J. Math. Soc. Japan
Vol. 62, No. 1 (2010) pp. 13–47
doi: 10.2969/jmsj/06210013

The cuspidal class number formula for certain quotient curves of the modular curve $X_0(M)$ by Atkin-Lehner involutions

By Toshikazu TAKAGI

(Received Apr. 16, 2008)

Abstract. We calculate the cuspidal class number of a certain quotient curve of the modular curve $X_0(M)$ with M square-free. For each factor r of M, let w_r denote the Atkin-Lehner type involution of $X_0(M)$. Let M_0 be a divisor of M, and W_0 the subgroup of the automorphism group of $X_0(M)$ consisting of all w_r with r dividing M_0. Our object is the quotient of $X_0(M)$ by W_0. In this paper, we consider the case where M is odd.

1. Introduction.

As is well known, the cuspidal divisor class group of a modular curve is finite (Manin [**6**], Drinfeld [**2**]). Concerning modular curves of type $X_0(n)$, $X_1(n)$, or $X(n)$, the full cuspidal class numbers are calculated by several authors (Ogg [**7**], Kubert and Lang [**4**], [**5**], Takagi [**9**], [**10**], [**11**], [**12**], [**13**]) though the choice of n is restricted. Concerning the curve $X_1(n)$ the order of a certain subgroup of the cuspidal divisor class group is also calculated (Klimek [**3**], Kubert and Lang [**4**], [**5**], Yu [**14**]) without any condition on n.

In this paper we consider another type of modular curves, which is a quotient of the modular curve $X_0(M)$ with M a square-free integer, and calculate its cuspidal class number. More precisely, for each factor r of M, let w_r denote the Atkin-Lehner type involution of $X_0(M)$ (Atkin-Lehner [**1**]). Let M_0 be a divisor of M, and W_0 the subgroup of the automorphism group of $X_0(M)$ consisting of all w_r with $r \mid M_0$. Our object is the quotient curve of $X_0(M)$ by W_0. This work is a continuation of [**12**].

In this paper, in order to avoid some complexity, we confine ourselves to considering only the case where M is odd.

Our main results are Theorems 7.8 and 7.14. As a special case, we have the following (Corollaries 7.9 and 7.15).

2000 *Mathematics Subject Classification.* Primary 11F03.
Key Words and Phrases. modular curve, modular unit, cuspidal class number.

Theorem. *Let p and q be distinct odd primes. Let X be the quotient curve of the curve $X_0(pq)$ by w_q. Then the cuspidal class number h of X is equal to the numerator of $(1/24)(p-1)(q+1)$ or $(1/12)(p-1)(q+1)$ according as $\left(\frac{p}{q}\right)=1$ or -1, respectively. The cuspidal divisor class group of X is a cyclic group of order h generated by the divisor class of $P_q - P_\infty$.*

In the theorem above, the symbol $\left(\frac{p}{q}\right)$ denotes the Legendre symbol. The symbols P_q and P_∞ denote the cusps on X represented by $1/q$ and ∞ respectively.

This theorem is related to a result by Ogg ([**8**, Corollary 1]), which proves that the divisor $P_1 + P_q - P_p - P_{pq}$ on $X_0(pq)$ defines a divisor class of order exactly equal to the numerator of $(1/24)(p-1)(q+1)$, where P_x $(x = 1,\ p,\ q,\ pq)$ denotes the cusp on $X_0(pq)$ represented by $1/x$. Note that the cusp P_{pq} coincides with the cusp represented by ∞.

The contents of the present paper are the following. In Sections 2–4, we summarize some results of [**12**, Sections 1–4]. In Section 4 some new results are added (Proposition 4.4 and Corollary 4.5). In Section 5 the value of $\Phi_\rho^{(p)}$ at the type s element δ_s is given. In Section 6 we determine the unit group on the quotient curve of $X_0(M)$ by W_0 (Theorem 6.4). It is our first main theorem. In Section 7 we divide the case into two (Cases I and II), and determine the cuspidal class number in each case (Theorems 7.8, 7.14). They are our main theorems. In Section 8 we determine the p-Sylow group of the cuspidal divisor class group for the case $p \neq 2,3$ (Theorem 8.1) and the case $p = 3$ under certain conditions (Theorem 8.5).

In the present paper we denote by $\boldsymbol{Z}$, $\boldsymbol{Q}$, $\boldsymbol{C}$, 1_2 the ring of rational integers, the field of rational numbers, the field of complex numbers, the two-by-two unit matrix, respectively. For any prime number p we denote by $\boldsymbol{Z}_p$, $\boldsymbol{Q}_p$ the ring of p-adic integers, the field of p-adic numbers, respectively.

2. Transformation formulas for Siegel functions.

In this section we summarize some results of [**12**, Section 1]. It is assumed that the reader is familiar with the contents of [**9**, Section 1].

2.1. The Principal congruence subgroup $\boldsymbol{\Gamma(I)}$ of $\boldsymbol{G(\sqrt{M})}$.

Let M be a square-free integer $(\neq 1)$ fixed throughout the present paper. We denote by T the set of all positive divisors of M, and regard it as a group with the product defined by $r \circ s = rs/(r,s)^2$ where (r,s) denotes the greatest common divisor of r and s $(r, s \in T)$. Let $\mathscr{O}$ be the order defined by $\mathscr{O} = \sum_{r\in T} \boldsymbol{Z}\sqrt{r}$. For any two positive integers n and m such that m is a divisor of M, put $I = n\sqrt{m}\mathscr{O}$. Then the set I is an ideal of the order $\mathscr{O}$. We assume that $N = nm \neq 1$.

Let $\Gamma(I)$ be the principal congruence subgroup of the group $G(\sqrt{M})$. (For the definitions of $G(\sqrt{M})$ and $\Gamma(I)$, we refer to [**9**, Section 1.1].) Let $\mathfrak{F}_I$ be the field of all automorphic functions with respect to the group $\Gamma(I)$ such that their Fourier coefficients belong to the cyclotomic field $k_N = \boldsymbol{Q}(e^{2\pi i/N})$. Let $\mathfrak{F}_1$ be the field of all automorphic functions with respect to the group $G(\sqrt{M})$ such that their Fourier coefficients belong to $\boldsymbol{Q}$. Then it is known ([**9**, Section 1 (1.15)]) that the field $\mathfrak{F}_I$ is a Galois extension of $\mathfrak{F}_1$, and its Galois group is isomorphic to the group $\mathscr{G}_I(\pm) = \mathscr{G}_I/\{\pm 1\}$, where $\mathscr{G}_I$ denotes the group consisting of all elements α of $GL_2(\mathscr{O}/I)$ which are of the form

$$\alpha = \begin{pmatrix} a\sqrt{r} & b\sqrt{r^*} \\ c\sqrt{r^*} & d\sqrt{r} \end{pmatrix} (\operatorname{mod} I) \tag{2.1}$$

with $a, b, c, d \in \boldsymbol{Z}$, $r \in T$, and $r^* = M/r$. Since the element r of T above is determined by the element α, we call it the *type* of α, and denote it by $t(\alpha)$. We denote by $\sigma(\alpha)$ the element of the Galois group $\operatorname{Gal}(\mathfrak{F}_I/\mathfrak{F}_1)$ corresponding to α.

2.2. Some properties of Siegel functions.

Here we recall some properties of Siegel functions. For any element $a = (a_1, a_2)$ of the set $\boldsymbol{Q}^2 - \boldsymbol{Z}^2$, the Siegel function $g_a(\tau)$ ($\tau \in \mathfrak{H}$) is defined in [**5**]. (The symbol $\mathfrak{H}$ denotes the upper half plane.) It has the following q-product

$$g_a(\tau) = -q_\tau^{(1/2)B_2(a_1)} e^{2\pi i a_2(a_1-1)/2}(1-q_z)\prod_{k=1}^{\infty}(1-q_\tau^k q_z)(1-q_\tau^k/q_z), \tag{2.2}$$

where $q_\tau = e^{2\pi i\tau}$, $q_z = e^{2\pi i z}$, $z = a_1\tau + a_2$, and $B_2(X) = X^2 - X + (1/6)$ (the second Bernoulli polynomial). If $b = (b_1, b_2) \in \boldsymbol{Z}^2$, then we have $g_{a+b}(\tau) = \varepsilon(a,b)g_a(\tau)$, where $\varepsilon(a,b)$ is a root of unity defined by

$$\varepsilon(a,b) = \exp\left[\frac{2\pi i}{2}(b_1b_2 + b_1 + b_2 + a_1b_2 - a_2b_1)\right]. \tag{2.3}$$

If $\alpha \in SL_2(\boldsymbol{Z})$, then we have $g_a(\alpha(\tau)) = \psi(\alpha)g_{a\alpha}(\tau)$, where ψ denotes the character of $SL_2(\boldsymbol{Z})$ appearing in the transformation formula for the square of the Dedekind η-function. Explicitly the value of $\psi(\alpha)$ with $\alpha = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ is given by

$$\psi(\alpha) = \begin{cases} (-1)^{(d-1)/2}\exp\left[\dfrac{2\pi i}{12}\left\{(b-c)d + ac(1-d^2)\right\}\right] & \text{if } d \text{ is odd,} \\ -i(-1)^{(c-1)/2}\exp\left[\dfrac{2\pi i}{12}\left\{(a+d)c + bd(1-c^2)\right\}\right] & \text{if } c \text{ is odd.} \end{cases} \tag{2.4}$$

In particular, we note that $\psi(-1_2) = -1$. (It is known that the kernel of ψ is a congruence subgroup of level 12 with index 12, and coincides with the commutator subgroup of $SL_2(\boldsymbol{Z})$.)

2.3. Modified Siegel functions with respect to the ideal I.

Here we define the modified Siegel functions with respect to the ideal I. Let r be an element of T, and $A_I'^{(r)}$ be the set of all row vectors u of the following form

$$u = \left(\frac{x}{n(m,r)}\sqrt{r}, \frac{y}{n(m,r^*)}\sqrt{r^*}\right), \tag{2.5}$$

where x and y are rational integers satisfying $u \notin \boldsymbol{Z}\sqrt{r} \times \boldsymbol{Z}\sqrt{r^*} = Z^{(r)}$. We call the element r of T above the *type* of u and denote it by $t(u)$. Put $A_I' = \bigcup_{r \in I} A_I'^{(r)}$ (disjoint). If u is an element of A_I' of type r, and α an element of $G(\sqrt{M})$ of type s $(r, s \in T)$, then the product $u\alpha$ is an element of A_I' of type $r \circ s$.

Let $u = (a_1\sqrt{r}, a_2\sqrt{r^*})$ be an element of A_I' of type r $(a_1, a_2 \in \boldsymbol{Q})$, and put $u^\circ = (a_1, a_2)$ $(\in \boldsymbol{Q}^2 - \boldsymbol{Z}^2)$. Then we define the modified Siegel function $g_u(\tau)$ $(\tau \in \mathfrak{H})$ with respect to the ideal I by

$$g_u(\tau) = g_{u^\circ}\left(\sqrt{\frac{r}{r^*}} \times \tau\right). \tag{2.6}$$

For an element $v = (b_1\sqrt{r}, b_2\sqrt{r^*})$ of $Z^{(r)}$ $(b_1, b_2 \in \boldsymbol{Z})$, write $v^\circ = (b_1, b_2)$ $(\in \boldsymbol{Z}^2)$. For elements $u \in A_I'^{(r)}$ and $v \in Z^{(r)}$, we put

$$\varepsilon(u, v) = \varepsilon(u^\circ, v^\circ). \tag{2.7}$$

Let

$$\alpha = \begin{pmatrix} a\sqrt{s} & b\sqrt{s^*} \\ c\sqrt{s^*} & d\sqrt{s} \end{pmatrix} \tag{2.8}$$

be an element of $G(\sqrt{M})$ of type s $(a, b, c, d \in \boldsymbol{Z},\ s \in T)$. For an element r of T, we put

$$\alpha^{(r)} = \begin{pmatrix} a(r,s) & b(r,s^*) \\ c(r^*,s^*) & d(r^*,s) \end{pmatrix}. \tag{2.9}$$

Then the matrix $\alpha^{(r)}$ belongs to $SL_2(\boldsymbol{Z})$.

Now we have the following transformation formulas for the modified Siegel functions ([**12**, Proposition 1.1]).

PROPOSITION 2.1. *Let u be an element of A'_I of type r.*
(1) *Let $v \in Z^{(r)}$. Then $g_{u+v}(\tau) = \varepsilon(u,v) g_u(\tau)$.*
(2) *Let $\alpha \in G(\sqrt{M})$. Then $g_u(\alpha(\tau)) = \psi_r(\alpha) g_{u\alpha}(\tau)$, where $\psi_r(\alpha) = \psi(\alpha^{(r)})$.*
(3) *Let $\alpha \in \Gamma(I)$. Then $g_u(\alpha(\tau)) = \varepsilon_u(\alpha)\psi_r(\alpha) g_u(\tau)$, where $\varepsilon_u(\alpha) = \varepsilon(u,v)$ with $v = u\alpha - u (\in Z^{(r)})$.*

Since the number $\varepsilon(u,v)$ (respectively $\psi_r(\alpha)$) in this proposition is a $2N$th root (respectively a 12th root) of unity, the function $g_u^{[2N,12]}$ depends only on the residue class of u modulo $Z^{(r)}$, and is invariant under the exchange $u \to -u$. (The symbol $[2N, 12]$ denotes the least common multiple of $2N$ and 12.) Moreover, the function $g_u^{[2N,12]}$ belongs to the function field $\mathfrak{F}_I$ and has no zeros and poles on the upper half plane $\mathfrak{H}$.

3. Modular units on the curve $X_0(M)$ and its quotient curves.

In this section we summarize some results of [**12**, Sections 2, 3].

3.1. The modular curve $X_0(M)$ and its quotient curves.

Let M be the square-free integer fixed in the present paper. Let $\Gamma_0(M)$ be the subgroup of $SL_2(\boldsymbol{Z})$ consisting of all elements of the form $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with $c \equiv 0 \pmod{M}$. Let Γ be a Fuchsian group of the first kind. We denote by X_Γ the complete nonsingular curve associated with the compactification of the quotient space $\Gamma\backslash\mathfrak{H}$. When $\Gamma = \Gamma_0(M)$, the curve X_Γ is written as $X_0(M)$. Let $f(\tau)$ ($\tau \in \mathfrak{H}$) be an automorphic function with respect to Γ. If the function $f(\tau)$ has no zeros and poles on $\mathfrak{H}$, we call f as a *modular unit* with respect to Γ and also a *modular unit* on the curve X_Γ.

Let T_0 be a subgroup of T. Let Γ_{T_0} be the subgroup of $G(\sqrt{M})$ consisting of all elements such that their types belong to T_0. When $T_0 = \{1\}$ $(= 1)$, the group Γ_1 is isomorphic to $\Gamma_0(M)$; more precisely,

$$\Gamma_1 = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{M} \end{pmatrix}^{-1} \Gamma_0(M) \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{M} \end{pmatrix}. \tag{3.1}$$

Hence, if $\Gamma = \Gamma_1$, then the curve $X_{\Gamma_1} (= X_1)$ is isomorphic to the modular curve $X_0(M)$. In general, if $\Gamma = \Gamma_{T_0}$, then the curve $X_{\Gamma_{T_0}}$ $(= X_{T_0})$ is a quotient curve of X_1 by a subgroup of the automorphism group of X_1. This subgroup can be described as follows. Since the group Γ_1 is a normal subgroup of Γ_{T_0} with

$\Gamma_{T_0}/\Gamma_1 \cong T_0$, to each element r of T_0 there exists an automorphism of the curve X_1, whose corresponding automorphism of the curve $X_0(M)$ is the Atkin-Lehner involution w_r. Moreover, the subgroup consisting of all w_r with $r \in T_0$ is isomorphic to the group T_0. Hence, the curve X_{T_0} is isomorphic to the quotient curve of $X_0(M)$ by the group consisting of all Atkin-Lehner involutions w_r with $r \in T_0$.

3.2. Cuspidal prime divisors.

We use the notation in [**9**, Section 1]. Let G_{A_+} be the adele group associated with $G(\sqrt{M})$, and U its unit subgroup. Let U_{T_0} be the subgroup of U consisting of all elements such that their types belong to T_0. Put $S = \boldsymbol{Q}^\times \ll \sqrt{M} \gg U_{T_0}$. Then to this S corresponds the function field $\mathfrak{F}_S$. For simplicity, we write $\mathfrak{F}(T_0)$ for this field $\mathfrak{F}_S$. Then the field $\boldsymbol{C}\mathfrak{F}(T_0)$ is the field of all automorphic functions with respect to the group Γ_{T_0}, and $\boldsymbol{Q}$ is algebraically closed in $\mathfrak{F}(T_0)$ ([**9**, Proposition 1.6]). It can be shown in a similar way to [**9**, Proposition 1.7] that the field $\mathfrak{F}(T_0)$ is the field of all automorphic functions with respect to Γ_{T_0} such that their Fourier coefficients belong to $\boldsymbol{Q}$. In particular, we have $\mathfrak{F}(T) = \mathfrak{F}_1$ (for the definition of $\mathfrak{F}_1$ see [**9**, Section 1]). The field $\mathfrak{F}(T_0)$ is an abelian extension of $\mathfrak{F}_1$ such that the Galois group is isomorphic to T/T_0. The field $\mathfrak{F}(1)$ $(T_0 = 1)$ is isomorphic to the function field $[= \mathfrak{F}_0(M)]$ which consists of all automorphic functions with respect to $\Gamma_0(M)$ such that their Fourier coefficients belong to $\boldsymbol{Q}$. More precisely, we have

$$\mathfrak{F}(1) = \left\{ f\left(\frac{\tau}{\sqrt{M}}\right) \,\middle|\, f(\tau) \in \mathfrak{F}_0(M) \right\}. \tag{3.2}$$

Let P_∞ denote the prime divisor of $\mathfrak{F}(T_0)$ defined by the q-expansion. Let P be a prime divisor of $\mathfrak{F}(T_0)$, and ν_P the valuation of P. For any element σ of $\mathrm{Gal}(\mathfrak{F}(T_0)/\mathfrak{F}_1)$ $(\cong T/T_0)$, the prime divisor P^σ is defined by $\nu_{P^\sigma}(h^\sigma) = \nu_P(h)$ $(h \in \mathfrak{F}(T_0))$. We can regard the prime divisor P_∞^σ as a prime divisor of $\boldsymbol{C}\mathfrak{F}(T_0)$, in other words, a point on the curve X_{T_0}. More precisely, let us denote by the same symbol σ the corresponding element of T/T_0. Let α be any element of $G(\sqrt{M})$ whose type belongs to the coset σ. Then the prime divisor P_∞^σ corresponds to the point on the curve X_{T_0} represented by $\alpha^{-1}(\infty)$. The set of the prime divisors P_∞^σ can be identified with the set of all the cusps on the curve X_{T_0}. The group T/T_0 and the set of all the cusps on the curve X_{T_0} correspond bijectively by the mapping $\sigma \mapsto P_\infty^\sigma$. We call the prime divisors P_∞^σ the *cuspidal prime divisors* of $\mathfrak{F}(T_0)$.

Let $\mathscr{D}$ be the free abelian group generated by the cuspidal prime divisors of $\mathfrak{F}(T_0)$, and $\mathscr{D}_0$ the subgroup of $\mathscr{D}$ consisting of all elements with degree 0. Let $\mathscr{F}$ (respectively $\mathscr{F}_{\boldsymbol{C}}$) be the group of all modular units in $\mathfrak{F}(T_0)$ (respectively

$\boldsymbol{C}\mathfrak{F}(T_0))$. Then we have $\mathscr{F}_{\boldsymbol{C}} = \boldsymbol{C}^{\times}\mathscr{F}$, hence we can identify the divisor group $\mathrm{div}(\mathscr{F})$ with the divisor group $\mathrm{div}(\mathscr{F}_{\boldsymbol{C}})$, and the factor group

$$\mathscr{C} = \mathscr{D}_0/\mathrm{div}(\mathscr{F}) \tag{3.3}$$

with the cuspidal divisor class group on the curve X_{T_0}.

Let $R = \boldsymbol{Z}[T/T_0]$ be the group ring of T/T_0, and R_0 the additive subgroup of R consisting of all elements with degree 0. Then the mapping $P_\infty^\sigma \mapsto \sigma$ defines an isomorphism

$$\varphi : \mathscr{D} \cong R \tag{3.4}$$

and we have $\varphi(\mathscr{D}_0) = R_0$.

3.3. The function $f_\rho^{(p)}$ and modular units.

Here we construct modular units in the field $\mathfrak{F}(T_0)$ by modified Siegel functions. Let p be any prime factor of M, and put $I_p = \sqrt{p}\mathscr{O}$. Let $\mathscr{R}_{I_p}^{(r)}$ $(r \in T)$ be the subset of $A_{I_p}'^{(r)}$ consisting of all elements u which are of the form $u = (0, (y/p)\sqrt{r^*})$ or $((x/p)\sqrt{r}, 0)$ according as $p \nmid r$ or $p \mid r$, where y (respectively x) is an integer satisfying $1 \le y \le p/2$ (respectively $1 \le x \le p/2$).

When $p = 2$ (this case occurs only when M is even), the set $\mathscr{R}_{I_2}^{(r)}$ contains only one element u that is $(0, (1/2)\sqrt{r^*})$ or $((1/2)\sqrt{r}, 0)$ according as $2 \nmid r$ or $2 \mid r$. For this element u, the Siegel function $g_u(\tau)$ is a square of an automorphic function. We can express square roots of the function $g_u(\tau)$ as products of modified Siegel functions with respect to the ideal $2\sqrt{2}\mathscr{O}$. For definiteness, we denote by $\sqrt{g_u}(\tau)$ one of the square roots defined by

$$\sqrt{g_u}(\tau) = \begin{cases} g_{(0,\sqrt{r^*}/4)}(\tau) \cdot g_{(\sqrt{r}/2,\sqrt{r^*}/4)}(\tau) \cdot c & \text{if } 2 \nmid r, \\ g_{(\sqrt{r}/4,0)}(\tau) \cdot g_{(\sqrt{r}/4,\sqrt{r^*}/2)}(\tau) \cdot (-c) & \text{if } 2 \mid r, \end{cases} \tag{3.5}$$

where $c = \exp[2\pi i \times (7/16)]$.

For an element u of $\mathscr{R}_{I_p}^{(r)}$, we define the function $\widehat{g}_u(\tau)$ by

$$\widehat{g}_u(\tau) = \begin{cases} g_u(\tau) & \text{if } p \neq 2, \\ \sqrt{g_u}(\tau) & \text{if } p = 2. \end{cases} \tag{3.6}$$

Now, for each prime factor p of M and each coset $\rho \in T/T_0$, we define the function $f_\rho^{(p)}(\tau)$ by

$$f_\rho^{(p)}(\tau) = \prod_{r\in\rho}\left\{\prod_{u\in\mathscr{R}_{I_p}^{(r)}} \widehat{g}_u(\tau)\right\}. \tag{3.7}$$

Then we have the following proposition ([**12**, Proposition 2.1]).

Proposition 3.1. *Let p be a prime factor of M, and ρ a coset in T/T_0. Then the function $\left(f_\rho^{(p)}\right)^{12p}$ is a modular unit contained in the function field $\mathfrak{F}(T_0)$. Moreover, if we identify* $\mathrm{Gal}(\mathfrak{F}(T_0)/\mathfrak{F}_1)$ *with T/T_0, then for an element $\sigma \in T/T_0$, we have*

$$\left\{\left(f_\rho^{(p)}\right)^{12p}\right\}^\sigma = \left(f_{\rho\sigma}^{(p)}\right)^{12p}.$$

3.4. The function h_ρ and modular units.

Here we construct another type of modular units in the field $\mathfrak{F}(T_0)$ by the Dedekind η-function $\eta(\tau)$. Let $H(\tau)$ be the function defined by

$$H(\tau) = \eta\left(\frac{\tau}{\sqrt{M}}\right) = t^{1/24}\prod_{n=1}^{\infty}(1-t^n), \tag{3.8}$$

where $t = \exp\left[2\pi i\tau/\sqrt{M}\right]$.

Now, for each coset $\rho \in T/T_0$, we define the function $h_\rho(\tau)$ by

$$h_\rho(\tau) = \frac{\prod_{r\in\rho} H(r\tau)}{\prod_{s\in[1]} H(s\tau)}, \tag{3.9}$$

where the symbol $[1]$ denotes the unit element of T/T_0, namely, $[1] = T_0$. In particular, we have $h_{[1]}(\tau) = 1$. In general, we denote by $[r]$ $(r \in T)$ the coset rT_0.

About the relation between $f_\rho^{(p)}(\tau)$ and $h_\rho(\tau)$, we have the following proposition ([**12**, Proposition 2.3]).

Proposition 3.2.

(1) *Let p be a prime factor of M, and ρ a coset in T/T_0. Then we have*

$$f_\rho^{(p)}(\tau) = \frac{h_{[p]\rho}(\tau)}{h_\rho(\tau)} \times c_1,$$

where c_1 is a nonzero constant. In particular, $f_{[1]}^{(p)}(\tau) = h_{[p]}(\tau) \times c_1$.

(2) *Let* p_i $(i = 1, \dots, k)$ *be prime factors of* M. *Then we have*

$$h_{[p_1]\cdots[p_k]}(\tau) = f^{(p_1)}_{[p_2]\cdots[p_k]}(\tau) \times f^{(p_2)}_{[p_3]\cdots[p_k]}(\tau) \times \cdots \times f^{(p_k)}_{[1]}(\tau) \times c_2,$$

where c_2 *is a nonzero constant.*

By Propositions 3.1 and 3.2, we see that the function $(h_\rho)^{12M}$ is a modular unit in the field $\mathfrak{F}(T_0)$. Later in Corollary 4.5 we shall see some stronger statements concerning the powers of $f^{(p)}_\rho$ and h_ρ.

3.5. The divisors of $f^{(p)}_\rho$ and h_ρ.

Put $\mathscr{D}_{\boldsymbol{Q}} = \mathscr{D} \otimes \boldsymbol{Q}$ and $R_{\boldsymbol{Q}} = R \otimes \boldsymbol{Q}$. Then we can extend the isomorphism (3.4) to an isomorphism $\mathscr{D}_{\boldsymbol{Q}} \cong R_{\boldsymbol{Q}}$, which we also denote by φ. Since the functions $\left(f^{(p)}_\rho\right)^{12p}$ and $(h_\rho)^{12M}$ are contained in the field $\mathfrak{F}(T_0)$, their divisors are well defined. We denote by $\operatorname{div}\left(f^{(p)}_\rho\right)$ and $\operatorname{div}(h_\rho)$ the elements of $\mathscr{D}_{\boldsymbol{Q}}$ defined by

$$\operatorname{div}\left(f^{(p)}_\rho\right) = \frac{1}{12p}\operatorname{div}\left(\left(f^{(p)}_\rho\right)^{12p}\right), \ \operatorname{div}(h_\rho) = \frac{1}{12M}\operatorname{div}\left((h_\rho)^{12M}\right). \qquad (3.10)$$

Let θ be the element of $R_{\boldsymbol{Q}}$ defined by

$$\theta = \frac{1}{24}\sum_{\rho \in T/T_0}\left(\sum_{r \in \rho} r\right)\rho = \frac{1}{24}\prod_{p|M}(1 + p[p]), \qquad (3.11)$$

where p runs through all prime factors of M. Then we have the following propositions ([**12**, Proposition 2.4, Lemma 3.1]).

PROPOSITION 3.3. *Let* p *be a prime factor of* M, *and* ρ *a coset in* T/T_0.

(1) $\varphi\left(\operatorname{div}\left(f^{(p)}_\rho\right)\right) = \rho([p] - 1)\theta$.

(2) $\varphi\left(\operatorname{div}(h_\rho)\right) = (\rho - 1)\theta$.

PROPOSITION 3.4. *The element* θ *is invertible in the algebra* $R_{\boldsymbol{Q}}$.

3.6. The group of modular units.

In [**12**, Section 3], we proved that every modular unit in the field $\mathfrak{F}(T_0)$ can be expressed by the functions h_ρ. Namely, we have the following theorem ([**12**, Theorem 3.3]).

THEOREM 3.5. *Let $g(\tau)$ be any modular unit in the field $\mathfrak{F}(T_0)$. Then there are rational integers $m(\rho)$ $(\rho \in T/T_0, \neq [1])$ and a rational number $c \neq 0$ such that*

$$g(\tau) = c \cdot \prod_{\rho \in T/T_0, \neq [1]} h_\rho(\tau)^{m(\rho)},$$

and moreover this expression is unique.

4. The characters $\Phi_\rho^{(p)}$ and Ψ_ρ.

In order to calculate the cuspidal class number, we need to determine the group $\mathscr{F}$ of all modular units in the function field $\mathfrak{F}(T_0)$. The determination reduces to the determination of the characters $\Phi_\rho^{(p)}$ and Ψ_ρ of the group Γ_{T_0}. In this section we recall some results of [**12**, Section 4] and add some new results (Proposition 4.4 and Corollary 4.5).

4.1. Definition of $\Phi_\rho^{(p)}$ and Ψ_ρ.

Let p be a prime factor of M, and ρ a coset in T/T_0. Since the functions $\left(f_\rho^{(p)}\right)^{12p}$ and $(h_\rho)^{12M}$ are automorphic functions with respect to the group Γ_{T_0}, we can define the characters $\Phi_\rho^{(p)}$ and Ψ_ρ of Γ_{T_0} by the following equations:

$$f_\rho^{(p)}(\alpha(\tau)) = \Phi_\rho^{(p)}(\alpha) \cdot f_\rho^{(p)}(\tau), \tag{4.1}$$

$$h_\rho(\alpha(\tau)) = \Psi_\rho(\alpha) \cdot h_\rho(\tau) \tag{4.2}$$

(for all $\alpha \in \Gamma_{T_0}$).

Let $g(\tau)$ be a function of the form

$$g(\tau) = \prod_{\rho \in T/T_0, \neq [1]} h_\rho(\tau)^{m(\rho)}, \tag{4.3}$$

where $m(\rho)$ are rational integers $(\rho \in T/T_0, \neq [1])$. Then the function $g(\tau)$ belongs to the group $\mathscr{F}$ of the modular units in the field $\mathfrak{F}(T_0)$ if and only if the following equation holds for all $\alpha \in \Gamma_{T_0}$:

$$\prod_{\rho \in T/T_0, \neq [1]} \left\{\Psi_\rho(\alpha)\right\}^{m(\rho)} = 1. \tag{4.4}$$

Thus, taking account of Theorem 3.5, in order to determine the group $\mathscr{F}$ of the modular units, we need to know the character Ψ_ρ. Let $\rho = [p_1] \cdots [p_k]$, where p_i $(i = 1, \ldots, k)$ are prime factors of M. Then, by (2) of Proposition 3.2, we have

$$\Psi_\rho(\alpha) = \Phi^{(p_1)}_{[p_2]\cdots[p_k]}(\alpha) \cdot \Phi^{(p_2)}_{[p_3]\cdots[p_k]}(\alpha) \cdot \cdots \cdot \Phi^{(p_k)}_{[1]}(\alpha) \tag{4.5}$$

(for all $\alpha \in \Gamma_{T_0}$). We shall first determine the character $\Phi^{(p)}_\rho$, and next the character Ψ_ρ by the relation (4.5).

4.2. Generators of the factor group $\Gamma_{T_0}/\pm\Gamma(\widetilde{M}\mathscr{O})$.

Put $e = 2$ or 4 according as M is odd or even. Also, put

$$\widetilde{M} = 2^e \cdot 3 \cdot \prod_{p|M, \neq 2,3} p, \tag{4.6}$$

where p runs through all prime factors of M satisfying $p \neq 2, 3$. Then we have the following proposition ([**12**, Lemma 4.2]).

Proposition 4.1. *Let p be a prime factor of M, and ρ a coset in T/T_0. Then the characters $\Phi^{(p)}_\rho$ and Ψ_ρ of Γ_{T_0} are trivial on the group $\pm\Gamma(\widetilde{M}\mathscr{O})$.*

Hence, in order to determine the characters $\Phi^{(p)}_\rho$ and Ψ_ρ, it is sufficient to determine their values for some elements of Γ_{T_0} which generate the factor group $\Gamma_{T_0}/\pm\Gamma(\widetilde{M}\mathscr{O})$.

For each prime factor q of $\widetilde{M}$ and an element s of T_0, we define the elements α_q, β_q, γ_q and δ_s as follows. Let α_q, β_q and γ_q be elements of Γ_{T_0} of type 1 which satisfy the following congruences:

$$\alpha_q \equiv \begin{pmatrix} 1 & \sqrt{M} \\ 0 & 1 \end{pmatrix} \pmod{q^f\mathscr{O}}, \quad \equiv 1_2 \pmod{q^{-f}\widetilde{M}\mathscr{O}}, \tag{4.7}$$

$$\beta_q \equiv \begin{pmatrix} 1 & 0 \\ \sqrt{M} & 1 \end{pmatrix} \pmod{q^f\mathscr{O}}, \quad \equiv 1_2 \pmod{q^{-f}\widetilde{M}\mathscr{O}}, \tag{4.8}$$

$$\gamma_q \equiv \begin{pmatrix} d^{-1} & 0 \\ 0 & d \end{pmatrix} \pmod{q^f\mathscr{O}}, \quad \equiv 1_2 \pmod{q^{-f}\widetilde{M}\mathscr{O}}, \tag{4.9}$$

where f is a positive integer such that $q^f \parallel \widetilde{M}$, and d is a positive integer such that d is a primitive root mod q or equal to 5 according as $q \neq 2$ or $q = 2$. Let δ_s be an element of Γ_{T_0} of type s which satisfies the following congruences for every prime factor q of $\widetilde{M}$ with $q^f \parallel \widetilde{M}$:

$$\delta_s \equiv \begin{cases} \begin{pmatrix} s^{-1}\sqrt{s} & 0 \\ 0 & \sqrt{s} \end{pmatrix} \pmod{q^f \mathscr{O}} & \text{if } (q,s)=1, \\ \begin{pmatrix} 0 & -\sqrt{s^*} \\ s^{*-1}\sqrt{s^*} & 0 \end{pmatrix} \pmod{q^f \mathscr{O}} & \text{if } (q,s)\neq 1. \end{cases} \tag{4.10}$$

Then the set of the elements α_q, β_q, γ_q and δ_s generates the factor group $\Gamma_{T_0}/\pm\Gamma(\widetilde{M}\mathscr{O})$, where s runs through a subset of T_0 which generates the group T_0.

Though the element γ_q depends on the choice of d, we do not indicate the dependence in its notation because as we shall see in the following subsection the values of $\Phi_\rho^{(p)}$ and Ψ_ρ at the element γ_q do not depend on d.

4.3. The values of $\Phi_\rho^{(p)}$ and Ψ_ρ at the elements α_q, β_q and γ_q.

The values of $\Phi_\rho^{(p)}$ and Ψ_ρ at the elements α_q, β_q and γ_q are given in the following propositions ([**12**, Propositions 4.1, 4.2]). The symbols Δ_p and Δ_ρ there are defined as follows. Let p be a prime factor of M, and ρ a coset in T/T_0. Then $\Delta_p = 1$ or $(-1)^{|T_0|}$ according as $p\neq 2$ or $p=2$. If $\rho=[p_1]\cdots[p_k]$ where p_i are prime factors of M, then $\Delta_\rho = \Delta_{p_1}\cdot\cdots\cdot\Delta_{p_k}$.

PROPOSITION 4.2. *Let p be a prime factor of M, and ρ a coset in T/T_0. Then for each prime factor q of $\widetilde{M}$, we have the following*:

$$\Phi_\rho^{(p)}(\alpha_q) = \begin{cases} \Delta_p \exp\left[-\dfrac{2\pi i}{8}\left(\displaystyle\sum_{s\in[p]\rho} s - \sum_{r\in\rho} r\right)\right] & \text{if } q=2, \\ \Delta_p \exp\left[\dfrac{2\pi i}{6}\left(\displaystyle\sum_{s\in[p]\rho} s - \sum_{r\in\rho} r\right)\right] & \text{if } q=3, \\ 1 & \text{if } q\neq 2,3, \end{cases}$$

$$\Phi_\rho^{(p)}(\beta_q) = \begin{cases} \Delta_p \exp\left[\dfrac{2\pi i}{8}\left(\displaystyle\sum_{s\in[p]\rho} s^* - \sum_{r\in\rho} r^*\right)\right] & \text{if } q=2, \\ \Delta_p \exp\left[-\dfrac{2\pi i}{6}\left(\displaystyle\sum_{s\in[p]\rho} s^* - \sum_{r\in\rho} r^*\right)\right] & \text{if } q=3, \\ 1 & \text{if } q\neq 2,3, \end{cases}$$

$$\Phi_\rho^{(p)}(\gamma_q) = \begin{cases} (-1)^{|T_0|} & \text{if } q=p, \\ 1 & \text{if } q\neq p. \end{cases}$$

PROPOSITION 4.3. *Let ρ be a coset in T/T_0. Then for each prime factor q of $\widetilde{M}$, we have the following*:

$$\Psi_\rho(\alpha_q) = \begin{cases} \Delta_\rho \exp\left[-\dfrac{2\pi i}{8}\left(\displaystyle\sum_{s\in\rho} s - \sum_{r\in[1]} r\right)\right] & \text{if } q = 2, \\ \Delta_\rho \exp\left[\dfrac{2\pi i}{6}\left(\displaystyle\sum_{s\in\rho} s - \sum_{r\in[1]} r\right)\right] & \text{if } q = 3, \\ 1 & \text{if } q \neq 2, 3, \end{cases}$$

$$\Psi_\rho(\beta_q) = \begin{cases} \Delta_\rho \exp\left[\dfrac{2\pi i}{8}\left(\displaystyle\sum_{s\in\rho} s^* - \sum_{r\in[1]} r^*\right)\right] & \text{if } q = 2, \\ \Delta_\rho \exp\left[-\dfrac{2\pi i}{6}\left(\displaystyle\sum_{s\in\rho} s^* - \sum_{r\in[1]} r^*\right)\right] & \text{if } q = 3, \\ 1 & \text{if } q \neq 2, 3, \end{cases}$$

$$\Psi_\rho(\gamma_q) = \begin{cases} -1 & \text{if } T_0 = 1 \text{ and } q \mid \rho, \\ 1 & \text{otherwise.} \end{cases}$$

In the expression for $\Psi_\rho(\gamma_q)$ in Proposition 4.3 with $T_0 = 1$, the coset ρ is identified with its unique representative. As a consequence of these propositions, we have the following.

PROPOSITION 4.4. *Let p be a prime factor of M, and ρ a coset in T/T_0.*
(1) *The character $\Phi_\rho^{(p)}$ takes its values in the group of 24th roots of unity, in the group of 12th roots of unity if $T_0 \neq 1$ or $p \neq 2$, and moreover in the group of 6th roots of unity if M is odd and $T_0 \neq 1$.*
(2) *The character Ψ_ρ takes its values in the group of 24th roots of unity, in the group of 12th roots of unity if M is odd or $T_0 \neq 1$, and moreover in the group of 6th roots of unity if M is odd and $T_0 \neq 1$.*

PROOF. (1) In the following we use Proposition 4.2. If $T_0 = 1$, then the element δ_1 $(s = 1)$ belongs to $\Gamma(\widetilde{M}\mathscr{O})$, hence $\Phi_\rho^{(p)}(\delta_1) = 1$. By the definition of δ_s the element δ_s^2 can be written as a product of elements γ_q modulo $\pm\Gamma(\widetilde{M}\mathscr{O})$. Hence, if $T_0 \neq 1$, we have $\Phi_\rho^{(p)}(\delta_s^2) = 1$, therefore $\Phi_\rho^{(p)}(\delta_s) = \pm 1$. Since $\sum_{s\in[p]\rho} s^* - \sum_{r\in\rho} r^* = \sum_{s\in[p]\rho^*} s - \sum_{r\in\rho^*} r$ with $\rho^* = \rho[M]$, we have $\Phi_\rho^{(p)}(\beta_2) = \left\{\Phi_{\rho^*}^{(p)}(\alpha_2)\right\}^{-1}$. Thus, it is sufficient to consider the value of α_2. The 24th roots part of the statement is obvious. Let us assume $p \neq 2$. Since $p^2 \equiv 1 \pmod 8$, we have $\sum_{s\in[p]\rho} s = \sum_{r\in\rho} p\circ r \equiv \sum_{r\in\rho} pr \pmod 8$, hence

$$\sum_{s\in[p]\rho} s - \sum_{r\in\rho} r \equiv (p-1)\sum_{r\in\rho} r \pmod 8. \tag{4.11}$$

This implies that the term on the left of the congruence (4.11) is even. Next, let us assume $p = 2$. Let ρ' (respectively ρ'') be the set of all $r \in \rho$ such that r is odd (respectively even). Since $2\circ r = 2r$ or $r/2$ according as $r \in \rho'$ or ρ'', the difference $2\circ r - r$ is always odd. Hence

$$\sum_{s\in[2]\rho} s - \sum_{r\in\rho} r = \sum_{r\in\rho}(2\circ r - r) \equiv |T_0| \pmod 2. \tag{4.12}$$

This implies that if $T_0 \neq 1$, then the term on the left of the equation (4.12) is even. Thus, $\sum_{s\in[p]\rho} s - \sum_{r\in\rho} r$ is even if $T_0 \neq 1$ or $p \neq 2$, which proves the 12th roots part of the statement. If M is odd and $T_0 \neq 1$, then the equation (4.11) implies that $\sum_{s\in[p]\rho} s - \sum_{r\in\rho} r$ is a multiple of 4, which proves the 6th roots part of the statement. (2) This follows from (1) and the relation (4.5). □

Corollary 4.5. *Let p be a prime factor of M, and ρ a coset in T/T_0.*
(1) *The unit group $\mathscr{F}$ of $\mathfrak{F}(T_0)$ contains the 24th power of $f_\rho^{(p)}$, the 12th power of $f_\rho^{(p)}$ if $T_0 \neq 1$ or $p \neq 2$, and moreover the 6th power of $f_\rho^{(p)}$ if M is odd and $T_0 \neq 1$.*
(2) *The unit group $\mathscr{F}$ of $\mathfrak{F}(T_0)$ contains the 24th power of h_ρ, the 12th power of h_ρ if M is odd or $T_0 \neq 1$, and moreover the 6th power of h_ρ if M is odd and $T_0 \neq 1$.*

5. Calculation of the value of $\Phi_\rho^{(p)}$ at δ_s.

In this section we calculate the value of $\Phi_\rho^{(p)}$ at δ_s. For our later use, it is sufficient to consider the case where $p \neq 2$ and $(p,s) = 1$. Since $\Phi_\rho^{(p)}(\delta_1) = 1$, we can assume that $s \neq 1$, hence $T_0 \neq 1$. Therefore, in the Subsections 5.1–5.4, we assume that

$$p \neq 2,\ (p,s) = 1,\ s \neq 1. \tag{5.1}$$

5.1. Decomposition into two parts.

By the definition (3.7) of $f_\rho^{(p)}(\tau)$ we have

$$f_\rho^{(p)}(\delta_s(\tau)) = \prod_{r\in\rho}\left\{\prod_{u\in\mathscr{R}_{I_p}^{(r)}} g_u(\delta_s(\tau))\right\}, \tag{5.2}$$

where $I_p = \sqrt{p}\mathscr{O}$. Since $g_u(\delta_s(\tau)) = \psi_r(\delta_s) g_{u\delta_s}(\tau)$ by Proposition 2.1, we have the decomposition into two parts:

$$f_\rho^{(p)}(\delta_s(\tau)) = \prod_{r\in\rho}\left\{\prod_{u\in\mathscr{R}_{I_p}^{(r)}} \psi_r(\delta_s)\right\} \cdot \prod_{r\in\rho}\left\{\prod_{u\in\mathscr{R}_{I_p}^{(r)}} g_{u\delta_s}(\tau)\right\}. \tag{5.3}$$

5.2. The ψ part.

LEMMA 5.1. $\psi_r(\delta_s) = \begin{cases} (-1)^{\frac{1}{2}\{(r^*,s)-1\}} & \text{if } (s,2)=1, \\ -i\cdot(-1)^{\frac{1}{2}\{(r,s^*)-1\}} & \text{if } (s,2)\neq 1. \end{cases}$

PROOF. Put

$$\delta_s = \begin{pmatrix} a\sqrt{s} & b\sqrt{s^*} \\ c\sqrt{s^*} & d\sqrt{s} \end{pmatrix}. \tag{5.4}$$

Assume $(s,6)=1$. In the definition (4.10) of δ_s, putting $q=2$ and 3, we have $as \equiv d \equiv 1 \pmod{2^e\cdot 3}$ and $b\equiv c\equiv 0 \pmod{2^e\cdot 3}$. Hence, $d(r^*,s)\equiv (r^*,s) \pmod 4$ and $b(r,s^*)\equiv c(r^*,s^*)\equiv 0 \pmod{12}$. Combining these results with $\psi_r(\delta_s) = \psi\left(\delta_s^{(r)}\right)$ and the equation (2.4), we have $\psi_r(\delta_s) = (-1)^{(1/2)\{(r^*,s)-1\}}$. (Note that $d(r^*,s)$ is odd.) The other cases $(s,6)=2$, 3, 6 can be treated similarly. □

In the decomposition (5.3), the ψ part is given as follows.

LEMMA 5.2.

$$\prod_{r\in\rho}\left\{\prod_{u\in\mathscr{R}_{I_p}^{(r)}} \psi_r(\delta_s)\right\} = \begin{cases} \exp\left[\dfrac{2\pi i}{2}\cdot\dfrac{1}{2}(p-1)\cdot\dfrac{1}{2}\displaystyle\sum_{r\in\rho}\{(r^*,s)-1\}\right] & \text{if } (s,2)=1, \\ \exp\left[\dfrac{2\pi i}{2}\cdot\dfrac{1}{2}(p-1)\cdot\dfrac{1}{2}\displaystyle\sum_{r\in\rho}(r,s^*)\right] & \text{if } (s,2)\neq 1. \end{cases}$$

PROOF. By the facts that $\psi_r(\delta_s)$ does not depend on u and that $\left|\mathscr{R}_{I_p}^{(r)}\right| = (1/2)(p-1)$, the case $(s,2)=1$ follows immediately from Lemma 5.1. Next, we have $\prod_{r\in\rho}\left\{\prod_{u\in\mathscr{R}_{I_p}^{(r)}}(-i)\right\} = \exp[2\pi i/2\cdot(1/2)(p-1)\cdot(1/2)|T_0|]$. (Since $T_0\neq 1$, the number $|\rho|=|T_0|$ is even.) From this and Lemma 5.1, the case $(s,2)\neq 1$ follows immediately. □

5.3. The $g_{u\delta_s}$ part with $r \in \rho^{(1)}$.

Let us denote by $\rho^{(1)}$ (respectively $\rho^{(2)}$) the set of all elements $r \in \rho$ with $p \nmid r$ (respectively $p \mid r$). Here we assume $r \in \rho^{(1)}$. In this case the element u of $\mathscr{R}_{I_p}^{(r)}$ is of the form

$$u = u(0, y; r) = \left(0, \frac{y}{p}\sqrt{r^*}\right), \tag{5.5}$$

where y is an integer with $1 \le y \le (p-1)/2$.

Let δ_s be written as in the equation (5.4). Then we have

$$u(0, y; r)\delta_s = \left(\frac{cy(r^*, s^*)}{p}\sqrt{r \circ s}, \frac{dy(r^*, s)}{p}\sqrt{(r \circ s)^*}\right). \tag{5.6}$$

Since $(p, s) = 1$ and $p \nmid r$, we have $p \mid (r^*, s^*)$ and $r \circ s \in \rho^{(1)}$. Also by the definition of δ_s and the assumption $(p, s) = 1$, we have $d \equiv 1 \pmod p$.

For each y $(1 \le y \le (p-1)/2)$, we denote by $k(y)$ the unique integer satisfying $1 \le k(y) \le (p-1)/2$ and

$$dy(r^*, s) \equiv \pm k(y) \pmod p. \tag{5.7}$$

We call y to be of *plus* (respectively *minus*) type if the plus (respectively minus) sign appears in the congruence (5.7). Note that if $y_1 \neq y_2$, then $k(y_1) \neq k(y_2)$.

Let l be an integer satisfying

$$dy(r^*, s) = \pm k(y) + pl. \tag{5.8}$$

Then we have

$$u(0, y; r)\delta_s = \pm u(0, k(y); r \circ s) + v, \tag{5.9}$$

where

$$v = \left(\frac{cy(r^*, s^*)}{p}\sqrt{r \circ s}, l\sqrt{(r \circ s)^*}\right). \tag{5.10}$$

Note that $v \in Z^{(r \circ s)}$. By Proposition 2.1 we have

$$\begin{aligned} &g_{u(0,y;r)\delta_s}(\tau) \\ &= \varepsilon(\pm u(0, k(y); r \circ s), v) \cdot g_{\pm u(0,k(y);r\circ s)}(\tau) \\ &= \begin{cases} \varepsilon(u(0, k(y); r \circ s), v) \cdot g_{u(0,k(y);r\circ s)}(\tau) & \text{if } y \text{ is of plus type,} \\ (-1) \cdot \varepsilon(-u(0, k(y); r \circ s), v) \cdot g_{u(0,k(y);r\circ s)}(\tau) & \text{if } y \text{ is of minus type.} \end{cases} \end{aligned} \tag{5.11}$$

In the equation (5.11) with y of minus type, we used the equalities (Proposition 2.1)

$$g_{u(0,k(y);r\circ s)}(\tau) = g_{u(0,k(y);r\circ s)}((-1_2)(\tau)) = \psi_{r\circ s}(-1_2) \cdot g_{-u(0,k(y);r\circ s)}(\tau) \tag{5.12}$$

and the fact $\psi_{r\circ s}(-1_2) = \psi(-1_2) = -1$.

LEMMA 5.3. *With the notation above, we have*

$$\varepsilon(\pm u(0, k(y); r \circ s), v) = \exp\left[\frac{2\pi i}{2}\{y + k(y)\}\right].$$

PROOF. Suppose that y is of plus type. By the definition, we have $\varepsilon(u(0, k(y); r \circ s), v) = \exp[2\pi i/2 \cdot \xi]$, where

$$\xi = \frac{cy(r^*, s^*)}{p} \cdot l + \frac{cy(r^*, s^*)}{p} + l - \frac{k(y)}{p} \cdot \frac{cy(r^*, s^*)}{p}.$$

If we put $q = p$ in the definition (4.10) of δ_s, we have $c \equiv 0 \pmod p$. Since $(r^*, s^*)/p \in \boldsymbol{Z}$, we have $\xi \in \boldsymbol{Z}$. First, assume $(s, 2) = 1$. If we put $q = 2$ in the definition of δ_s, we have $c \equiv 0 \pmod 2$ and $d \equiv 1 \pmod 2$. Thus, $\xi \equiv l \pmod 2$. Since p and $d(r^*, s)$ are odd, the equation (5.8) implies $l \equiv y + k(y) \pmod 2$. This proves the case. Next, assume $(s, 2) \neq 1$. If we put $q = 2$ in the definition of δ_s, we have $c \equiv 1 \pmod 2$ and $d \equiv 0 \pmod 2$. Since $(r^*, s^*)/p$ is an odd integer, we have $\xi \equiv yl + y + l - k(y) \cdot y \pmod 2$. Since p is odd and d is even, the equation (5.8) implies $l \equiv k(y) \pmod 2$. Thus we have $\xi \equiv y + k(y) \pmod 2$. This completes the proof of the case where y is of plus type. In the proof above, if we exchange $k(y)$ by $-k(y)$, we obtain $\xi \equiv y - k(y) \pmod 2$. Since $y - k(y) \equiv y + k(y) \pmod 2$, we have the proof of the case where y is of minus type. □

Let us denote by $\sharp\{y : -\}$ the number of y which is of minus type.

LEMMA 5.4. *We have*

$$(-1)^{\sharp\{y:-\}} = \left(\frac{(r^*, s)}{p}\right),$$

where the symbol on the right term denotes the Legendre symbol.

PROOF. As was noticed above, we have $d \equiv 1 \pmod p$. Hence, by the equation (5.7), $y(r^*, s) \equiv \pm k(y) \pmod p$. This implies $\prod_{y=1}^{(p-1)/2}\{y(r^*, s)\} \equiv (-1)^{\sharp\{y:-\}} \prod_{y=1}^{(p-1)/2} k(y) \pmod p$. Since $\prod_{y=1}^{(p-1)/2} y \equiv \prod_{y=1}^{(p-1)/2} k(y) \pmod p$, we have

$(r^*, s)^{(p-1)/2} \equiv (-1)^{\sharp\{y:-\}} \pmod{p}$. On the other hand, it is well known that $(r^*, s)^{(p-1)/2} \equiv \left(\frac{(r^*,s)}{p}\right) \pmod{p}$. Therefore, $(-1)^{\sharp\{y:-\}} \equiv \left(\frac{(r^*,s)}{p}\right) \pmod{p}$. Since $p \neq 2$, this congruence implies the equality. □

In the decomposition (5.3), the $g_{u\delta_s}$ part with $r \in \rho^{(1)}$ is given as follows.

LEMMA 5.5.

$$\prod_{r\in\rho^{(1)}} \left\{ \prod_{u\in\mathscr{R}^{(r)}_{I_p}} g_{u\delta_s}(\tau) \right\} = \prod_{r\in\rho^{(1)}} \left(\frac{(r^*,s)}{p}\right) \cdot \prod_{r\in\rho^{(1)}} \left\{ \prod_{u\in\mathscr{R}^{(r)}_{I_p}} g_u(\tau) \right\}.$$

PROOF. Let r be an element of $\rho^{(1)}$. By the equation (5.11) and Lemmas 5.3–5.4, we have

$$\begin{aligned}
\prod_{u\in\mathscr{R}^{(r)}_{I_p}} g_{u\delta_s}(\tau) &= \prod_{y:+} g_{u(0,y;r)\delta_s}(\tau) \cdot \prod_{y:-} g_{u(0,y;r)\delta_s}(\tau) \\
&= \prod_{y:+} \exp\left[\frac{2\pi i}{2}\{y+k(y)\}\right] \cdot g_{u(0,k(y);r\circ s)}(\tau) \\
&\qquad \times \prod_{y:-}(-1) \exp\left[\frac{2\pi i}{2}\{y+k(y)\}\right] \cdot g_{u(0,k(y);r\circ s)}(\tau) \\
&= (-1)^{\sharp\{y:-\}} \cdot \exp\left[\frac{2\pi i}{2}\left\{\sum_y y + \sum_y k(y)\right\}\right] \cdot \prod_y g_{u(0,k(y);r\circ s)}(\tau) \\
&= \left(\frac{(r^*,s)}{p}\right) \cdot \prod_{u\in\mathscr{R}^{(r\circ s)}_{I_p}} g_u(\tau),
\end{aligned}$$

where $y:+$ (respectively $y:-$) means that y is of plus (respectively minus) type. We have used the equality $\sum_y y = \sum_y k(y)$. Since $(p,s)=1$ and $p \nmid r$, we have $p \nmid r\circ s$, namely $r \circ s \in \rho^{(1)}$. This implies that if r runs through all the elements of $\rho^{(1)}$, then so does $r \circ s$. Hence the equality of the lemma follows. □

LEMMA 5.6. *The number $|\rho^{(1)}|$ of the elements of $\rho^{(1)}$ is even, and we have*

$$\prod_{r\in\rho^{(1)}} \left(\frac{(r^*,s)}{p}\right) = \left(\frac{s}{p}\right)^{\frac{1}{2}|\rho^{(1)}|}.$$

PROOF. Since $s \neq 1$, if $r \in \rho^{(1)}$, then $r \circ s \in \rho^{(1)}$ and $r \circ s \neq r$. This implies that the set $\rho^{(1)}$ is a disjoint union of several pairs $\{r, r \circ s\}$, hence $|\rho^{(1)}|$ is even, and we can express the set $\rho^{(1)}$ as a disjoint union of two subsets $\rho_1^{(1)}$ and $\rho_2^{(1)}$ such that $r \in \rho_1^{(1)}$ if and only if $r \circ s \in \rho_2^{(1)}$. Now it is easy to see that for any elements $t_1, t_2 \in T$ the following equality holds:

$$(t_1, t_2)(t_1 \circ t_2, t_2) = t_2. \tag{5.13}$$

If we put $t_1 = r^*$ and $t_2 = s$ in the equation (5.13) and notice that $r^* \circ s = (r \circ s)^*$, we have $(r^*, s)((r \circ s)^*, s) = s$. Using this relation, we have

$$\prod_{r \in \rho^{(1)}} \left(\frac{(r^*, s)}{p} \right) = \prod_{r \in \rho_1^{(1)}} \left\{ \left(\frac{(r^*, s)}{p} \right) \left(\frac{((r \circ s)^*, s)}{p} \right) \right\} = \prod_{r \in \rho_1^{(1)}} \left(\frac{s}{p} \right) = \left(\frac{s}{p} \right)^{\left|\rho_1^{(1)}\right|}.$$

Since $\left|\rho_1^{(1)}\right| = (1/2)\left|\rho^{(1)}\right|$, the proof is completed. $\square$

5.4. The $g_{u\delta_s}$ part with $r \in \rho^{(2)}$.

Here we assume $r \in \rho^{(2)}$, namely $p \mid r$. In this case the element u of $\mathscr{R}_{I_p}^{(r)}$ is of the form

$$u = u(x, 0; r) = \left(\frac{x}{p} \sqrt{r}, 0 \right), \tag{5.14}$$

where x is an integer with $1 \leq x \leq (p-1)/2$.

As before, let δ_s be written as in the equation (5.4). Then we have

$$u(x, 0; r)\delta_s = \left(\frac{ax(r, s)}{p} \sqrt{r \circ s}, \frac{bx(r, s^*)}{p} \sqrt{(r \circ s)^*} \right). \tag{5.15}$$

Since $(p, s) = 1$ and $p \mid r$, we have $p \mid (r, s^*)$ and $r \circ s \in \rho^{(2)}$. By the definition of δ_s and the assumption $(p, s) = 1$, we have $a \equiv s^{-1} \pmod{p}$.

For each x $(1 \leq x \leq (p-1)/2)$, we denote by $k(x)$ the unique integer satisfying $1 \leq k(x) \leq (p-1)/2$ and

$$ax(r, s) \equiv \pm k(x) \pmod{p}. \tag{5.16}$$

We call x to be of *plus* (respectively *minus*) type if the plus (respectively minus) sign appears in the congruence (5.16). Note that if $x_1 \neq x_2$, then $k(x_1) \neq k(x_2)$.

Let l be an integer satisfying

$$ax(r,s) = \pm k(x) + pl. \tag{5.17}$$

Then we have

$$u(x,0;r)\delta_s = \pm u(k(x),0;r\circ s) + v, \tag{5.18}$$

where

$$v = \left(l\sqrt{r\circ s}, \frac{bx(r,s^*)}{p}\sqrt{(r\circ s)^*} \right). \tag{5.19}$$

As before, we have $v \in Z^{(r\circ s)}$, and by Proposition 2.1

$$\begin{aligned} &g_{u(x,0;r)\delta_s}(\tau) \\ &= \begin{cases} \varepsilon(u(k(x),0;r\circ s),v)\cdot g_{u(k(x),0;r\circ s)}(\tau) & \text{if } x \text{ is of } + \text{ type,} \\ (-1)\cdot\varepsilon(-u(k(x),0;r\circ s),v)\cdot g_{u(k(x),0;r\circ s)}(\tau) & \text{if } x \text{ is of } - \text{ type.} \end{cases} \end{aligned} \tag{5.20}$$

Lemma 5.7. *With the notation above, we have*

$$\varepsilon(\pm u(k(x),0;r\circ s),v) = \exp\left[\frac{2\pi i}{2}\{x+k(x)\}\right].$$

Proof. Since the proof is similar to that of Lemma 5.3, we only sketch it. Suppose that x is of plus type. We have $\varepsilon(u(k(x),0;r\circ s),v) = \exp[2\pi i/2\cdot\xi]$ where

$$\xi = l\cdot\frac{bx(r,s^*)}{p} + l + \frac{bx(r,s^*)}{p} + \frac{k_r^s(x)}{p}\cdot\frac{bx(r,s^*)}{p}.$$

Putting $q = p$ in the definition of δ_s, we have $b \equiv 0 \pmod p$. Since $(r,s^*)/p \in \boldsymbol{Z}$, we have $\xi \in \boldsymbol{Z}$. First, assume $(s,2) = 1$. By the definition of δ_s, we have $b \equiv 0 \pmod 2$ and $a \equiv 1 \pmod 2$. Hence, $\xi \equiv l \pmod 2$. Since p and $a(r,s)$ are odd, the equation (5.17) implies $l \equiv x + k(x) \pmod 2$. This proves the case. Next, assume $(s,2) \neq 1$. By the definition of δ_s, we have $b \equiv 1 \pmod 2$ and $a \equiv 0 \pmod 2$. Since $(r,s^*)/p$ is an odd integer, we have $\xi \equiv lx + l + x + k(x)x \pmod 2$. Since p is odd and a is even, we have $l \equiv k(x) \pmod 2$ by the equation (5.17). This completes the case of plus type. Exchanging $k(x)$ by $-k(x)$, we have the proof for minus type x. $\square$

Let us denote by $\sharp\{x : -\}$ the number of x which is of minus type.

LEMMA 5.8. *We have*

$$(-1)^{\sharp\{x:-\}} = \left(\frac{s(r,s)}{p}\right),$$

where the symbol on the right term denotes the Legendre symbol.

PROOF. Since the proof is similar to that of Lemma 5.4, we only sketch it. Since $a \equiv s^{-1} \pmod{p}$, we have $\{s^{-1}(r,s)\}^{(p-1)/2} \equiv (-1)^{\sharp\{x:-\}} \pmod{p}$ the same as Lemma 5.4. Since $(s^{-1})^{(p-1)/2} \equiv s^{(p-1)/2} \pmod{p}$, we have the result. □

In the decomposition (5.3), the $g_{u\delta_s}$ part with $r \in \rho^{(2)}$ is given as follows.

LEMMA 5.9.

$$\prod_{r\in\rho^{(2)}} \left\{ \prod_{u\in\mathscr{R}_{I_p}^{(r)}} g_{u\delta_s}(\tau) \right\} = \prod_{r\in\rho^{(2)}} \left(\frac{s(r,s)}{p}\right) \cdot \prod_{r\in\rho^{(2)}} \left\{ \prod_{u\in\mathscr{R}_{I_p}^{(r)}} g_u(\tau) \right\}.$$

PROOF. Let r be an element of $\rho^{(2)}$. Then, the same as the proof of Lemma 5.5, we have

$$\prod_{u\in\mathscr{R}_{I_p}^{(r)}} g_{u\delta_s}(\tau) = \left(\frac{s(r,s)}{p}\right) \cdot \prod_{u\in\mathscr{R}_{I_p}^{(r\circ s)}} g_u(\tau)$$

using the equation (5.20) and Lemmas 5.7–5.8. If r runs through $\rho^{(2)}$, so does $r \circ s$. Thus we have the proof. □

LEMMA 5.10. *The number $\left|\rho^{(2)}\right|$ of the elements of $\rho^{(2)}$ is even, and we have*

$$\prod_{r\in\rho^{(2)}} \left(\frac{s(r,s)}{p}\right) = \left(\frac{s}{p}\right)^{\frac{1}{2}|\rho^{(2)}|}.$$

PROOF. Similarly to the proof of Lemma 5.6, we can show that the set $\rho^{(2)}$ is a disjoint union of two subsets $\rho_1^{(2)}$ and $\rho_2^{(2)}$ such that $r \in \rho_1^{(2)}$ if and only if $r \circ s \in \rho_2^{(2)}$, whence $|\rho^{(2)}|$ is even. Setting $t_1 = r$ and $t_2 = s$ in the equation (5.13), we have $(r,s)(r\circ s, s) = s$. Thus, we have

$$\prod_{r\in\rho^{(2)}}\left(\frac{s(r,s)}{p}\right)=\prod_{r\in\rho_1^{(2)}}\left\{\left(\frac{s(r,s)}{p}\right)\left(\frac{s(r\circ s,s)}{p}\right)\right\}=\prod_{r\in\rho_1^{(2)}}\left(\frac{s^3}{p}\right)=\left(\frac{s}{p}\right)^{\left|\rho_1^{(2)}\right|}.$$

Since $\left|\rho_1^{(2)}\right|=(1/2)|\rho^{(2)}|$, the proof is completed. □

5.5. The value of $\Phi_\rho^{(p)}$ at the element δ_s.

The value $\Phi_\rho^{(p)}(\delta_s)$ with $p\neq 2$ and $(p,s)=1$ is given as follows. Since $\Phi_\rho^{(p)}(\delta_s)=1$ if $s=1$, we consider the case $s\neq 1$, whence $T_0\neq 1$ and $|T_0|$ is even.

Proposition 5.11. *Let p be a prime factor of M, and ρ a coset in T/T_0. Let s be an element of T_0. Assume that $T_0\neq 1$ and $s\neq 1$. Also assume that $p\neq 2$ and $(p,s)=1$. Then we have*

$$\Phi_\rho^{(p)}(\delta_s)=\begin{cases}\exp\left[\dfrac{2\pi i}{2}\cdot\dfrac{1}{2}(p-1)\cdot\dfrac{1}{2}\displaystyle\sum_{r\in\rho}\{(r^*,s)-1\}\right]\cdot\left(\dfrac{s}{p}\right)^{\frac{1}{2}|T_0|} & \textit{if } (s,2)=1,\\ \exp\left[\dfrac{2\pi i}{2}\cdot\dfrac{1}{2}(p-1)\cdot\dfrac{1}{2}\displaystyle\sum_{r\in\rho}(r,s^*)\right]\cdot\left(\dfrac{s}{p}\right)^{\frac{1}{2}|T_0|} & \textit{if } (s,2)\neq 1.\end{cases}$$

Proof. This follows immediately from Lemmas 5.2, 5.5, 5.6, 5.9, 5.10 and the following equalities:

$$\left(\frac{s}{p}\right)^{\frac{1}{2}|\rho^{(1)}|}\cdot\left(\frac{s}{p}\right)^{\frac{1}{2}|\rho^{(2)}|}=\left(\frac{s}{p}\right)^{\frac{1}{2}\left(|\rho^{(1)}|+|\rho^{(2)}|\right)}=\left(\frac{s}{p}\right)^{\frac{1}{2}|\rho|}=\left(\frac{s}{p}\right)^{\frac{1}{2}|T_0|}.$$

□

6. Determination of the unit group $\mathscr{F}$ with $T_0=\langle M_0\rangle$.

6.1. The values $\Phi_\rho^{(p)}(\delta_q)$ and $\Psi_\rho(\delta_q)$ with $T_0=\langle M_0\rangle$.

For any divisor N of M, we denote by $\langle N\rangle$ the subgroup of T consisting of all factors r of N. Henceforth, we take a divisor M_0 of M, and consider the case $T_0=\langle M_0\rangle$. Put $M_1=M/M_0$. Then, for each coset $\rho\in T/T_0$, there exists a unique factor r of M_1 such that r is contained in ρ. We denote this integer r by r_ρ. The mapping $\rho\mapsto r_\rho$ gives an isomorphism from T/T_0 to $\langle M_1\rangle$. Since the group T_0 is generated by the prime factors of M_0, in order to determine the characters $\Phi_\rho^{(p)}$ and Ψ_ρ, it is sufficient to determine the values at the elements δ_q for all prime factors q of M_0 (cf. Propositions 4.2, 4.3).

Proposition 6.1. *Let $T_0=\langle M_0\rangle$, p a prime factor of M, and ρ a coset in T/T_0. Assume that p is odd. Then for each odd prime factor q of M_0 $(\neq 1)$, we have*

$$\Phi_\rho^{(p)}(\delta_q) = \begin{cases} 1 & \text{if } p = q, \\ \left(\dfrac{p}{q}\right)^{\frac{1}{2}|T_0|} & \text{if } p \neq q, \end{cases}$$

where the symbol $\left(\frac{p}{q}\right)$ *denotes the Legendre symbol.*

PROOF. First, suppose that $p = q$. Since this condition implies $p \in T_0$, the function $f_\rho^{(p)}(\tau)$ is a constant (Proposition 3.2). Hence, we have $\Phi_\rho^{(p)}(\delta_q) = 1$. Next, suppose that $p \neq q$. We prove first $\sum_{r \in \rho}(r^*, q) = (q+1) \cdot (1/2)|T_0|$. Put $\rho^* = \{r^* \mid r \in \rho\}$ $(= \rho \circ [M])$. Since $q \in T_0$, we have $r^* \circ q \in \rho^*$ for all $r \in \rho$. Since either r^* or $r^* \circ q$ is prime to q and the other a multiple of q, half of the elements of ρ^* are prime to q and the others are multiples of q. From this the equality follows immediately. By the use of this equality, we have

$$\begin{aligned} \frac{1}{2}(p-1) \cdot \frac{1}{2}\sum_{r \in \rho}\{(r^*, s) - 1\} &= \frac{1}{2}(p-1) \cdot \frac{1}{2}\left\{(q+1) \cdot \frac{1}{2}|T_0| - |T_0|\right\} \\ &= \frac{1}{4}(p-1)(q-1) \cdot \frac{1}{2}|T_0|. \end{aligned}$$

Thus, by Proposition 5.11 and the law of quadratic reciprocity, we have

$$\Phi_\rho^{(p)}(\delta_q) = \left\{(-1)^{\frac{1}{4}(p-1)(q-1)} \cdot \left(\frac{q}{p}\right)\right\}^{\frac{1}{2}|T_0|} = \left(\frac{p}{q}\right)^{\frac{1}{2}|T_0|}.$$

□

PROPOSITION 6.2. *Let* $T_0 = \langle M_0 \rangle$, *and* ρ *a coset in* T/T_0. *Assume that* r_ρ *is odd. Then for each odd prime factor* q *of* M_0 $(\neq 1)$, *we have*

$$\Psi_\rho(\delta_q) = \left(\frac{r_\rho}{q}\right)^{\frac{1}{2}|T_0|},$$

where the symbol $\left(\frac{r_\rho}{q}\right)$ *denotes the Legendre symbol.*

PROOF. First, suppose that $\rho = T_0$. Then $r_\rho = 1$, hence the right term of the equality is 1. On the other hand, we have $h_\rho(\tau) = 1$, whence $\Psi_\rho(\delta_q) = 1$. Thus the equality holds. Next, suppose that $\rho \neq T_0$. Let $r_\rho = p_1 \cdot \cdots \cdot p_l$ be the prime factorization. Then $p_i \neq q$ for all i because r_ρ is a factor of M_1. Also the primes p_i are odd because r_ρ is odd by the assumption. Thus, by the previous proposition and the equation (4.5), we have

$$\Psi_\rho(\delta_q) = \Phi^{(p_1)}_{[p_2]\cdots[p_l]}(\delta_q) \cdot \Phi^{(p_2)}_{[p_3]\cdots[p_l]}(\delta_q) \cdot \cdots \cdot \Phi^{(p_l)}_{[1]}(\delta_q)$$
$$= \left(\frac{p_1}{q}\right)^{\frac{1}{2}|T_0|} \cdot \left(\frac{p_2}{q}\right)^{\frac{1}{2}|T_0|} \cdots \cdot \left(\frac{p_l}{q}\right)^{\frac{1}{2}|T_0|} = \left(\frac{r_\rho}{q}\right)^{\frac{1}{2}|T_0|}.$$

□

6.2. Determination of the unit group $\mathscr{F}$.

Now we determine the condition that a product of the functions h_ρ is an automorphic function with respect to the group Γ_{T_0}. For simplicity, we denote by $S(M_0)$ the sum of all factors of M_0. Then $S(M_0) = \prod_{q|M_0}(1+q)$, where q runs through all prime factors of M_0.

THEOREM 6.3. *Let $T_0 = \langle M_0 \rangle$. Assume that M is odd, $M_0 \neq 1$, and $M_1 \neq 1$. Let $m(r)$ be rational integers parametrized by all factors $r \neq 1$ of M_1. Then the function*

$$g(\tau) = \prod_{\rho \in T/T_0, \neq [1]} h_\rho(\tau)^{m(r_\rho)}$$

belongs to the group $\mathscr{F}$ of all modular units in the function field $\mathfrak{F}(T_0)$ if and only if the integers $m(r)$ satisfy the following conditions (1), (2) *and* (3):
(1) $S(M_0) \cdot \sum_{r|M_1,\neq 1}\{(r-1) \cdot m(r)\} \equiv 0 \pmod{24}$,
(2) *if* $3 \mid M_1$*, then* $S(M_0) \cdot \sum_{r|M_1,(r,3)=1}\{r \cdot m(3r)\} \equiv 0 \pmod 3$*,*
(3) *if M_0 is a prime integer q and there exists a prime factor p of M_1 satisfying* $\left(\frac{p}{q}\right) = -1$*, then* $\prod_{r|M_1,\neq 1} \left(\frac{r}{q}\right)^{m(r)} = 1$*.*

PROOF. The condition that the function $g(\tau)$ belongs to $\mathscr{F}$ is equivalent to that the equation (4.4) holds in all the cases where $\alpha = \alpha_q$, β_q, γ_q with q prime factors of $\widetilde{M}$, and δ_q with q prime factors of M_0. Since $\Psi_\rho(\alpha_q) = \Psi_\rho(\beta_q) = 1$ for $q \neq 2, 3$, and $\Psi_\rho(\gamma_q) = 1$ for all q by Proposition 4.3, it is sufficient to consider the cases $\alpha = \alpha_2$, α_3, β_2, β_3, and δ_q $(q \mid M_0)$. Let $\alpha = \alpha_2$. Since $\sum_{s\in\rho} s = \sum_{r|M_0}(r \cdot r_\rho) = r_\rho \cdot S(M_0)$ for any coset ρ, we have by the proposition cited above

$$\prod_{\rho \in T/T_0,\neq[1]} \Psi_\rho(\alpha_2)^{m(r_\rho)} = \exp\left[-\frac{2\pi i}{8} \cdot S(M_0) \cdot \sum_{\rho\in T/T_0,\neq[1]} \{(r_\rho - 1)\cdot m(r_\rho)\}\right],$$

whence the equation (4.4) with $\alpha = \alpha_2$ is equivalent to

$$S(M_0) \cdot \sum_{r|M_1,\neq 1} \{(r-1)\cdot m(r)\} \equiv 0 \pmod 8. \tag{6.1}$$

Let $\alpha = \beta_2$. Similarly to the case above, since $r_{\rho^*} = M_1/r_\rho$, we have the congruence

$$S(M_0) \cdot \sum_{r|M_1,\neq 1} \left\{ \left(\frac{M_1}{r} - M_1 \right) \cdot m(r) \right\} \equiv 0 \pmod 8. \tag{6.2}$$

Since M is odd, we have $r^2 \equiv 1 \pmod 8$. Hence, $M_1/r - M_1 \equiv r^2 \cdot M_1/r - M_1 \equiv M_1 \cdot (r-1) \pmod 8$. Since $(M_1, 8) = 1$, the congruence (6.2) is equivalent to (6.1). Similarly, the equation (4.4) with $\alpha = \alpha_3$ gives the congruence

$$S(M_0) \cdot \sum_{r|M_1,\neq 1} \{(r-1) \cdot m(r)\} \equiv 0 \pmod 3, \tag{6.3}$$

and the one with $\alpha = \beta_3$ gives

$$S(M_0) \cdot \sum_{r|M_1,\neq 1} \left\{ \left(\frac{M_1}{r} - M_1 \right) \cdot m(r) \right\} \equiv 0 \pmod 3. \tag{6.4}$$

The combination of the two congruences (6.1) and (6.3) coincides with the condition (1) of the theorem. Assume $3 \nmid M_1$. Then $r^2 \equiv 1 \pmod 3$ for $r \mid M_1$, whence the congruence (6.4) is equivalent to the congruence (6.3), and contained in the condition (1). Next, assume $3 \mid M_1$. Then the summation in the congruence (6.4) can be replaced by $\sum\{M_1/r \cdot m(r)\}$ where r runs through all factors of M_1 with $3 \mid r$. Put $r = 3r_1$ and $M_3 = M_1/3$. Then $\sum\{M_1/r \cdot m(r)\} \equiv \sum\{M_3/r_1 \cdot m(3r_1)\} \pmod 3$, where r_1 runs through all factors of M_1 with $(r_1, 3) = 1$. Since $r_1^2 \equiv 1 \pmod 3$, we have $M_3/r_1 \equiv r_1^2 \cdot M_3/r_1 \equiv M_3 \cdot r_1 \pmod 3$. Since $(M_3, 3) = 1$, this implies that the congruence (6.4) is equivalent to the condition (2) of the theorem. Let $\alpha = \delta_q$. Assume that M_0 is composite. Then $(1/2)|T_0|$ is even, hence $\Psi_\rho(\delta_q) = 1$ for all q by Proposition 6.2. Next, assume that M_0 is a prime integer q, and that $\left(\frac{p}{q}\right) = 1$ for all prime factors p of M_1. Then again, $\Psi_\rho(\delta_q) = 1$ for all q by Proposition 6.2. Thus, in the result, we have the condition (3) of the theorem. $\square$

By Theorems 3.5 and 6.3, we have the characterization of the unit group $\mathscr{F}$.

THEOREM 6.4. *Let $T_0 = \langle M_0 \rangle$. Assume that M is odd, $M_0 \neq 1$, and $M_1 \neq 1$. Then the group $\mathscr{F}$ of all modular units in the function field $\mathfrak{F}(T_0)$ consists of all functions $g(\tau)$ which have the form $g(\tau) = c \prod_{\rho \in T/T_0, \neq [1]} h_\rho(\tau)^{m(r_\rho)}$, where c is a nonzero rational number, and $m(r)$ are rational integers parametrized by all factors $r \neq 1$ of M_1 such that the conditions* (1), (2) *and* (3) *of Theorem* 6.3 *are satisfied.*

REMARK 6.5. If $M_1 = 1$, then the number of the cusps of the curve X_{T_0} is one. Therefore the unit group $\mathscr{F}$ consists of all nonzero rational numbers.

7. Calculation of the cuspidal class number with $T_0 = \langle M_0 \rangle$.

In this section we calculate the cuspidal class number of the curve X_{T_0} with $T_0 = \langle M_0 \rangle$. First in Section 7.1 we reduce the problem to one of purely algebraic nature without the assumption $T_0 = \langle M_0 \rangle$. After Section 7.2 we assume that $T_0 = \langle M_0 \rangle$. Because of the condition (3) of Theorem 6.3, we shall divide the problem into two cases.

7.1. Reduction to an algebraic problem with T_0 general.

In this Section 7.1 we make no assumptions on the group T_0 except for $T_0 \neq T$. Let R, R_0, $\mathscr{D}$, and $\mathscr{C}$ be the same as in Section 3.2. Let $\varphi : \mathscr{D} \cong R$ be the isomorphism (3.4), and θ the element of $R_{\boldsymbol{Q}}$ defined by the equation (3.11).

We denote by $I(T_0)$ the subset of R_0 consisting of all elements $\alpha = \sum m(\rho) \cdot (\rho - 1)$ $(\rho \in T/T_0, \neq [1],\ m(\rho) \in \boldsymbol{Z})$ such that the function $g_\alpha(\tau) = \prod h_\rho(\tau)^{m(\rho)}$ $(\rho \in T/T_0, \neq [1])$ belongs to the group $\mathscr{F}$ of all modular units in the function field $\mathfrak{F}(T_0)$. Then we have the following proposition.

PROPOSITION 7.1. *For any $T_0 \neq T$, we have*

$$\varphi(\operatorname{div}(\mathscr{F})) = I(T_0)\theta.$$

PROOF. This follows immediately from (2) of Proposition 3.3 and Theorem 3.5 □

By this proposition we have

$$\mathscr{C} \cong R_0 / I(T_0)\theta. \tag{7.1}$$

Hence the cuspidal class number h of the curve X_{T_0} is given by

$$h = [R_0 : I(T_0)\theta]. \tag{7.2}$$

Let A and B be two lattices of $R_{\boldsymbol{Q}}$, and C a lattice contained in $A \cap B$. Then the quotient $[A : C]/[B : C]$ does not depend on the choice of C. We denote this number by $[A : B]$. It satisfies the usual multiplicative property, namely $[A : B] = [A : D][D : B]$. In particular, by (7.2) above, we have $h = [R_0 : R_0\theta] \cdot [R_0\theta : I(T_0)\theta]$. Since θ is invertible (Proposition 3.4), we have $[R_0\theta : I(T_0)\theta] = [R_0 : I(T_0)]$, thus

$$h = [R_0 : R_0\theta] \cdot [R_0 : I(T_0)]. \tag{7.3}$$

On the value $[R_0 : R_0\theta]$, we have the following.

PROPOSITION 7.2. *For any $T_0 \neq T$, we have*

$$[R_0 : R_0\theta] = \prod_{\chi \neq 1} \left\{ \frac{1}{24} \prod_{p \mid M} (p + \chi([p])) \right\},$$

where χ runs through all non-trivial characters of T/T_0 and p all prime factors of M.

PROOF. This can be proved the same as [**12**, Proposition 5.2]. □

Though the following proposition is not necessary in the calculation of h, we include it because of interest.

PROPOSITION 7.3. *For any $T_0 \neq T$, both of the sets $I(T_0)$ and $I(T_0)\theta$ are ideals of the ring R.*

PROOF. First we consider the case of $I(T_0)\theta$. Let $\sigma \in \mathrm{Gal}(\mathfrak{F}(T_0)/\mathfrak{F}_1)$, and P a prime divisor of $\mathfrak{F}(T_0)$. As was seen in Section 3.2, P^σ is cuspidal if and only if P is. This implies that if $g \in \mathscr{F}$, then also $g^\sigma \in \mathscr{F}$. Let us identify the group T/T_0 with $\mathrm{Gal}(\mathfrak{F}(T_0)/\mathfrak{F}_1)$. Then we have $\mathrm{div}(g^\sigma) = \sum_{\rho \in T/T_0} \nu_{P_\infty^\rho}(g^\sigma) \cdot P_\infty^\rho$. Hence, $\varphi(\mathrm{div}(g^\sigma)) = \sum_{\rho \in T/T_0} \nu_{P_\infty^\rho}(g^\sigma) \cdot \rho = \sum_{\rho \in T/T_0} \nu_{P_\infty^{\rho\sigma}}(g) \cdot \rho = \sigma \circ \left(\sum_{\rho \in T/T_0} \nu_{P_\infty^{\rho\sigma}}(g) \cdot \rho\sigma \right) = \sigma \circ \varphi(\mathrm{div}(g))$. The relation $\sigma \circ \varphi(\mathrm{div}(g)) = \varphi(\mathrm{div}(g^\sigma))$ implies that $\varphi(\mathrm{div}(\mathscr{F}))$ is an ideal of R. Thus, by Proposition 7.1, $I(T_0)\theta$ is an ideal of R. The statement that $I(T_0)$ is an ideal follows from this and the fact that θ is invertible in $R_{\boldsymbol{Q}}$. □

7.2. The ideal $I(T_0)$ with $T_0 = \langle M_0 \rangle$.

Hereafter we consider the case $T_0 = \langle M_0 \rangle$ as in Section 6.1. The following is a restatement of Theorem 6.4.

THEOREM 7.4. *Let $T_0 = \langle M_0 \rangle$. Assume that M is odd, $M_0 \neq 1$, and $M_1 \neq 1$. Then the ideal $I(T_0)$ coincides with the set of all elements $\alpha = \sum m(r) \cdot ([r] - 1)$ of R_0 $(r \mid M_1, \neq 1)$ such that $m(r)$ are rational integers satisfying the conditions* (1), (2) *and* (3) *of Theorem* 6.3.

7.3. Calculation of the cuspidal class number: Case I.

Now we calculate the cuspidal class number of the curve X_{T_0} with $T_0 = \langle M_0 \rangle$. By the relation (7.3) and Proposition 7.2, it is sufficient to consider the index $[R_0 : I(T_0)]$. In this Section 7.3, we restrict ourselves to the case where the condition (3) on the ideal $I(T_0)$ stated in Theorem 7.4 is null. We call it Case I. In other words, we assume that one of the following conditions is satisfied.

Case I-1: M is odd, M_0 is a prime q, $M_1 \neq 1$ and every prime factor p of M_1 satisfies $\left(\frac{p}{q}\right) = 1$.

Case I-2: M is odd, M_0 is composite, and $M_1 \neq 1$.

Let I_1 be the subgroup of R_0 consisting of all elements

$$\alpha = \sum_{r \mid M_1, \neq 1} m(r) \cdot ([r] - 1) \tag{7.4}$$

such that $m(r)$ are rational integers satisfying the condition (1) of Theorem 6.3. We consider the indices $[R_0 : I_1]$ and $[I_1 : I(T_0)]$ separately.

Let $M_1 = p_1 \cdots p_k$ be the prime factorization of M_1, and $\delta = (p_1 - 1, \dots, p_k - 1)$ the greatest common divisor.

Lemma 7.5. *Let δ be as above. Then $\sum_{r \mid M_1} (r-1)\boldsymbol{Z} = \delta \boldsymbol{Z}$.*

Proof. The inclusion $\sum_{r \mid M_1} (r-1)\boldsymbol{Z} \supset \delta \boldsymbol{Z}$ is obvious. Put $r' = r - 1$ for each factor r of M_1. Let $r = p_{(1)} \cdots p_{(l)}$ be the prime factorization of $r \neq 1$. Since $r' = \prod_i (1 + p'_{(i)}) - 1 \in \delta \boldsymbol{Z}$, we have the reverse inclusion $\sum_{r \mid M_1} (r-1)\boldsymbol{Z} \subset \delta \boldsymbol{Z}$. This proves the lemma. □

Since M_0 $(\neq 1)$ and M_1 $(\neq 1)$ are odd, the numbers $S(M_0)$ and δ are even integers. Let d be the greatest common divisor of 6 and $(1/4)\delta S(M_0)$:

$$d = \left(6, \frac{1}{4}\, \delta S(M_0)\right). \tag{7.5}$$

Lemma 7.6. *Let d be as above. Then $[R_0 : I_1] = 6/d$.*

Proof. Let α be an element of R_0 written as in the equation (7.4). Let $\varphi : R_0 \to \boldsymbol{Z}$ be the homomorphism defined by $\varphi(\alpha) = S(M_0) \cdot \sum \{(r-1) \cdot m(r)\}$ $(r \mid M_1, \neq 1)$. Then by Lemma 7.5, we have $\varphi(R_0) = S(M_0) \cdot \delta \boldsymbol{Z}$. Let $\phi : \boldsymbol{Z} \to \boldsymbol{Z}/24\boldsymbol{Z}$ be the homomorphism induced by the reduction modulo 24. Let $a = (24, \delta S(M_0))$ be the greatest common divisor. Then $a\boldsymbol{Z} = 24\boldsymbol{Z} + \delta S(M_0)\boldsymbol{Z}$. This implies that $\phi(\varphi(R_0)) = \phi(a\boldsymbol{Z}) = a\boldsymbol{Z}/24\boldsymbol{Z}$. Since $(\phi \circ \varphi)^{-1}(0) = I_1$, we have $R_0/I_1 \cong a\boldsymbol{Z}/24\boldsymbol{Z}$. Hence, $[R_0 : I_1] = 24/a = 6/d$. □

Lemma 7.7. *We have $[I_1 : I(T_0)] = 3$ or 1 according as the following three conditions* (i), (ii) *and* (iii) *are satisfied, or not*: (i) $3 \nmid S(M_0)$, (ii) $3 \mid M_1$, (iii) *there exists a prime factor p of M_1 satisfying $p \equiv 2 \pmod 3$.*

Proof. If $3 \mid S(M_0)$, then the condition (2) on $I(T_0)$ stated in Theorem 7.4 is trivial. Also, if $3 \nmid M_1$, the same condition on $I(T_0)$ is null. Thus if one of the conditions (i) and (ii) does not hold, we have $I_1 = I(T_0)$. Assume the condition (iii) does not hold. In this case every factor r of M_1 satisfies $r \equiv 0$ or $1 \pmod 3$. Let α be an element of I_1 written as in (7.4). Then replacing (mod 24) by (mod 3) in the condition (1) of Theorem 6.3, we have $S(M_0) \cdot \sum\{(-1) \cdot m(r)\} \equiv 0 \pmod 3$, where r runs through all factors of M_1 with $r \equiv 0 \pmod 3$. If we write $r = 3r_1$ for r with $r \equiv 0 \pmod 3$, then $r_1 \equiv 1 \pmod 3$, so that $m(3r_1) \equiv r_1 \cdot m(3r_1) \pmod 3$. This implies that α satisfies the condition (2) of Theorem 6.3. Thus we have $I_1 = I(T_0)$. Assume that all the conditions (i), (ii) and (iii) hold. Let α be an element of I_1 written as in (7.4). Let $\varphi : I_1 \to \boldsymbol{Z}$ be the homomorphism defined by $\varphi(\alpha) = S(M_0) \cdot \sum\{r \cdot m(3r)\}$ $(r \mid M_1,\ (r,3) = 1)$, and $\phi : \boldsymbol{Z} \to \boldsymbol{Z}/3\boldsymbol{Z}$ the homomorphism induced by the reduction modulo 3. We prove $\phi(\varphi(I_1)) = \boldsymbol{Z}/3\boldsymbol{Z}$. Let p be a prime factor of M_1 satisfying $p \equiv 2 \pmod 3$, and put $\alpha_p = 8([3]-1) + 8([p]-1)$ $(\in R_0)$. Then we have $\alpha_p \in I_1$. In fact, concerning this element α_p, the value of the term on the left-hand side of the congruence in (1) of Theorem 6.3 is equal to $S(M_0) \cdot 8(p+1)$, which is a multiple of 24, hence $\alpha_p \in I_1$. Now we have $\varphi(\alpha_p) = 8S(M_0)$, whence $\phi(\varphi(\alpha_p))$ is a non zero element of $\boldsymbol{Z}/3\boldsymbol{Z}$. This proves $\phi(\varphi(I_1)) = \boldsymbol{Z}/3\boldsymbol{Z}$. Since $(\phi \circ \varphi)^{-1}(0) = I(T_0)$, we have $I_1/I(T_0) \cong \boldsymbol{Z}/3\boldsymbol{Z}$. This proves the lemma. □

By the equation (7.3), Proposition 7.2, and Lemmas 7.6–7.7, we have the following theorem. For simplicity, we put $a_{(3)} = 3$ or 1 according as all the conditions (i), (ii) and (iii) in Lemma 7.7 are satisfied, or not.

Theorem 7.8. *Assume that Case* I *holds. Let d and $a_{(3)}$ be as above. Then the cuspidal class number h of the curve X_{T_0} with $T_0 = \langle M_0 \rangle$ is given by*

$$h = \frac{6a_{(3)}}{d} \cdot \prod_{\chi \neq 1} \left\{ \frac{1}{24} \prod_{p \mid M} (p + \chi([p])) \right\},$$

where χ runs through all non-trivial characters of T/T_0 and p all prime factors of M.

Corollary 7.9. *Let $M = pq$, where p and q are distinct odd primes with $\left(\frac{p}{q}\right) = 1$. Put $T_0 = \langle q \rangle$. Then the cuspidal class number h of the curve X_{T_0} is the numerator of $(1/24)(p-1)(q+1)$. The cuspidal divisor class group is a cyclic group of order h generated by the class of the divisor corresponding to $[p]-1$.*

7.4. Calculation of the cuspidal class number: Case II.

In this Section 7.4, we consider the case, Case II, where the following condition is satisfied.

Case II: M is odd, M_0 is a prime q, and there exists a prime factor p of M_1 satisfying $\left(\frac{p}{q}\right) = -1$.

Let J_1 (respectively J_2) be the subgroup of R_0 consisting of all elements

$$\alpha = \sum_{r \mid M_1, \neq 1} m(r) \cdot ([r] - 1) \tag{7.6}$$

such that $m(r)$ are rational integers satisfying the condition (3) (respectively (1) and (3)) of Theorem 6.3. We consider the indices $[R_0 : J_1]$, $[J_1 : J_2]$ and $[J_2 : I(T_0)]$ separately.

For each factor r of M_1, put $e(r) = 1$ or 0 according as $\left(\frac{r}{q}\right) = -1$ or 1. Then the condition (3) of Theorem 6.3 can be written as follows:

$$\sum_{r \mid M_1, \neq 1} e(r) \cdot m(r) \equiv 0 \ (\mathrm{mod}\, 2). \tag{7.7}$$

Lemma 7.10. $[R_0 : J_1] = 2$.

Proof. Let α be an element of R_0 written as in (7.6). Let $\varphi : R_0 \to \boldsymbol{Z}$ be the homomorphism defined by $\varphi(\alpha) = \sum e(r) \cdot m(r)$ $(r \mid M_1, \neq 1)$. Let p be a prime factor of M_1 satisfying $\left(\frac{p}{q}\right) = -1$. If $\alpha = [p] - 1$, then $\varphi(\alpha) = 1$. Hence $\varphi(R_0) = \boldsymbol{Z}$. Let $\phi : \boldsymbol{Z} \to \boldsymbol{Z}/2\boldsymbol{Z}$ be the homomorphism induced by the reduction modulo 2. Then $\phi(\varphi(R_0)) = \boldsymbol{Z}/2\boldsymbol{Z}$ and $(\phi \circ \varphi)^{-1}(0) = J_1$. This implies $[R_0 : J_1] = 2$. $\square$

Let $M_1 = \prod_i p_i \cdot \prod_j l_j$ $(1 \leq i \leq a,\ 1 \leq j \leq b)$ be the prime factorization of M_1, where p_i (respectively l_j) are prime factors satisfying $\left(\frac{p_i}{q}\right) = -1$ (respectively $\left(\frac{l_j}{q}\right) = 1$). If $a \geq 2$, let $\delta_1 = (p_2 - p_1, \ldots, p_a - p_1)$ (> 0) be the greatest common divisor, and put $d_1 = (1/4)(q+1)\delta_1$. If $a = 1$, put $d_1 = 0$. If $b \geq 1$, let $\delta_2 = (l_1 - 1, \ldots, l_b - 1)$ be the greatest common divisor, and put $d_2 = (1/4)(q+1)\delta_2$. If $b = 0$, put $d_2 = 0$. Note that d_1 and d_2 are non-negative integers.

Lemma 7.11. *Let $\varphi : J_1 \to \boldsymbol{Z}$ be the homomorphism defined by $\varphi(\alpha) = (q+1) \cdot \sum\{(r-1) \cdot m(r)\}$ $(r \mid M_1, \neq 1)$, where α is of the form* (7.6)*. Let d_1 and d_2 be as above, and $D = (2(p_1 - 1)(q+1), 4d_1, 4d_2)$ the greatest common divisor. Then $\varphi(J_1) = D\boldsymbol{Z}$.*

Proof. First we prove $\varphi(J_1) \supset D\boldsymbol{Z}$. If $\alpha = 2([p_1] - 1)$, then $\alpha \in J_1$ and $\varphi(\alpha) = (q+1) \cdot (p_1 - 1) \cdot 2$, whence $\varphi(J_1) \supset 2(p_1 - 1)(q+1)\boldsymbol{Z}$. If $a \geq 2$, for each index i $(2 \leq i \leq a)$, put $\alpha = -([p_1] - 1) + ([p_i] - 1)$. Then $\alpha \in J_1$ and $\varphi(\alpha) = (q+1) \cdot (p_i - p_1)$, whence $\varphi(J_1) \supset (q+1)(p_i - p_1)\boldsymbol{Z}$. If $b \geq 1$, for each index j

$(1 \le j \le b)$, put $\alpha = [l_j] - 1$. Then $\alpha \in J_1$ and $\varphi(\alpha) = (q+1) \cdot (l_j - 1)$, whence $\varphi(J_1) \supset (q+1)(l_j-1)\boldsymbol{Z}$. Thus we have $\varphi(J_1) \supset 2(p_1-1)(q+1)\boldsymbol{Z} + \sum_i (q+1)(p_i - p_1)\boldsymbol{Z} + \sum_j (q+1)(l_j-1)\boldsymbol{Z} = D\boldsymbol{Z}$. Second we prove $\varphi(J_1) \subset D\boldsymbol{Z}$. Let α be an element of J_1 written as in (7.6). Since α satisfies the condition (7.7), there exists an integer k with $\sum_{r|M_1,\neq 1} e(r) \cdot m(r) = 2k$. Since $m(p_1) = 2k - \sum' e(r) \cdot m(r)$, we have $\varphi(\alpha) = (q+1)\{(p_1-1) \cdot m(p_1) + \sum'(r-1) \cdot m(r)\} = (q+1)[2(p_1-1) \cdot k + \sum'\{r - 1 - e(r)(p_1-1)\} \cdot m(r)]$, where $\sum'$ means the summation over r with $r \mid M_1$, $\neq 1$ and $\neq p_1$. Thus it is sufficient to prove that the number

$$f(r) = (q+1)\{r - 1 - e(r)(p_1 - 1)\}$$

is contained in $D\boldsymbol{Z}$ $(r \mid M_1, \neq 1, p_1)$. Let us write $r' = r - 1$ for each factor r of M_1. Then by the definition of D, we have (i) $(q+1)p_i' \equiv (q+1)p_1' \pmod{D\boldsymbol{Z}}$ $(1 \le i \le a)$, (ii) $(q+1)l_j' \equiv 0 \pmod{D\boldsymbol{Z}}$ $(1 \le j \le b)$, and (iii) $(q+1)p_1' \cdot h \equiv 0 \pmod{D\boldsymbol{Z}}$ for any $h \in 2\boldsymbol{Z}$. It is easy to see that we have (iv) $(q+1)s_1's_2' \equiv 0 \pmod{D\boldsymbol{Z}}$ for any two prime factors s_1 and s_2 of M_1. Now we prove $f(r) \in D\boldsymbol{Z}$. Let $r = t_1 \cdots t_c$ be the prime factorization of r. By the equation $r' = r - 1 = (1+t_1') \cdots (1+t_c') - 1$ and the property (iv), we have (v) $(q+1)r' \equiv (q+1)t_1' + \cdots + (q+1)t_c' \pmod{D\boldsymbol{Z}}$. Assume that $e(r) = 0$, i.e. $\left(\frac{r}{q}\right) = 1$. Then the number $n(r)$ of the prime factor $p \mid M_1$ with $\left(\frac{p}{q}\right) = -1$ which appears in the set $\{t_1, \ldots, t_c\}$ is even. Hence $f(r) = (q+1)r' \equiv (q+1)t_1' + \cdots + (q+1)t_c' \equiv (q+1)p_1' \cdot n(r) \equiv 0 \pmod{D\boldsymbol{Z}}$ by the properties (v), (i), (ii) and (iii). This implies $f(r) \in D\boldsymbol{Z}$. Next assume that $e(r) = 1$, i.e. $\left(\frac{r}{q}\right) = -1$. Then the number $n(r)$ defined the same as above is odd. Hence we have $f(r) = (q+1)r' - (q+1)p_1' \equiv (q+1)t_1' + \cdots + (q+1)t_c' - (q+1)p_1' \equiv (q+1)p_1' \cdot \{n(r) - 1\} \equiv 0 \pmod{D\boldsymbol{Z}}$ by the properties (v), (i), (ii) and (iii). This implies $f(r) \in D\boldsymbol{Z}$, and completes the proof. $\square$

Let d be the following greatest common divisor

$$d = \left(6, \frac{1}{2}(p_1-1)(q+1), d_1, d_2\right). \tag{7.8}$$

LEMMA 7.12. *Let d be as above. Then $[J_1 : J_2] = 6/d$.*

PROOF. Let $\varphi : J_1 \to \boldsymbol{Z}$ and D be the same as in Lemma 7.11. Let $\phi : \boldsymbol{Z} \to \boldsymbol{Z}/24\boldsymbol{Z}$ be the homomorphism induced by the reduction modulo 24. Since $4d = (24, D)$, we have $4d\boldsymbol{Z} = 24\boldsymbol{Z} + D\boldsymbol{Z}$. This and Lemma 7.11 imply $\phi(\varphi(J_1)) = \phi(D\boldsymbol{Z}) = 4d\boldsymbol{Z}/24\boldsymbol{Z}$. Since $(\phi \circ \varphi)^{-1}(0) = J_2$, we have $J_1/J_2 \cong 4d\boldsymbol{Z}/24\boldsymbol{Z} \cong d\boldsymbol{Z}/6\boldsymbol{Z}$. This completes the proof. $\square$

Lemma 7.13. *We have* $[J_2 : I(T_0)] = 3$ *or* 1 *according as the following three conditions* (i), (ii) *and* (iii) *are satisfied, or not*: (i) $3 \nmid S(M_0)(= q+1)$, (ii) $3 \mid M_1$, (iii) *there exists a prime factor* p *of* M_1 *satisfying* $p \equiv 2 \pmod 3$.

Proof. This can be proved the same as Lemma 7.7. $\square$

By the equation (7.3), Proposition 7.2, and Lemmas 7.10, 7.12 and 7.13, we have the following theorem. For simplicity, we put $a_{(3)} = 3$ or 1 according as all the conditions (i), (ii) and (iii) in Lemma 7.13 are satisfied, or not.

Theorem 7.14. *Assume that Case* II *holds. Let* d *and* $a_{(3)}$ *be as above. Then the cuspidal class number* h *of the curve* X_{T_0} *with* $T_0 = \langle M_0 \rangle$ *is given by*

$$h = \frac{12 a_{(3)}}{d} \cdot \prod_{\chi \neq 1} \left\{ \frac{1}{24} \prod_{p \mid M} (p + \chi([p])) \right\},$$

where χ *runs through all non-trivial characters of* T/T_0 *and* p *all prime factors of* M.

Corollary 7.15. *Let* $M = pq$, *where* p *and* q *are distinct odd primes with* $\left(\frac{p}{q}\right) = -1$. *Put* $T_0 = \langle q \rangle$. *Then the cuspidal class number* h *of the curve* X_{T_0} *is the numerator of* $(1/12)(p-1)(q+1)$. *The cuspidal divisor class group is a cyclic group of order* h *generated by the class of the divisor corresponding to* $[p] - 1$.

8. The p-Sylow group of the cuspidal divisor class group.

In this section we study the p-Sylow group of the cuspidal divisor class group of the curve X_{T_0}. In Section 8.1 we consider the case where T_0 is general. In Section 8.2 we consider the case where $p = 3$ and $T_0 = \langle M_0 \rangle$.

8.1. The p-Sylow group with T_0 general.

In this Section 8.1 we make no assumptions on the group T_0 except for $T_0 \neq T$.

Let χ be a character of the group T/T_0, and e_χ the element of $R_{\boldsymbol{Q}}$ defined by

$$e_\chi = \frac{1}{|T/T_0|} \sum_{\rho \in T/T_0} \chi(\rho)\rho. \tag{8.1}$$

These e_χ are the elementary idempotents of $R_{\boldsymbol{Q}}$. Let $a(\chi)$ be the eigenvalue of θ belonging to e_χ, i.e., $\theta e_\chi = a(\chi) e_\chi$. Then we have

$$a(\chi) = \frac{1}{24} \prod_{p \mid M} (1 + p\chi([p])). \tag{8.2}$$

THEOREM 8.1. *Let $a(\chi)$ be as above, and p a prime $\neq 2, 3$. Then $a(\chi) \in \boldsymbol{Z}_p$ for all χ, and the p-Sylow group of the cuspidal divisor class group of the curve X_{T_0} is isomorphic to the direct sum*

$$\bigoplus_{\chi \neq 1} (\boldsymbol{Z}_p / a(\chi) \boldsymbol{Z}_p),$$

where χ runs through all non-trivial characters of T/T_0.

PROOF. Since $p \neq 2, 3$, the fact $a(\chi) \in \boldsymbol{Z}_p$ is obvious. In the following we consider the elements e_χ, $a(\chi)$ and θ as contained in $R \otimes \boldsymbol{Q}_p$. As is well-known the p-Sylow group of a finite abelian group G is isomorphic to $G \otimes \boldsymbol{Z}_p$. Hence, by the isomorphism (7.1), the p-Sylow group of $\mathscr{C}$ is isomorphic to $\mathscr{C} \otimes \boldsymbol{Z}_p \cong (R_0 / I(T_0)\theta) \otimes \boldsymbol{Z}_p \cong (R_0 \otimes \boldsymbol{Z}_p)/(I(T_0)\theta \otimes \boldsymbol{Z}_p) \cong (R_0 \otimes \boldsymbol{Z}_p)/((I(T_0) \otimes \boldsymbol{Z}_p)\theta)$. By Corollary 4.5 we have $R_0 \supset I(T_0) \supset 24R_0$. Since $p \neq 2, 3$, this implies $I(T_0) \otimes \boldsymbol{Z}_p = R_0 \otimes \boldsymbol{Z}_p$. Thus we have $\mathscr{C} \otimes \boldsymbol{Z}_p \cong (R_0 \otimes \boldsymbol{Z}_p)/((R_0 \otimes \boldsymbol{Z}_p)\theta)$. Since $p \neq 2$, the set of the elements e_χ with $\chi \neq 1$ constitutes a basis of $R_0 \otimes \boldsymbol{Z}_p$ over $\boldsymbol{Z}_p$ (Takagi [**12**, Lemma 6.1]). Hence we have $\mathscr{C} \otimes \boldsymbol{Z}_p \cong (\bigoplus \boldsymbol{Z}_p e_\chi)/((\bigoplus \boldsymbol{Z}_p e_\chi)\theta) \cong (\bigoplus \boldsymbol{Z}_p e_\chi)/(\bigoplus \boldsymbol{Z}_p e_\chi \theta) \cong (\bigoplus \boldsymbol{Z}_p e_\chi)/(\bigoplus \boldsymbol{Z}_p a(\chi) e_\chi) \cong \bigoplus (\boldsymbol{Z}_p / a(\chi) \boldsymbol{Z}_p)$. □

PROPOSITION 8.2. *Assume that the index $[R_0 : I(T_0)]$ is prime to 3. Then $a(\chi) \in \boldsymbol{Z}_3$ for all $\chi \neq 1$, and the 3-Sylow group of the cuspidal divisor class group of the curve X_{T_0} is isomorphic to the direct sum*

$$\bigoplus_{\chi \neq 1} (\boldsymbol{Z}_3 / a(\chi) \boldsymbol{Z}_3),$$

where χ runs through all non-trivial characters of T/T_0.

PROOF. As in the proof of Theorem 8.1 we have the isomorphism $\mathscr{C} \otimes \boldsymbol{Z}_3 \cong (R_0 \otimes \boldsymbol{Z}_3)/((I(T_0) \otimes \boldsymbol{Z}_3)\theta)$. By the assumption we have $I(T_0) \otimes \boldsymbol{Z}_3 = R_0 \otimes \boldsymbol{Z}_3$, whence $\mathscr{C} \otimes \boldsymbol{Z}_3 \cong (R_0 \otimes \boldsymbol{Z}_3)/((R_0 \otimes \boldsymbol{Z}_3)\theta)$. Since the set of the elements e_χ with $\chi \neq 1$ is a basis of $R_0 \otimes \boldsymbol{Z}_3$ over $\boldsymbol{Z}_3$, we have $\mathscr{C} \otimes \boldsymbol{Z}_3 \cong (\bigoplus \boldsymbol{Z}_3 e_\chi)/(\bigoplus \boldsymbol{Z}_3 a(\chi) e_\chi)$. Thus we have the inclusion $\boldsymbol{Z}_3 a(\chi) e_\chi \subset \boldsymbol{Z}_3 e_\chi$, which implies $a(\chi) \in \boldsymbol{Z}_3$. This completes the proof. □

8.2. The 3-Sylow group with $T_0 = \langle M_0 \rangle$.

Here we consider the case where $p = 3$ and $T_0 = \langle M_0 \rangle$.

PROPOSITION 8.3. *Let $T_0 = \langle M_0 \rangle$. Assume that M is odd, $M_0 \neq 1$, $M_1 \neq 1$, and that either the following condition* (i) *or* (ii) *is satisfied*: (i) $3 \mid S(M_0)$, (ii) *every prime factor p of M_1 satisfies $p \equiv 1 \pmod 3$. Then the index $[R_0 : I(T_0)]$ is prime to* 3.

Proof. We consider the Cases I and II separately. First, assume that the condition of Case I is satisfied (Section 7.3). By the proof of Theorem 7.8, we have $[R_0 : I(T_0)] = 6a_{(3)}/d$. It is easy to see that if either of the conditions (i), (ii) holds, then $a_{(3)} = 1$ and $3 \mid d$. This implies that the index $[R_0 : I(T_0)]$ is prime to 3. Next, assume that the condition of Case II is satisfied (Section 7.4). By the proof of Theorem 7.14, we have $[R_0 : I(T_0)] = 12a_{(3)}/d$. As in the Case I, we see again that if either of the conditions (i), (ii) holds, then $a_{(3)} = 1$ and $3 \mid d$. Hence we see that the index $[R_0 : I(T_0)]$ is prime to 3. □

Remark 8.4. If neither the condition (i) nor (ii) is satisfied, then the index $[R_0 : I(T_0)]$ is not prime to 3.

By Propositions 8.2 and 8.3 we have the following theorem.

Theorem 8.5. *Let $T_0 = \langle M_0 \rangle$. Assume that M, M_0 and M_1 satisfy the condition of Proposition* 8.3*. Then $a(\chi) \in \boldsymbol{Z}_3$ for all $\chi \neq 1$, and the* 3*-Sylow group of the cuspidal divisor class group of the curve X_{T_0} is isomorphic to the direct sum*

$$\bigoplus_{\chi \neq 1} (\boldsymbol{Z}_3/a(\chi)\boldsymbol{Z}_3),$$

where χ runs through all non-trivial characters of T/T_0.

References

[1] A. O. L. Atkin and J. Lehner, Hecke Operators on $\Gamma_0(m)$, Math. Ann., **185** (1970), 134–160.

[2] V. G. Drinfeld, Two theorems on modular curves, Funct. Anal. Appl., **7** (1973), 155–156.

[3] S. Klimek, Thesis, Berkeley, 1975.

[4] D. Kubert and S. Lang, The index of Stickelberger ideals of order 2 and cuspidal class numbers, Math. Ann., **237** (1978), 213–232.

[5] D. Kubert and S. Lang, Modular Units, Grundlehren der Mathematischen Wissenschaften, **244**, Springer-Verlag, Berlin, 1981.

[6] J. Manin, Parabolic points and zeta functions of modular curves, Izv. Akad. Nauk SSSR, Ser. Mat., **36** (1972), AMS translation 19–64.

[7] A. Ogg, Rational points on certain elliptic modular curves, AMS Conference, St. Louis, 1972, pp. 211–231.

[8] A. Ogg, Hyperelliptic modular curves, Bull. Soc. Math. France, **102** (1974), 449–462.

[9] T. Takagi, Cuspidal class number formula for the modular curves $X_1(p)$, J. Algebra, **151** (1992), 348–374.

[10] T. Takagi, The cuspidal class number formula for the modular curves $X_1(p^m)$, J. Algebra, **158** (1993), 515–549.

[11] T. Takagi, The cuspidal class number formula for the modular curves $X_1(3^m)$, J. Math. Soc. Japan, **47** (1995), 671–686.

[12] T. Takagi, The cuspidal class number formula for the modular curves $X_0(M)$ with M square-free, J. Algebra, **193** (1997), 180–213.

[13] T. Takagi, The cuspidal class number formula for the modular curves $X_1(2^{2n+1})$, J. Algebra, **319** (2008), 3535–3566.

[14] J. Yu, A cuspidal class number formula for the modular curves $X_1(N)$, Math. Ann., **252** (1980), 197–216.

Toshikazu TAKAGI

Faculty of Arts and Sciences at Fujiyoshida
Showa University
Fujiyoshida
Yamanashi 403-0005, Japan
E-mail: takagi@cas.showa-u.ac.jp