Cuspidal Class Number Formula for the Modular Curves \( X_1(p) \)

TOSHIKAZU TAKAGI

College of Arts and Sciences, Showa University, Hatanodai, Shinagawa-ku, Tokyo 142, Japan

Communicated by Walter Feit
Received November 15, 1990

INTRODUCTION

The fact that the cuspidal divisor class group of a modular curve is finite was proved by Manin [14] and Drinfeld [1]. However, if we want to know the cuspidal class number, we need more specific information about the units on the modular curve. For the modular curve \( X_0(p) \) with \( p \) a prime, Ogg [15] determined its cuspidal class number. Kubert and Lang [5–13] developed a general theory of modular units and computed the cuspidal class number for the curves \( X(p^n) \) (\( p \neq 2, 3 \)). They also considered a certain subgroup of the cuspidal divisor class group for the curves \( X_1(p^n) \), but not the cuspidal divisor class group itself. It seems to be of some interest to determine the (full) cuspidal class number for \( X_1(p^n) \). The purpose of the present paper is to determine the cuspidal class number for \( X_1(p) \). In our subsequent papers we shall consider the curves \( X_1(p^n) \).

Let \( p \) be a prime \( \neq 2, 3 \). Let \( \chi \) be a non-trivial character of \( (\mathbb{Z}/p\mathbb{Z})^* \), and let \( B_{2,\chi} \) be the generalized Bernoulli number associated to \( \chi \). Let \( h_1(p) \) be the cuspidal class number of \( X_1(p) \). Then our main result is the following formula:

\[
    h_1(p) = p^2 \left( \prod_{\chi \neq 1} \frac{1}{B_{2,\chi}} \right)^2.
\]

A cusp on \( X_1(p) \) is said to be of the first type if it is lying above the cusp 0 on \( X_0(p) \). Let \( h_1^0(p) \) be the order of the subgroup of the cuspidal divisor class group generated by the cusps of the first type. Then a formula for \( h_1^0(p) \) is obtained by Klimek [4] (see also [13]). Comparing it with our formula above, we have

\[
    h_1(p) = (h_1^0(p))^2.
\]
(The formula for \( h_0^2(p) \) is now completely extended to the case of the curve \( X_1(N) \) with \( N \) arbitrary. About this result, see Yu [21].) Let \( C, C^0, C^\infty \) be the cuspidal divisor class group, the subgroup generated by the cusps of the first type, the subgroup generated by the cusps which are lying above the cusp \( \infty \) on \( X_0(p) \), respectively. Then Kubert and Lang [11, Section 6] raised the problem to consider the relationship between the two groups \( C \) and \( C^0 + C^\infty \). We shall prove that \( C/(C^0 + C^\infty) \) is a cyclic group, and that it is isomorphic to the cuspidal divisor class group of \( X_0(p) \). For more details, see Theorem 4.2 and its corollaries.

Our idea of the proof is the following. Instead of considering the group \( \Gamma_1(p) \), we consider a certain conjugate group \( \Gamma \) of it, and take its normalizer \( G(\sqrt{p}) \) in \( SL_2(\mathbb{R}) \). Then the group \( G(\sqrt{p}) \) plays a similar role to \( SL_2(\mathbb{Z}) \), and we can regard \( \Gamma \) as a principal congruence subgroup of \( G(\sqrt{p}) \). Then we can proceed analogously to the case of the principal congruence subgroups of \( SL_2(\mathbb{Z}) \).

In Section 1 we modify the Shimura exact sequence to be suitable for our group \( G(\sqrt{p}) \). In fact we consider more general groups \( G(\sqrt{M}) \) than \( G(\sqrt{p}) \). In Section 2 we prove the fullness of (modified) Siegel functions (Theorem 2.1). In Section 3 we determine the unit group on \( X_1(p) \) explicitly (Theorems 3.1, 3.2). We see that the unit group is generated by the (modified) Siegel functions. In Section 4 we express the cuspidal class number as an index of a Stickelberger ideal in a group ring, and compute it in a similar way to Kubert and Lang (Theorem 4.1). Also we determine the structure of the groups \( C^0 \cap C^\infty \) (Theorem 4.2) and \( C/(C^0 + C^\infty) \) (Corollary 2).

### 1. The Shimura Exact Sequence for \( G(\sqrt{M}) \)

1. In this section we consider a family of groups \( G(\sqrt{M}) \) which are parametrized by all square-free \( M \in \mathbb{N} \), and modify the Shimura exact sequence to be suitable for all members of this family. In our study of the cuspidal class number of \( X_1(p) \) with \( p \) a prime, we need only the case \( M = p \). But when we consider a modular curve \( X_1(N) \) for an arbitrary \( N \in \mathbb{N} \), the case of general \( M \) will be necessary. Moreover, we can generalize the theory of modular units of Kubert and Lang [13] to all members of this family in a completely analogous manner. So we consider here the case of general \( M \).

2. Let \( M \) be a positive square-free integer. Then the group \( G(\sqrt{M}) \) is defined to be the subgroup of \( SL_2(\mathbb{R}) \) consisting of all matrices of the form

\[
\begin{pmatrix}
a \sqrt{r} & b \sqrt{r^*} \\
c \sqrt{r^*} & d \sqrt{r}
\end{pmatrix}
\]  

(1.1)
where \( r \) denotes a positive divisor of \( M \), \( r^* = M/r \), and \( a, b, c, d \) are rational integers satisfying \( adr - bcr^* = 1 \). In particular, if \( M = 1 \), then \( G(\sqrt{1}) = SL_2(\mathbb{Z}) \). We say that the element (1.1) is of type \( r \). In this section we denote \( G(\sqrt{M}) \) by \( \Gamma \) for simplicity. Let \( T \) denote the set of all positive divisors of \( M \). Let \( \Gamma^{(r)} \) (\( r \in T \)) denote the set of all elements of type \( r \) and put \( \Gamma^e = \Gamma^{(1)} \). Then \( \Gamma^e \) is a normal subgroup of \( \Gamma \) and \( \Gamma^{(r)} \) is a coset class of \( \Gamma^e \). The group \( \Gamma^e \) is isomorphic to the group \( \Gamma_0(M) \), where \( \Gamma_0(M) \) denotes the subgroup of \( SL_2(\mathbb{Z}) \) consisting of all matrices \( \begin{pmatrix} a & b \\ c & d \end{pmatrix} \) with \( c = 0 \mod M \). We can define a group structure on the set \( T \) by the one-to-one mapping \( r \mapsto \Gamma^{(r)} \). Then \( T \cong \Gamma/\Gamma^e \cong (\mathbb{Z}/2\mathbb{Z})^t \), where \( t \) denotes the number of prime factors of \( M \). We denote by \( r \cdot s \) the product of \( r \) and \( s \) in the group \( T \). Let \( G \) be a subgroup of \( \Gamma \). Let \( T(G) \) be the set of all \( r \in T \) such that \( G \) has an element of type \( r \). Then the set \( T(G) \) is a subgroup of \( T \). We call \( T(G) \) the type group of \( G \). Let \( K \) be the field generated over \( \mathbb{Q} \) by all \( \sqrt{r} \) (\( r \in T \)). Let \( \mathfrak{O} = \sum_{r \in T} \mathbb{Z} \sqrt{r} \). Then \( \mathfrak{O} \) is an order in the ring of all integers of \( K \). Let \( I \) be a non-zero ideal of \( \mathfrak{O} \). Then we define the principal congruence subgroup \( \Gamma(I) \) to be the set of all elements of \( \Gamma \) which are congruent to the unit matrix \((= 1_2) \mod I \).

**Remark.** Let \( N(\Gamma_0(M)) \) be the normalizer of \( \Gamma_0(M) \) in \( SL_2(\mathbb{R}) \). Then it can be shown that

\[
G(\sqrt{M}) = \left( \begin{array}{cc} 1 & 0 \\ 0 & \sqrt{M} \end{array} \right)^{-1} N(\Gamma_0(M)) \left( \begin{array}{cc} 1 & 0 \\ 0 & \sqrt{M} \end{array} \right).
\]

The group \( G(\sqrt{M}) \) is a discrete subgroup of \( SL_2(\mathbb{R}) \) commensurable with \( SL_2(\mathbb{Z}) \) up to a conjugation and has the following properties common to \( SL_2(\mathbb{Z}) \). (1) It is maximal among the discrete subgroups of \( SL_2(\mathbb{R}) \). (2) It has only one equivalence class of cusps (as a transformation group on the upper half plane.) (3) The elements of each matrix are algebraic integers. Moreover the family of \( G(\sqrt{M}) \) is "complete," namely it satisfies the following (4) and (5). (4) If \( G \) is a subgroup of \( SL_2(\mathbb{R}) \) commensurable with \( SL_2(\mathbb{Z}) \), then \( G \) is conjugate to a subgroup of \( G(\sqrt{M}) \) for a suitable \( M \). (5) If \( M_1 \neq M_2 \), then \( G(\sqrt{M_1}) \) is not conjugate to \( G(\sqrt{M_2}) \). The properties (1), (4), (5) were proved by Helling [2, 3]. The properties (2) and (3) are crucial in the generalization of the theory of modular units of Kubert and Lang. (The groups \( G(\sqrt{q}) \) with \( q \) a prime were previously considered by the author [17, 18].)

3. Here we summarize several elementary results. Let \( I \) be a non-zero ideal of \( \mathfrak{O} \). Let \( p \) be a prime and put \( I_p = I \otimes \mathbb{Z}_p \cap \mathfrak{O} \). Since \( \mathfrak{O} \otimes \mathbb{Z}_p = \mathfrak{O} + I \otimes \mathbb{Z}_p \), we have a canonical isomorphism

\[
\mathfrak{O} \otimes \mathbb{Z}_p / I \otimes \mathbb{Z}_p \cong \mathfrak{O} / I_p.
\]
Let $N$ be the positive integer determined by $I \cap \mathbb{Z} = N \mathbb{Z}$. Then we see easily that if $p^r \mid N$, then $I_p \cap \mathbb{Z} = p^r \mathbb{Z}$. Hence if $p \nmid N$, then $I_p = \emptyset$, and if $p_1 \neq p_2$, then $I_{p_1} + I_{p_2} = \emptyset$. Since $\bigcap_p I_p = I$, by the Chinese remainder theorem we have a canonical isomorphism

$$\prod_{p \mid N} \mathbb{Z}/I_p \cong \mathbb{Z}/I. \quad (1.3)$$

Now we consider a subgroup $\mathcal{G}(I)$ of $GL_2(\mathbb{C}/I)$ which plays an analogous role to $GL_2(\mathbb{Z}/N \mathbb{Z})$ in the case of $M = 1$. The group $\mathcal{G}(I)$ is defined as follows. When $I = \emptyset$, then $\mathcal{G}(I) = 1$. When $I \neq \emptyset$, $\mathcal{G}(I)$ is the set of all elements $g \in GL_2(\mathbb{C}/I)$ which satisfies the equation

$$g \equiv \begin{pmatrix} a \sqrt{r} & b \sqrt{r^*} \\ c \sqrt{r^*} & d \sqrt{r} \end{pmatrix} \pmod{I}. \quad (1.4)$$

where $r$ is an element of $T$, $r^* = M/r$, and $a$, $b$, $c$, $d$ are rational integers. Then $\mathcal{G}(I)$ is a subgroup of $GL_2(\mathbb{C}/I)$. Let $\mathcal{G}_u(I)$ be the subgroup of $\mathcal{G}(I)$ consisting of all elements $g$ such that $\det(g) \equiv 1 \pmod{I}$. Let $D(I)$ be the subgroup of $\mathcal{G}(I)$ consisting of all elements $g$ satisfying the equation

$$g \equiv (1 \ 0) \pmod{I}$$

for some rational integer $d$. Then we have $\mathcal{G}(I) = \mathcal{G}_u(I) \cdot D(I)$. The group $\mathcal{G}_u(I)$ is an analogue of $SL_2(\mathbb{Z}/N \mathbb{Z})$.

**Proposition 1.1.** The reduction map $\Gamma \to \mathcal{G}_u(I)$ induces an isomorphism $\Gamma/\Gamma(I) \cong \mathcal{G}_u(I)$.

**Proof.** As in the case of $SL_2(\mathbb{Z}/N \mathbb{Z})$, this follows from the following well known lemma. Q.E.D.

**Lemma 1.** Let $a$, $b$, $c$, $d$, $r$, $s$, $N$ be rational integers satisfying $rsN \neq 0$, $(r, s) = 1$, and $adr - bcs \equiv 1 \pmod{N}$. Then there exist rational integers $a_1$, $b_1$, $c_1$, $d_1$ such that they are congruent to $a$, $b$, $c$, $d$ modulo $N$, respectively, and satisfy $a_1 d_1 r - b_1 c_1 s = 1$.

Let $\mathcal{G}^e(I)$ be the subgroup of $\mathcal{G}(I)$ consisting of all elements $g \in \mathcal{G}(I)$ such that they satisfy the equation $(1.4)$ with $r = 1$. Let $T(I)$ be the subset of $T$ consisting of all $r \in T$ such that Eq. $(1.4)$ holds for $g = 1_2$. Then $T(I)$ is a subgroup of $T$.

**Proposition 1.2.** (1) $\mathcal{G}(I)/\mathcal{G}^e(I) \cong T/T(I)$.

(2) $T(I) = T(\Gamma(I))$.

**Proof.** It is easy to see that for any $g \in \mathcal{G}(I)$ an element $r \in T$ satisfying $(1.4)$ is determined modulo $T(I)$.

If we put $\varphi(g) = r T(I)$, we have a homomorphism $\varphi : \mathcal{G}(I) \to T/T(I)$. Since $\varphi$ is surjective and $\ker \varphi = \mathcal{G}^e(I)$,
we have the isomorphism of (1). Next we show (2). Let \( r \in T(I) \). Then there exist rational integers \( a, b, c, d \) satisfying the equation \( \left( \begin{array}{cc} a \sqrt{r} & b \sqrt{r} \\ c \sqrt{r} & d \sqrt{r} \end{array} \right) \equiv \left( \begin{array}{cc} 1 & 0 \\ 0 & 1 \end{array} \right) \) (mod \( I \)). Then Lemma 1 implies that there exists an element \( g \) of \( T(I) \) of type \( r \). This implies \( r \in T(G(I)) \). Hence we have \( T(I) \subseteq T(G(I)) \). The reverse inclusion follows immediately from the definition. Q.E.D.

4. Now we define an adele group \( G_{A+} \) associated to \( G(\sqrt{M}) \). Let \( K \) be as before. Let \( p \) be a prime. We put

\[
K_p = \mathbb{Q}_p \otimes \mathbb{Q} K = \sum_{r \in T} \mathbb{Q}_p \otimes \sqrt{r},
\]

\[
K_\infty = \mathbb{R} \otimes \mathbb{Q} K = \sum_{r \in T} \mathbb{R} \otimes \sqrt{r}.
\]

Let \( G_p \) (resp. \( G_{\infty+} \)) be the subgroup of \( GL_2(K_p) \) (resp. \( GL_2(K_\infty) \)) consisting of all matrices \( g \) satisfying

\[
g = \left( \begin{array}{cc} a \otimes \sqrt{r} & b \otimes \sqrt{r^*} \\ c \otimes \sqrt{r^*} & d \otimes \sqrt{r} \end{array} \right),
\]

(1.5)

where \( r \in T, r^* = M/r, a, b, c, d \in \mathbb{Q}_p \) (resp. \( \mathbb{R} \)) and \( adr - bcr^* \neq 0 \) (resp. \( > 0 \)). We call \( r \) in (1.5) the type of \( g \). Let \( U_p \) be the subgroup of \( G_p \) consisting of all elements \( g \) satisfying (1.5) with \( a, b, c, d \in \mathbb{Z}_p \) and \( adr - bcr^* \in \mathbb{Z}_p^* \). Then the group \( G_{A+} \) is defined to be the subgroup of \( \prod_p G_p \times G_{\infty+} \) consisting of all elements \( g = \prod g_p \times g_\infty \) (\( g_p \in G_p, g_\infty \in G_{\infty+} \)) satisfying the following conditions (1) and (2):

1. There is an element \( r \in T \) such that the types of \( g_p \) and \( g_\infty \) are all \( r \).
2. The components \( g_p \) are contained in \( U_p \) except for a finite number of primes \( p \).

We call the element \( r \) in (1) the type of \( g \). Put \( K_A = \mathbb{Q}_A \otimes \mathbb{Q} K \). Then \( G_{A+} \) may be also defined as the subgroup of \( GL_2(K_A) \) consisting of all \( g \) which can be written in the form (1.5) with \( a, b, c, d \in \mathbb{Q}_A \) and \( a_\infty, d_\infty r - b_\infty c_\infty r^* > 0 \). Put \( U = G_{A+} \cap \prod_p U_p \times U_\infty \). We denote by \( G_{A+}^e \) (resp. \( U^e \)) the set of all elements \( g \) of \( G_{A+} \) (resp. \( U \)) such that the type of \( g \) is 1. Then \( G_{A+}^e \) and \( U^e \) are subgroups of \( G_{A+} \) and \( U \) respectively.

**Proposition 1.3.** \( G_{A+}/G_{A+}^e \cong U/U^e \cong (\mathbb{Z}/2\mathbb{Z})^t \).

**Proof.** Use the mapping \( g \mapsto r \) (= the type of \( g \)). Q.E.D.

Let \( U_p^e \) (resp. \( G_{\infty+}^e \)) be the set of all elements of type 1 in \( U_p \).
CUSPIDAL CLASS NUMBER FORMULA

Then $U^c_r$ and $G^c_{\infty+}$ are subgroups of $U_r$ and $G_{\infty+}$, respectively. Let us consider the mapping

$$
\left( \begin{array}{cc}
  a \otimes 1 & b \otimes \sqrt{M} \\
  c \otimes \sqrt{M} & d \otimes 1
\end{array} \right) \mapsto \left( \begin{array}{cc}
  a & b \\
  cM & d
\end{array} \right)
$$

defined on $U^c_r$ or $G^c_{\infty+}$. Then we have the isomorphisms

$$
U^c_r \cong \begin{cases}
  GL_2(\mathbb{Z}_p) & \text{if } p \nmid M, \\
  V_p & \text{if } p \mid M,
\end{cases}
$$

$$
G^c_{\infty+} \cong GL_2(\mathbb{R})_+,
$$

where $V_p$ denotes the subgroup of $GL_2(\mathbb{Z}_p)$ consisting of all matrices $(a \ b) \ (c \ d)$ with $c = 0 \pmod p$. Hence we have the following isomorphism:

$$
U^c_r \cong \prod_{p \mid M} GL_2(\mathbb{Z}_p) \times \prod_{p \nmid M} V_p \times GL_2(\mathbb{R})_+. \quad (1.6)
$$

Since the right hand side of (1.6) has the usual locally compact topology, we define the topology of $U^c$ by this isomorphism. Also we define the topology of $G_{A+}$ to be the weakest one such that $U^c$ is an open subset and $G_{A+}$ is a topological group.

Let $\mathfrak{O}$ be the order in $K$ defined before. Let $I$ be a non-zero ideal of $\mathfrak{O}$ and let $N$ be the positive integer satisfying $I \cap \mathbb{Z} = NZ$. Let $\rho: U \rightarrow \prod_{p \mid N} U_p$ be the projection. Let $\iota: \prod_{p \mid N} U_p \rightarrow \prod_{p \mid N} GL_2(\mathbb{Z}_p \otimes \mathfrak{O})$ be the inclusion. Let $\rho: \prod_{p \mid N} GL_2(\mathbb{Z}_p \otimes \mathfrak{O}) \rightarrow \prod_{p \mid N} GL_2(\mathbb{Z}_p \otimes \mathfrak{O}/\mathbb{Z}_p \otimes I)$ be the homomorphism induced by the reduction map modulo $\mathbb{Z}_p \otimes I$. Let $f_1: \prod_{p \mid N} GL_2(\mathbb{Z}_p \otimes \mathfrak{O}/\mathbb{Z}_p \otimes I) \cong \prod_{p \mid N} GL_2(\mathbb{O}/I_p)$ and $f_2: \prod_{p \mid N} GL_2(\mathbb{O}/I_p) \cong GL_2(\mathbb{O}/I)$ be the isomorphisms induced by the ones defined in (1.2) and (1.3). Then combining these mappings we have a homomorphism $\varphi = f_2 \circ f_1 \circ \rho \circ \iota \circ \rho$: $U \rightarrow GL_2(\mathbb{O}/I)$. Put $U(I) = \ker \varphi$. Then

$$
U(I) = \{ g \in U \mid g_p \equiv 1_2 \pmod{\mathbb{Z}_p \otimes I} \ \forall p \mid N \}.
$$

PROPOSITION 1.4. The homomorphism $\varphi$ above induces an isomorphism $U/I(U(I)) \cong \mathfrak{G}(I)$.

Proof. It is sufficient to prove $\text{Im} \varphi = \mathfrak{G}(I)$. First we show $\text{Im} \varphi \subset \mathfrak{G}(I)$. Let $\varphi(g) (a \sqrt{\gamma} c \sqrt{\delta}, b \sqrt{\gamma} d \sqrt{\delta})$ (mod $I$). This implies $\text{Im} \varphi \subset \mathfrak{G}(I)$. Next we show $\mathfrak{G}(I) \subset \text{Im} \varphi$. Let $h$ be an element of $\mathfrak{G}(I)$ and put $h = (\alpha \sqrt{\gamma} \beta \sqrt{\delta}) (mod I)$ with $a, b, c, d \in \mathbb{Z}$. Then $(adr - bcr, N) = 1$. Let $\alpha, \beta, \gamma, \delta$ be elements of
$Q_A$ defined by $\alpha_p = a, \beta_p = b, \gamma_p = c, \delta_p = d$ if $p \nmid N; \alpha_p = \delta_p = 0, \beta_p = \gamma_p = 1$ if $p \mid N$ and $p \mid r; \alpha_p = \delta_p = 1, \beta_p = \gamma_p = 0$, if $p \nmid N$ and $p \nmid r$, $\alpha_\infty = \delta_\infty = 1, \beta_\infty = \gamma_\infty = 0$. Put $g = (\frac{a \otimes \sqrt{r}}{\gamma}, \frac{b \otimes \sqrt{r}}{\delta}, \frac{c \otimes \sqrt{r}}{\delta})$. Then $g \in U$ and $\varphi(g) = h$. Hence we have $\mathcal{G}(I) \subset \text{Im} \varphi$.

Q.E.D.

5. Now we modify the Shimura exact sequence to be suitable for our group $G(\sqrt{M})$. Let us recall the results of Shimura [16]. Let $\mathcal{F}_N^{(1)} (N \in \mathbb{N})$ be the field of all modular functions with respect to the principal congruence subgroup $\Gamma(N)$ of $SL_2(\mathbb{Z})$ such that the Fourier coefficients belong to the cyclotomic field $\mathbb{Q}(e^{2\pi i/N}) = k_N$. Put $\mathcal{F}^{(1)} = \bigcup_N \mathcal{F}_N^{(1)}$. Then we have the Shimura exact sequence [16, Theorem 6.23]

$$1 \longrightarrow \mathbb{Q}^*GL_2(\mathbb{R})_+ \longrightarrow GL_2(Q_A)_+ \longrightarrow \sigma \longrightarrow \text{Aut}(\mathcal{F}^{(1)}) \longrightarrow 1,$$

where $\sigma$ is a continuous homomorphism and induces a topological group isomorphism

$$GL_2(Q_A)_+/\mathbb{Q}^*GL_2(\mathbb{R})_+ \cong \text{Aut}(\mathcal{F}^{(1)}).$$

The action of $\sigma$ is described as follows. Let $h(\tau) \in \mathcal{F}^{(1)}$ and let $\alpha \in GL_2(Q)_+$. Then

$$h^{\sigma(\alpha)}(\tau) = h(\alpha(\tau)).$$

(1.8)

Let $u = (\begin{smallmatrix} 1 \\ 0 \\ 0 \\ 1 \end{smallmatrix})$ with $\delta \in \prod_p \mathbb{Z}_p^* \times \mathbb{R}_+$. Assume $h(\tau) \in \mathcal{F}_N^{(1)}$. Let $h(\tau) = \sum_{n-m} a_n q^n$ be the Fourier expansion where $q = e^{2\pi i/N}, m \in \mathbb{Z}$ and $a_n \in k_N$. Take an integer $d \in \mathbb{Z}$ such that $d \equiv 1 (mod \mathbb{N} \mathbb{Z}_p)$ for every $p \mid N$. Let $\sigma_d$ be the automorphism of $k_N$ defined by $\zeta_N^{\sigma_d} = \zeta_N^d$ where $\zeta_N = e^{2\pi i/N}$. Then

$$h^{\sigma(u)}(\tau) = \sum_{n-m} a_n^d q^n.$$  

(1.9)

The action of $\sigma$ can be completely known by (1.8) and (1.9).

Now we consider the case of general $M$. Put

$$\mathcal{F}^{(M)} = \{ h(\tau/\sqrt{M}) | h(\tau) \in \mathcal{F}^{(1)} \}.$$  

Then the mapping $h(\tau) \mapsto h(\tau/\sqrt{M})$ induces an isomorphism

$$\text{Aut}(\mathcal{F}^{(1)}) \cong \text{Aut}(\mathcal{F}^{(M)}).$$  

(1.10)

Let $\varphi' : G_A+ \rightarrow GL_2(Q_A)_+$ be the mapping defined by

$$\begin{pmatrix} a \otimes \sqrt{r} & b \otimes \sqrt{r^*} \\ c \otimes \sqrt{r^*} & d \otimes \sqrt{r} \end{pmatrix} \mapsto \begin{pmatrix} ar & b \\ cr & dr \end{pmatrix}.$$  

(1.11)
CUSPIDAL CLASS NUMBER FORMULA 355

Then \( \varphi' \) is not a homomorphism, but the restriction of \( \varphi' \) on \( G_{A+}^e \) is a conjugation by \( (1 \otimes \sqrt{r})^{-1} \), and induces an isomorphism \( G_{A+}^e \cong GL_2(Q_A)_+^e \). Let \( \varphi'(g_0) = g \) with \( g_0 \in G_{A+}^e \). Then \( \varphi'^{-1}(g) = \{ g_0(1 \otimes \sqrt{r})^{-1} \mid r \in T \} \). Let \( \langle M \rangle \) be the subgroup of \( Q^* \) (\( \cong GL_2(Q_A)_+^e \)) generated by all \( r \in T \). Let \( \langle \sqrt{M} \rangle \) be the subgroup of \( G_{A+}^e \) generated by all \( (1 \otimes \sqrt{r})_1 \) (\( r \in T \)). Let \( \varphi: G_{A+}^e \rightarrow GL_2(Q_A)_+^e \langle \sqrt{M} \rangle \) be the composition of \( \varphi' \) and the canonical homomorphism \( GL_2(Q_A)_+^e \rightarrow GL_2(Q_A)_+^e \langle \sqrt{M} \rangle \). Then \( \varphi \) is a surjective homomorphism and \( \ker \varphi \) is \( \langle \sqrt{M} \rangle \). Hence we have an isomorphism

\[
G_{A+}^e \langle \sqrt{M} \rangle \cong GL_2(Q_A)_+^e \langle \sqrt{M} \rangle.
\] (1.12)

It is easy to see that \( \varphi^{-1}(Q^*) = Q^* \langle \sqrt{M} \rangle \) and \( \varphi^{-1}(GL_2(R)_+ \langle \sqrt{M} \rangle ) = G_{A+}^e \langle \sqrt{M} \rangle \). By this and (1.12) we have an isomorphism

\[
G_{A+}^e/Q^*G_{A+}^e \langle \sqrt{M} \rangle \cong GL_2(Q_A)_+^e/Q^*GL_2(R)_+^e.
\] (1.13)

Then combining the three isomorphisms (1.13), (1.7), and (1.10) we have

\[
G_{A+}^e/Q^*G_{A+}^e \langle \sqrt{M} \rangle \cong Aut(\mathbb{H}_{(M)}).
\] (1.14)

Since \( \varphi' \) coincides on \( U^e \) with the isomorphism (1.6), the isomorphism (1.12) is a homeomorphism. Hence (1.13) and (1.14) are also homeomorphisms. Let \( \sigma: G_{A+}^e \rightarrow Aut(\mathbb{H}_{(M)}) \) be the surjective homomorphism determined by (1.14). (We use the same notation \( \sigma \) as in the case of \( M = 1 \).) Then we have the following theorem which is a modification of [16, Theorem 6.23].

**Theorem 1.11.** The sequence

\[
1 \rightarrow Q^*G_{A+}^e \langle \sqrt{M} \rangle \rightarrow G_{A+} \xrightarrow{\sigma} Aut(\mathbb{H}_{(M)}) \rightarrow 1
\]

is exact, so that \( Aut(\mathbb{H}_{(M)}) \) is isomorphic to \( G_{A+}^e/Q^*G_{A+}^e \langle \sqrt{M} \rangle \) as a topological group.

Let \( G_{Q+} \) be the subgroup of \( G_{A+} \) consisting of all \( g (\in G_{A+}) \) of the form (1.5) with \( a, b, c, d \in Q \). Then by the mapping \( g \rightarrow (a\sqrt{r}, b\sqrt{r}, c\sqrt{r}, d\sqrt{r}) \) the group \( G_{Q+} \) can be embedded into \( GL_2(R)_+^e \). By this embedding we define the action of \( G_{Q+} \) on the upper half plane \( \mathbb{H} \).

**Proposition 1.5.** Let \( h(\tau) \) be an element of \( \mathbb{H}_{(M)} \).

1. Let \( \alpha \in C_{Q+} \). Then \( h^{(\alpha)}(\tau) = h(\alpha(\tau)) \).

2. Let \( h(\tau) = \sum_{n=-m}^{\infty} a_n q^n \) be the Fourier expansion with \( q = e^{2\pi i r / \sqrt{M}} \) (\( N \in N \)), \( m \in Z \), and \( a_n \in k_N \). Let \( u = (1 \otimes 1, 0, \delta \otimes 1) \in U \) with \( \delta \in \prod_p Z_p^* \times R_+^* \).
Let \( d \in \mathbb{Z} \) be an integer satisfying \( d \equiv \delta_p \pmod{N \mathbb{Z}_p} \) for every \( p \mid N \). Then \( h^{a(u)}(\tau) = \sum_{n=m}^{\infty} a_n q^n \).

**Proof.** These follows immediately from (1.8), (1.9), the definition of \( \sigma ((1.14)) \), and the definition of the action of \( G_{Q^+} \) on \( \mathfrak{H} \). Q.E.D.

Let \( \mathcal{Z}(M) \) be the set of all open subgroups \( S \) of \( G_{A^+} \) containing \( Q^+G_{\infty}^+ \ll \sqrt{M} \) such that \( S/Q^+G_{\infty}^+ \ll \sqrt{M} \) is compact. For each \( S \in \mathcal{Z}(M) \), put

\[
\mathfrak{H}_S = S \cap G_{Q^+},
\]

\[
\mathfrak{H}_S = \{ h \in \mathfrak{H}(M) \mid h^{a(\gamma)} = h \forall \gamma \in S \}.
\]

Let \( k_S \) be the finite abelian extension of \( Q \) corresponding to the subgroup \( Q^+ \cdot \det(S) \) of \( Q^+ \) (cf. [16, p. 144]). Then we have the following proposition which is a modification of [16, Prop. 6.27].

PROPOSITION 1.6. For any \( S \in \mathcal{Z}(M) \), \( \Gamma_S \) is commensurable with \( Q^+ \ll \sqrt{M} \) \( \Gamma \), (so that \( \Gamma_S/Q^+ \ll \sqrt{M} \) is a Fuchsian group of the first kind commensurable with \( \Gamma\{\pm 1\} \)), and \( \mathfrak{H}_S \) is the field of all automorphic functions with respect to \( \Gamma_S \). Furthermore, \( k_S \) is algebraically closed in \( \mathfrak{H}_S \).

**Proof.** Let \( S' \) be the subgroup of \( GL_2(Q_{A^+}) \) corresponding to \( S \) by the isomorphism (1.13). Then the proposition follows immediately from [16, Prop. 6.27] and the following: (1) Let \( \Gamma_S^\infty = \Gamma_S \cap G_{Q^+}^\infty \). Then \( \Gamma_S^\infty = (0_1 0_1 \sqrt{M})^{-1} \Gamma_S (0_1 0_1 \sqrt{M}) \) and \( [\Gamma_S : \Gamma_S^\infty] = 2^\prime \). (2) \( \mathfrak{H}_S = \{ h(\tau/\sqrt{M}) \mid h \in \mathfrak{H}_S \} \). (3) \( k_S = k S' \). (2) is obvious. Let \( \phi' \) be the mapping (1.11). Then for any \( g \in G_{A^+} \), \( Q^+ \cdot \det(g) = Q^+ \cdot \det(g) \). Since \( \phi' (S) = S' \), we have \( Q^+ \cdot \det(S') = Q^+ \cdot \det(S) \). This proves (3). Let us consider (1). Let \( G \) (resp. \( G' \)) be a subgroup of \( G_{A^+} \) (resp. \( GL_2(Q_{A^+}) \)) containing \( \ll \sqrt{M} \) (resp. \( \ll \sqrt{M} \)) satisfying \( G/\ll \sqrt{M} \cong G'/\ll \sqrt{M} \) by the isomorphism (1.12). Put \( G^e = G \cap G_{A^+} \). Then it is easy to see that \( G^e = (0_1 0_1 \sqrt{M})^{-1} G^e (0_1 0_1 \sqrt{M}) \) (in the group \( GL_2(K_A) \)) and that \( G = \bigcup_{e \in T} G^e \cdot (1 \otimes r)^{-1} 1_2 \). Thus it is sufficient to show \( \Gamma_S/\ll \sqrt{M} \cong \Gamma_S/\ll \sqrt{M} \), or equivalently \( \phi'(\Gamma_S) = \Gamma_S \). First we note that \( g \in G_{Q^+} \) if and only if \( \phi'(g) \in GL_2(Q_{A^+}) \). If \( g \in \Gamma_S = S \cap G_{Q^+} \), then \( \phi'(g) \in \phi'(S) \cap GL_2(Q_{A^+}) = \Gamma_S \). Hence \( \phi'(\Gamma_S) \subset \Gamma_S \). Conversely if \( g \in \Gamma_S \), then \( g \in \phi'(S) \) for some \( g \in S \). Since \( g \in GL_2(Q_{A^+}) \), we have \( g \in S \cap G_{Q^+} = \Gamma_S \). Hence \( \Gamma_S \subset \phi'(\Gamma_S) \). Thus \( \phi'(\Gamma_S) = \Gamma_S \). Q.E.D.

Now we consider special types of \( S \). Let \( \mathfrak{O} \) be the order in \( K \) defined before. Let \( I \) be a non-zero ideal of \( \mathfrak{O} \) and let \( N \) be the positive integer determined by \( I \cap Z = N \mathbb{Z} \). Put \( S = S(I) = Q^+ \ll \sqrt{M} \ U(I) \). Then it is easy to see that \( \Gamma_S = Q^+ \ll \sqrt{M} \ \Gamma(I) \) and \( k_S = k_N \). We write \( \mathfrak{H}_S = \mathfrak{H}_I \), and
when $I = \emptyset = (1)$, we write $\mathfrak{H}_S = \mathfrak{H}_1$ simply. The field $\mathfrak{H}_S$ is a Galois extension of $\mathfrak{H}_1$. Since $U \cap \mathbf{Q}^\times \langle \sqrt{M} \rangle U(I) = \pm U(I)$, we have $\text{Gal}(\mathfrak{H}_S/\mathfrak{H}_1) \cong S((1))/S(I) \cong U/\pm U(I)$. With this and Proposition 1.4 we have

$$\text{Gal}(\mathfrak{H}_S/\mathfrak{H}_1) \cong \mathfrak{H}(I)/\{\pm 1\}. \quad (1.15)$$

When $M = 1$ and $I = N\mathbf{Z}$ ($\emptyset = \mathbf{Z}$), it is known that $\mathfrak{H}_S = \mathfrak{H}_N^{(1)}$ (cf. [16, p. 154]). More generally the field $\mathfrak{H}_I$ can be characterized as follows.

**Proposition 1.7.** Let $I$ and $N$ be as above. Then $\mathfrak{H}_I$ is the field of all automorphic functions with respect to $\Gamma(I)$ such that the Fourier coefficients belong to $k_N$.

**Proof.** Let $\mathfrak{H}'$ be the field of all automorphic functions with respect to $\Gamma(I)$ such that the Fourier coefficients belong to $k_N$. Then $\mathfrak{H}_I \subseteq \mathfrak{H}'$ by Propositions 1.5 and 1.6. Conversely let $h(\tau)$ be an element of $\mathfrak{H}'$. Then there exists a positive integer $N_1$ such that $N_1$ is a multiple of $N$ and $h(\tau) \in \mathfrak{H}_I$ with $J = N_1 \emptyset$. Thus in order to prove $h(\tau) \in \mathfrak{H}_I$ it is sufficient to show that $U(I)$ is generated by $U(J)$, $\Gamma(I)$ and the set of all $(\begin{smallmatrix} 1 & 0 \\ \delta & 1 \end{smallmatrix})$, where $\delta \in \prod \mathbf{Z}_p^\times \times \mathbf{R}$, and $\delta_\tau \equiv 1 \pmod{N\mathbf{Z}_p}$ ($\forall \tau \mid N$). Let $D$ be the set of all $(\begin{smallmatrix} 1 & 0 \\ \delta & 1 \end{smallmatrix})$ with $\delta \in \prod \mathbf{Z}_p^\times \times \mathbf{R}$. Then $U = U(J) \Gamma D$ by Propositions 1.1 and 1.4. Let $\alpha \in U(I)$ and put $\alpha = \alpha_1 \gamma \mu$ with $\alpha_1 \in U(J)$, $\gamma \in \Gamma$, and $\mu \in D$. Then $\gamma \mu = \alpha_1^{-1} \alpha \in U(I)$. This implies $\delta_\mu \equiv 1 \pmod{N\mathbf{Z}_p}$ ($\forall \tau \mid N$). Hence $\mu \in U(I)$ and $\gamma \in \Gamma(I)$. This proves the proposition. Q.E.D.

We do not use the following proposition, but include it here for the interest.

**Proposition 1.8.** Let $S$ be the subgroup of $GL_2(\mathbf{Q}_A^+)$ corresponding to $\mathbf{Q}^\times \langle \sqrt{M} \rangle U$ by (1.13). Then $S$ is maximal in the family $\mathfrak{Z}'^{(1)}$.

**Proof.** Let $S'$ be an element of $\mathfrak{Z}'^{(1)}$ and assume $S \subseteq S'$. Then $\Gamma_S \subseteq \Gamma_{S'}$. Since $k_S = \mathbf{Q}$, we have $\text{ad } k_S \cap k_{S'} = \mathbf{Q}$, hence $k_S = k_{S'}$. The groups $\Gamma_S/\mathbf{Q}^\times \subseteq \Gamma_{S'}/\mathbf{Q}^\times$ are both Fuchsian groups of the first kind. Since $\Gamma_S/\mathbf{Q}^\times \cong \Gamma/\{\pm 1\}$ is maximal in the set of the Fuchsian groups of the first kind (see Remark in Section 1.2), we have $\Gamma_S/\mathbf{Q}^\times = \Gamma_{S'}/\mathbf{Q}^\times$, hence $\Gamma_S = \Gamma_{S'}$. Then by [16, Lemma 6.29] we have $S = S'$. Q.E.D.

2. FULLNESS OF SIEGEL FUNCTIONS

1. Henceforth we assume that $p$ is a fixed prime number. (After Section 3 we assume $p \neq 2, 3$.)

The group $\Gamma_1(p)$ is a subgroup of $SL_2(\mathbf{Z})$ consisting of all matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with $a \equiv d \equiv 1 \pmod{p}$ and $c \equiv 0 \pmod{p}$. Let $\Gamma$ be a Fuchsian group of
the first kind. Then the quotient space $\Gamma \backslash \mathbb{H}$ can be completed to a complete non-singular curve denoted by $X_{\Gamma}$. When $\Gamma = \Gamma_{1}(p)$, the curve $X_{\Gamma}$ is denoted by $X_{1}(p)$. Though our purpose is to determine the cuspidal class number of $X_{1}(p)$, we consider another curve instead of $X_{1}(p)$.

Let $M$ and $\mathcal{O}$ be the same as in Section 1. Put $M = p$ and $I = \sqrt{p} \mathcal{O}$. Then we denote the curve $X_{\mathcal{O}}$ with $\Gamma = \Gamma(I)$ by $X(\sqrt{p})$. Since $\Gamma(I) = \left( \begin{smallmatrix} 1 & 0 \\ 0 & \sqrt{p} \end{smallmatrix} \right)^{-1}$, $\Gamma_{1}(p) \left( \begin{smallmatrix} 1 & 0 \\ 0 & \sqrt{p} \end{smallmatrix} \right)$, the curve $X(\sqrt{p})$ is isomorphic to $X_{1}(p)$. Hence the cuspidal class number of $X(\sqrt{p})$ is equal to that of $X_{1}(p)$, so that we consider the curve $X(\sqrt{p})$.

Put $S = \mathbb{Q}^\times \langle \sqrt{p} \rangle U(I)$. We denote the function field $\mathfrak{F}_{S}$ simply by $\mathfrak{F}$. Then $\mathfrak{F}$ is the field of all automorphic functions with respect to $\Gamma(\sqrt{p} \mathcal{O})$ such that the Fourier coefficients belong to $k_{p} = \mathbb{Q}(e^{2\pi i/p})$ (Proposition 1.7), and the field $C_{\mathfrak{F}}$ can be identified with the field of all meromorphic functions on $X(\sqrt{p})$ (Proposition 1.6). Every element $h$ of $\mathfrak{F}$ has the $q$-expansion $\sum_{n=-m}^{\infty} a_{n}q^{n}$ with $q = e^{2\pi i/p}$ and $a_{m} \neq 0 (\equiv k_{p})$. Let $P_{\infty}$ be the prime of $\mathfrak{F}$ corresponding to the valuation $v_{\infty}$ defined by $v_{\infty}(h) = m$. Then the residue field of $P_{\infty}$ is $k_{p}$, hence the degree of $P_{\infty}$ is one. Thus above $P_{\infty}$ there lies only one prime of $C_{\mathfrak{F}}$, which is denoted by $P_{\infty}$. The prime $P_{\infty,C}$ corresponds to the infinite point $\infty$ on $X(\sqrt{p})$. We call the prime $P_{\infty}$ (resp. $P_{\infty,C}$) the standard cuspidal prime of $\mathfrak{F}$ (resp. $C_{\mathfrak{F}}$). Let $\mathfrak{F}_{1}$ be the same as in Section 1.5. Then the Galois group $\text{Gal}(\mathfrak{F}/\mathfrak{F}_{1})$ can be identified with the group $\mathfrak{S}(\pm) = \mathfrak{S}(\sqrt{p} \mathcal{O})/\{ \pm 1 \}$ ((1.15)), where $\mathfrak{S} = \mathfrak{S}(\sqrt{p} \mathcal{O})$ consists of all matrices $(a_{ij})$ and $(c_{ij})$ in $GL_{2}(\mathcal{O}/\sqrt{p} \mathcal{O})$ with $a, b, c, d \in (\mathbb{Z}/p \mathbb{Z})^{\times}$. We call the former of type 1 and the latter of type $p$. Let $P$ be a prime of $\mathfrak{F}$ and let $v_{P}$ be the valuation of $P$. For each element $h \in \mathfrak{F}$, we define the prime $P_{h}$ of $\mathfrak{F}$ by $v_{P}(h) = v_{P}(h) \ (h \in \mathfrak{F})$. This defines a right action of $\text{Gal}(\mathfrak{F}/\mathfrak{F}_{1})$. When $P = P_{\infty}$, the degree of $P_{h}$ is also one. So that above $P_{\infty}$ there lies only one prime of $C_{\mathfrak{F}}$, which is denoted by $P_{\infty,C}$. Let $D = D(\sqrt{p} \mathcal{O})$ and $\mathfrak{D}_{u} = \mathfrak{D}_{u}(\sqrt{p} \mathcal{O})$ be the subgroups of $\mathfrak{S}$ defined in Section 1.3. If $\sigma$ is an element of $D$, then we have $P_{\sigma} = P_{\infty}$ by Proposition 1.5, hence $P_{\infty,C} = P_{\infty,C}$. If $\sigma$ is an element of $\mathfrak{D}_{u}(\pm) = \mathfrak{D}_{u}/\{ \pm 1 \}$, then there exists an element $\alpha$ of $G(\sqrt{p})$ such that $\sigma = \alpha \ (\text{mod } \Gamma(\sqrt{p} \mathcal{O}))$ by Proposition 1.1. In this case the prime $P_{\infty}^{\alpha}$ corresponds to the point on $X(\sqrt{p})$ represented by $x^{-1}(\infty)$. Thus for any element $\sigma$ of $\text{Gal}(\mathfrak{F}/\mathfrak{F}_{1})$ the prime $P_{\infty}^{\alpha}$ corresponds to some cusp on $X(\sqrt{p})$. Moreover, since all cusps of $G(\sqrt{p})$ (and $\Gamma(\sqrt{p} \mathcal{O})$) can be written as $\alpha^{-1}(\infty)$ with an element $\alpha$ of $G(\sqrt{p})$, the primes $P_{\infty}^{\alpha,C}$ exhaust all cusps on $X(\sqrt{p})$. We call the primes $P_{\infty}^{\alpha}$ (resp. $P_{\infty,C}^{\alpha}$) the cuspidal primes of $\mathfrak{F}$ (resp. $C_{\mathfrak{F}}$).

Let $\mathcal{D}$ (resp. $\mathcal{D}_{C}$) be the free abelian group generated by the cuspidal primes of $\mathfrak{F}$ (resp. $C_{\mathfrak{F}}$), and let $\mathcal{D}_{0}$ (resp. $\mathcal{D}_{C,0}$) be the subgroup of $\omega$ (resp. $\mathcal{D}_{C}$) of divisors of degree 0. Let $\mathcal{F}$ (resp. $\mathcal{F}_{C}$) be the group of non-zero...
functions in \( \mathcal{F} \) (resp. \( \mathcal{C}/\mathcal{F} \)) such that the divisors have support within the cuspidal primes. The factor group

\[
\mathcal{C} = \mathcal{C}(\sqrt{p}) = \mathcal{D}_{C,0}/\text{div} \mathcal{F}_C
\]

is called the \textit{cuspidal divisor class group} on \( X(\sqrt{p}) \). The order of \( \mathcal{C} \) is the \textit{cuspidal class number} of \( X(\sqrt{p}) \). By the mapping \( \mathcal{D} \cong \mathcal{D}_C \) and \( \mathcal{D}_0 \cong \mathcal{D}_{C,0} \). We see later that \( \mathcal{F}_C = \mathbb{C}^\times \mathcal{F} \) (see the argument after Theorem 2.1). So that we have \( \text{div} \mathcal{F} \cong \text{div} \mathcal{F}_C \), hence \( \mathcal{D}_0/\text{div} \mathcal{F} \cong \mathcal{C} \).

Let \( C = C(\sqrt{p} \mathcal{O}) \) be the abelian subgroup of \( \mathcal{C} \) consisting of all matrices \( \left( \begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix} \right) \) with \( a, b \in (\mathbb{Z}/p\mathbb{Z})^\times \). Put \( C(\pm) = C/\{ \pm 1 \} \). Then we have the unique decomposition

\[
\mathcal{C}(\pm) = C(\pm) D = DC(\pm).
\] (2.1)

We call \( C \) (resp. \( C(\pm) \)) the \textit{Cartan group} in \( \mathcal{C} \) (resp. \( \mathcal{C}(\pm) \)). We can see easily that the isotropy group of \( \mathcal{P}_\infty \) is \( D \). Let us denote by \( \sigma(\alpha) \) the element of \( \text{Gal}(\mathcal{F}/\mathcal{F}_1) \) corresponding to \( \alpha \in \mathcal{C}(\pm) \). Then (2.1) shows that the mapping \( \alpha \mapsto P_\infty^{\sigma(\alpha)} \) gives a one-to-one correspondence between the Cartan group \( C(\pm) \) and the set of cuspidal primes of \( \mathcal{C} \). Put \( R = \mathbb{Z}[\mathcal{C}(\pm)] \) and let \( R_0 \) be the subgroup of \( R \) of elements of degree 0. Then by this correspondence we have

\[
R \cong \mathcal{C} \quad \text{and} \quad R_0 \cong \mathcal{D}_0.
\] (2.2)

**Remark.** Let \( \kappa \) be any rational integer prime to \( p \). Let \( C(\kappa) \) be the subgroup of \( \mathcal{C} \) consisting of all matrices \( \left( \begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix} \right) \) and \( \left( \begin{smallmatrix} 0 & \kappa b \\ 1 & 0 \end{smallmatrix} \right) \). Then the group \( C(\kappa) \) also satisfies (2.1) in place of \( C \). We also call this group \( C(\kappa) \) a Cartan group. In the present paper we take \( \kappa = 1 \) for simplicity. Though we can define Cartan groups in a more intrinsic manner, we omit it here. We do it elsewhere in a more general setting such that \( M \) and \( I \) are arbitrary.

2. We recall the definition of Siegel functions [13]. Let \( a = (a_1, a_2) \) be an element of \( \mathbb{Q}^2 - \mathbb{Z}^2 \). Then the Siegel function \( g_a \) is defined by

\[
g_a(\tau) = \mathcal{I}_a(\tau) A^{1/12}(\tau),
\]

where \( \mathcal{I}_a(\tau) \) is the Klein form and \( A^{1/12}(\tau) \) is a 12th root of \( A(\tau) \):

\[
\mathcal{I}_a(\tau) = e^{-1/2i(a_1 \eta_1 + a_2 \eta_2)^2} \sigma(z, [\tau, 1]),
\]

\[
A^{1/12}(\tau) = 2\pi i \eta(\tau)^2.
\]

Here \( \eta_1, \eta_2 \) are the quasi periods of the Weierstrass zeta function associated with the period lattice \([\tau, 1]\), \( \sigma \) is the corresponding Weierstrass sigma function.
function, \( z = a_1 \tau + a_2 \), and \( \eta(\tau) \) is the Dedekind eta function. The Siegel function has the \( q \)-product

\[
g_a(\tau) = - q_\tau^{(1/2)} B_2(a_1) e^{2 \pi i a_2 (a_1 - 1/2)} (1 - q_\tau) \prod_{n=1}^{\infty} (1 - q_\tau^n q_z)(1 - q_\tau^n q_z)
\]

where \( q_\tau = e^{2 \pi i \tau} \), \( q_z = e^{2 \pi i z} \), and \( B_2(X) = X^2 - X + 1/6 \) is the second Bernoulli polynomial. Let \( a \in \mathbb{Q}^2 - \mathbb{Z}^2 \) and \( b \in \mathbb{Z}^2 \). Then the Klein forms satisfy the transformation formula

\[
f_{a+b}(\tau) = \varepsilon(a, b) f_a(\tau),
\]

where \( \varepsilon(a, b) \) is a root of unity given by

\[
\varepsilon(a, b) = \exp \left[ \frac{2 \pi i}{2} (b_1 b_2 + b_1 + b_2 + a_1 b_2 - a_2 b_1) \right].
\]

On the other hand, from the transformation formula for the eta function we have

\[
A^{1/12}(\alpha(\tau)) = j(\alpha, \tau) \psi(\alpha) A^{1/12}(\alpha),
\]

where \( \alpha = (a \ b \ c \ d) \in SL_2(\mathbb{Z}) \), \( j(\alpha, \tau) = c \tau + d \), and \( \psi \) is a character of \( SL_2(\mathbb{Z}) \). We quote the explicit expression of \( \psi \) from Weber [20, Section 38, pp. 125–127].

**Proposition 2.1.** Let \( \psi \) be the character of \( SL_2(\mathbb{Z}) \) defined above. Let \( \alpha = (a \ b \ c \ d) \) be any element of \( SL_2(\mathbb{Z}) \). Then

1. \( \psi(-\alpha) = -\psi(\alpha) \).
2. When \( d \) is odd,

\[
\psi(\alpha) = (-1)^{(d-1)/2} \exp \left[ \frac{2 \pi i}{12} \{(b - c) d + ac(1 - d^2)\} \right].
\]
3. When \( c \) is odd,

\[
\psi(\alpha) = -i(-1)^{(c-1)/2} \exp \left[ \frac{2 \pi i}{12} \{(a + d) c + bd(1 - c^2)\} \right].
\]

From Proposition 2.1 it follows immediately that ker \( \psi \) is a congruence subgroup of \( SL_2(\mathbb{Z}) \) of level 12 and of index 12. As is well known, the commutator of \( SL_2(\mathbb{Z}) \) has also index 12. Hence ker \( \psi \) is the commutator of \( SL_2(\mathbb{Z}) \).

Now we modify Siegel functions so as to be suitable for the group
CUSPIDAL CLASS NUMBER FORMULA

For each element \( r \in T \), put \( Z^{(r)} = \mathbb{Z} \sqrt{r} \times \mathbb{Z} \sqrt{r^*} \) and \( A^{(r)} = (1/r) \mathbb{Z} \sqrt{r} \times (1/r^*) \mathbb{Z} \sqrt{r^*} - Z^{(r)} \). For an element \( u = (a_1, a_2, \sqrt{r}) \in A^{(r)} \), put \( u^{(r)} = (a_1, a_2) \in \mathbb{Q}^2 - \mathbb{Z}^2 \). Then the function \( g_u(t) \) is defined by

\[
g_u(t) = g_{u^{(r)}} \left( \frac{\sqrt{r}}{\sqrt{r^*}} t \right). \tag{2.4}\]

For \( v \in Z^{(r)} \), put \( \varepsilon(u, v) = \varepsilon(u^{(r)}, v^{(r)}) \), where \( v^{(r)} \in \mathbb{Z}^2 \) is defined similarly to \( u^{(r)} \). Let \( \alpha = (a^{(r)}, b^{(r)}, c^{(r)}, d^{(r)}) \) be an element of \( G(\sqrt{r}) \). Then put \( \alpha^{(r)} = (c^{(r)}, b^{(r)}, d^{(r)}, a^{(r)}) \in \text{SL}_2(\mathbb{Z}) \).

**PROPOSITION 2.2.** Let \( u \) be an element of \( A^{(r)} \).

(1) Let \( v \in Z^{(r)} \). Then \( g_{u + v}(t) = \varepsilon(u, v) g_u(t) \).

(2) Let \( \alpha \in G(\sqrt{r}) \). Then \( g_u(\alpha(t)) = \psi(\alpha) g_u(t) \), where \( \psi(\alpha) = \psi(\alpha^{(r)}) \).

(3) Let \( \alpha \in \Gamma(\sqrt{p} \emptyset) \). Then \( g_u(\alpha(t)) = \varepsilon(\alpha) \psi(\alpha) g_u(t) \), where \( \varepsilon(\alpha) = \varepsilon(u, v) \) with \( v = u(\alpha - 1) \in Z^{(r)} \).

**Proof.** (1) follows immediately from the transformation formula for the Klein forms. (2) follows from the transformation formula for \( A^{(r)} \). (3) follows from (1) and (2). Q.E.D.

In the notation of Proposition 2.2 \( \varepsilon(u, v) \) is a 2\( p \)th root of unity and \( \psi(\alpha) \) is a 12\( \text{th} \) root of unity. So that \( g_u^{12p} \) depends only on the residue class of \( u \) modulo \( Z^{(r)} \) and is also invariant under the exchange of \( u \) by \( -u \). Moreover \( g_u^{12p} \) is a modular function with respect to \( \Gamma(\sqrt{p} \emptyset) \) and has no zeros and poles on \( \mathfrak{B} \). By the \( q \)-products for Siegel functions we see that the Fourier coefficients of \( g_u^{12p} \) belong to \( k_p \). Hence \( g_u^{12p} \) is an element of the group \( \mathfrak{F} \). Put \( \mathcal{A}^{(r)} = (A^{(r)}/Z^{(r)})/\{ \pm 1 \} \) and \( \mathcal{A} = \mathcal{A}^{(1)} \cup \mathcal{A}^{(r)} \) (disjoint). Then the group \( \mathcal{G}(\pm) \) operates on \( \mathcal{A} \) by the right multiplication of matrices. If \( u \in \mathcal{A}^{(r)} \) and if \( \alpha \in \mathcal{G}(\pm) \) is of type \( s \), then \( u\alpha \in \mathcal{A}^{(r,s)} \). For \( u \in \mathcal{A} \) and for \( \sigma(\alpha) \in \text{Gal}(\mathbb{Q}/\mathbb{Q}) \) (\( \alpha \in \mathcal{G}(\pm) \)) we have

\[
(g_u^{12p})^{\sigma(\alpha)} = g_{u\alpha}^{12p}. \tag{2.5}\]

In fact if \( \alpha \) is an element of \( \mathcal{G}_u(\pm) \), then (2.5) follows from Proposition 1.5(1) and Proposition 2.2(2). If \( \alpha \) is an element of \( D \), then (2.5) follows from Proposition 1.5(2) and the \( q \)-products for Siegel functions. Since \( \mathcal{G}(\pm) = \mathcal{G}_u(\pm) D \), (2.5) holds for all \( \alpha \in \mathcal{G}(\pm) \).

Now we consider the divisor of \( g_u^{12p} \). For any \( x \in \mathbb{R} \) we denote by \( \langle x \rangle \) the real number defined by \( 0 \leq \langle x \rangle < 1 \) and \( \langle x \rangle \equiv x \mod \mathbb{Z} \). Let \( u \in \mathcal{A}^{(r)} \) and let \( u' = (u'_1, u'_2) \in A^{(r)} \) be a representative of \( u \). Put \( u'_1 = a'_1 \sqrt{r} \). Then the
number \( rB_2(\langle a'_i \rangle) \) does not depend on the choice of \( u' \), but depends only on \( u \). So we denote it by \( B_{2,r}(\langle u_1 \rangle) \).

**Proposition 2.3.** Let \( u \) be an element of \( \mathcal{A}(r) \). Then the divisor of \( g_u^{12p} \) is given by

\[
\text{div}(g_u^{12p}) = \frac{12p}{2} \sum_{a \in \mathcal{C}(\pm)} B_{2,r,s}(\langle (u\alpha)_1 \rangle) P_{\infty}^{p(a^{-1})},
\]

where \( s \) denotes the type of \( \alpha \).

**Proof:** The order at \( P_{\infty} \) can be obtained by the \( q \)-products for Siegel functions. Then the formula follows immediately from (2.5). \( \square \)

3. Now we consider the group ring \( R \). Let us define the Stickelberger element \( \theta \in R_Q = \mathbb{Q}[[\mathcal{C}(\pm)]] \) by

\[
\theta = \frac{1}{2} \sum_{a \in \mathcal{C}(\pm)} B_{2,p,s}(\langle (w\alpha)_1 \rangle) \alpha^{-1},
\]

where \( s \) denotes the type of \( \alpha \) and \( w \) denotes the element of \( \mathcal{A}(p) \) represented by \((\sqrt{p}/p, 0)\). If we denote by \( \sigma_{+,a} \) and \( \sigma_{-,b} \) the elements \((a, 0)\) and \((0, b)\) of \( \mathcal{C}(\pm) \) \((a, b \in \mathbb{Z}/p\mathbb{Z})^* / \{ \pm 1 \}\), respectively, then

\[
\theta = \frac{1}{2} \left\{ \sum_{a=1}^{(p-1)/2} p B_2\left(\frac{a}{p}\right) \sigma_{+,a}^{-1} + \sum_{b=1}^{(p-1)/2} \frac{1}{6} \sigma_{-,b}^{-1} \right\}.
\]

We denote by \( C^e(\pm) \) the set of all \( \sigma_{+,a} \). Then \( C^e(\pm) \) is a subgroup of \( \mathcal{C}(\pm) \) of index 2, and is isomorphic to \((\mathbb{Z}/p\mathbb{Z})^* / \{ \pm 1 \}\). Let \( \chi \) be a character of \( \mathcal{C}(\pm) \) and let \( e_\chi \) be the idempotent in \( R_e = \mathbb{C}[[\mathcal{C}(\pm)]] \) associated to \( \chi \):

\[
e_\chi = \frac{1}{|\mathcal{C}(\pm)|} \sum_{\alpha \in \mathcal{C}(\pm)} \chi(\alpha) \alpha^{-1}.
\]

Then \( \theta e_\chi = (\frac{1}{2} B_{2,\chi,c}) e_\chi \), where \( B_{2,\chi,c} \) is the Bernoulli–Cartan number defined by

\[
B_{2,\chi,c} = \sum_{a \in \mathcal{C}(\pm)} B_{2,p,s}(\langle (w\alpha)_1 \rangle) \chi(\alpha),
\]

where \( s \) denotes the type of \( \alpha \). Let \( \chi_0 \) be the character of \((\mathbb{Z}/p\mathbb{Z})^* / \{ \pm 1 \}\) obtained by the restriction of \( \chi \) to \( C^e(\pm) \). If \( \chi_0 \neq 1 \), then \( B_{2,\chi,0} = B_{2,\chi_0} \), where \( B_{2,\chi_0} \) denotes the generalized Bernoulli number associated to \( \chi_0 \), namely,

\[
B_{2,\chi_0} = p^{(p-1)/2} \sum_{a=1}^{(p-1)/2} B_2\left(\frac{a}{p}\right) \chi_0(a).
\]
Now we prove the fullness of functions $g_u^{12p}$. Let $\mathcal{F}$ be the subgroup of $\mathcal{F}$ consisting of all functions $g$ in $\mathcal{F}$ which can be written as $g = c \prod_u g_u^{m(u)}$, where $c \in k_p^*$, $m(u) \in \mathbb{Z}$, and $g_u$ is a function (2.4) with $r$ and $u$ arbitrary. Since the rank of $\mathcal{D}_0$ is $c(p)-1$, the rank of $\mathcal{F}/k_p^*$ is at most $c(p)-1$, where $c(p) = |C(\pm)|$ is the number of cusps of $X(\sqrt{p})$ and is equal to $p-1$ if $p \neq 2$, or equal to 2 if $p = 2$.

Theorem 2.1. The group $\mathcal{F}/k_p^*$ has the possible maximal rank $c(p)-1$.

Proof. Let $\mathcal{F}'$ be the subgroup of $\mathcal{F}$ generated by all $g_u^{12p}$. Then it is sufficient to prove that the rank of $\mathcal{F}'$ modulo constants is $c(p)-1$, namely, that the rank of div $\mathcal{F}'$ is $c(p)-1$. We identify the cuspidal divisor group $\mathcal{D}$ with $\mathcal{R}$ by (2.2). Since the group $C(\pm)$ operates on $\mathcal{A}$ transitively, every element $u$ of $\mathcal{A}$ can be written uniquely as $u = w\alpha$ with $\alpha \in C(\pm)$. Then by Proposition 2.3 we have div$(g_w^{12p}) = 12p\theta\alpha$. This implies div $\mathcal{F}' = 12p\theta R \subset R_0$. Put $V = \theta R_0 \subset C R_0$. Then it is sufficient to prove $\dim_C V = c(p)-1$. Let $\chi$ be a character of $C(\pm)$. We show that if $\chi \neq 1$ then $e_\chi \in V$, hence $\dim_C V = c(p)-1$. As is seen above, we have $\theta e_\chi = (\frac{1}{2}B_{2,x,C}) e_\chi$. So that it is sufficient to show that if $\chi \neq 1$ then $B_{2,x,C} \neq 0$. If $x_0 \neq 1$, then $B_{2,x,C} = B_{2,z_0}$. The fact $B_{2,z_0} \neq 0$ is well known (see, e.g., Washington [19, p. 30]), hence $B_{2,x,C} \neq 0$. If $x_0 = 1$, then $\chi(\sigma_{-1}) = -1$. Hence by direct calculations, we have $B_{2,\sigma_{-1}} = -(p-1)/6 \neq 0$. Q.E.D.

As a consequence of this theorem, we have $\mathcal{F}_C = C^* \mathcal{F}$. In fact, since $\mathcal{F}_C/C^* \mathcal{F}$ is a finite group, if $g \in \mathcal{F}_C$, then some power of $g$ belongs to $C^* \mathcal{F}$. This implies $g \in C^* \mathcal{F}$.

The functions $g_u^{12p} (u \in \mathcal{A})$ are the conjugates of $g_w^{12p}$ over $\mathcal{F}_1$. Hence the product of $g_u^{12p}$ is an element of $\mathcal{F}_1$. Since the group $G(\sqrt{p})$ has only one equivalence class of cusps, this product must be a constant. In fact we have

$$\prod_{u \in \mathcal{A}} g_u^{12p} = p^{6p}. \quad (2.6)$$

Theorem 2.1 shows that this is the only one relation among the functions $g_u^{12p}$.

3. Determination of the Unit Group $\mathcal{F}$

1. From now on we assume $p \neq 2, 3$. The reasons why we exclude 2 and 3 are that they are exceptional primes, and that the modular curves $X_1(2), X_1(3)$ have genus 0, so that the cuspidal class numbers are 1. In this section we shall determine the unit group $\mathcal{F}$.

First we determine the group $\mathcal{F}$. Let $u$ be an element of $A^{(r)}$. Then we
call $r$ the type of $u$, and write $u = ((x/r) \sqrt{r}, (y/r^*) \sqrt{r^*}) (x, y \in \mathbb{Z})$. Let $m(u)$ be a rational integer and let us consider a function $g = \prod_u g_u^{m(u)}$. Since the Fourier coefficients of $g_u$ belong to the field $k_p$ (because of $p \neq 2$), the condition $g \in \mathcal{G}$ is equivalent to that $g$ is a modular function with respect to $\Gamma(\sqrt{p} \mathbb{O})$. By Proposition 2.2(3), this condition is equivalent to the following:

$$\prod_u \{ \varepsilon_u(x) \psi_u(x) \}^{m(u)} = 1 \quad \forall x \in \Gamma(\sqrt{p} \mathbb{O}).$$  \hspace{1cm} (3.1)

**Lemma 3.1.** If $x \in \Gamma(12p\mathbb{O})$, then $\varepsilon_u(x) = \psi_u(x) = 1$.

**Proof.** This follows immediately from (2.3) and Proposition 2.1. Q.E.D.

Put $G_k = \Gamma(\sqrt{p} \mathbb{O})/\Gamma(k\mathbb{O})$, for $k = 3, 4, p$. Then $G_k \cong SL_2(\mathbb{Z}/k\mathbb{Z})$ for $k = 3, 4$, and we have a canonical decomposition $\Gamma(\sqrt{p} \mathbb{O})/\Gamma(12p\mathbb{O}) \cong G_3 \times G_4 \times G_p$. We can take elements $\alpha_k$ and $\beta_k$ of $\Gamma(\sqrt{p} \mathbb{O})$ $(k = 3, 4, p)$ such that $\alpha_k \equiv (1 \sqrt{p}) (\text{mod } k\mathbb{O})$, $\beta_k \equiv (1 0) (\text{mod } k\mathbb{O})$, and $\alpha_k \equiv \beta_k \equiv (1 0)$ (mod $l\mathbb{O}$) for all $l = 3, 4, p$ with $l \neq k$.

**Lemma 3.2.** The set $\{ \alpha_k, \beta_k \} (k = 3, 4, p)$ generates the factor group $\Gamma(\sqrt{p} \mathbb{O})/\Gamma(12p\mathbb{O})$.

**Proof.** In fact it is easy to see that each group $G_k$ $(k = 3, 4, p)$ is generated by $(1 \sqrt{p})$ and $(1 0)$. From this the lemma follows. Q.E.D.

**Lemma 3.3.** (1) If $k = r = p$, then $\varepsilon_u(\alpha_k) = \exp[(2\pi i/p) \xi_1]$, otherwise $\varepsilon_u(\alpha_k) = 1$. Here $\xi_1$ is an integer satisfying $\xi_1 = 2^{-1} x^2$ (mod $p$).

(2) If $k = r^* = p$ ($r = 1$), then $\varepsilon_u(\beta_k) = \exp[(2\pi i/p) \xi_2]$, otherwise $\varepsilon_u(\beta_k) = 1$. Here $\xi_2$ is an integer satisfying $\xi_2 = 2^{-1} y^2$ (mod $p$).

**Proof.** Since (2) is similar to (1), we prove only (1). Let $\alpha = (a/b \sqrt{p})$ be an element of $\Gamma(\sqrt{p} \mathbb{O})$ $(a, b, c, d \in \mathbb{Z})$. Then by (2.3) we have $\varepsilon_u(\alpha) = \exp[(2\pi i/2) \xi]$, where $\xi \in \mathbb{Q}$ and $\xi \equiv ar^*x(bx + 1) + dry(cy + 1) + (b/r) x^2 + bx - (c/r^*) y^2 + cy$ (mod $2\mathbb{Z}$). (Here we used the condition $\det(\alpha) = 1$. Put $\alpha = \alpha_k$. Then, since $a \equiv d \equiv 0$ (mod 12) and $c \equiv 0$ (mod 12p), we have $\xi \equiv (b/r) x^2 + bx$ (mod $2\mathbb{Z}$). If $k = 3$, then $b \equiv 0$ (mod 4p), hence $\xi \equiv 0$ (mod $2\mathbb{Z}$). This implies $\varepsilon_u(\alpha_k) = 1$. If $k = 4$, then $b/r$ and $b$ are both odd integers, hence $\xi \equiv x^2 + x \equiv x(x + 1) \equiv 0$ (mod $2\mathbb{Z}$). This implies $\varepsilon_u(\alpha_k) = 1$. If $k = p = r$, then $r = 1$. Since $b \equiv 0$ (mod 12), we have $\xi \equiv 0$ (mod $2\mathbb{Z}$), hence $\varepsilon_u(\alpha_k) = 1$. Lastly let $k = p = r$. Since $b$ is even, we can write $bx^2/r = 2\xi_1^2/p$ with an integer $\xi_1$. Hence $\xi \equiv 2\xi_1^2/p$ (mod $2\mathbb{Z}$), and $\varepsilon_u(\alpha_k) = \exp[(2\pi i/p) \xi_1]$. Since $b \equiv 1$ (mod $p$), we have $\xi_1 \equiv 2^{-1} x^2$ (mod $p$). Q.E.D.
Lemma 3.4. (1) \( \psi,(z_k) = \exp[(2\pi i/3) r] \) \( (k = 3) \), \( \exp[(2\pi i/4)(-r)] \) \( (k = 4) \), 1 \( (k = p) \).

(2) \( \psi,(\beta_k) = \exp[(2\pi i/3)(-r^*)] \) \( (k = 3) \), \( \exp[(2\pi i/4) r^*] \) \( (k = 4) \), 1 \( (k = p) \).

Proof. Since (2) is similar to (1), we consider only (1). Let \( x \) be the same as in the proof of Lemma 3.3. Then \( x^{(r)} = \left(1 + \frac{b r}{1 + dp} \right) \). Assume \( d \equiv 0 \) \( (\text{mod} \ 12) \). Then by Proposition 2.1, we have \( \psi,(z) = \psi,(x^{(r)}) = \exp[(2\pi i/12)(br - cr^*)] \) (even when \( 1 + dp < 0 \)). Let \( x = x_k \). Then \( c \equiv d \equiv 0 \) \( (\text{mod} \ 12) \), hence \( \psi,(z_k) = \exp[(2\pi i/12) br] \). If \( k = 3 \), then \( b \equiv 0 \) \( (\text{mod} \ 4) \). Let \( b = 4b_1 \). Since \( b \equiv 1 \) \( (\text{mod} \ 3) \), we have \( b_1 \equiv 1 \) \( (\text{mod} \ 3) \). Hence \( \psi,(z_k) = \exp[(2\pi i/3) b_1 r] = \exp[(2\pi i/3) r] \). If \( k = 4 \), then \( b \equiv 0 \) \( (\text{mod} \ 3) \). Let \( b = 3b_2 \). Since \( b \equiv 1 \) \( (\text{mod} \ 4) \), we have \( b_2 \equiv -1 \) \( (\text{mod} \ 4) \). Hence \( \psi,(z_k) = \exp[(2\pi i/4) b_2 r] = \exp[(2\pi i/4)(-r)] \). If \( k = p \), then \( b \equiv 0 \) \( (\text{mod} \ 12) \). Hence \( \psi,(z_k) = 1 \).

Q.E.D.

Now combining Lemmas 3.1–3.4 with (3.1), we have the characterization of the group \( \mathcal{S} \).

Theorem 3.1. The group \( \mathcal{S} \) consists of all functions \( g \) of the form \( g = c \prod g_{u}^{m(u)} \), where \( c \in k_{p}^{*} \), \( m(u) \in \mathbb{Z} \), and \( \{m(u)\} \) satisfies the following conditions:

(i) \( \sum_{u: \text{type} = p} m(u) x^2 \equiv 0 \) \( \text{(mod } p\text{)} \).
(ii) \( \sum_{u: \text{type} = 1} m(u) y^2 \equiv 0 \) \( \text{(mod } p\text{)} \).
(iii) \( \sum_{u} m(u) r \equiv 0 \) \( \text{(mod 12)} \).
(iv) \( \sum_{u} m(u) r^* \equiv 0 \) \( \text{(mod 12)} \).

2. Now we prove \( \mathcal{F} = \mathcal{S} \). Let \( u \) be as above. If \( (x, y) \) satisfies one of the conditions

(i) \( 1 \leq x \leq \frac{1}{2}(p - 1) \), \( y = 0 \) \text{ or } (ii) \( x = 0 \), \( 1 \leq y \leq \frac{1}{2}(p - 1) \),

then we call \( u \) reduced, and denote by \( \mathcal{R} \) the set of all reduced \( u \). Note that \( \mathcal{R} \) is a complete set of representatives of \( \mathcal{S} \). We call any function in \( C_{\mathcal{F}}^{(p)} \) a modular function.

Lemma 3.5. Let \( l \) be a prime number and let \( m: \mathcal{R} \rightarrow \mathbb{Z} \) be a mapping. If \( \prod_{u \in \mathcal{R}} g_{u}^{m(u)} = g^{l} \) with \( g \) modular, then the residue classes of \( m(u) \) modulo \( l \) are equal to each other.

Proof. The following proof is based on the method of [13]. Let \( f \neq 0 \) be a modular function and let \( f = \sum a_{n} q_{N}^{n} \) be its Fourier expansion with \( q_{N} = e^{2\pi i N / \sqrt{p}} \). Let \( a_{m} q_{N}^{m} \) be the lowest term. Then the power series \( f^{*} = \)
The reduced form of \( f \) is called the reduced form of \( f \). Let \( g_u^* \) and \( g^* \) be the reduced form of \( g_u \) and \( g \), respectively. Then we have

\[
\prod_{u \in \mathcal{A}} (g_u^*)^{m(u)} = (g^*)^l.
\] (3.3)

By the \( q \)-products for Siegel functions, \( g_u^* \) is a power series of \( q_1 \) \((N=1)\) and has coefficients in the ring of cyclotomic integers \( \mathcal{O}_p \) in \( k_p \). On the other hand from the relation of the lemma it follows that the Fourier coefficients of \( \zeta_l g \) with some \( l \)th root of unity \( \zeta_l \) belong to \( k_p \). So that by a consequence of a theorem of Shimura [13, Chap. 4, Lemma 3.1], the coefficients of \( \zeta_l g \) have bounded denominators, hence the coefficients of \( g^* \) belong to \( k_p \) and also have bounded denominators. Then by (3.3) and the Gauss lemma for power series with bounded denominators, we see that the power series \( g^* \) also has coefficients in \( \mathcal{O}_p \). Let \( a_1 \) be the coefficient of \( q_1 \) in \( g_u^* \). Then

\[
a_1 = \begin{cases} 
-(\zeta+x+\zeta-x) & \text{if } x=0, \\
-1 & \text{if } x=1, y=0, \\
0 & \text{if } x \neq 0, 1, y=0,
\end{cases}
\]

where \( \zeta = e^{2\pi i/p} \). We write \( m(x, y) \) instead of \( m(u) \). Then the coefficient of \( q_1 \) in the power series \( \prod_{u \in \mathcal{A}} (g_u^*)^{m(u)} \) is given by

\[
-m(1, 0) - \sum_{y=1}^{(p-1)/2} m(0, y)(\zeta^y + \zeta^{-y}).
\] (3.4)

Since this is equal to the coefficient of \( q_1 \) in \((g^*)^l\), (3.4) must be congruent to 0 modulo \( l \). Then by [13, Chap. 4, Lemma 2.3] we have

\[
m(0, 1) \equiv m(0, 1) \equiv \cdots \equiv m(0, (p-1)/2) \pmod{l}.
\] (3.5)

Let \( U \) be the group defined in Section 1.4. Let \( \alpha \) be an element of \( U \) whose finite part is \((0, 1)\). (The type of \( \alpha \) is \( p \).) Then applying \( \sigma(\alpha) \) to the relation of the lemma, we have \( \prod_{u \in \mathcal{A}} (g_u^{\sigma(\alpha)}(u))^{m(u)} = (g_1^{\sigma(\alpha)})^l \), where \( g_1 = \zeta_l g \in \mathcal{G}(p) \). Let \( u\alpha = ((y/r^*) \sqrt{r^*}, (x/r) \sqrt{r}) \). Then by (2.5) we have \( g_u^{\sigma(\alpha)} = cg_{ux} \), where \( c \) is a root of unity. Let \( m' : \mathcal{A} \to \mathbb{Z} \) be the mapping defined by \( m'(u\alpha) = m(u) \), namely \( m'(x, y) = m(y, x) \). Then we have \( g_u^{m'(\alpha)} = g_2 \) with \( g_2 \) modular. Since the situation is the same as above, we have the following relations by (3.5): \( m'(1, 0) \equiv m'(0, 1) \equiv \cdots \equiv m'(0, (p-1)/2) \pmod{l} \), in other words,

\[
m(0, 1) \equiv m(1, 0) \equiv \cdots \equiv m((p-1)/2, 0) \pmod{l}.
\] (3.6)

By (3.5) and (3.6) the proof is completed. Q.E.D.
LEMMA 3.6. Let \( l \) and \( m \) be the same as in Lemma 3.5. If \( g \in G \) and \( g' = \prod_{u \in \mathfrak{M}} g_u^{m(u)} \), then \( g \in \mathcal{S} \).

Proof. By Lemma 3.5 we have \( \prod_{u \in \mathfrak{M}} g_u^{m(u)} = (\prod_{u \in \mathfrak{M}} g_u)^k \times (\prod_{u \in \mathfrak{M}} g_u^{m(u)})^l \) with \( k, m'(u) \in \mathbb{Z} \). Since \( \prod_{u \in \mathfrak{M}} g_u \) is a constant by (2.6), it follows that \( g = c \prod_{u \in \mathfrak{M}} g_u^{m(u)} \) with \( c \in \mathbb{C}^\times \). Since \( g \) and \( g_u \) have Fourier coefficients in \( k_p, \) we have \( c \in k_x^\times \). This implies \( \prod_{u \in \mathfrak{M}} g_u^{m(u)} = c^{-1}g \in G, \) hence \( g \in \mathcal{S} \).

Q.E.D.

THEOREM 3.2. The group \( G \) coincides with the group \( \mathcal{S} \).

Proof. Since \( G/\mathcal{S} \) is a torsion group by Theorem 2.1, if \( g \in G \), then some power of \( g \) belongs to \( \mathcal{S} \). Hence it is sufficient to prove that if \( l \) is a prime, and if \( g \in G \) and \( g' \in \mathcal{S} \), then \( g \in \mathcal{S} \). Since \( g' \in \mathcal{S} \), we have \( (cg)' = \prod_{u \in \mathfrak{M}} g_u^{m(u)} \), where \( c \in \mathbb{C}^\times \) and \( m(u) \in \mathbb{Z} \). This implies that the Fourier coefficients of \( \zeta_{i}cg \) with some \( l \)th root of unity \( \zeta_i \) belong to \( k_p, \) hence \( \zeta_{i}cg \in G \). Then by Lemma 3.6 we have \( \zeta_{i}cg \in \mathcal{S} \). Since \( g \in G \), we have \( \zeta_i c \in k_x^\times \), hence \( g \in \mathcal{S} \).

Q.E.D.

By Theorems 3.1 and 3.2 we conclude that the group \( G \) consists of all functions \( c \prod_{u \in \mathfrak{M}} g_u^{m(u)} \) such that \( c \in k_x^\times \) and \( \{m(u)\} \) satisfies the conditions (i)–(iv) in Theorem 3.1. The fact that \( \prod_{u \in \mathfrak{M}} g_u \) is a constant is the only one relation among the functions \( g_u, \) and its precise value is the following:

\[
\prod_{u \in \mathfrak{M}} g_u = \sqrt{p} e^{-\left(\frac{p-1}{4}\right) n_l}.
\]

4. COMPUTATION OF THE CUSPIDAL CLASS NUMBER

1. By the results of Section 3 we can transform the problem of computing the cuspidal class number to a problem of purely algebraic nature. Namely, if we identify the cuspidal divisor group \( \mathcal{D} \) with the group ring \( R \) by (2.2), then \( \text{div} \ G \) is a subgroup of \( R_0 \) described in the following proposition, and the cuspidal class number is equal to the index \([R_0: \text{div} \ G]\).

Let \( \theta, \sigma_{+, a}, \sigma_{-, b} \) be as in Section 2.3. Let \( I_{12} \) be the set of all elements \( \sum_{x \in C(\pm)} m(\alpha) \alpha \) of \( R (m(\alpha) \in \mathbb{Z}) \) satisfying the following conditions:

\[
(i) \quad \sum_{a=1}^{(p-1)/2} m(\sigma_{+, a}) a^2 \equiv 0 \pmod{p}, \quad (4.1)
\]

\[
(ii) \quad \sum_{b=1}^{(p-1)/2} m(\sigma_{-, b}) b^2 \equiv 0 \pmod{p}, \quad (4.2)
\]

\[
(iii) \quad \sum_{a=1}^{(p-1)/2} m(\sigma_{+, a}) + p \sum_{b=1}^{(p-1)/2} m(\sigma_{-, b}) \equiv 0 \pmod{12}. \quad (4.3)
\]
Then \(I_{12}\) is an ideal of \(R\). Note that \(p^2 \equiv 1 \pmod{24}\) because of \(p \neq 2, 3\). This implies that the condition (4.3) is equivalent to the following:

\[
(iii') \quad p \sum_{a=1}^{(p^2-1)/2} m(\sigma_+, a) + \sum_{b=1}^{(p-1)/2} m(\sigma_-, b) \equiv 0 \pmod{12}.
\]

**Proposition 4.1.** \(\text{div } F = I_{12}\theta\).

**Proof.** By the results of Section 3, the group \(F\) consists of all functions \(g = c \prod_{a \in \mathbb{A}} s_{u}^{m(u)}\) where \(c \in k_{p}^{x}\) and \(\{m(u)\}\) satisfies the conditions (i)-(iv) in Theorem 3.1. For each \(u\) let \(\alpha\) be the unique element of \(C(\pm)\) such that \(u = w\alpha\) in \(\mathbb{A}\). If \(\alpha = \sigma_+, a\), then \(r = p, x = a \pmod{p}, y = 0\). If \(\alpha = \sigma_-, b\), then \(r = 1, x = 0, y = b \pmod{p}\). Since \(\text{div}(g_{u}^{(12p)}) = 12p\theta\) by Proposition 2.3, we have \(12p \text{div}(g) = \text{div}(g_{u}^{(12p)}) = \sum m(u) \text{div}(g_{u}^{12p}) = 12p \sum m(u) \theta\), hence \(\text{div}(g) = (\sum m(u) x) \theta\). Put \(m(x) = m(u)\). Then the conditions (i)-(iv) in Theorem 3.1 are equivalent to (4.1)-(4.4). This proves the proposition.

Q.E.D.

**Remark.** We may call the ideal \(R\theta \cap R\) the Stickelberger ideal (cf. [13]). We can prove that it coincides with \(I_{12}\theta\), but we omit its proof because we do not need the result.

2. We note that \(\text{deg } \theta = 0\). This follows from the fact that \(\text{div}(g_{u}^{(12p)}) = 12p\theta\). Since \(p^2 \equiv 1 \pmod{24}\), we denote by \(l\) the integer \((p^2 - 1)/24\). Put \(\mu = \sum_{x \in C(\pm)} \alpha, \mu_+ = \sum_{a=1}^{(p^2-1)/2} \sigma_+, \mu_- = \sum_{b=1}^{(p-1)/2} \sigma_-\).

**Lemma 4.1.** \(\xi \in I_{12}\) and \(\xi \theta = 0\) if and only if \(\xi \in \mathbb{Z}\mu\).

**Proof.** \(\mu \theta = (\text{deg } \theta) \mu = 0\). That \(\mu \in I_{12}\) can be verified directly. Conversely, assume \(\xi \in R_{C}\) and \(\xi \theta = 0\). Since the set of idempotents \(e_{\chi}\) is a basis of \(R_{C}\), we can write \(\xi = \sum_{\chi} a(\chi) e_{\chi}\) with \(a(\chi) \in C\). Then \(0 = \xi \theta = \xi \sum_{\chi} a(\chi) B_{\chi, B_{\chi}, C} e_{\chi}\). Since if \(\chi \neq 1\), then \(B_{\chi, B_{\chi}, C} \neq 0\) (see the proof of Theorem 2.1), we have \(a(\chi) = 0\) for all \(\chi \neq 1\). Hence \(\xi = a_{(1)} e_{1} \in C\mu\). If \(\xi \in I_{12}\), then \(\nu \in \mathbb{Z}\mu\).

Q.E.D.

Let \(I_{12l}\) (resp. \(I_{0}\)) be the set of all elements of \(I_{12}\) which satisfy that the left hand side of (4.3) is congruent to 0 modulo 121 (resp. equal to 0).

**Lemma 4.2.** (1) \([I_{12} \theta : I_{12l}\theta] = l\).

(2) \(I_{12l}\theta = I_{0}\theta\).

**Proof.** (1) Let \(\eta = \xi \theta\) with \(\xi = \sum m(x) \alpha \in I_{12}\). Let \(k = k(\xi)\) be the integer determined by \(\sum_{x} m(\sigma_+, a) + \sum_{b} m(\sigma_-, b) = 12k\). Then the residue class of \(k\) modulo \(l\) depends only on \(\eta\). In fact, let \(\xi'\) be another element of \(I_{12}\) satisfying \(\eta = \xi' \theta\). Then \((\xi - \xi') \theta = 0\), hence by Lemma 4.1
CUSPIDAL CLASS NUMBER FORMULA

\[ \xi - \xi' = n\mu \text{ with } n \in \mathbb{Z}. \]  
This implies that \( k(\xi) - k(\xi') = nl \), hence \( k(\xi) \equiv k(\xi') \) (mod \( l \)). Put \( \varphi(\eta) = k \) (mod \( l \)). Then \( \varphi \) is a homomorphism from \( I_{12\theta} \) to \( \mathbb{Z}/l\mathbb{Z} \). Since \( \ker \varphi = I_{12\theta} \), it is sufficient to prove that \( \varphi \) is surjective. Let \( k \in \mathbb{Z}/l\mathbb{Z} \) be any element. Since \( (p, l) = 1 \), we can choose an integer \( x \) satisfying \( px \equiv k \) (mod \( l \)). Then \( \xi = 12px\sigma_{+,1} \) satisfies that \( \xi \in I_{12} \) and \( \varphi(\xi\theta) = k \). (2) \( k(\mu) = l \), hence \( \mu \in I_{12\theta} \). If \( \xi \in I_{12\theta} \) and \( k(\xi) = nl \) (\( n \in \mathbb{Z} \)), then \( k(\xi - n\mu) = 0 \), hence \( \xi - n\mu \in I_0 \). This implies \( I_{12\theta} = I_0 + \mathbb{Z}\mu \), so that \( I_{12\theta} = \theta_0 \) by Lemma 4.1. Q.E.D.

By Proposition 4.1 and Lemma 4.2, the cuspidal class number is equal to \( [R_0 : I_0\theta]/l \). Put \( s = (1/12)(p\mu_+ + \mu_-) \), \( 0' = 0 - s \).

**Lemma 4.3.**

1. \( I_0s = \mathbb{Z}2l\mu_+ \).
2. \( I_0\theta = R_0 \cap (I_0\theta' + \mathbb{Z}2l\mu_+). \)

**Proof.** (1) The inclusion \( \subset \) can be verified immediately. In order to prove the equality, take the element \( \xi = \sum m(a) \alpha \) defined by \( m(\sigma_{+,1}) = p \), \( m(\sigma_{+,a}) = 0 \) \( (a = 2, \ldots, (p - 1)/2) \), \( m(\sigma_{-,1}) = 2 - p \), \( m(\sigma_{-,b}) = 2 \) \( (b = 2, \ldots, (p - 1)/2) \). Then we have \( \xi \in I_0 \) and \( \xi s = 2l\mu_+ \). This proves (1). (2) The inclusion \( \subset \) is obvious by (1). Let \( \eta = \xi\theta' + 2ln\mu_+ \) with \( \xi \in I_0 \) and \( n \) an integer. Suppose \( \deg \eta = 0 \). Since \( \deg \theta' = -l \), we have \( n = \deg \xi/(p - 1) \). Put \( \eta_1 = \xi\theta = \xi\theta' + \xi s \). By (1), \( \xi s = 2n_1l\mu_+ \) with some integer \( n_1 \). Since \( \deg \eta_1 = 0 \), we have \( n_1 = \deg \xi/(p - 1) \) \((= n)\). Hence \( \eta = \eta_1 \in I_0\theta \). This proves the reverse inclusion. Q.E.D.

By Lemma 4.3 we have

\[ R_0/I_0\theta \cong (R_0 + I_0\theta' + \mathbb{Z}2l\mu_+)/(I_0\theta' + \mathbb{Z}2l\mu_+). \]  

For an integer \( d \), let \( R_d \) denote the subgroup of \( R \) consisting of all elements \( \xi \) satisfying \( \deg \xi \equiv 0 \) (mod \( d \)).

**Lemma 4.4.**

1. \( R_0 + I_0\theta' + \mathbb{Z}2l\mu_+ = R_{(p - 1)l} \).
2. \( I_0\theta' + \mathbb{Z}2l\mu_+ = I_{12\theta} \theta' + \mathbb{Z}2l\mu_+ \).

**Proof.** (1) If \( \xi = \sum m(a) \alpha \in I_0 \), then we have \( \deg \xi = -(p - 1) \sum b m(\sigma_{-,b}) \in (p - 1) \mathbb{Z} \). Hence \( \deg(I_0\theta') \in (p - 1) l\mathbb{Z} \). Since \( \deg(2l\mu_+) = (p - 1)l \), we have the equation of the lemma. (2) By the proof of Lemma 4.2(2), \( I_{12\theta} = I_0 + \mathbb{Z}\mu \), hence \( I_{12\theta} = I_0\theta' + \mathbb{Z}\mu\theta' \). Put \( \xi = p\mu_+ - \mu_- \). Then \( \xi \in I_0 \) and \( \mu = \xi\theta' + 2ln\mu_+ \) with \( n = (p + 1)/2 \). This implies the inclusion \( \supset \). The reverse inclusion is obvious. Q.E.D.
Now we consider the following inclusion:

\[ R \supset R_{(p-1)l} \supset I_{12l} \theta' + \mathbb{Z}2l \mu_+ \supset I_{12l} \theta'. \] (4.6)

Put \( R_{+,Q} = \mathbb{Q}[C'(\pm)] \). Then \( R_{+,Q} \) is a subalgebra of \( R_Q \).

**Lemma 4.5.** The element \( \theta' \) is invertible in the group algebra \( R_{+,Q} \), hence also invertible in the group algebra \( R_Q \).

*Proof.* Let \( \chi \) be an algebra homomorphism of \( R_{+,Q} \) into \( \mathbb{C} \). Then \( \chi \) induces a character \( \chi \) of \( C' \). If \( \chi \neq 1 \), then \( \chi(\theta') = \sum_{I_2} \neq 0 \). If \( \chi = 1 \), then \( \chi(\theta') = -1 \neq 0 \). Thus for any \( \chi \) we have \( \chi(\theta') \neq 0 \). This implies that \( \theta' \) is invertible in \( R_{+,Q} \). Q.E.D.

**Lemma 4.6.**

1. \( [R : R_{(p-1)l}] = (p-1)l \).
2. \( [I_{12l} \theta' + \mathbb{Z}2l \mu_+ : I_{12l} \theta'] = (p+1)/2 \).

*Proof.* (1) Obvious. (2) The left hand side is equal to \( [\mathbb{Z}2l \mu_+ : \mathbb{Z}2l \mu_+ \cap I_{12l} \theta'] \). Let \( \xi \theta' = 2ln \mu_+ \) with \( \xi \in I_{12l} \) and \( n \in \mathbb{Z} \). By Lemma 4.5, \( \theta' \) has an inverse \( \theta'^{-1} \) in \( R_{+,Q} \). Then \( \xi = 2ln \mu_+ \theta'^{-1} = 2ln \deg(\theta'^{-1}) \mu_+ = -2n \mu_+ \). Since \( \xi \in I_{12l} \), we see \( n \in (p+1)/2 \mathbb{Z} \). Put \( \xi = -(p+1) \mu_+ \). Then \( \xi \in I_{12l} \) and \( \xi \theta' = (p+1)/2 \cdot 2l \mu_+ \). Thus we have \( I_{12l} \theta' \cap \mathbb{Z}2l \mu_+ = (p+1)/2 \cdot \mathbb{Z}2l \mu_+ \). This proves (2). Q.E.D.

Let \( A, B \) be two lattices in \( R_Q \), and let \( C \) be a lattice contained in \( A \cap B \). Then \( [A : C]/[B : C] \) is independent of the choice of \( C \). We denote this number by \( [A : B] \). Then it satisfies the usual multiplicative property, namely \( [A : B] = [A : D][D : B] \). In particular, we have

\[ [R : I_{12l} \theta'] = [R : R \theta'][R \theta' : I_{12l} \theta']. \] (4.7)

**Lemma 4.7.**

1. \( [R : R \theta'] = 2^2([\prod_{I \neq 1} \frac{1}{2} \mathbb{B}_{2,x}]^2) \).
2. \( [R \theta' : I_{12l} \theta'] = [R : I_{12l}] = 12l p^2 \).

In the product of (1), \( \chi \) is taken over all non-trivial characters of \( (\mathbb{Z}/p\mathbb{Z})^\times/\{ \pm 1 \} \).

*Proof.* (1) \( [R : R \theta'] = [R : R p \theta']/[R \theta' : R p \theta'] \). Put \( R_+ = \mathbb{Z}[C'(\pm)], R_- = \sigma_{-1} R_+ \). Then \( R = R_+ \oplus R_- \). Since \( p \theta' \in R_+ \), we have \( R/R p \theta' \cong (R_+ / R_+ p \theta') \oplus (R_-/R_- p \theta') \cong (R_+ / R_+ p \theta')^2 \), and \( [R_+ : R_+ p \theta'] = \pm \det_{R_+ Q}(p \theta') \). Since \( \mathbb{C}[C' \pm] = R_+ (C) \) is a direct sum of one-dimensional subspaces corresponding to all characters \( \chi \) of \( C'(\pm) \), we have \( \det_{R_+ Q}(p \theta') = \prod_{I} \chi(p \theta') = p^{n/2} \prod_{I} \chi(\theta') \). Here \( n = |C(\pm)| \), and \( \chi(\theta') \) is the same as in the proof of Lemma 4.5. Since \( \theta' \) is invertible in \( R_Q \) (Lemma 4.5), we have \( [R \theta' : R p \theta'] = [R : R p] = p^n \). This proves (1).
(2) Since \( \theta' \) is invertible in \( R_Q \), we have \([R\theta':I_{12j}\theta']=[R:I_{12j}]\). Let
\[
\phi: R \to (\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/12\mathbb{Z})
\]
be the homomorphism defined by
\[
\phi((x,y,z)) = (\phi_1(x), \phi_2(x), \phi_3(x)) \mod p,
\]
where
\[
\phi_1(x) = \sum_{\alpha \in \mathbb{Z}} m(\alpha) x, \quad \phi_2(x) = \sum_{\beta \in \mathbb{Z}} m(\beta) y,
\]
\[
\phi_3(x) = \sum_{\gamma \in \mathbb{Z}} m(\gamma) z.
\]
Let \( \mathcal{C} \) be the element defined by
\[
m(\alpha) = \begin{cases} 1 & (\alpha = 2, \ldots, (p - 1)/2), \\ 0 & (\forall \beta). \end{cases}
\]
Let \( \mathcal{C}_1 = \mathcal{C}_1 \) and \( \mathcal{C}_2 = \mathcal{C}_2 \) be the elements of \( \mathbb{Z} \) defined by
\[
\mathcal{C}_1 = \mathcal{C}_1 \mathcal{C}_2, \quad \mathcal{C}_2 = \mathcal{C}_1 \mathcal{C}_2.
\]
Then \( \phi((1,0,0), \phi((0,1,0), \phi((0,0,1). \)
Hence \( \phi \) is surjective. Since \( \ker \phi = \mathbb{Z}_{12} \), (2) is proved. Q.E.D.

Now combining these lemmas with (4.5)-(4.7), we obtain the cuspidal class number of \( X(\sqrt{p}) \), which is equal to that of \( X_1(p) \).

**Theorem 4.1.** The cuspidal class number of the modular curve \( X_1(p) \) is given by
\[
h_1(p) = p^2 \left( \prod_{x \neq 1} \frac{1}{B_{2x}} \right)^2.
\]

A cusp on \( X_1(p) \) is said to be of the first type if it is lying above the cusp \( 0 \) on \( X_0(p) \). Let \( \mathcal{C}^0 \) be the subgroup of \( \mathcal{C} \) which is generated by the cusps of the first type. Then the order \( h_1(p) \) of \( \mathcal{C}(p) \) is already known (Klimek [4], see also [13]). Comparing it with Theorem 4.1, we have

**Corollary 1.** \( h_1(p) = (h_0(p))^2 \).

3. Let \( \mathcal{C}^\infty \) be the subgroup of \( \mathcal{C} \) which is generated by the cusps which are lying above the cusp \( \infty \) on \( X_0(p) \). Then \( \mathcal{C}^0 \cong \mathcal{C}^\infty \). Kubert and Lang ([11, Section 6]) raised the problem to consider the relationship between the two groups \( \mathcal{C} \) and \( \mathcal{C}^0 + \mathcal{C}^\infty \). Corollary 1 suggests the possibility that \( \mathcal{C} = \mathcal{C}^0 \oplus \mathcal{C}^\infty \). But this is not the case in general. We consider the intersection \( \mathcal{C}^0 \cap \mathcal{C}^\infty \).

Let \( R_+ \) and \( R_- \) be the same as in the proof of Lemma 4.7. Then
\( R = R_+ \oplus R_- \). For any \( \xi \in R \), let us denote by \( \xi_+ \) and \( \xi_- \) the elements of \( R_+ \) and \( R_- \), respectively, defined by \( \xi = \xi_+ + \xi_- \). Put \( R_{0,+} = R_0 \cap R_+ \), \( R_{0,-} = R_0 \cap R_- \), \( I_{0,+} = I_0 \cap R_+ \), \( I_{0,-} = I_0 \cap R_- \). Note that \( I_{0,+} \subset R_{0,+} \) and \( I_{0,-} \subset R_{0,-} \). Then, in our notation the groups \( \mathcal{C}^\infty \) and \( \mathcal{C}^0 \) corresponds to \( R_{0,+}/R_{0,+} \cap I_{12} \theta \) and \( R_{0,-}/R_{0,-} \cap I_{12} \theta \), respectively.

**Lemma 4.8.**

1. \( R_{0,+} \cap I_{12} \theta = I_{0,+} \theta. \)

2. \( R_{0,-} \cap I_{12} \theta = I_{0,-} \theta. \)

**Proof.** (2) follows from (1) by multiplying \( \sigma_{-1} \). (1) If \( \xi \in I_{0,+} \), then
\[
\xi \theta = \xi \theta_+ + \xi \theta_- = \xi \theta_+ + (\deg \xi) \theta_- = \xi \theta_+.
\]
This implies the inclusion \( \supseteq \).
Conversely, let $\xi \in I_{12}$ and $\xi \theta \in R_{0,+}$. Then $0 = (\xi \theta)_+ = \xi_+ \theta_- + \xi_- \theta_+ = \deg(\xi_+) \theta_- + \xi_- \theta_+$, hence

$$\xi_- \theta_+ = -\deg(\xi_+) \theta_. \quad (4.8)$$

Let $e_\chi$ be the idempotent in $R_{+,c}$ corresponding to a character $\chi$ of $C^\omega(\pm)$. Then $\xi_- \theta_+ e_\chi = -\deg(\xi_+) \theta_- e_\chi$. If $\chi \neq 1$, then $\theta_- e_\chi = 0$ and $\theta_+ e_\chi = \frac{1}{2} B_{2,2} e_\chi$. Since $B_{2,2} \neq 0$, we have $\xi_- e_\chi = 0$. This implies that $\xi_- \in C_{\mu_+}$, hence $\xi_- = n\mu_+$ with $n \in \mathbb{Z}$ because $\xi \in I_{12}$. Put $\xi' = \xi - n\mu$. Then $\xi' \in I_{12} \cap R_+$, and $\xi \theta = \xi' \theta$ (Lemma 4.1). Replacing $\xi$ by $\xi'$, we have $\deg \xi' = 0$ by (4.8), hence $\xi' \in I_{0,+}$. This proves the reverse inclusion.

Q.E.D.

The group $C^0 \cap C^\infty$ corresponds to the subgroup $G = (R_{0,+}/R_{0,+} \cap I_{12}) \cap (R_+ / R_+ \cap I_{12})$ of $R_+ I_{12}$. For an element $\alpha \in G$, put $\alpha = \eta_+ \equiv -\eta_- (\mod I_{12})$, where $\eta_+ \in R_{0,+}$ and $\eta_- \in R_{0,-}$. Then $\eta = \eta_+ + \eta_- \in I_{12}$, hence $\eta = \xi \theta$ with some $\xi \in I_{12}$. Put $I_{12}^+ = \{ \xi \in I_{12} \mid \deg \xi_+ = \deg \xi_- \}$.

**Lemma 4.9.** Let $\alpha \in G$ and $\xi \in I_{12}$ be as above.

1. $\xi \in I_{12}^+$.
2. The class of $\xi$ modulo $I_{0,+} + I_{0,-} + \mathbb{Z}\mu$ is uniquely determined by $\alpha$.
3. Let $\varphi(\alpha)$ be the class of $\xi$ in (2). Then $\varphi$ induces an isomorphism $G \cong I_{12}^+/(I_{0,+} + I_{0,-} + \mathbb{Z}\mu)$.

**Proof.**

1. $\eta_+ = (\xi \theta)_+ = \xi_+ \theta_- + (\deg \xi_-) \theta_+$. Since $\deg \eta_+ = 0$ and $\deg \theta_+ = -\deg(\theta_-)$, we have $0 = (\deg \xi_+ - \deg \xi_-) \deg \theta_+$. Hence $\deg \xi_+ = \deg \xi_-$. (2) Let $\eta'_+ \in R_{0,+}$ and $\eta'_- \in R_{0,-}$ be other elements satisfying $\alpha = \eta'_+ \equiv -\eta_- (\mod I_{12})$. Put $\eta' = \eta_+ + \eta' = \xi \theta$ with $\xi' \in I_{12}$. Since $\eta_+ - \eta'_+ \in R_{0,+} \cap I_{12}$, we have $\eta_+ - \eta'_+ = \xi_{0,+} \theta$ with $\xi_{0,+} \in I_{0,+}$ by Lemma 4.8. Similarly, $\eta_- - \eta'_- = \xi_{0,-} \theta$ with $\xi_{0,-} \in I_{0,-}$. Put $\xi_0 = \xi_{0,+} + \xi_{0,-}$. Then $\eta = \eta_+ + \xi_0 \theta$, hence $\eta = \xi \theta = (\xi' + \xi_0) \theta$. This implies $\xi - \xi' \in I_{0,+} + I_{0,-} + \mathbb{Z}\mu$ by Lemma 4.1. (3) If $\varphi(\alpha) = 0$, then $\xi \in I_{0,+} + I_{0,-} + \mathbb{Z}\mu$. Replacing $\xi$ by $\xi - n\mu$ with some integer $n$, we may assume $\xi \in I_{0,+}$ and $\xi \in I_{0,-}$. Then $\eta = \xi \theta = \xi_+ \theta_- + \xi_- \theta_+$, hence $\alpha = \eta_- = \xi_+ \theta_+ = \xi_- \theta_+ = 0 (\mod I_{12})$, which proves the injectivity of $\varphi$. To prove the surjectivity, take any $\xi' \in I_{12}^+$ and put $\eta' = \xi' \theta$. Then $\deg \eta' = (\deg \xi' - \deg \xi') \deg \theta_+ = 0$, and $\deg \eta' = 0$. Thus the element $\alpha' = \eta' \mod I_{12}$ belongs to $G$ and satisfies $\varphi(\alpha') = \xi' \mod (I_{0,+} + I_{0,-} + \mathbb{Z}\mu)$. Q.E.D.

Let us define a homomorphism $\phi: I_{12}^+/(I_{0,+} + I_{0,-} + \mathbb{Z}\mu) \to \mathbb{Z}/((p-1)/2)\mathbb{Z}$ by $\phi(\xi) = \deg \xi_+ \mod (p-1)/2$. Since $\deg \mu_+ = (p-1)/2$, this is well defined.
Lemma 4.10. Let \( \phi \) be as above.

(1) \( \phi \) is injective.

(2) Let \( \delta_1 = (1 + p, 12) \) and \( \delta_2 = ((p - 1)/2, 12/\delta_1) \). Then \( \text{Im} \phi = (12/\delta_1)\mathbb{Z}/((p - 1)/2)\mathbb{Z} \). Hence \( |\text{Im} \phi| = (p - 1)/(2\delta_2) \).

Proof. (1) If \( \phi(\xi) = 0 \), then \( \deg \xi^+ = n(p - 1)/2 \) with some integer \( n \). Put \( \xi' = \xi - nu \). Since \( \xi \in I^*_2 \), we have \( \deg \xi^+ = \deg \xi^+ = 0 \). Hence \( \xi' \in I_{0,+}^* + I_{0,-}^* \), so that \( \xi \in I_{0,+}^* + I_{0,-}^* + \mathbb{Z} \mu \). This proves (1). (2) If \( \xi \in I_{2,1}^* \), then \( (\deg \xi^+)(1 + p) \equiv 0 \pmod{12} \). Hence \( \deg \xi^+ \equiv 0 \pmod{12/\delta_1} \), so that \( \text{Im} \phi \subset (12/\delta_1)\mathbb{Z}/((p - 1)/2)\mathbb{Z} \). Put \( \xi = (12p/\delta_1)(\sigma_{+,1} + \sigma_{-1}) \). Then \( \xi \in I_{2,1}^* \) and \( \phi(\xi) = 12p/\delta_1 \pmod{(p - 1)/2} \). Since \( (p, (p - 1)/2) = 1 \), \( \text{Im} \phi \) is generated by \( 12/\delta_1 \). This proves (2).

By Lemmas 4.9 and 4.10 we have the following:

Theorem 4.2. The group \( \mathcal{C}^0 \cap \mathcal{C}^\infty \) is a cyclic group of order \( v \), where \( v = (p - 1)d/12 \) and \( d \) is the denominator of \( (p - 1)/12 \), namely, \( d = 1, 2, 3, 6 \) according as \( p \equiv 1, 7, 5, 11 \pmod{12} \).

Corollary 2. The factor group \( \mathcal{C}/(\mathcal{C}^0 + \mathcal{C}^\infty) \) is a cyclic group of order \( v \), and is generated by the class of \( P_\infty - P_0 \), where \( P_\infty \) (resp. \( P_0 \)) is the prime divisor corresponding to the cusp \( \infty \) (resp. \( 0 \)) on \( X_1(p) \).

Proof. By Theorem 4.1, Corollary 1, and Theorem 4.2, the order of \( \mathcal{C}/(\mathcal{C}^0 + \mathcal{C}^\infty) \) is \( v \). The rest follows from the equation \( R_0 = R_{0,+} + R_{0,-} + \mathbb{Z}(\sigma_{+,1} - \sigma_{-,1}) \), which we prove now. For any \( \xi = \sum m(\alpha)\alpha \in R_0 \), put \( \xi_1 = \sum_a(m(\alpha_+)\alpha - \sigma_{+,a}) \), \( \xi_2 = \sum_a(m(\sigma_{+,a}) + m(\sigma_{-,a}))\sigma_{-,a} \). Then \( \xi = \xi_1 + \xi_2 \) and \( \xi_2 \in R_{0,-} \). Since \( \sigma_{+,a} - \sigma_{-,a} = (\sigma_{+,a} - \sigma_{+,1}) + (\sigma_{-,1} - \sigma_{-,a}) + (\sigma_{+,1} - \sigma_{-,1}) \), the equation follows.

Corollary 3. The factor group \( \mathcal{C}/(\mathcal{C}^0 + \mathcal{C}^\infty) \) is isomorphic to the cuspidal divisor class group of \( X_0(p) \).

Proof. By Corollary 2 and Ogg [15, Theorem on p. 228]. Q.E.D.

By Theorem 4.2, \( \mathcal{C}^0 \cap \mathcal{C}^\infty = 0 \) if and only if \( p = 5, 7, 13 \). In these cases \( \mathcal{C} = \mathcal{C}^0 \oplus \mathcal{C}^\infty \). Since \( h_1(5) = h_1(7) = 1 \), the only non-trivial case is \( p = 13 \). We have \( h_1(13) = 19^2 \), hence \( \mathcal{C}^0 \cong \mathcal{C}^\infty \cong \mathbb{Z}/19\mathbb{Z} \) and \( \mathcal{C} \cong (\mathbb{Z}/19\mathbb{Z})^2 \). (The fact \( \mathcal{C}^0 \cong \mathbb{Z}/19\mathbb{Z} \) is also observed in Ogg [15] by using Eisenstein series.)

When \( p = 11 \), we have \( h_1(11) = 5^2 \) and \( v = 5 \). Hence \( \mathcal{C}^0 = \mathcal{C}^\infty \cong \mathbb{Z}/5\mathbb{Z} \). We can verify that the class of \( P_\infty - P_0 \) is of order 25. Hence \( \mathcal{C} \) is a cyclic group of order 25 generated by the class of \( P_\infty - P_0 \).
REFERENCES


17. T. Takagi, Classification of normal congruence subgroups of $G(\sqrt{q})$ which is a conjugate of the normalizer of $I(q)$ ($q$: a prime), *J. College Arts Sci., Showa Univ.* 18 (1987), 63-99.


