J. Math. Soc. Japan
Vol. 47, No. 4, 1995

The cuspidal class number formula for the modular curves $X_1(3^m)$

Dedicated to Professor Hideo Shimizu on his 60th birthday

By Toshikazu TAKAGI

(Received Oct. 15, 1992)
(Revised Dec. 20, 1993)

Introduction.

In the previous papers [7, 8], we determined the cuspidal class numbers of the modular curves $X_1(p^m)$ for prime numbers $p\neq 2, 3$. The purpose of this paper is to determine the cuspidal class number of the modular curve $X_1(3^m)$. Let h' be the number obtained by the substitution of 3 for p in the cuspidal class number formula for the case $p\neq 2, 3$ ([8, Theorem 7.1, Theorem 8.1]). Let $h_1(3^m)$ be the cuspidal class number of the curve $X_1(3^m)$. Then our main results (Theorem 3.1, Theorem 4.1) show $h_1(3^m)=h'/3$ if $m\geqq 2$. (If $m=1$, then $h_1(3)=h'/3^2=1$.) As is well known, the cuspidal divisor class groups of the modular curves are finite (Manin [5], Drinfeld [1]). As far as the author knows, the (full) cuspidal class numbers are determined in the following cases of modular curves. Let p be a prime number $\neq 2, 3$. Ogg [6] determined the cuspidal class number of the modular curve $X_0(p)$. Kubert-Lang [3, 4] determined the cuspidal class number of the modular curve $X(p^n)$. Takagi [7, 8] determined the cuspidal class number of the modular curve $X_1(p^m)$. (Klimek [2], Kubert-Lang [3, 4] and Yu [10] determined the order of a certain subgroup of the cuspidal divisor class group of the modular curve $X_1(N)$.)

The contents of this paper are the following. In Section 1, we summarize some results and definitions of [8, Section 1-5]. In [8], we assumed $p\neq 2$, and the assumption $p\neq 3$ was used only in Section 6-8. So the results of this section hold for all $p\neq 2$. Here we define modified Siegel functions, construct modular units on the curve $X_1(p^m)$, embed the cuspidal divisor group into a ring R, and define a special element θ of the algebra $R\otimes\boldsymbol{Q}$. In Section 2, we determine the group of modular units on the curve $X_1(3^m)$ precisely (Theorem 2.2). In Section 3, we determine the principal divisor group as a subgroup of the ring R, which is expressed as $I_4\theta$ where I_4 is a subgroup of R. In Sections 3 and 4, we calculate the cuspidal class number of the curves $X_1(3^{2n})$ and $X_1(3^{2n+1})$, respectively (Theorem 3.1, Theorem 4.1). In the calculation, we use

the algebraic structure of $R\otimes C$ that it has a basis consisting of orthogonal idempotents. Essentially, the cuspidal class number is the product of eigenvalues of the element θ.

In this 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.

1. Summary of some results.

1. We recall some results and definitions from [8, Section 1-5]. Let p be a prime number $\neq 2$. After Section 2 we put $p=3$. Let $N=p^m$ be a fixed prime power. We consider the conjugate Γ of the group $\Gamma_1(N)$ defined by $\Gamma=\begin{pmatrix}1 & 0\\ 0 & \sqrt{N}\end{pmatrix}^{-1}\Gamma_1(N)\begin{pmatrix}1 & 0\\ 0 & \sqrt{N}\end{pmatrix}$. Let X_Γ be the complete non-singular curve associated with the quotient space $\Gamma\backslash\mathfrak{H}$ of the upper half plane $\mathfrak{H}$ by Γ. Then the curve X_Γ is isomorphic to the curve $X_1(N)$. By a technical reason it is convenient to consider the curve X_Γ instead of $X_1(N)$.

We divide the case into the following two:

(I) $m=2n$ with $n\geqq 1$.

(II) $m=2n+1$ with $n\geqq 0$.

In case (I) (resp. (II)) the group Γ is a subgroup of $SL_2(\boldsymbol{Z})$ (resp. $G(\sqrt{p})$). (For the definition of $G(\sqrt{p})$, see [7].) Let $M=1$ or p according as m satisfies the condition (I) or (II), respectively. Then Γ is a subgroup of $G(\sqrt{M})$.

Let $\mathfrak{F}_\Gamma$ be the field of all automorphic functions with respect to Γ whose Fourier coefficients belong to the cyclotomic field $k_N=\boldsymbol{Q}(e^{2\pi i/N})$. The field k_N is algebraically closed in $\mathfrak{F}_\Gamma$. The field $\boldsymbol{C}\mathfrak{F}_\Gamma$ can be identified with the function field on the curve X_Γ.

Let $\mathcal{O}=\boldsymbol{Z}+\sqrt{M}\boldsymbol{Z}$. Put $I=p^{2n}\sqrt{M}\mathcal{O}$. Then I is an ideal of $\mathcal{O}$. Let $\Gamma(I)$ be the principal congruence subgroup of $G(\sqrt{M})$ (see [7]). Let X_I be the complete non-singular curve associated with the quotient space $\Gamma(I)\backslash\mathfrak{H}$. Let $\mathfrak{F}_I$ be the field of all automorphic functions with respect to $\Gamma(I)$ whose Fourier coefficients belong to the cyclotomic field k_N. Then the field k_N is algebraically closed in $\mathfrak{F}_I$. The field $\boldsymbol{C}\mathfrak{F}_I$ can be identified with the function field on the curve X_I. Since $\Gamma\supset\Gamma(I)$, we have $\mathfrak{F}_\Gamma\subset\mathfrak{F}_I$. The extension $\mathfrak{F}_I/\mathfrak{F}_\Gamma$ is an abelian extension whose Galois group is isomorphic to the group $(\boldsymbol{Z}/p^n\boldsymbol{Z})^2$.

Let $\mathfrak{F}_1$ be field of all automorphic functions with respect to $G(\sqrt{M})$ whose Fourier coefficients belong to the field $\boldsymbol{Q}$. Then the extension $\mathfrak{F}_I/\mathfrak{F}_1$ is normal, whose Galois group is isomorphic to the group $\mathcal{G}_I(\pm)$. Here $\mathcal{G}_I(\pm)=\mathcal{G}_I/\{\pm 1\}$, and $\mathcal{G}_I$ is the group of all elements $\alpha=\begin{pmatrix}a\sqrt{r} & b\sqrt{r^*}\\ c\sqrt{r^*} & d\sqrt{r}\end{pmatrix}$ (mod I) contained in $GL_2(\mathcal{O}/I)$ with $a, b, c, d\in\boldsymbol{Z}$, $r\mid M$, and $r^*=M/r$. The number r ($=1$ or M) is

called the *type* of α and denoted by $t(\alpha)$. Let $C(\pm)=C/\{\pm 1\}$. Here C is the abelian subgroup of $\mathcal{G}_I$ (called a Cartan subgroup) consisting of all elements $\alpha=\begin{pmatrix} a\sqrt{r} & \kappa b\sqrt{r^*} \\ b\sqrt{r^*} & a\sqrt{r} \end{pmatrix} \pmod{I}$ with $a, b\in \boldsymbol{Z}$. The number κ is chosen as follows, and fixed throughout the paper. In case (I), let κ be an integer prime to p $(\neq 2)$ satisfying $(\kappa/p)=-1$, where (κ/p) denotes the Legendre symbol. In case (II), let $\kappa=1$. We write $a=a(\alpha)$ and $b=b(\alpha)$.

2. Let P_∞ be the prime divisor of $\mathfrak{F}_I$ defined by the q-expansion. Let $\sigma: \mathcal{G}_I(\pm)\cong \mathrm{Gal}(\mathfrak{F}_I/\mathfrak{F}_1)$ be the isomorphism. Then every conjugate of P_∞ over $\mathfrak{F}_1$ can be written as $P_\infty^{\sigma(\alpha)}$ with a unique element α of $C(\pm)$. The conjugates of P_∞ can be identified with the cusps on the curve X_I. So the cusps on the curve X_I can be parametrized by the elements of the abelian group $C(\pm)$. We call the conjugates of the prime P_∞ the cuspidal primes of $\mathfrak{F}_I$.

For a prime P of $\mathfrak{F}_I$ we denote by $[P]$ the prime divisor of the field $\mathfrak{F}_\Gamma$ induced by P. If P is a cuspidal prime of $\mathfrak{F}_I$, then we call $[P]$ a cuspidal prime of the field $\mathfrak{F}_\Gamma$. The cuspidal primes of $\mathfrak{F}_\Gamma$ can be identified with the cusps on the curve X_Γ. Let $\mathcal{D}$ be the free abelian group generated by the cuspidal primes of $\mathfrak{F}_\Gamma$, and let $\mathcal{D}_0$ be the subgroup of $\mathcal{D}$ of divisors of degree 0. Let $\mathcal{F}$ (resp. $\mathcal{F}_C$) be the group of non-zero functions in $\mathfrak{F}_\Gamma$ (resp. $\boldsymbol{C}\mathfrak{F}_\Gamma$) whose divisors have support within the cuspidal primes. (The elements of $\mathcal{F}_C$ are called modular units.) Then $\mathcal{F}_C=\boldsymbol{C}^\times\mathcal{F}$, and we can identify $\mathrm{div}(\mathcal{F})$ with $\mathrm{div}(\mathcal{F}_C)$. We call the factor group

$$\mathcal{C}=\mathcal{D}_0/\mathrm{div}(\mathcal{F}) \tag{1.1}$$

the *cuspidal divisor class group* on X_Γ and the order of $\mathcal{C}$ the *cuspidal class number* of X_Γ (namely, of $X_1(p^m)$).

The cuspidal primes of $\mathfrak{F}_\Gamma$ can be written as $[P_\infty^{\sigma(\alpha)}]$ with $\alpha\in C$. For two elements α and β of C, let $\alpha\sim\beta$ be the equivalence relation defined by $[P_\infty^{\sigma(\alpha)}]=[P_\infty^{\sigma(\beta)}]$. Then the cuspidal primes of $\mathfrak{F}_\Gamma$ are parametrized by the equivalence classes of C. This equivalence relation can be described by the use of the subgroups C_k and D_k of C which are defined as follows. Let k be an integer with $0\leqq k\leqq n$. Let $C_k^{(1)}$ (resp. $C_k^{(-1)}$) be the set consisting of all elements α of C satisfying $b(\alpha)t(\alpha)^*\equiv 0 \pmod{p^kM}$ (resp. $a(\alpha)t(\alpha)\equiv 0 \pmod{p^kM}$). Put $C_k=C_k^{(1)}\cup C_k^{(-1)}$. Let D_k be the set consisting of all elements α of $C_0^{(1)}$ satisfying $a(\alpha)\equiv 1 \pmod{p^{n+k}M}$ and $b(\alpha)\equiv 0 \pmod{p^n}$. Then the sets C_k, $C_k^{(1)}$, and D_k are subgroups of C. They satisfy $C=C_0\supset C_1\supset\cdots\supset C_n\supset\pm D_0\supset\pm D_1\supset\cdots\supset\pm D_n$. For $1\leqq k\leqq n-1$, $[C_k: C_{k+1}]=p$. For $0\leqq k\leqq n-1$, $[D_k: D_{k+1}]=p$. For $1\leqq k\leqq n$, $[C_k: C_k^{(1)}]=2$, and $C_k^{(-1)}=C_k^{(1)}\begin{pmatrix} 0 & \kappa \\ 1 & 0 \end{pmatrix}$. When $M=1$, we have $C_0=C_0^{(1)}=C_0^{(-1)}$. When $M=p$, we have $[C_0: C_1]=p$, $[C_0: C_0^{(1)}]=2$, and $C_0^{(-1)}=C_0^{(1)}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. In

both cases of M, $C_0^{(1)}$ is the set of all elements of C of type 1. Now, if $\alpha\in C_k-C_{k+1}$, we call k the *order* of α, and denote it by $\mathrm{ord}(\alpha)$. (When $k=n$, we put $C_{n+1}=\emptyset$.) Then the equivalence relation can be described as follows. For two elements α and β of C, α is equivalent to β if and only if they have the same order $(=k)$ and also they belong to the same coset of $\pm D_k$.

Put $G_k=C_k/\pm D_n$, $G_k^{(\varepsilon)}=C_k^{(\varepsilon)}/\pm D_n$ $(\varepsilon=\pm 1)$, and $H_k=\pm D_k/\pm D_n$. Then we have a filtration $G=G_0\supset G_1\supset\cdots\supset G_n\supset H_0\supset\cdots\supset H_n=1$. This filtration defines a subring R of the group ring $\boldsymbol{Z}[G]$ of G by

$$R=\sum_{k=0}^{n}\boldsymbol{Z}[(G_k-G_{k+1})/H_k], \tag{1.2}$$

where $G_{n+1}=\emptyset$, and a coset xH_k denotes the element $\sum_{y\in H_k}xy$. The rank of R is equal to that of the divisor group $\mathcal{D}$. Let $[P_\infty^{\sigma(\alpha)}]$ be a cuspidal prime, where α is an element of C of order k. Then the mapping $[P_\infty^{\sigma(\alpha)}]\mapsto p^k\alpha H_k$ defines an embedding

$$\varphi:\mathcal{D}\longrightarrow R. \tag{1.3}$$

Let D be any element of $\mathcal{D}$. Then the embedding φ satisfies the equation $\deg(\varphi(D))=p^n\deg(D)$. Let R_0 be the subgroup of R consisting of all elements of degree 0. Then $\varphi(\mathcal{D}_0)\subset R_0$. Let R^c be the subgroup of R consisting of all elements $\sum f(x)x$ satisfying $f(x)\equiv 0 \pmod{p^{\mathrm{ord}(x)}}$, where the *order* of x $(=\mathrm{ord}(x))$ is the number k such that $x\in G_k-G_{k+1}$. Put $R_0^c=R^c\cap R_0$. Then $\varphi(\mathcal{D})=R^c$ and $\varphi(\mathcal{D}_0)=R_0^c$.

3. We recall some properties of Siegel functions. For any element $a=(a_1, a_2)$ of $\boldsymbol{Q}^2-\boldsymbol{Z}^2$, the Siegel function $g_a(\tau)$ $(\tau\in\mathfrak{H})$ is defined in [4]. It has the q-product

$$g_a(\tau)=-q_\tau^{(1/2)B_2(a_1)}e^{2\pi i a_2(a_1-1)/2}(1-q_z)\prod_{k=1}^{\infty}(1-q_\tau^k q_z)(1-q_\tau^k/q_z), \tag{1.4}$$

where $q_\tau=e^{2\pi i\tau}$, $q_z=e^{2\pi iz}$ $(z=a_1\tau+a_2)$, and $B_2(X)=X^2-X+(1/6)$ is the second Bernoulli polynomial. If $b=(b_1, b_2)\in\boldsymbol{Z}^2$, then

$$g_{a+b}(\tau)=\varepsilon(a, b)g_a(\tau), \tag{1.5}$$

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

$$\varepsilon(a, b)=\exp\left[\frac{2\pi i}{2}(b_1b_2+b_1+b_2+a_1b_2-a_2b_1)\right]. \tag{1.6}$$

If $\alpha\in SL_2(\boldsymbol{Z})$, then

$$g_a(\alpha(\tau))=\psi(\alpha)g_{a\alpha}(\tau), \tag{1.7}$$

where ψ is the character of $SL_2(\boldsymbol{Z})$ appearing in the transformation law of the

square of the Dedekind η-function. Explicitly, ψ is given as follows (Weber [9, pp. 125-127]). Let $\alpha=\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be any element of $SL_2(\boldsymbol{Z})$. Then

$$\psi(\alpha)=\begin{cases} (-1)^{(d-1)/2}\exp\left[\dfrac{2\pi i}{12}\{(b-c)d+ac(1-d^2)\}\right] & \text{if } d \text{ is odd,} \\ -i(-1)^{(c-1)/2}\exp\left[\dfrac{2\pi i}{12}\{(a+d)c+bd(1-c^2)\}\right] & \text{if } c \text{ is odd.} \end{cases} \tag{1.8}$$

Note that $\psi(-1_2)=-1$, and that $\ker(\psi)$ is a congruence subgroup of level 12 and of index 12. (It can be shown that the kernel is the commutator subgroup.)

In order to construct modular units in $\mathfrak{F}_\Gamma$, we define a set A'_k in the following. Let k be an integer with $0\leqq k\leqq n$. Let $\varepsilon=\pm 1$, and put $h=k\varepsilon$. Put $A'_k=A'^{(1)}_k\cup A'^{(-1)}_k$, where $A'^{(\varepsilon)}_k$ is a set defined as follows. First, suppose $M=1$. If $k=0$, then put $A'^{(1)}_0=A'^{(-1)}_0=(1/p^n)\boldsymbol{Z}^2-\boldsymbol{Z}^2$, and define the *sign* of $u\in A'_0$ to be 1. If $k\geqq 1$, then let $A'^{(\varepsilon)}_k$ be the set of all pairs $u=(a, \varepsilon)$ with $a\in(1/p^{n+h})\boldsymbol{Z}\times(1/p^{n-h})\boldsymbol{Z}-\boldsymbol{Z}^2$. We call ε the *sign* of u. When the sign is specified, we identify u with its row vector part a. Formally, we define the *type* of $u\in A'_k$ $(0\leqq k\leqq n)$ to be 1, and denote it by $t(u)$. Next, suppose $M=p$. Put $A'^{(\varepsilon)}_k=(1/p^{n+h}r)\boldsymbol{Z}\sqrt{r}\times(1/p^{n-h}r^*)\boldsymbol{Z}\sqrt{r^*}-\boldsymbol{Z}\sqrt{r}\times\boldsymbol{Z}\sqrt{r^*}$, where $r=p$ or 1 according as $\varepsilon=1$ or -1, respectively. If $u\in A'^{(\varepsilon)}_k$, we call ε the *sign* of u, and r the *type* of u. We denote the type of u by $t(u)$.

Let $u=(a_1\sqrt{r}, a_2\sqrt{r^*})$ be an element of A'_k of sign ε and type r. Put $h=k\varepsilon$ and $u^\circ=(a_1, a_2)$ $(\in\boldsymbol{Q}^2-\boldsymbol{Z}^2)$. We define the function $g_{k,u}(\tau)$ on the upper half plane $\mathfrak{H}$ by

$$g_{k,u}(\tau)=g_{u^\circ}(\sqrt{r/r^*}p^h\tau). \tag{1.9}$$

These functions $g_{k,u}$ will generate the unit group $\mathfrak{F}$.

We state the fundamental properties of $g_{k,u}$ in the following. For $r=1$ or M, put $Z^{(r)}=\boldsymbol{Z}\sqrt{r}\times\boldsymbol{Z}\sqrt{r^*}$. For $v=(b_1\sqrt{r}, b_2\sqrt{r^*})\in Z^{(r)}$, let $v^\circ=(b_1, b_2)$ $(\in\boldsymbol{Z}^2)$. For $u\in A'_k$ with $t(u)=r$ and $v\in Z^{(r)}$, put $\varepsilon(u, v)=\varepsilon(u^\circ, v^\circ)$. Let $\alpha=\begin{pmatrix} a\sqrt{s} & b\sqrt{s^*} \\ c\sqrt{s^*} & d\sqrt{s} \end{pmatrix}$ be any element of $G(\sqrt{M})$, where $a, b, c, d\in\boldsymbol{Z}$, $s=1$ or M. Let r be as above. Put $\alpha^{(r)}=\begin{pmatrix} a(r, s) & b(r, s^*) \\ c(r^*, s^*) & d(r^*, s) \end{pmatrix}$. Then $\alpha^{(r)}$ is an element of $SL_2(\boldsymbol{Z})$. Let $E^{(1)}_k$ (resp. $E^{(-1)}_k$) $(0\leqq k\leqq n)$ be the subset of $G(\sqrt{M})$ consisting of all elements α satisfying $bs^*\equiv cs^*\equiv 0 \pmod{p^kM}$ (resp. $as\equiv ds\equiv 0 \pmod{p^kM}$). Put $E_k=E^{(1)}_k\cup E^{(-1)}_k$. Then E_k and $E^{(1)}_k$ are subgroups of $G(\sqrt{M})$. The group E_k acts on the set A'_k as follows. Let α be an element of $E^{(\delta)}_k$ $(\delta=\pm 1)$ expressed as above. Let

$$u=\left(\frac{x}{p^{n+h}r}\sqrt{r},\ \frac{y}{p^{n-h}r^*}\sqrt{r^*}\right) \tag{1.10}$$

be an element of $A_k'^{(\varepsilon)}$ of type r ($h=k\varepsilon$), where $x, y\in\boldsymbol{Z}$. We denote by $u\circ\alpha$ the element of $A_k'^{(\delta\varepsilon)}$ given by

$$u\circ\alpha=\begin{cases}\left(\dfrac{ax+p^hcry}{p^{n+h}r}\sqrt{r},\ \dfrac{p^{-h}br^*x+dy}{p^{n-h}r^*}\sqrt{r^*}\right) & \text{if } \delta=1,\\ \left(\dfrac{p^{-h}ar^*x+cy}{p^{n-h}r^*}\sqrt{r^*},\ \dfrac{bx+p^hdry}{p^{n+h}r}\sqrt{r}\right) & \text{if } \delta=-1.\end{cases} \tag{1.11}$$

Then the mapping $u\mapsto u\circ\alpha$ is a group operation. Let $A=\begin{pmatrix}1 & 0\\ 0 & p^h\end{pmatrix}$, and put $\alpha_{(h)}=A^{-1}\alpha A$ or $p^hA^{-1}\alpha A^{-1}$ according as $\delta=1$ or -1. Then $\alpha_{(h)}\in G(\sqrt{M})$, and $u\circ\alpha=u\alpha_{(h)}$. (In [8], $\alpha_{(h)}$ was written as $\alpha^{(h)}$. Since we have already defined the notation $\alpha^{(r)}$, this expression is misleading.) The fundamental properties of the function $g_{k,u}$ are described in the following proposition ([8, Proposition 3.1]).

PROPOSITION 1.1. *Let u be an element of A_k' of sign ε and type r. Put $h=k\varepsilon$.*

(1) *Let $v\in Z^{(r)}$. Then $g_{k,u+v}(\tau)=\varepsilon(u, v)g_{k,u}(\tau)$.*

(2) *Let $\alpha\in E_k$. Then $g_{k,u}(\alpha(\tau))=\psi_u(\alpha)g_{k,u\circ\alpha}(\tau)$, where $\psi_u(\alpha)=\psi((\alpha_{(h)})^{(r)})$.*

(3) *Let $\alpha\in\Gamma$ ($\subset E_k^{(1)}$). Then $g_{k,u}(\alpha(\tau))=\varepsilon_u(\alpha)\psi_u(\alpha)g_{k,u}(\tau)$, where $\varepsilon_u(\alpha)=\varepsilon(u, v)$ with $v=u\circ\alpha-u$ ($\in Z^{(r)}$).*

This proposition implies that the function $g_{k,u}^{12N}$ belongs to the group $\mathfrak{F}$ of the modular units in $\mathfrak{F}_\Gamma$. The function $g_{k,u}^{12N}$ depends only on the residue class of u modulo $Z^{(r)}$, and is invariant under the exchange $u\to-u$.

Put $\mathcal{A}_k'^{(\varepsilon)}=(A_k'^{(\varepsilon)}/Z^{(r)})/\{\pm1\}$ and $\mathcal{A}_k'=\mathcal{A}_k'^{(1)}\cup\mathcal{A}_k'^{(-1)}$. Then for an element u of $\mathcal{A}_k'$, the notation $g_{k,u}^{12N}$ is well defined. For elements of $\mathcal{A}_k'$, we again use the terminology sign and type. Let $\mathcal{G}_k^{(1)}$ (resp. $\mathcal{G}_k^{(-1)}$) ($0\leqq k\leqq n$) be the subset of $\mathcal{G}_I$ consisting of all elements $\begin{pmatrix}a\sqrt{s} & b\sqrt{s^*}\\ c\sqrt{s^*} & d\sqrt{s}\end{pmatrix}$ (mod I) with $bs^*\equiv cs^*\equiv0$ (mod p^kM) (resp. $as\equiv ds\equiv0$ (mod p^kM)). Put $\mathcal{G}_k=\mathcal{G}_k^{(1)}\cup\mathcal{G}_k^{(-1)}$. Then $\mathcal{G}_k$ and $\mathcal{G}_k^{(1)}$ are subgroups of $\mathcal{G}_I$. The group $\mathcal{G}_k$ acts on the set $\mathcal{A}_k'$ in a manner similar to the case of E_k. Namely, for $\alpha\in\mathcal{G}_k^{(\delta)}$, and for $u\in\mathcal{A}_k'$ of sign ε and type r, we denote by $u\circ\alpha$ the element of $\mathcal{A}_k'$ of sign $\delta\varepsilon$ given by (1.11). In particular, the group C_k acts on $\mathcal{A}_k'$, and the group $\pm D_k$ acts trivially. Hence the group G_k/H_k acts on $\mathcal{A}_k'$. Let $u\in\mathcal{A}_k'$ and $\alpha\in\mathcal{G}_k$. Then

$$(g_{k,u}^{12N})^{\sigma(\alpha)}=g_{k,u\circ\alpha}^{12N}. \tag{1.12}$$

4. We shall see that any element of $\mathfrak{F}$ can be expressed as a product of

the functions $g_{k,u}$ modulo constants. In fact, the set A'_k is superfluous. We define a subset $A_k^{(\varepsilon)}$ of $A_k'^{(\varepsilon)}$ as follows. Let u be an element of $A_k'^{(\varepsilon)}$ expressed as (1.10). Then $A_k^{(\varepsilon)}$ is the subset of $A_k'^{(\varepsilon)}$ consisting of all u with the following property. When $k\neq n$, $(x, p)=(y, p)=1$. When $k=n$, $(x, p)=1$ or $(y, p)=1$ according as $\varepsilon=1$ or -1. Put $A_k=A_k^{(1)}\cup A_k^{(-1)}$. Let $\mathcal{A}_k^{(\varepsilon)}$ be the subset of $\mathcal{A}_k'^{(\varepsilon)}$ corresponding to $A_k^{(\varepsilon)}$. Put $\mathcal{A}_k=\mathcal{A}_k^{(1)}\cup\mathcal{A}_k^{(-1)}$. We call elements of A_k or $\mathcal{A}_k$ *primitive*. Put

$$w_k=\left(\frac{1}{p^{n+k}M}\sqrt{M}, 0\right), \tag{1.13}$$

which is an element of A'_k of sign 1 and of type M. If $k=n$, w_n is primitive. Then the set $(G_k-G_{k+1})/H_k$ corresponds to the set $\mathcal{A}_k$ bijectively by the mapping $\alpha\mapsto w_k\circ\alpha$. Hence $|\bigcup_{k=0}^{n}\mathcal{A}_k|$ is equal to the number of the cusps of the curve X_Γ. We define a subset $\mathcal{R}_k^{(\varepsilon)}$ of $A_k^{(\varepsilon)}$ to be the set of all elements $u\in A_k^{(\varepsilon)}$ which satisfy one of the conditions (i) or (ii):

(i) $1\leqq x\leqq(p^{n+h}r-1)/2$, $0\leqq y\leqq p^{n-h}r^*-1$,

(ii) $x=0$, $1\leqq y\leqq(p^{2n}r^*-1)/2$.

(Case (ii) occurs only when $k=n$ and $\varepsilon=-1$.) Put $\mathcal{R}_k=\mathcal{R}_k^{(1)}\cup\mathcal{R}_k^{(-1)}$. The set $\mathcal{R}_k$ (resp. $\mathcal{R}_k^{(\varepsilon)}$) is a complete set of representatives of $\mathcal{A}_k$ (resp. $\mathcal{A}_k^{(\varepsilon)}$). In [8, Section 6], we assumed $p\neq2, 3$. But from the beginning of [8, Section 6.2] to the end of the proof of [8, Theorem 6.2], the assumption $p\neq3$ is not used. So that [8, Theorem 6.2] holds including the case $p=3$, which is the following.

THEOREM 1.1. *Any element g of the unit group $\mathcal{F}$ can be expressed as $g=c\prod_{0\leq k\leq n}\prod_{u\in\mathcal{R}_k}g_{k,u}^{m(k;u)}$, where $c\in k_N^\times$ and $m(k;u)$ are integers.*

By [8, (4.3)], the product $\prod_{0\leq k\leq n}\prod_{u\in\mathcal{R}_k}g_{k,u}$ is a constant. By [8, Theorem 4.1], this is the only relation among the functions $g_{k,u}$ with $u\in\mathcal{R}_k$.

5. Let φ be the embedding (1.3). Put $R_Q=R\otimes\boldsymbol{Q}$ and $R_C=R\otimes\boldsymbol{C}$. Let θ be the element of R_Q defined by

$$\theta=\frac{1}{12N}\varphi(\mathrm{div}\,(g_{n,w_n}^{12N})). \tag{1.14}$$

(This element plays an analogous role to the Stickelberger element in the theory of cyclotomic fields.) The explicit expression of θ can be given by [8, Proposition 3.2]. Let u be an element of $\mathcal{A}'_k$ expressed as $u=w_k\circ\alpha$ with $\alpha\in G_k$. Put $G(u)=\{\beta\in G_k\,|\,u=w_k\circ\beta\}$. Then $G(n)=\alpha H_k$, and we have ([8, (4.2)])

$$\varphi(\mathrm{div}\,(g_{k,u}^{12N}))=12N\Big(\sum_{\beta\in G(u)}\beta\Big)\theta\,. \tag{1.15}$$

(In the proof of (1.15), [8, Proposition 3.3] was used. In order to prove the proposition, the author used direct calculations of divisors. But it follows im-

mediately from (1.12) without any calculations of divisors.) In particular, u is primitive if and only if the order of α is k. If the element u runs through the set of all primitive elements, then the elements $\sum_{\beta\in G(u)}\beta$ constitute a basis of R over $\boldsymbol{Z}$. For each $0\leqq k\leqq n$, let $\mathfrak{X}_k$ be the set of characters χ of the group G_k/H_k which satisfy $\chi|H_{k-1}\neq 1$ when $k\geqq 1$. Put $\mathfrak{X}=\bigcup_{k=0}^{n}\mathfrak{X}_k$. If $\chi\in\mathfrak{X}_k$, we say that the *order* of χ is k, and denote it by $\mathrm{ord}(\chi)$. For every $\chi\in\mathfrak{X}$ $(\mathrm{ord}(\chi)=k)$, put

$$e_\chi=\frac{1}{|G_k|}\sum_{x\in G_k}\chi(x)x^{-1}. \tag{1.16}$$

Then the set of all elements e_χ is a basis of R_C over $\boldsymbol{C}$, and also they satisfy the orthogonality relation ([8, Proposition 1.2]): for $\chi_i\in\mathfrak{X}$ $(i=1, 2)$, $e_{\chi_1}\cdot e_{\chi_2}=e_{\chi_1}$ if $\chi_1=\chi_2$, or $=0$ otherwise. Let $B_{2,k,\chi}$ be the Bernoulli Cartan number associated with χ of order k. For the definition of $B_{2,k,\chi}$, see [8, (4.1)]. Then the element e_χ is an eigenvector of θ:

$$\theta e_\chi=\left(\frac{1}{2}p^n\overline{B_{2,k,\chi}}\right)e_\chi, \tag{1.17}$$

where the overline indicates the complex conjugate. If $\chi=1$ is the trivial character of G/H_0 $(\mathrm{ord}(1)=0)$, then $B_{2,0,1}=0$. If $\chi\neq 1$, then $B_{2,k,\chi}\neq 0$ ([8, Proposition 5.2-5.5]).

2. Determination of the unit group on $X_1(3^m)$.

1. From now on until to the end of this paper, we assume $p=3$. In this section, we determine the unit group $\mathcal{F}$ on the curve X_Γ which is isomorphic to the curve $X_1(3^m)$. This section is similar to [8, Section 6].

By Theorem 1.1, any element of $\mathcal{F}$ can be written as a product of the Siegel functions. Here we study conditions under which a product of Siegel functions $g_{k,u}$ belongs to $\mathcal{F}$. For each $0\leqq k\leqq n$, let $m(k;\ ):A'_k\to\boldsymbol{Z}$ be a mapping such that $m(k;u)=0$ except for a finite number of u. Put

$$g=\prod_{0\leqq k\leqq n}\prod_{u\in A'_k}g_{k,u}^{m(k;u)}. \tag{2.1}$$

Since the Fourier coefficients of $g_{k,u}$ belong to the field k_N, the condition $g\in\mathcal{F}$ is equivalent to saying that g is a modular function with respect to Γ. By (3) of Proposition 1.1, this condition is equivalent to the following:

$$\prod_{0\leqq k\leqq n}\prod_{u\in A'_k}\{\varepsilon_u(\alpha)\psi_u(\alpha)\}^{m(k;u)}=1\qquad\forall\alpha\in\Gamma. \tag{2.2}$$

We note that ε_u and ψ_u are characters of the group Γ. Let us assume that u is written as (1.10). For $\alpha\in\Gamma$, let us write as

$$\alpha=\begin{pmatrix}1+aN & 3^nb\sqrt{M}\\ 3^nc\sqrt{M} & 1+dN\end{pmatrix} \tag{2.3}$$

where $a, b, c, d\in\boldsymbol{Z}$. Then using the condition $\det(\alpha)=1$, we have $\varepsilon_u(\alpha)=\exp[(2\pi i/2)\xi]$, where ξ is an element of $\boldsymbol{Q}$ satisfying

$$\begin{aligned}\xi\equiv{}& 3^{n-h}ar^*x(bx+1)+3^{n+h}dry(cy+1)\\ &+bx\left(\frac{x}{3^{n+h}r}+1\right)+cy\left(-\frac{y}{3^{n-h}r^*}+1\right)\pmod{2\boldsymbol{Z}}.\end{aligned} \tag{2.4}$$

LEMMA 2.1. *If* $\alpha\in\Gamma(4\cdot3^nN\mathcal{O})$, *then* $\varepsilon_u(\alpha)=\psi_u(\alpha)=1$.

PROOF. Easily verified by (1.8) and (2.4). Q.E.D.

Put $G_{(4)}=\Gamma/\Gamma(4\mathcal{O})$, and $G_{(3)}=\Gamma/\Gamma(3^nN\mathcal{O})$. Then $G_{(4)}\cong SL_2(\boldsymbol{Z}/4\boldsymbol{Z})$, and $\Gamma/\Gamma(4\cdot3^nN\mathcal{O})\cong G_{(4)}\times G_{(3)}$. Let α_4 and β_4 be elements of Γ such that $\alpha_4\equiv\begin{pmatrix}1 & \sqrt{M}\\ 0 & 1\end{pmatrix}\pmod4$, $\beta_4\equiv\begin{pmatrix}1 & 0\\ \sqrt{M} & 1\end{pmatrix}\pmod4$, and $\alpha_4\equiv\beta_4\equiv1_2\pmod{3^nN}$. Let α_3, β_3, γ_3 be elements of Γ such that $\alpha_3\equiv\begin{pmatrix}1 & 3^n\sqrt{M}\\ 0 & 1\end{pmatrix}\pmod{3^nN}$, $\beta_3\equiv\begin{pmatrix}1 & 0\\ 3^n\sqrt{M} & 1\end{pmatrix}\pmod{3^nN}$, $\gamma_3\equiv\begin{pmatrix}1-N & 0\\ 0 & 1+N\end{pmatrix}\pmod{3^nN}$, and $\alpha_3\equiv\beta_3\equiv\gamma_3\equiv1_2\pmod4$.

LEMMA 2.2. *The elements* α_l, β_l $(l=3, 4)$, *and* γ_3 *generate the factor group* $\Gamma/\Gamma(4\cdot3^nN\mathcal{O})$.

PROOF. Elementary. Q.E.D.

LEMMA 2.3. $\varepsilon_u(\gamma_3)=\psi_u(\gamma_3)=1$.

PROOF. Easily verified by (1.8) and (2.4). Q.E.D.

LEMMA 2.4. (1) $\psi_u(\alpha_3)=\exp[(2\pi i/N)3^{n+h-1}rN]$. $\varepsilon_u(\alpha_3)=\exp[(2\pi i/N)\xi_1]$, *where* ξ_1 *is an integer satisfying* $\xi_1\equiv2^{-1}3^{n-h}r^*x^2\pmod N$.

(2) $\psi_u(\beta_3)=\exp[(2\pi i/N)(-3^{n-h-1}r^*N)]$. $\varepsilon_u(\beta_3)=\exp[(2\pi i/N)\xi_2]$, *where* ξ_2 *is an integer satisfying* $\xi_2\equiv-2^{-1}3^{n+h}ry^2\pmod N$.

PROOF. These can be proved by (1.8) and (2.4). Since the proof is similar to that of [8, Lemma 6.4], we omit it. Q.E.D.

LEMMA 2.5. (1) $\varepsilon_u(\alpha_4)=1$. $\psi_u(\alpha_4)=\exp[(2\pi i/4)(-3^kr)]$.

(2) $\varepsilon_u(\beta_4)=1$. $\psi_u(\beta_4)=\exp[(2\pi i/4)3^kr^*]$.

PROOF. These can be proved by (1.8) and (2.4). Since the proof is similar to that of [8, Lemma 6.5], we omit it. Q.E.D.

By these lemmas and (2.2), we have the following

THEOREM 2.1. *Let* g *be a function given by* (2.1). *Then* g *belongs to the*

unit group $\mathfrak{F}$ *if and only if the relations* (i), (ii), (iii) *hold*:

(i) $\sum_{0\le k\le n}\sum_{u\in A'_k} 3^{n-h}r^*x^2m(k\,;u)-(N/3)\sum_{u\in A'^{(-1)}_n} m(n\,;u)\equiv 0 \pmod N$.

(ii) $\sum_{0\le k\le n}\sum_{u\in A'_k} 3^{n+h}ry^2m(k\,;u)-(N/3)\sum_{u\in A'^{(1)}_n} m(n\,;u)\equiv 0 \pmod N$.

(iii) $\sum_{0\le k\le n}\sum_{u\in A'_k} 3^k rm(k\,;u)\equiv 0 \pmod 4$.

PROOF. By Lemmas 2.1-2.3, the condition is equivalent to saying that the relation (2.2) holds for the four elements α_l and β_l ($l=3, 4$). If we put $\alpha=\alpha_3$ (resp. β_3) in (2.2), then we obtain the relation (i) (resp. (ii)) by Lemma 2.4. If we put $\alpha=\alpha_4$ in (2.2), then we obtain the relation (iii) by Lemma 2.5. If we put $\alpha=\beta_4$ in (2.2), then again by Lemma 2.5, we obtain a congruence relation (iii') which is (iii) with r replaced by r^*. Since $r^*M\equiv r \pmod 4$, (iii') is equivalent to (iii). Q.E.D.

By Theorems 1.1 and 2.1, we have the characterization of the unit group $\mathfrak{F}$.

THEOREM 2.2. *The unit group* $\mathfrak{F}$ *consists of all functions* g *of the form* $g=c\prod_{0\le k\le n}\prod_{u\in\mathfrak{R}_k} g_{k,u}^{m(k,u)}$, *where* $c\in k_N^\times$ *and* $m(k\,;u)$ *are integers satisfying the relations* (i), (ii) *and* (iii) *of Theorem* 2.1 *where* A'_k, $A'^{(-1)}_n$, $A'^{(1)}_n$ *are replaced by* $\mathfrak{R}_k$, $\mathfrak{R}^{(-1)}_n$, $\mathfrak{R}^{(1)}_n$, *respectively*.

3. Calculation of the cuspidal class number of $X_1(3^{2n})$.

1. We reduce the problem of calculating the cuspidal class number to a problem of purely algebraic nature in the ring R. This section is similar to [8, Section 7].

Let φ be the embedding (1.3) of $\mathfrak{D}$ into R. Then $\varphi(\mathfrak{D}_0)=R_0^c$. We determine the image of $\mathrm{div}(\mathfrak{F})$. Let α be an element of C_k. Then the elements $3^{n-k}a(\alpha)^2t(\alpha) \pmod N$ and $3^{n-k}b(\alpha)^2t(\alpha)^* \pmod N$ of $\boldsymbol{Z}/N\boldsymbol{Z}$ are dependent only on the coset class $\pm\alpha D_k$. So for any element $\alpha\in G_k/H_k$, we can define two elements $3^{n-k}a(\alpha)^2t(\alpha)$ and $3^{n-k}b(\alpha)^2t(\alpha)^*$ of $\boldsymbol{Z}/N\boldsymbol{Z}$. Let I_4 be the set of all elements $\sum_{\alpha\in G} m(\alpha)\alpha$ of R ($m(\alpha)\in\boldsymbol{Z}$) which satisfy the following conditions (i)-(iii):

(3.1)

(i) $$\sum_{k=0}^{n}\sum_{\alpha\in(G_k-G_{k+1})/H_k} 3^{n-k}a(\alpha)^2t(\alpha)m(\alpha)-(N/3)\sum_{\alpha\in G_n^{(-1)}} m(\alpha)\equiv 0 \pmod N,$$

(ii) $$\sum_{k=0}^{n}\sum_{\alpha\in(G_k-G_{k+1})/H_k} 3^{n-k}b(\alpha)^2t(\alpha)^*m(\alpha)-(N/3)\sum_{\alpha\in G_n^{(1)}} m(\alpha)\equiv 0 \pmod N,$$

(iii) $$\sum_{\alpha\in G} t(\alpha)m(\alpha)\equiv 0 \pmod 4.$$

PROPOSITION 3.1. $\varphi(\mathrm{div}(\mathfrak{F}))=I_4\theta$.

PROOF. Since the proof is similar to that of [8, Proposition 7.1], we give

only a sketch. Let $g=c\prod_k \prod_u g_{k,u}^{m(k;u)}$ be any element of $\mathfrak{F}$ (Theorem 2.2). Then by (1.15), $\varphi(\mathrm{div}(g))=\sum_k \sum_u \sum_{\alpha\in G(u)} m(k;u)\alpha\theta$. For any $\alpha\in G$, put $m(\alpha)=m(k;u)$, where $k=\mathrm{ord}(\alpha)$ and $u=w_k\circ\alpha$. Then $\varphi(\mathrm{div}(g))=(\sum_{\alpha\in G} m(\alpha)\alpha)\theta$. When $u=w_k\circ\alpha$, we have $3^{n-h}t(u)^*x^2\equiv 3^{n-k}a(\alpha)^2t(\alpha) \pmod N$, and $3^{n+h}t(u)y^2\equiv 3^{n-k}b(\alpha)^2t(\alpha)^* \pmod N$. Also, $u\in\mathfrak{R}_n^{(-1)}$ (resp. $\mathfrak{R}_n^{(1)}$) if and only if $\alpha\in G_n^{(-1)}$ (resp. $G_n^{(1)}$). Hence, the equations (i) and (ii) of Theorem 2.2 become (i) and (ii) of (3.1), respectively. If we use $|H_k|=3^{n-k}\equiv 3^{n+k} \pmod 4$, we can prove that the equation (iii) of Theorem 2.2 is equivalent to (iii) of (3.1).

Q.E.D.

This proposition implies that the cuspidal class number is equal to the index $[R_0^c: I_4\theta]$. Put $\mu=\sum_{\alpha\in G}\alpha$.

LEMMA 3.1. $[R_0: R_0^c]=3^a$, *where* $a=3^{m-2}(2n^2+4n)-n$. (*Here, m is the exponent of* $N=3^m$, *namely* $m=2n$ *or* $2n+1$).

PROOF. This follows from the definitions of R_0 and R_0^c. Since the proof is exactly the same as that of [8, Lemma 7.1], we omit it. Q.E.D.

LEMMA 3.2. $\xi\in I_4$ *and* $\xi\theta=0$ *if and only if* $\xi\in\boldsymbol{Z}\mu$.

PROOF. Since $\deg(\theta)=0$, we have $\mu\theta=(\deg(\theta))\mu=0$. The fact $\mu\in I_4$ can be verified directly. (But the calculation is not so easy.) As another proof, we can use the fact that the product $g=\prod_{0\le k\le n}\prod_{u\in\mathfrak{R}_k} g_{k,u}$ is a constant. Since g belongs to $\mathfrak{F}$, Theorem 2.1 and the proof of Proposition 3.1 imply $\mu\in I_4$. Conversely, let $\xi\in R_C$ and $\xi\theta=0$. Then by the same argument as in the proof of [8, Lemma 7.2], we have $\xi\in\boldsymbol{C}\mu$. Hence, if $\xi\in I_4$, then $\xi\in\boldsymbol{Z}\mu$. Q.E.D.

2. Now we assume $N=3^{2n}$, so $M=1$. Put $\theta'=\theta-s$, where $s=(1/4)\mu$.

LEMMA 3.3. $I_4\theta=R_0\cap(I_4\theta'+\boldsymbol{Z}\mu)$.

PROOF. The inclusion $I_4\theta\subset R_0$ follows from Proposition 3.1. For $\xi\in I_4$, we have $\xi\theta=\xi\theta'+\xi s=\xi\theta'+(\det(\xi)/4)\mu\in I_4\theta'+\boldsymbol{Z}\mu$. This proves the inclusion $\subset$. Conversely, let $\eta=\xi\theta'+k\mu$, where $\xi\in I_4$ and $k\in\boldsymbol{Z}$. Suppose $\deg(\eta)=0$. Since $\deg(\theta')=-|G|/4$ and $\deg(\mu)=|G|$, we have $\deg(\xi)=4k$. Hence, $\xi\theta=\xi\theta'+(\deg(\xi)/4)\mu=\xi\theta'+k\mu=\eta$. This proves the reverse inclusion $\supset$. Q.E.D.

By Lemma 3.3, we have the isomorphism

$$R_0/I_4\theta\cong(R_0+I_4\theta'+\boldsymbol{Z}\mu)/(I_4\theta'+\boldsymbol{Z}\mu). \tag{3.2}$$

For an integer d, let R_d denote the set of all $\xi\in R$ such that $\deg(\xi)\equiv 0 \pmod d$.

LEMMA 3.4. $R_0+I_4\theta'+\boldsymbol{Z}\mu=R_{|G|}$.

PROOF. For $\xi\in I_4$, the fact $\xi\theta'\in R$ is implicit in the proof of Lemma 3.3.

Since $\deg(\xi\theta')=-(\deg(\xi)/4)|G|\in\boldsymbol{Z}|G|$ and $\deg(\mu)=|G|$, we have the equality of the lemma. Q.E.D.

LEMMA 3.5. *The element θ' is invertible in the algebra R_Q.*

PROOF. Since the set of all e_χ is a basis of R_C, we can write $\theta'=\sum a(\chi)e_\chi$. Since they are orthogonal idempotents, we have $\theta' e_\chi=a(\chi)e_\chi$, and θ' is invertible in R_C if and only if $a(\chi)\neq 0$ for all χ. By (1.17) and the definition of θ', we have $a(\chi)=(3^n/2)\overline{B_{2,k,\chi}}\neq 0$ $(\chi\neq 1)$, $-|G|/4\neq 0$ $(\chi=1)$. Thus θ' is invertible in R_C. Since $\theta'\in R_Q$, this implies that θ' is invertible in R_Q. Q.E.D.

Now we consider the inclusion:

$$R\supset R_{|G|}\supset I_4\theta'+\boldsymbol{Z}\mu\supset I_4\theta'. \tag{3.3}$$

By Lemmas 3.1, 3.4 and (3.2), we see that the cuspidal class number is equal to $[R_{|G|}: I_4\theta'+\boldsymbol{Z}\mu]/3^a$, where a is the integer in Lemma 3.1.

LEMMA 3.6. (1) $[R: R_{|G|}]=|G|(=4\cdot 3^{3n-2})$.
(2) $[I_4\theta'+\boldsymbol{Z}\mu: I_4\theta']=|G|/4$.

PROOF. (1) This is obvious. (2) The left-hand side is equal to $[\boldsymbol{Z}\mu: \boldsymbol{Z}\mu\cap I_4\theta']$. Let $\xi\theta'=k\mu$, where $\xi\in I_4$ and $k\in\boldsymbol{Z}$. Since θ' has the inverse θ'^{-1} (Lemma 3.5), we have $\xi=k\mu\theta'^{-1}=k\deg(\theta'^{-1})\mu=(-4k/|G|)\mu$. Since $\xi\in I_4$, we have $k\in(|G|/4)\boldsymbol{Z}$. Put $\xi=-\mu$. Then $\xi\in I_4$ and $\xi\theta'=(|G|/4)\mu$. Thus we have $\boldsymbol{Z}\mu\cap I_4\theta'=(|G|/4)\boldsymbol{Z}\mu$. This proves (2). Q.E.D.

For two lattices A and B of R_Q, let C be a lattice contained in $A\cap B$. Then $[A: C]/[B: C]$ 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, we have

$$[R: I_4\theta'] = [R: R\theta'][R\theta': I_4\theta']. \tag{3.4}$$

LEMMA 3.7. (1) $[R: R\theta']=(|G|/4)\prod_{\chi\neq 1}|(3^n/2)B_{2,k,\chi}|$.
(2) $[R\theta': I_4\theta']=4\cdot 3^{4n}$.

PROOF. (1) Let $\theta' e_\chi=a(\chi)e_\chi$. Then $[R: R\theta']=|\det(\theta')|=|\prod a(\chi)|$. The eigenvalues $a(\chi)$'s are given in the proof of Lemma 3.5. This proves (1). (2) Since θ' is invertible, we have $[R\theta': I_4\theta']=[R: I_4]$. Let $\varphi: R\to(\boldsymbol{Z}/3^{2n}\boldsymbol{Z})^2\times(\boldsymbol{Z}/4\boldsymbol{Z})$ be the homomorphism defined by $\varphi(\xi)=(\varphi_1(\xi), \varphi_2(\xi), \varphi_3(\xi))$, where $\varphi_1(\xi)$, $\varphi_2(\xi)$, $\varphi_3(\xi)$ are the left-hand sides of (i), (ii), (iii) of (3.1), respectively. Let x be an integer satisfying $4x\equiv 1 \pmod{3^{2n}}$. Put $\xi_1=(4x)1_G+(4x\cdot 3^{2n-1})\alpha$, and $\xi_2=(4x\cdot 3^{2n-1})1_G+(4x)\alpha$, where 1_G denotes the unity of G, and α denotes the element of $G_n^{(-1)}$ represented by $\begin{pmatrix}0 & \kappa\\ 1 & 0\end{pmatrix}$. Let y be an integer satisfying $3^{2n}y\equiv 1 \pmod 4$.

Put $\xi_3=(3^{2n}y)1_G$. Then $\varphi(\xi_1)=(1, 0, 0)$, $\varphi(\xi_2)=(0, 1, 0)$, $\varphi(\xi_3)=(0, 0, 1)$. Hence, φ is surjective. Since $\ker(\varphi)=I_4$, we have the proof. Q.E.D.

By (3.3), (3.4), Lemmas 3.6 and 3.7, we obtain the cuspidal class number.

THEOREM 3.1. *The cuspidal class number of the modular curve* $X_1(3^{2n})$ *is given by*

$$h_1(3^{2n}) = 3^e \prod_{\chi \neq 1} \left| \frac{1}{2} B_{2,k,\chi} \right|,$$

where $e=2+n+2\cdot 3^{2n-2}n^2$, *and* χ *runs through all characters* $\neq 1$ *in* $\mathfrak{X}$.

REMARK 3.1. Let h' be the number obtained by the substitution of 3 for p in the formula of [8, Theorem 7.1] (which is the formula for the case $p\neq 2, 3$). Then $h_1(3^{2n})=h'/3$.

4. Calculation of the cuspidal class number of $X_1(3^{2n+1})$.

1. In this section, we assume $N=3^{2n+1}$, so $M=3$. Since the case $n=0$ is exceptional and the genus of the curve $X_1(3)$ is 0, we assume $n\geqq 1$. This section is similar to [8, Section 8]. Let $I_{4\cdot 3^{3n}}$ (resp. I_0) be the set of all elements of I_4 which satisfy that the left-hand side of (iii) of (3.1) is congruent to 0 modulo $4\cdot 3^{3n}$ (resp. equal to 0).

LEMMA 4.1. (1) $[I_4\theta : I_{4\cdot 3^{3n}}\theta]=3^{3n-1}$.
(2) $I_{4\cdot 3^{3n}}\theta=I_0\theta$.

PROOF. (1) Let $\eta=\xi\theta$, where $\xi=\sum m(\alpha)\alpha\in I_4$. Put $d(\xi)=\{\sum_{\alpha\in G} t(\alpha)m(\alpha)\}/4$ $(\in \boldsymbol{Z})$. Then the residue class of $d(\xi)$ modulo 3^{3n} depends only on η. In fact, let ξ' be another element of I_4 satisfying $\eta=\xi'\theta$. Then $(\xi'-\xi)\theta=0$; hence by Lemma 3.2, $\xi'-\xi=k\mu$ with $k\in\boldsymbol{Z}$. Since $d(\mu)=3^{3n}$, we have $d(\xi')\equiv d(\xi) \pmod{3^{3n}}$. Now, put $\varphi(\eta)=d(\xi) \pmod{3^{3n}}$. Then φ is a homomorphism from $I_4\theta$ to $\boldsymbol{Z}/3^{3n}\boldsymbol{Z}$. Since $\ker(\varphi)=I_{4\cdot 3^{3n}}\theta$, it is sufficient to prove $\mathrm{Im}(\varphi)=3\boldsymbol{Z}/3^{3n}\boldsymbol{Z}$. Let η and ξ be as above. Then $\varphi(\eta)\equiv d(\xi)\equiv 4d(\xi)\equiv\sum_{\alpha\in G^{(1)}} m(\alpha) \pmod 3$. When $k\neq n$, $|H_k|=3^{n-k}\equiv 0 \pmod 3$. So we have $\varphi(\eta)\equiv\sum_{\alpha\in G_n^{(1)}} m(\alpha) \pmod 3$. The condition (i) of (3.1) implies that the latter is congruent to 0 modulo 3. Hence we have $\mathrm{Im}(\varphi)\subset 3\boldsymbol{Z}/3^{3n}\boldsymbol{Z}$. Next, put $\xi=16\cdot 1_G-4\alpha$, where α denotes the element of $G_n^{(1)}$ represented by $\begin{pmatrix}2 & 0\\ 0 & 2\end{pmatrix}$. Then $\xi\in I_4$ and $d(\xi)=3$. This proves (1). (2) Since $d(\mu)=3^{3n}$, we have $\mu\in I_{4\cdot 3^{3n}}$. If $\xi\in I_{4\cdot 3^{3n}}$, then $d(\xi)=3^{3n}k$ with $k\in\boldsymbol{Z}$. Hence $d(\xi-k\mu)=0$; namely, $\xi-k\mu\in I_0$. This implies $I_{4\cdot 3^{3n}}=I_0+\boldsymbol{Z}\mu$. So by Lemma 3.2, we have $I_{4\cdot 3^{3n}}\theta=I_0\theta$. Q.E.D.

By Proposition 3.1, Lemmas 3.1 and 4.1, we see that the cuspidal class

number is equal to $[R_0: I_0\theta]/3^{a+3n-1}$, where a is the integer in Lemma 3.1. For an element $\xi=\sum_\alpha m(\alpha)\alpha$ of R, write $\xi_+=\sum_{\alpha\in G^{(1)}} m(\alpha)\alpha$ and $\xi_-=\sum_{\alpha\in G^{(-1)}} m(\alpha)\alpha$. Put $\theta'=\theta-s$, where $s=(1/4)\sum_{\alpha\in G} t(\alpha)^*\alpha=(1/4)(3\mu_+ +\mu_-)$.

LEMMA 4.2. (1) $I_0 s\subset \boldsymbol{Z}\mu_+$.
(2) $I_0\theta=R_0\cap(I_0\theta'+\boldsymbol{Z}\mu_+)$.

PROOF. (1) For $\xi\in R$, we have $\xi s=(1/4)(\xi_+ +\xi_-)(3\mu_+ +\mu_-)=(1/4)\{3\deg(\xi_+)+\deg(\xi_-)\}\mu_+ +(1/4)\{\deg(\xi_+)+3\deg(\xi_-)\}\mu_-$. If $\xi\in I_0$, then $\deg(\xi_+)+3\deg(\xi_-)=0$. Hence $\xi s=-2\deg(\xi_-)\mu_+\in \boldsymbol{Z}\mu_+$. This proves (1). (2) The inclusion $\subset$ follows from (1). Let $\eta=\xi\theta'+k\mu_+$, where $\xi\in I_0$ and $k\in\boldsymbol{Z}$. Suppose $\deg(\eta)=0$. Since $\deg(\theta')=-\deg(\mu_+)$, we have $k=\deg(\xi)$. Put $\eta_1=\xi\theta=\xi\theta'+\xi s$. (1) implies $\xi s=k_1\mu_+$ with some $k_1\in\boldsymbol{Z}$. Then we have again $k_1=\deg(\xi)(=k)$. Hence $\eta=\eta_1\in I_0\theta$. This gives the reverse inclusion $\supset$. Q.E.D.

By Lemma 4.2, we have the isomorphism

$$R_0/I_0\theta\cong(R_0+I_0\theta'+\boldsymbol{Z}\mu_+)/(I_0\theta'+\boldsymbol{Z}\mu_+). \tag{4.1}$$

For an integer d, let R_d denote the set of all $\xi\in R$ such that $\deg(\xi)\equiv 0 \pmod d$.

LEMMA 4.3. $R_0+I_0\theta'+\boldsymbol{Z}\mu_+=R_{|G^{(1)}|}$.

PROOF. For $\xi\in I_0$, $\xi\theta'=\xi\theta-\xi s\in R$ (Lemma 4.2). Since $\deg(\xi\theta')=-\deg(\xi)|G^{(1)}|$ and $\deg(\mu_+)=|G^{(1)}|$, we have the equality. Q.E.D.

LEMMA 4.4. *The element* $\xi=3\mu_+-\mu_-$ *belongs to* I_0, *and satisfies* $\xi\theta'=3^{2n-1}\mu-2\cdot 3^{2n-1}(3^{n+1}+1)\mu_+$.

PROOF. We can verify by direct calculations that both μ_+ and μ_- satisfy (i) and (ii) of (3.1). This implies $3\mu_+-\mu_-\in I_0$. Next, we have $\xi\theta'=4\deg(\theta_-)\mu-8\{\deg(\theta_-)+\deg(s_-)\}\mu_+$. (Here, the relations $\mu_-=\mu-\mu_+$, $\deg(\theta_+)=-\deg(\theta_-)$, and $\deg(s_+)=3\deg(s_-)$ are used.) Since $\deg(\theta_-)=3^{2n-1}/4$ and $\deg(s_-)=3^{3n}/4$, we have the result. (The calculation of $\deg(\theta_-)$ is not so easy. In [8, Lemma 8.4], we calculated it directly. But there is another method. Here, let p be any prime $\neq 2$. Let χ_0 be the non-trivial character of G/H_0 such that $\chi_0|G^{(1)}=1$. We see easily $\theta e_{\chi_0}=(-2\deg(\theta_-))e_{\chi_0}$. Then by (1.17), we have $-2\deg(\theta_-)=(p^n/2)B_{2,0,\chi_0}$. On the other hand, we have $B_{2,0,\chi_0}=-(p-1)p^n/6$ ([8, Proposition 5.5]). This gives the value of $\deg(\theta_-)$.) Q.E.D.

LEMMA 4.5. $I_0\theta'+\boldsymbol{Z}\mu_+=I_{4\cdot 3^{3n}}\theta'+\boldsymbol{Z}\mu_+$.

PROOF. The inclusion $\subset$ is obvious. In the proof of Lemma 4.1, we obtained $I_{4\cdot 3^{3n}}=I_0+\boldsymbol{Z}\mu$. Since $\mu\theta'=\deg(\theta')\mu=-3^{3n}\mu$, we have $I_{4\cdot 3^{3n}}\theta'=I_0\theta'+\boldsymbol{Z}3^{3n}\mu$. By Lemma 4.4, $3^{3n}\mu=3^{n+1}\xi\theta'+2\cdot 3^{3n}(3^{n+1}+1)\mu_+\in I_0\theta'+\boldsymbol{Z}\mu_+$, where $\xi=3\mu_+-\mu_-$. This implies the reverse inclusion $\supset$. Q.E.D.

Let χ_0 be the unique non-trivial character of G/H_0 such that $\chi_0|G^{(1)}=1$.

LEMMA 4.6. *The element θ' is invertible in the algebra R_Q.*

PROOF. As in the proof of Lemma 3.5, write as $\theta'=\sum a(\chi)e_\chi$. Then it is sufficient to show $a(\chi)\neq 0$ for all χ. By (1.17) and the definition of θ', we have $a(\chi)=(3^n/2)\overline{B_{2,k,\chi}}\neq 0$ $(\chi\neq 1, \chi_0)$, $-3^{2n-1}(3^{n+1}+1)/2\neq 0$ $(\chi=\chi_0)$, $-3^{3n}\neq 0$ $(\chi=1)$. This proves the lemma. Q.E.D.

Now we consider the inclusion:

$$R \supset R_{|G^{(1)}|} \supset I_{4\cdot 3^{3n}}\theta'+\boldsymbol{Z}\mu_+ \supset I_{4\cdot 3^{3n}}\theta' . \tag{4.2}$$

By Lemmas 4.3, 4.5 and (4.1), we see that the cuspidal class number is equal to $[R_{|G^{(1)}|}: I_{4\cdot 3^{3n}}\theta'+\boldsymbol{Z}\mu_+]/3^{a+3n-1}$, where a is the integer in Lemma 3.1.

LEMMA 4.7. (1) $[R: R_{|G^{(1)}|}]=|G^{(1)}|(=3^{3n})$.
(2) $[I_{4\cdot 3^{3n}}\theta'+\boldsymbol{Z}\mu_+ : I_{4\cdot 3^{3n}}\theta']=2\cdot 3^{3n}(3^{n+1}+1)$.

PROOF. (1) This is obvious. (2) Put $l=2\cdot 3^{3n}(3^{n+1}+1)$. It is sufficient to prove $\boldsymbol{Z}\mu_+\cap I_{4\cdot 3^{3n}}\theta'=l\boldsymbol{Z}\mu_+$. Let $\xi\theta'=k\mu_+$, where $\xi\in I_{4\cdot 3^{3n}}$ and $k\in\boldsymbol{Z}$. Then $\xi=k\mu_+\theta'^{-1}$. Put $\xi_0=3\mu_+-\mu_-$. By Lemma 4.4, $l\mu_+\theta'^{-1}=3^{3n}\mu\theta'^{-1}-3^{n+1}\xi_0=-(\mu+3^{n+1}\xi_0)$. Put $\eta_0=\mu+3^{n+1}\xi_0$ $(\in I_{4\cdot 3^{3n}})$. Then $\xi=(-k/l)\eta_0$. Since $\xi\in I_{4\cdot 3^{3n}}$ and $\deg((\eta_0)_+)+3\deg((\eta_0)_-)=4\cdot 3^{3n}$, we have $k\in l\boldsymbol{Z}$. This proves the inclusion $\subset$. The reverse inclusion $\supset$ follows from $l\mu_+=-\eta_0\theta'$. Thus (2) is proved. Q.E.D.

Similarly to (3.4), we have

$$[R: I_{4\cdot 3^{3n}}\theta'] = [R: R\theta'][R\theta' : I_{4\cdot 3^{3n}}\theta'] . \tag{4.3}$$

LEMMA 4.8. (1) $[R: R\theta']=(1/6)3^{5n}(3^{n+1}+1)\prod_{\chi\neq 1,\chi_0}|(3^n/2)B_{2,k,\chi}|$.
(2) $[R\theta' : I_{4\cdot 3^{3n}}\theta']=4\cdot 3^{7n+1}$.

PROOF. (1) Let $\theta' e_\chi=a(\chi)e_\chi$. Then $[R: R\theta']=|\det(\theta')|=|\prod a(\chi)|$. The eigenvalues $a(\chi)$'s are given in the proof of Lemma 4.6. This proves (1). (2) Since θ' is invertible, we have $[R\theta' : I_4\theta']=[R: I_4]$. Let $\varphi: R\to(\boldsymbol{Z}/3^{2n+1}\boldsymbol{Z})^2\times(\boldsymbol{Z}/4\cdot 3^{3n}\boldsymbol{Z})$ be the homomorphism defined by $\varphi(\xi)=(\varphi_1(\xi), \varphi_2(\xi), \varphi_3(\xi))$, where $\varphi_1(\xi)$, $\varphi_2(\xi)$, $\varphi_3(\xi)$ are the left-hand sides of (i), (ii), (iii) of (3.1), respectively. Let $\phi: (\boldsymbol{Z}/3^{2n+1}\boldsymbol{Z})^2\times(\boldsymbol{Z}/4\cdot 3^{3n}\boldsymbol{Z})\to(\boldsymbol{Z}/3\boldsymbol{Z})^3$ be the homomorphism induced by the reduction. Let A be the subgroup of $(\boldsymbol{Z}/3\boldsymbol{Z})^3$ consisting of all elements (x, y, z) which satisfy $x\equiv z \pmod 3$. Put $G=\phi^{-1}(A)$. Now we prove $\varphi(R)=G$, which implies the desired equation $[R: I_{4\cdot 3^{3n}}]=4\cdot 3^{7n+1}$. First, put $\xi_1=-1_G+\alpha$, $\xi_3=4\cdot 1_G-\alpha$, and $\xi_2=3\beta-3\xi_3$, where 1_G denotes the unity of G, α denotes the element of $G_n^{(1)}$ represented by $\begin{pmatrix}2 & 0\\ 0 & 2\end{pmatrix}$, and β is the element of $G_n^{(-1)}$ represented

by $\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$. Then $\varphi(\xi_1)=(3, 0, 0)$, $\varphi(\xi_2)=(0, 3, 0)$, $\varphi(\xi_3)=(0, 0, 3)$. This implies $\varphi(R)\supset\ker(\phi)$. Second for $\xi=\sum m(\alpha)\in R$, we see easily $\varphi_1(\xi)\equiv\varphi_3(\xi)\equiv\sum_{\alpha\in G_n^{(1)}} m(\alpha)$ (mod 3). This implies $\phi(\varphi(R))\subset A$. Lastly, we have $\varphi(1_G)\equiv(1, 0, 1)$ (mod 3) and $\varphi(\beta)\equiv(0, 1, 0)$ (mod 3). Since A is generated by (1, 0, 1) and (0, 1, 0), we have $\phi(\varphi(R))\supset A$. Summarizing these results, we have $\varphi(R)=G$. Q.E.D.

By (4.2), (4.3), Lemmas 4.7 and 4.8, we obtain the cuspidal class number.

THEOREM 4.1. *Let $h_1(3^{2n+1})$ be the cuspidal class number of the modular curve $X_1(3^{2n+1})$. If $n\geqq 1$, then*

$$h_1(3^{2n+1})=3^e\prod_{\chi\neq 1,\chi_0}\left|\frac{1}{2}B_{2,k,\chi}\right|,$$

where $e=1+2n+2\cdot 3^{2n-1}(n+n^2)$, and χ runs through all characters $\neq 1, \chi_0$ in $\mathfrak{X}$. If $n=0$, then $h_1(3)=1$.

REMARK 4.1. Let h' be the number obtained by the substitution of 3 for p in the formula of [8, Theorem 8.1] (which is the formula for the case $p\neq 2, 3$). Then $h_1(3^{2n+1})=h'/3$ if $n\geqq 1$, $h'/3^2$ if $n=0$.

References

[1] V.G. Drinfeld, Two theorems on modular curves, Functional Anal. Appl., 7 (1973), 155-156.

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

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

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

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

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

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

[8] T. Takagi, The cuspidal class number formula for the modular curves $X_1(p^m)$, J. Algebra, **157** (1993), 515-549.

[9] H. Weber, Lehrbuch der Algebra, Vol. III, Chelsea, New York.

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

Toshikazu TAKAGI

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