frac{a+j_1 c}{8} \ \frac{b+j_1 d}{8}) \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$ with $(a + j_1 c)/8 \in \mathbb{Z}$. Meanwhile, by the following elementary lemma we obtain the assertion. Let p be a prime and $r, s \in \mathbb{Z}$ such that $(p, rs) = 1$. Then $\frac{1-\zeta_{p^n}^r}{1-\zeta_{p^n}^s}$ is a unit of $\mathbb{Z}[\zeta_{p^n}]$. Indeed, $s \in (\mathbb{Z}/p^n\mathbb{Z})^\times$ implies that $r \equiv st \bmod p^n$ for some $t \in \mathbb{Z}$, and so

$$\frac{1 - \zeta_{p^n}^r}{1 - \zeta_{p^n}^s} = \frac{1 - \zeta_{p^n}^{st}}{1 - \zeta_{p^n}^s} = 1 + \zeta_{p^n}^s + \cdots + \zeta_{p^n}^{s(t-1)} \in \mathbb{Z}[\zeta_{p^n}].$$

Similarly, $\frac{1-\zeta_{p^n}^s}{1-\zeta_{p^n}^r} \in \mathbb{Z}[\zeta_{p^n}]$. This completes the proof. □

Next let N be a positive integer, K be an imaginary quadratic field and let $z \in K \cap \mathfrak{H}$ 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. Further, let

$$f_{(a_1 \ a_2)}(z) = \frac{g_2(\mathbb{Z}z + \mathbb{Z}) g_3(\mathbb{Z}z + \mathbb{Z})}{\Delta(\mathbb{Z}z + \mathbb{Z})} \wp(a_1 z + a_2; \mathbb{Z}z + \mathbb{Z})$$

be the first Fricke function defined as in [13] §6.1 where $(a_1 \ a_2) \in \mathbb{Q}^2 - \mathbb{Z}^2$. By the notation $K \cdot \mathfrak{F}'(z)$ in the following theorem we mean the field generated over K by all the values $h(z)$, where $h \in \mathfrak{F}'$ is defined and finite at z. And, let $\mathfrak{F}_N$ stand for the field of all modular functions of level N rational over $\mathbb{Q}(\zeta_N)$.

Theorem 13. *With the notations as above, let x (respectively, y) be the least positive integer such that $x = (Nx, a)$ (respectively, $y = (Ny, c)$), and let*

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

Then for any field $\mathfrak{F}'$ described 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 $\mathfrak{F}_{min}^{(i)} \subset \mathfrak{F}'' \subset \mathfrak{F}_{max}$ for some $i = 1, \cdots, 4$ or $\mathfrak{F}_N \subset \mathfrak{F}'' \subset \mathfrak{F}_{max}$, then $K \cdot \mathfrak{F}''(z)$ is also the ray class field modulo N over K.

Proof. [5] Theorem 29. □

Here we will make use of the following lemma to show that the units mentioned in Theorem 12 really generate some ray class fields over imaginary quadratic fields.

Lemma 14. *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 13, if $(N, a) = 1$ then x in Theorem 13 is equal to 1. Therefore the inclusions $\mathfrak{F}_{min}^{(2)} = A_0(\Gamma_1(N), \mathbb{Q}) \subset A_0(\Gamma', \mathbb{Q}) \subset A_0(\Gamma(N), \mathbb{Q}) \subset \mathfrak{F}_N \subset \mathfrak{F}_{max}$ imply the lemma. □

Theorem 15. *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 $K(v(\tau))$ is the ray class field modulo 8 over K if $(2, a) = 1$. In particular, if $\mathbb{Z}[\tau]$ is the ring of integers in K, then $K(v(\tau))$ is the ray class field modulo 8 over K.*

Proof. Since $v(\tau)$ is a Hauptmodul for $\Gamma_1(8) \cap \Gamma^0(2)$ with rational Fourier coefficients and $\Gamma(8) \subset \Gamma_1(8) \cap \Gamma^0(2) \subset \Gamma_1(8)$, we obtain the first assertion by Lemma 14. In particular, if $\mathbb{Z}[\tau]$ is the ring of integers in K, then $a = 1$ and hence we conclude the last assertion immediately. □

By the same arguments in this section we are able to obtain similar results for the Rogers-Ramanujan continued fraction $r(\tau)$ which is a Hauptmodul for $\Gamma(5)$ with rational Fourier coefficients ([8]). More precisely, $r(\tau)$ becomes a modular unit over $\mathbb{Z}$ so that its singular value $r(\tau)$ at any imaginary quadratic argument τ is a unit. Further, with the notations as in Theorem 15, $K(r(\tau))$ is the ray class field modulo 5 over K if $(5, a) = 1$.

References

1. B. C. Berndt, H. H. Chan, S.-S. Huang, S.-Y. Kang, J. Sohn and S. H. Son, *The Rogers-Ramanujan continued fraction*, J. Comput. Appl. Math., 105 (1999), 9-24.
2. B. C. Berndt, H. H. Chan and L.-C. Zhang, *Explicit evaluations of the Rogers-Ramanujan continued fraction*, J. Reine Angew. Math., 480 (1996), 141-159.
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 and S.-S. Huang, *On the Ramanujan-Göllnitz-Gordon continued fraction*, Ramanujan J., 1 (1997), 75-90.
5. B. Cho and J. K. Koo, *Construction of class fields over imaginary quadratic fields and applications*, submitted.
6. D. Cox, *Primes of the Form $x^2 + ny^2$*, John Wiley & Sons, 1989.

7. W. Duke, *Continued fractions and modular functions*, Bull. Amer. Math. Soc., 42 (2005), 137-162.
8. A. Gee and M. Honsbeek, *Singular values of the Rogers-Ramanujan continued fraction*, Ramanujan J., 11 (2006), 267-284.
9. N. Ishida and N. Ishii, *The equations for modular function fields of principal congruence subgroups of prime level*, Manuscripta Math., 90 (1996), 271-285.
10. K. Iwasawa, *Algebraic Functions*, AMS Mathematical Monographs, 1993.
11. D. Kubert and S. Lang, *Modular Units*, Springer-Verlag, 1981.
12. S. Lang, *Elliptic Functions*, Springer-Verlag, 1987.
13. G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Iwanami Shoten and Princeton University Press, 1971.
14. K. R. Vasuki and B. R. Srivatsa Kumar, *Certain identities for Ramanujan-Göllnitz-Gordon continued fraction*, J. Comput. Appl. Math., 187 (2006), 87-95.

Department of Mathematical Sciences, Korea Advanced Institute of Science and Technology, 373-1 Guseong-dong, Yuseong-gu, Daejeon 305-701, Korea
E-mail address: bam@math.kaist.ac.kr

Department of Mathematical Sciences, Korea Advanced Institute of Science and Technology, 373-1 Guseong-dong, Yuseong-gu, Daejeon 305-701, Korea
E-mail address: jkkoo@math.kaist.ac.kr

Department of Mathematical Sciences, Korea Advanced Institute of Science and Technology, 373-1 Guseong-dong, Yuseong-gu, Daejeon 305-701, Korea
E-mail address: ykpark@math.kaist.ac.kr