J. Math. Soc. Japan
Vol. 21, No. 4, 1969

Hecke polynomials of modular groups and congruence zeta functions of fibre varieties

By Yasuo MORITA

(Received Jan. 30, 1969)
(Revised July 14, 1969)

§ 0. Introduction.

0-1. In [*HP*], Y. Ihara proved that the Hecke polynomials $H_k^{(p)}(u)$ of the elliptic modular group $SL(2, Z)$ can be expressed by the congruence zeta functions of some algebraic varieties. There, he used some properties of imaginary quadratic fields and elliptic curves defined over finite fields. But in the preface of [*HP*], he stated that more intrinsic proof and generalization to higher level cases would be obtained by using the group

$$\Gamma_p = PL^+(2, Z^{(p)}) = \{x \in GL(2, Z^{(p)}) \mid \det x = p\text{-power}\}/\pm p\text{-powers}\,,$$

where $Z^{(p)} = \bigcup_{n=0}^{\infty} p^{-n}Z \subset Q$. We shall carry out this program in this paper.

0-2. Let p be a prime number, $\Gamma = PSL(2, Z^{(p)})$ and Δ be its subgroup of finite index. We shall define the Hecke polynomial of Δ and study it in this paper. We shall treat only subgroups of $PSL(2, Z^{(p)})$, which is a subgroup of $PL^+(2, Z^{(p)})$ of index 2. This restriction simplifies the calculations and notations to a fair degree. Moreover, this restriction makes no difference if we are interested only in the absolute values of the zeros of the Hecke polynomials (cf. § 1, Remark 2). But, of course, we can obtain similar results in the general case.

In the first section, we define the Hecke operators $T_k(\Delta, m)$ which act on the space of the cusp forms of weight k ($k = 2, 4, \cdots$) with respect to the Fuchsian group $\Delta^0 = \Delta \cap PSL(2, Z)$. If $\Delta = PSL(2, Z^{(p)})$, then our operators coincide with the well-known Hecke operators $T_k(p^{2m})$ which were studied by Hecke. We prove a recursion formula of $T_k(\Delta, m)$ and consequently obtain the following equality;

$$\sum_{m=1}^{\infty} \frac{1}{p^{ms}} T_k(\Delta, m) = \{1 - p^{2(k-1)}p^{-s}I\}/\{I - (T_k(\Delta, 1) - p^{k-1}I)p^{-s} + p^{2(k-1)}Ip^{-2s}\}\,,$$

where I denotes the identity operator. So, we define the Hecke polynomial by

$$H_k(\Delta\,; u) = \det\{I - (T_k(\Delta, 1) - p^{k-1}I)u + p^{2(k-1)}Iu^2\}\,,$$

where u is an indeterminate. Then we obtain the following expression from the recursion formula of $T_k(\Delta, m)$ and the self-adjointness of $T_k(\Delta, m)$;

$$\log H_k(\Delta ; u) = -\sum_{m=1}^{\infty} tr\, U_k(\Delta, m)\frac{u^m}{m},$$

where

$$U_k(\Delta, m) = T_k(\Delta, m) - p^{k-1}T_k(\Delta, m-1).$$

In the next section, we define the infinite set $\mathcal{P}(\Delta)\cup\mathcal{P}_\infty(\Delta)$ of "prime divisors" of the group Δ, as in [*CMP*]. This is, up to minor differences, the set of Δ-conjugacy classes of all Δ-fixed points on the upper half plane $\mathfrak{H} = \{z \in C \mid \mathrm{Im}(z) > 0\}$. Then we define the zeta functions $Z_k^H(\Delta ; u)$ $(k = 2, 4, 6, \cdots)$ of the group Δ by

$$\log Z_k^H(\Delta ; u)$$
$$= \sum_{m=1}^{\infty}\Big[\sum_{P \in \mathcal{P}(\Delta)\cup\mathcal{P}_\infty(\Delta)} (\text{some quantity which depends only on } P, k, m)\Big]\frac{(p^{k-1}u)^m}{m}.$$

If $k = 2$, then this zeta function coincides, up to minor factors, with the zeta function which was defined in [*CMP*]. In general case, we can make the calculations simple and clear by using these zeta functions. We prove

$$H_k(\Delta ; u) \doteqdot Z_k^H(\Delta ; u) \qquad \text{(equal up to correcting terms)}.$$

We call this equation as *the first equality*. This equality can be proved by calculating the traces of $U_k(\Delta, m)$, using the Eichler-Selberg trace formula and some thorems in [*CMP*] which tell what and how many Δ^0-conjugacy classes are contained in a Δ-conjugacy class $P = \{z\}_\Delta \in \mathcal{P}(\Delta)\cup\mathcal{P}_\infty(\Delta)$.

In the last section, we quote a theorem from [*CMP*] which we call Theorem *CM*. This theorem *CM* tells that there is a finite separable algebraic extension L over the rational functional field $K = F_{p^2}(j)$ such that the decomposition law of the prime divisors of K in L can be written by means of the "decomposition law" of the Γ-conjugacy classes into Δ-conjugacy classes. Let Ω be the universal domain of characteristic p. Let E_j $(j \in \Omega - \{0, 12^3\})$ be the elliptic curve defined by the Tate's equation;

$$Y^2Z + XYZ = X^3 - \frac{36}{j-12^3}XZ^2 - \frac{1}{j-12^3}Z^3 \quad \text{in} \quad P^2(\Omega).$$

Let U_r $(r = 0, 1, 2, \cdots)$ be the fibre variety defined by

$$U_r = \bigcup_{j \in \Omega - \{0, 12^3\}} j \times \underbrace{E_j \times \cdots \times E_j}_{r \text{ copies}} \subset \Omega \times \underbrace{P^2(\Omega) \times \cdots \times P^2(\Omega)}_{r \text{ copies}}.$$

This is a fibre variety over $\Omega - \{0, 12^3\}$ which is a model of $K = F_{p^2}(j)$. Let V_r be the pull back of U_r by the covering map π to the model V_0 of L which is the complement of $\pi^{-1}(\{0, 12^3\})$ in the complete non-singular model of L.

Then V_r is a fibre variety over V_0 defined over the finite field F_{p^2}. Then, since we can determine the characteristic roots of the Frobenius endomorphism of E_j (j algebraic over F_{p^2}) in terms of Γ, we can calculate the number of the algebraic points of V_r whose projections on the base curve V_0 lie on a fixed algebraic point of V_0. On the other hand, we can calculate the number of algebraic points on V_0 by means of Theorem *CM*. Consequently, we have

$$Z_k^H(\Delta\,;u)\doteqdot\prod_{r=0}^{k-2}Z_r^c(L,\,A_{k-2,r}\,;u)\qquad\text{(equal up to correcting terms)},$$

where $Z_r^c(L,\,A_{k-2,r}\,;u)$ are rational functions of u which can be expressed by the congruence zeta functions $Z_l^c(\Delta\,;u)$ of the algebraic varieties V_l over the finite field F_{p^2}. We call this equation as *the second equality*.

Now, from the first and the second equality, we obtain an expression of the Hecke polynomial by means of the congruence zeta functions of algebraic varieties;

$$H_k(\Delta\,;u)\doteqdot\prod_{r=0}^{k-2}Z_r^c(L,\,A_{k-2,r}\,;u)\qquad\text{(equal up to correcting terms)}.$$

This is a generalization of the main result in [*HP*] and of [*CMP*], Vol. 1, p. 192, Corollary up to minor differences.

Finally, I want to express my gratitude to Professor Y. Ihara who gave me this problem and gave us a lecture about the Congruence Monodromy Problems at University of Tokyo.

§ 1. Hecke polynomials.

1-1. *Structure of the Hecke ring* $\mathfrak{R}(\Delta^0,\Delta)$. To prove self-adjointness and recursion formula of Hecke operators, we shall study the structure of Hecke rings. Let Z, Q, R, C be respectively the ring of rational integers, the field of rational numbers, the field of real numbers, and the field of complex numbers. For any prime number p, we denote by $Z^{(p)}=\bigcup_{n=0}^{\infty}p^{-n}Z$, Z_p and Q_p respectively the p-complementary-localization of Z, the p-completion of Z, and the p-completion of Q. Let $\Gamma=PSL(2,\,Z^{(p)})$ be the modular group over $Z^{(p)}$ and Δ be a subgroup of Γ of finite index $[\Gamma:\Delta]<\infty$. We can regard Δ as a dense subgroup of the topological group $PSL(2,\,R)$ or the topological group $G=PSL(2,\,Q_p)$ by the natural imbedding.

Now, for any integer $l\geqq 0$, we write

$$\Delta^l=\Delta\cap U\begin{pmatrix}p & 0\\ 0 & p^{-l}\end{pmatrix}U\,,\tag{1}$$

where $U=PSL(2,\,Z_p)$. Since $\Delta=\bigcup_{l=0}^{\infty}\Delta^l$ (disjoint union), we can define the *length*

of an element δ of Δ and the *length of a double coset* $\Delta^0\delta\Delta^0$ by $l(\delta)=l$ if $\delta\in\Delta^l$ and by $l(\Delta^0\delta\Delta^0)=l$ if $\Delta^0\delta\Delta^0=\Delta^l$ respectively.

PROPOSITION 1. *We have bijective maps*

$$\begin{array}{ccc} \Delta^0\backslash\Delta & \xrightarrow{\sim} & U\backslash G \\ \cup & & \cup \\ \Delta^0\delta & \longmapsto & U\delta\,, \end{array} \tag{2}$$

$$\begin{array}{ccc} \Delta^0\backslash\Delta/\Delta^0 & \xrightarrow{\sim} & U\backslash G/U \\ \cup & & \cup \\ \Delta^0\delta\Delta^0 & \longmapsto & U\delta U\,, \end{array} \tag{3}$$

and a natural isomorphism between two Hecke rings

$$\begin{array}{ccc} \mathcal{R}(\Delta^0,\Delta) & \xrightarrow{\sim} & \mathcal{R}(U,G) \\ \cup & & \cup \\ \Delta^0\delta\Delta^0 & \longmapsto & U\delta U\,. \end{array} \tag{4}$$

PROOF. We note that Δ, U are a dense subgroup of G, an open compact subgroup of G respectively, and that $\Delta^0=\Delta\cap U$. Hence, taking the p-adic closure, we have $(\overline{\Delta^0\delta})=U\delta$ and $(\overline{\Delta^0\delta\Delta^0})=U\delta U$. Let Ug (resp. UgU) be any element of $U\backslash G$ (resp. $U\backslash G/U$). Since Ug (resp. UgU) is open in G and Δ is dense in G, we can take an element $\delta\in\Delta$ which is contained in Ug (resp. UgU). Then we have $U\delta=Ug$ (resp. $U\delta U=UgU$) and thus proved the surjectivity of (2) (resp. the surjectivity of (3)). The injectivity of (2) is trivial. For the injectivity of (3), let $U\delta U=U\delta' U$ with $\delta,\delta'\in\Delta$. Then we have $\delta'=u_1\delta u_2$ with $u_1, u_2\in U$. Let ε_1 be an element of Δ^0 which is sufficiently close to u_1. Since U is open, we may assume that $\varepsilon_2=\delta^{-1}\varepsilon_1^{-1}\delta'$ belongs to U. Therefore we have $\delta'=\varepsilon_1\delta\varepsilon_2$ with $\varepsilon_1,\varepsilon_2\in\Delta^0$. Consequently we have $\Delta^0\delta\Delta^0=\Delta^0\delta'\Delta^0$ and proved the injectivity of (3).

Now, since U is an open compact subgroup of G, we can define the Hecke ring $\mathcal{R}(U,G)$. Therefore, the bijectivities of (2) and (3) show that we can define the Hecke ring $\mathcal{R}(\Delta^0,\Delta)$. Let $\sigma_0=\Delta^0\alpha\Delta^0$, $\tau_0=\Delta^0\beta\Delta^0$, $\rho_0=\Delta^0\gamma\Delta^0$, $\sigma=U\alpha U$, $\tau=U\beta U$ and $\rho=U\gamma U$ $(\alpha,\beta,\gamma\in\Delta)$. Then we see easily from the bijectivities of (2) and (3) that the structure constants $\mu(\sigma_0\cdot\tau_0;\rho_0)$ and $\mu(\sigma\cdot\tau;\rho)$ are equal. Therefore the map (4) induces an injective homomorphism. Now, by the surjectivity of (3), this map is surjective. Therefore we have proved that the map (4) is an isomorphism. Q. E. D.

COROLLARY 1. $[\Gamma^0:\Delta^0]=[\Gamma:\Delta]<\infty$.

COROLLARY 2. *We have a natural isomorphism*

$$\begin{array}{ccc} \mathcal{R}(\Delta^0,\Delta) & \xrightarrow{\sim} & \mathcal{R}(\Gamma^0,\Gamma) \\ \cup & & \cup \\ \Gamma^0\delta\Gamma^0 & \longmapsto & \Gamma^0\delta\Gamma^0 \end{array} \tag{5}$$

which preserves the lengths of double cosets.

COROLLARY 3. *$\mathcal{R}(\Delta^0, \Delta)$ is a commutative ring with one double coset $\Delta^0\delta\Delta^0$ of length l. We denote such a coset by $\sigma(\Delta, l)$.*

PROOF. The commutativity of $\mathcal{R}(U, G)$ is well-known. Therefore, Proposition 1 shows the commutativity of $\mathcal{R}(\Delta^0, \Delta)$. The second part is clear from the bijectivity of (3) and the theory of elementary divisors. Q. E. D.

COROLLARY 4. *Δ^l contains just $p^{2l}+p^{2l-1}$ right Δ^0-cosets and $p^{2l}+p^{2l-1}$ left Δ^0-cosets.*

PROOF. Corresponding results about U and G are well-known. Therefore, by the bijectivities of (2) and (3), we have Corollary 4. Q. E. D.

1-2. *Representations of the Hecke ring $\mathcal{R}(\Delta^0, \Delta)$ on the spaces of cusp forms.*

Now we shall define the Hecke operators and the Hecke polynomials, and prove self-adjointness and recursion formula. Since $\Gamma^0 = PSL(2, Z)$ and $[\Gamma^0 : \Delta^0] < \infty$, Δ^0 is a Fuchsian group of the first kind. Let $\mathfrak{S}_k(\Delta)$ $(k = 2, 4, 6, \cdots)$ be the space of the cusp forms of weight k with respect to the Fuchsian group Δ^0. For any integer $m \geqq 0$, we define an element of $\mathcal{R}(\Delta^0, \Delta)$ by

$$\mathfrak{T}(\Delta, m) = \sum_{l=0}^{m} p^m \cdot \sigma(\Delta, l)\,, \tag{6}$$

and a Hecke operator $T(m) = T_k(\Delta, m)$ acting on $\mathfrak{S}_k(\Delta)$ by

$$\mathfrak{S}_k(\Delta) \ni f(X) \longmapsto p^{2m(k-1)} \sum_i f\left(\frac{a_i X + b_i}{c_i X + d_i}\right)(c_i X + d_i)^{-k} \in \mathfrak{S}_k(\Delta)\,, \tag{7}$$

where $\delta_i = \begin{pmatrix} a_i & b_i \\ c_i & d_i \end{pmatrix} \in M_2(Z)$ runs over all the representatives $\Delta^0\delta_i$ of the left Δ^0-cosets contained in $\mathfrak{T}(\Delta, m)$.

REMARK 1. $T_k(\Gamma, m)$ coincides with the well-known Hecke operator $T_k(p^{2m})$ which was studied by Hecke.

PROPOSITION 2. *$T(m) = T_k(\Delta, m)$ are self-adjoint operators and have the following recursion formula;*

$$T(m+1) = (T(1) - p^{k-1})T(m) - p^{2(k-1)}T(m-1) \qquad (m \geqq 1)\,. \tag{8}$$

PROOF. The first part is an immediate consequence of the invariance of double cosets by the adjoint map

$$\Delta^0 \begin{pmatrix} a & b \\ c & d \end{pmatrix} \Delta^0 \longmapsto \Delta^0 \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \Delta^0\,. \tag{9}$$

This invariance follows from the bijectivity of (3) and the theory of elementary divisors for $PSL(2, Q_p)$.

For the second part, Corollary 2 of Proposition 1 shows that we may assume $\Delta = \Gamma$. Now, in this case, we can prove the second assertion by using the well-known recursion formula

(10) $$T_k(p^{m+1}) = T_k(p)T_k(p^m) - p^{k-1}T_k(p^{m-1}) .$$ Q. E. D.

Now we obtain from the recursion formula

(11) $$\sum_{m=1}^{\infty} \frac{1}{p^{ms}} T(m) = \{1-p^{2(k-1)}p^{-s}\}I/\{I-(T(1)-p^{k-1}I)p^{-s}+p^{2(k-1)}Ip^{-2s}\} .$$

So, we define the *Hecke polynomial* by

(12) $$H(u) = H_k(\Delta ; u) = \det \{I-(T_k(\Delta, 1)-p^{k-1}I)u+p^{2(k-1)}Iu^2\} ,$$

where I denotes the identity operator and u denotes a variable.

REMARK 2. Let $\Delta = \Gamma = PSL(2, Z^{(p)})$. Let $H_k^{(p)}(u) = \det \{I-T_k(p)u+p^{k-1}Iu^2\}$ be the usual Hecke polynomial attached to the elliptic modular group $SL(2, Z)$. Let $H_k^{(p)}(u) = \prod_{j=1}^{N}(1-\beta_j u)(1-\beta_j' u)$. Then our Hecke polynomial can be written as $H_k(\Gamma ; u) = \prod_{j=1}^{N}(1-\beta_j^2 u)(1-\beta_j'^2 u)$. In particular, our Hecke polynomial $H_k(\Gamma, u)$ determines the absolute values of the roots of $H_k^{(p)}(u) = 0$.

PROPOSITION 3. *For any natural number m, put*

(13) $$U(m) = U_k(\Delta, m) = T_k(\Delta, m) - p^{k-1}T_k(\Delta, m-1) .$$

Then we have a following expression of Hecke polynomial;

(14) $$\log H_k(\Delta ; u) = -\sum_{m=1}^{\infty} tr\, U_k(\Delta, m)\frac{u^m}{m} .$$

PROOF. By Corollary 3 of Proposition 1 and by Proposition 2, we can diagonise $T(m)$ $(m \geqq 0)$ at the same time. Let a_j $(1 \leqq j \leqq N = \dim \mathfrak{S}_k(\Delta))$ be the eigenvalues of $T(1)$ and put

(15) $$1-(a_j-p^{k-1})u+p^{2(k-1)}u^2 = (1-\alpha_j u)(1-\alpha_j' u) .$$

Then we have $H(u) = \prod_{j=1}^{N}(1-\alpha_j u)(1-\alpha_j' u)$. Hence we have

(16) $$-\log H(u) = \sum_{m=1}^{\infty} \left(\sum_{j=1}^{N} \alpha_j^m + \alpha_j'^m \right) \frac{u^m}{m} .$$

By the way, the recursion formula of $T(m)$ shows that the eigenvalues of $U(m)$ are $\alpha_j^m + \alpha_j'^m$ $(1 \leqq j \leqq N)$. Consequently we have proved the above proposition. Q. E. D.

1-3. EXAMPLE. Let N be a natural number which is prime to p. We define the principal congruence subgroup of Γ of the level N by

(17) $$\Gamma(N) = \{\gamma \in PSL(2, Z^{(p)}) \mid \gamma \equiv 1 \pmod N\} .$$

We see clearly that $\Gamma(N)$ is of finite index in Γ and that the Fuchsian group attached to it is

(18) $$\Gamma(N)^0 = \{\gamma \in PSL(2, Z) \mid \gamma \equiv 1 \pmod N\} .$$

All our arguments in this paper may apply to this group.

REMARK 3. Mennicke has proved in [9] that any subgroup of finite index of $PSL(2, Z^{(p)})$ contains some such group $\Gamma(N)$. Therefore our Fuchsian group Δ^0 contains some $\Gamma(N)^0$. Consequently Δ^0 must be a congruence subgroup of $PSL(2, Z)$.

§ 2. Zeta functions of the group Δ.

2-1. *Prime divisors of the group Δ and its zeta functions.* We denote by $\mathfrak{H}$ the upper half plane $\{z \in C \mid \operatorname{Im} z > 0\}$. Then Δ operates on $\mathfrak{H}$ by

$$\Delta \ni \delta = \begin{pmatrix} a & b \\ c & d \end{pmatrix} : \mathfrak{H} \ni z \longmapsto \frac{az+b}{cz+d} \in \mathfrak{H}. \tag{19}$$

For any point $z \in \mathfrak{H}$, we put $\Delta_z = \{\delta \in \Delta \mid \delta z = z\}$. If $\Delta_z \neq \{1\}$ we call z a *Δ-fixed point.* We say, $z, z' \in \mathfrak{H}$ are *Δ-equivalent* if there is an element $\delta \in \Delta$ such that $\delta z = z'$. We denote by $\{z\}_\Delta$ the Δ-equivalence class containing z and by $\mathcal{P}(\Delta)$ and by $\mathcal{Q}(\Delta)$ the set of all the Δ-equivalence classes of all the Δ-fixed points on $\mathfrak{H}$ with $|\Delta_z| = \infty$ and $|\Delta_z| < \infty$ respectively.

We denote by the same letter i, the maps

$$i : \mathcal{P}(\Delta) \longrightarrow \mathcal{P}(\Gamma) \tag{20}$$

and

$$i : \mathcal{Q}(\Delta) \longrightarrow \mathcal{Q}(\Gamma) \tag{21}$$

which are induced by the natural injection $\Delta \subset \Gamma = PSL(2, Z^{(p)})$. We say $\delta, \delta' \in \Delta$ *Δ-conjugate* (resp. *Δ^0-conjugate*) when there is an element $\eta \in \Delta$ (resp. $\eta \in \Delta^0$) such that $\delta = \eta \delta' \eta^{-1}$.

Let z be a Δ-fixed point. Then it is known that Δ_z is isomorphic to either a product of a finite cyclic group and an infinite cyclic group, or a finite cyclic group according to $\{z\}_\Delta \in \mathcal{P}(\Delta)$ or $\{z\}_\Delta \in \mathcal{Q}(\Delta)$ respectively (cf. [*CMP*] Vol. 1, p. 17 or [*CMP*], Vol. 2, p. 26). Let $P = \{z\}_\Delta \in \mathcal{P}(\Delta) \cup \mathcal{Q}(\Delta)$ and e_P be the order of the finite cyclic part. If $P \in \mathcal{P}(\Delta)$, let δ_P and ε_P be a generator of the infinite cyclic part and a generator of the finite cyclic part respectively. If $P \in \mathcal{Q}(\Delta)$, let ε_P be a generator of the finite cyclic group. We know that if $P \in \mathcal{P}(\Delta)$, then any eigenvalue ρ_P of δ_P is contained in Q_P and the absolute value of the p-order of ρ_P does not depend on a special choice of δ_P and ρ_P (cf. [*CMP*], Vol. 1, Chap. 1, p. 18). Therefore we define the *degree* of Δ-fixed points $P = \{z\}_\Delta \in \mathcal{P}(\Delta)$ by $\deg P = |\operatorname{ord}_P(\rho_P)|$. Moreover for any element $P \in \mathcal{P}(\Delta) \cup \mathcal{Q}(\Delta)$, we denote by ζ_P one of the characteristic roots of ε_P. It is a root of unity (cf. [*CMP*], Vol. 2, p. 25).

Now let $\mathcal{P}_\infty(\Delta) = \{P_0(1), \cdots, P_0(g_0)\}$ be the set of all Δ-equivalence classes of all the cuspidal points with respect to Δ^0. Clearly it is a finite set. Let

∞ denote the only such equivalence class of Γ. Let $\Gamma_\infty=\left\{\begin{pmatrix}*&*\\0&*\end{pmatrix}\in\Gamma\right\}$ and $\Gamma_\infty^{(r)}=\left\{\begin{pmatrix}1&*\\0&1\end{pmatrix}\in\Gamma\right\}$. We write $\Gamma=\bigcup_{i=1}^{g_0}\Delta\varphi^{(i)}\Gamma_\infty$, where $\varphi^{(i)}\in\Gamma$ satisfies $\varphi^{(i)}(\infty)=P_0(i)$. Here we may assume $\varphi^{(i)}\in\Gamma^0$ because $\Delta\backslash\Gamma=\Delta^0\backslash\Gamma^0$. We write $\Delta_{P_0(i)}=\varphi^{(i)}\Gamma_\infty\varphi^{(i)-1}\cap\Delta$ (resp. $\Delta_{P_0(i)}^{(r)}=\varphi^{(i)}\Gamma_\infty^{(r)}\varphi^{(i)-1}\cap\Delta$) and call it the decomposition group (resp. the innertia group) of $P_0(i)$. We denote the group index $[\varphi^{(i)}\Gamma_\infty\varphi^{(i)-1}/\varphi^{(i)}\Gamma_\infty^{(r)}\varphi^{(i)-1}:\ \Delta_{P_0(i)}/\Delta_{P_0(i)}^{(r)}]$ by $\deg P_0(i)=f_0(i)$ and call it the *degree* of $P_0(i)$. We call the set $\mathfrak{P}(\Delta)\cup\mathfrak{P}_\infty(\Delta)$ the *set of the prime divisors* of the group Δ.

Now the definition of the *zeta functions* $Z^H(u)=Z_k^H(\Delta;u)$ $(k=2,4,\cdots)$ *of the group* Δ is given by the following expression;

(22)

$$\log Z_k^H(\Delta;u)$$

$$=\sum_{m=1}^{\infty}\left[\sum_{\substack{\{\mathfrak{P}(\Delta)\ni P\\ \deg P\mid m\}}}\deg P\frac{1}{e_P}\sum_{j=1}^{e_P}\frac{(\rho_P^{\frac{m}{\deg P}}\zeta_P^j)^{k-1}-(\rho_P'^{\frac{m}{\deg P}}\zeta_P'^j)^{k-1}}{\rho_P^{\frac{m}{\deg P}}\zeta_P^j-\rho_P'^{\frac{m}{\deg P}}\zeta_P'^j}+\sum_{\substack{\{\mathfrak{P}_\infty(\Delta)\ni P\\ \deg P\mid m\}}}\deg P\right]\frac{(p^{k-1}u)^m}{m}.$$

This definition is a generalization of the zeta function $\zeta_\Gamma(u)$ in [*CMP*], Vol. 1, Chap. 1, p. 18.

2-2. *The first equality.* Now we shall study the relations between the Hecke polynomials $H_k(\Delta;u)$ and the zeta functions $Z_k^H(\Delta;u)$ of the group Δ. For this purpose, we shall study the Δ-fixed points which are caused by the torsions of Δ. First we see that $P_1=\left\{\omega=\frac{-1+\sqrt{-3}}{2}\right\}_\Gamma$ and $P_2=\{i=\sqrt{-1}\}_\Gamma$ are the only Γ-conjugacy classes of the fixed points on $\mathfrak{H}$ whose isotropy groups have torsions. Therefore, to study the torsion of Δ, let $\Gamma=\bigcup_{j=1}^{g_1}\Delta\varphi_1^{(j)}\Gamma_\omega$ $(\varphi_1^j\in\Gamma^0)$ and $\Gamma=\bigcup_{j=1}^{g_2}\Delta\varphi_2^{(j)}\Gamma_i$ $(\varphi_2^{(j)}\in\Gamma^0)$ be the double coset decompositions of Γ, and $P_1(1),\cdots,P_1(g_1)$ and $P_2(1),\cdots,P_2(g_2)$ be the corresponding Δ-conjugacy classes of points on $\mathfrak{H}$. Let

(23) $$\varphi_1^{(j)}(\Gamma_\omega\cap\Gamma^0)\varphi_1^{(j)-1}\subset\Delta^0 \text{ if and only if } j\leqq\nu_\omega$$

and

(24) $$\varphi_2^{(j)}(\Gamma_i\cap\Gamma^0)\varphi_2^{(j)-1}\subset\Delta^0 \text{ if and only if } j\leqq\nu_i.$$

Then $P_1(j)\in\mathfrak{P}(\Delta)$ and $P_2(j)\in\mathfrak{P}(\Delta)$ if and only if $p\equiv1 \bmod 3$ and $p\equiv1 \bmod 4$ respectively. Moreover $P_1(j)\in\mathfrak{Q}(\Delta)$ and $P_2(j)\in\mathfrak{Q}(\Delta)$ if and only if $p\equiv-1 \bmod 3$ or $p=2$ or 3 and $j\leqq\nu_\omega$ and $p\equiv-1 \bmod 4$ or $p=2$ or 3 and $j\leqq\nu_i$ respectively. Still more, if $P_1(j)$ and $P_2(j)\in\mathfrak{P}(\Delta)\cup\mathfrak{Q}(\Delta)$, then their ramification index is

$$e(P_1(j))=\begin{cases}3 & \cdots\ j\leqq\nu_\omega\\ 1 & \cdots\ j>\nu_\omega\end{cases} \tag{25}$$

and

$$e(P_2(j))=\begin{cases}2 & \cdots\ j\leqq\nu_i\\ 1 & \cdots\ j>\nu_i\,.\end{cases} \tag{26}$$

Then, if $e(P_1(j))$ or $e(P_2(j))\neq 1$, we see that we can put $\zeta_{P_1(j)}=\omega$ or $\zeta_{P_2(j)}=i$ respectively. All of these facts can be proved easily by using theorems in [*CMP*], Vol. 2, p. 25, p. 27, p. 31, p. 36 and p. 39. In the following, we put for $l=1, 2$

$$f_l(j)=\begin{cases}\deg P_l(j) & \cdots\ P_l(j)\in\mathcal{P}(\Delta)\\ 1 & \cdots\ P_l(j)\in\mathcal{Q}(\Delta)\end{cases} \tag{27}$$

to simplify the notations.

Now we shall quote some lemmas which are necessary to prove the first equality.

LEMMA 1. *Let r, k, l be integers.*

(i) *If $P\in\mathcal{P}(\Delta)$ or $P\in\mathcal{Q}(\Delta)$ and $r\neq 0$, then*

$$\{\delta_P^r\varepsilon_P^0\}_\Delta,\ \{\delta_P^{-r}\varepsilon_P^0\}_\Delta,\ \{\delta_P^r\varepsilon_P^1\}_\Delta,\ \{\delta_P^{-r}\varepsilon_P^1\}_\Delta,\ \cdots,\ \{\delta_P^r\varepsilon_P^{e_P-1}\}_\Delta,\ \{\delta_P^{-r}\varepsilon_P^{e_P-1}\}_\Delta,$$

$$\{\varepsilon_P^0\}_\Delta,\ \{\varepsilon_P^1\}_\Delta,\ \cdots,\ \{\varepsilon_P^{e_P-1}\}_\Delta$$

or

$$\{\varepsilon_P^0\}_\Delta,\ \{\varepsilon_P^1\}_\Delta,\ \cdots,\ \{\varepsilon_P^{e_P-1}\}_\Delta$$

are respectively all different.

(ii) *If $P\in\mathcal{P}(\Delta)$ and $r\neq 0$, then $\{\delta_P^r\varepsilon_P^l\}_\Delta\cap\Delta^{\deg P|r|+k}$ contains just*

$$\begin{cases}0 & \Delta^0\text{-conjugacy class} \quad \text{if} \quad k<0\\ \deg P & \Delta^0\text{-conjugacy classes if} \quad k=0\\ \deg P(p^k-p^{k-1}) & \Delta^0\text{-conjugacy classes if} \quad k>0\,.\end{cases}$$

(iii) *If Δ is a subgroup of $\Gamma=PSL(2, Z^{(p)})$ of finite index and $P\in\mathcal{P}(\Delta)\cup\mathcal{Q}(\Delta)$ with $e_P\neq 1$, then $\{\varepsilon_P^l\}_\Delta\cap\Delta^k$ $(l\not\equiv 0 \bmod e_P)$ contains just*

$$\begin{cases}\deg P & \Delta^0\text{-conjugacy classes if} \quad k=0\\ \deg P\left\{p^k-\left(\dfrac{Q(\zeta_P)}{p}\right)p^{k-1}\right\} & \Delta^0\text{-conjugacy classes if} \quad k>0\,,\end{cases}$$

where $\deg P$ *should be replaced by* 1 *if* $P\in\mathcal{Q}(\Delta)$, *and* $\left(\dfrac{Q(\zeta_P)}{p}\right)$ *denotes the Legendre symbol.*

(iv) *We take an element $\lambda\in\Gamma^0$ such that $\lambda(\Delta_{P_0(i)}\cap\Delta^0)\lambda^{-1}=\bigcup_{n=-\infty}^{\infty}\begin{pmatrix}1 & N\\ 0 & 0\end{pmatrix}^n$. Then we have*

$$\lambda\Delta_{P_0(k)}\lambda^{-1}=\left\{\begin{pmatrix}\beta & N\alpha\\ 0 & \beta^{-1}\end{pmatrix}\middle|\begin{matrix}\alpha\in Z^{(p)}\\ \beta\in(p^{f_0(i)})^Z\end{matrix}\right\}. \tag{28}$$

For the proof, see [*CMP*], Vol. 2, p. 10, p. 20, p. 27, p. 31, p. 36, p. 39.

LEMMA 2. *We have*

(i) *The Δ-equivalence class $P_0(i)$ contains just $f_0(i)$ cuspidal points.*

(ii)

$$\begin{aligned}\dim \mathfrak{S}_k(\Delta)=&\frac{k-1}{12}[\Gamma^0:\Delta^0]-\frac{1}{2}\sum_{i=1}^{g_0}f_0(i)+\frac{1}{3}\sum_{j=1}^{\nu_\omega}f_1(j)-\left\{\left\{\frac{k}{3}\sum_{j=1}^{\nu_\omega}f_1(j)\right\}\right\}\\&+\frac{1}{4}\sum_{j=1}^{\nu_i}f_2(j)-\left\{\left\{\frac{k}{4}\sum_{j=1}^{\nu_i}f_2(j)\right\}\right\}+\begin{cases}0 & \cdots k>2\\ 1 & \cdots k=2,\end{cases}\end{aligned} \tag{29}$$

where $\{\{x\}\}$ $(x\in Q)$ denotes the decimal part of x.

PROOF. (i) is special case of [*CMP*], Vol. 2, p. 14. (ii) is easy from the theorem of Riemann-Roch and from the fact that $P_1(j)$ $(j\leqq\nu_\omega)$ or $P_2(j)$ $(j\leqq\nu_i)$ contains just $f_1(j)$ elliptic points of order 3 or just $f_2(j)$ elliptic points of order 2 up to Δ^0-conjugacy. Q. E. D.

LEMMA 3. (The Eichler-Selberg trace-formula). *Let $\Delta^0\subset PSL(2,R)$ be any Fuchsian group of the first kind. Let δ be an element of $GL(2,R)/\pm1$ such that $\delta/\sqrt{\det(\delta)}$ does not belong to Δ^0 and that Δ^0 and $\delta^{-1}\Delta^0\delta$ are commensurable. Let $\Delta^0\delta\Delta^0$ act on the space of the cusp forms of the weight k $(k=2,4,\cdots)$ as before* (cf. § 1, (7)). *Let $S(\delta)$ be the trace of this linear endomorphism. Then $S(\delta)$ can be written, as*

$$S(\delta)=S_1(\delta)+S_2(\delta)+S_3(\delta), \tag{30}$$

where $S_i(\delta)$ $(i=1,2,3)$ are defined as follows;

(i)

$$S_1(\delta)=\sum_{\nu}\mathrm{Res}\,(\nu), \tag{31}$$

where ν moves all the representatives of all the elliptic Δ^0-conjugacy classes (i. e., such conjugacy classes that have a fixed point on $\mathfrak{H}$) contained in $\Delta^0\delta\Delta^0$, and if we denote the index of the centralizer of ν in Δ^0 by e_ν and the eigenvalues of ν by $\pm\{\rho_\nu,\rho'_\nu\}$, then

$$\mathrm{Res}\,(\nu)=-\frac{1}{2}\cdot\frac{1}{e_\nu}\cdot(\rho_\nu^{k-1}-\rho_\nu'^{k-1})/(\rho_\nu-\rho'_\nu). \tag{32}$$

(ii)

$$S_2(\delta)=\sum_{c}\sum_{\nu}\mathrm{Res}\,(\nu), \tag{33}$$

where c moves all the Δ^0-conjugacy classes of all the cuspidal points of Δ^0 and ν moves all the representatives of the left Δ^0-coset contained in $\Delta^0\delta\Delta^0$ and fixing c. Further, if we write $\lambda\Delta_c^0\lambda^{-1}=\bigcup_{n=-\infty}^{\infty}\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}^n$ and $\lambda\nu\lambda^{-1}/\sqrt{\det(\delta)}=$

$\begin{pmatrix} a_\nu & b_\nu \\ 0 & d_\nu \end{pmatrix}/\sqrt{a_\nu d_\nu}$ *with an element* $\lambda \in PSL(2, R)$ *and with mutually prime positive integers* a_ν *and* d_ν, *then*

$$\text{Res}(\nu) = \begin{cases} 0 & \cdots\ a_\nu > d_\nu \\ -\dfrac{a_\nu^{k-1} d_\nu^{-1}}{1-e^{2\pi i b_\nu}} (\det(\nu))^{\frac{k-2}{2}} & \cdots\ a_\nu = d_\nu \\ -a_\nu^{k-1} d_\nu^{-1} (\det(\nu))^{\frac{k-2}{2}} & \cdots\ a_\nu < d_\nu . \end{cases} \tag{34}$$

(iii) $S_3(\delta)$ *does not vanish only in the case of* $k=2$. *Then* $S_3(\delta)$ *is the arithmetical mean of the number of right* Δ^0*-cosets contained in* $\Delta^0\delta\Delta^0$ *and the number of left* Δ^0*-cosets contained in* $\Delta^0\delta\Delta^0$.

We quote this lemma from Eichler [4].

Now we can prove *the first equality*:

THEOREM 1. *Let* Δ *be a subgroup of finite index of* $PSL(2, Z^{(p)})$. *Then the Hecke polynomial* $H_k(\Delta; u)$ *can be expressed by means of the zeta function* $Z_k^H(\Delta; u)$ (cf. (22)) *of the group* Δ *as follows;*

$$H_k(\Delta; u) = Z_k^H(\Delta; u) \times c_1'(u) \times c_2'(u) , \tag{35}$$

where

$$c_1'(u) = (1-p^{k-1}u)^{-\varepsilon} , \tag{36}$$

$$c_2'(u) = \begin{cases} 1 & \cdots\ k > 2 \\ (1-u)(1-p^2u) & \cdots\ k = 2 , \end{cases} \tag{37}$$

and

$$\begin{aligned} \varepsilon = {} & \frac{(k-1)(p-1)}{12}[\Gamma : \Delta] \\ & + (p-1)\left[\frac{1}{3}\sum_{j=1}^{\nu_\omega} f_1(j) - \left\{\left\{\frac{k}{3}\sum_{j=1}^{\nu_\omega} f_1(j)\right\}\right\}\right] \\ & + (p-1)\left[\frac{1}{4}\sum_{j=1}^{\nu_i} f_2(j) - \left\{\left\{\frac{k}{4}\sum_{j=1}^{\nu_i} f_2(j)\right\}\right\}\right] \\ & + \frac{1}{3}\sum_{j=1}^{\nu_\omega} f_1(j)\left\{p - \left(\frac{-3}{p}\right)\right\} \begin{cases} 0 & \cdots\ k \equiv 1 \mod 3 \\ 1 & \cdots\ k \equiv -1 \mod 3 \\ -1 & \cdots\ k \equiv 0 \mod 3 \end{cases} \\ & + \frac{1}{4}\sum_{j=1}^{\nu_i} f_2(j)\left\{p - \left(\frac{-1}{p}\right)\right\}(-1)^{\frac{k-2}{2}} , \end{aligned} \tag{38}$$

where $\left(\dfrac{-1}{p}\right)$ *and* $\left(\dfrac{-3}{p}\right)$ *denote the Legendre symbols and* $\{\{x\}\}$ $(x \in Q)$ *denotes the decimal part of* x.

We note that $c_1'(u)$ (resp. $c_2'(u)$) is a correcting term which is caused by the volume of $\Delta^0\backslash\mathfrak{H}$ and the torsion of Δ^0 (resp. by the case $k=2$).

PROOF. By Proposition 3, we have only to prove

$$-tr\, U_k(\Delta, m) = \left(\text{the coefficient of } \frac{u^m}{m} \text{ in } \log Z^H(u)\right) + \varepsilon p^{m(k-2)} - \begin{cases} 0 & \cdots k>2 \\ 1+p^{2m} & \cdots k=2. \end{cases} \tag{39}$$

For this purpose, we shall calculate the trace of the Hecke operator $U_k(\Delta, m)$ using Lemma 3.

(i) The terms which come from the elliptic points.

First we shall calculate the term coming from $\{\delta_P^r \varepsilon_P^l\}_\Delta$ with $P \in \mathfrak{P}(\Delta)$ and $r \neq 0$. Let $\deg P = d$, $e_P = e$ and $m = |r|d + \mu$. We contend that

$$\begin{cases} 0 & \cdots \mu < 0 \\ -\deg P \cdot p^\mu \cdot \dfrac{1}{e} \displaystyle\sum_{l=0}^{e-1} \frac{(\rho_P^r \zeta_P^l)^{(k-1)} - (\rho_P'^r \zeta_P'^l)^{(k-1)}}{\rho_P^r \zeta_P^l - \rho_P'^r \zeta_P'^l} p^{m(k-2)} & \cdots \mu \geqq 0 \end{cases} \tag{40}$$

comes from $\Delta(P, r) = \bigcup_{l=0}^{e-1} [\{\delta_P^r \varepsilon_P^l\}_\Delta \cup \{\delta_P^{-r} \varepsilon_P^l\}_\Delta]$ to the trace of $T(m)$. Then, since $\mu = 0$ if and only if $\deg P = d \mid m$, we see that

$$\begin{cases} 0 & \cdots \deg P \nmid m \\ -\deg P \cdot \dfrac{1}{e} \cdot \displaystyle\sum_{l=0}^{e-1} \frac{(\rho_P^r \zeta_P^l)^{(k-1)} - (\rho_P'^r \zeta_P'^l)^{(k-1)}}{\rho_P^r \zeta_P^l - \rho_P'^r \zeta_P'^l} p^{m(k-2)} & \cdots \deg P \mid m \end{cases} \tag{41}$$

comes from $\bigcup_{r=0}^{m/\deg P} \Delta(P, r)$ into the trace of $U(m) = T(m) - p^{k-1} T(m-1)$. Therefore, just the first sum of the coefficients of u^m/m in $\log Z^H(u)$ comes from these conjugacy classes.

Now we shall prove the above contention. By Lemma 1, we know that $\{\delta_P^{\pm r} \varepsilon_P^l\}_\Delta \cap \Delta^{rd+i}$ contains just

$$\begin{cases} 0 & \cdots i<0 \\ \deg P & \cdots i=0 \\ \deg P(p^i - p^{i-1}) & \cdots i>0. \end{cases} \tag{42}$$

Δ^0-conjugacy classes. By the definition of ρ_P and ζ_P, their eigenvalues are $\pm\{\rho_P^{\pm r} \zeta_P^l, \rho_P'^r \zeta_P'^l\}$. Therefore, from each Δ^0-conjugacy class, there comes

$$-\frac{1}{2} \frac{1}{e} \frac{(\rho_P^{\pm r} \zeta_P^l)^{(k-1)} - (\rho_P'^{\pm r} \zeta_P'^l)^{(k-1)}}{(\rho_P^{\pm r} \zeta_P^l) - (\rho_P'^{\pm r} \zeta_P'^l)} p^{m(k-2)} \tag{43}$$

to the trace of $T(m)$. Now, by the definition of $\mathfrak{T}(\Delta, m)$ and $T(m)$, we must sum up from $l=0$ to $l=e_P-1$ and from $i=rd-m+1$ to $i=\mu$ with "two times of" above multiplicities (since r may be replaced by $-r$). Consequently we have the above contention.

We can calculate the term coming from $\{\varepsilon_P^l\}_{\Delta}$ with $P \in \mathcal{P}(\Delta) \cup \mathcal{Q}(\Delta)$, $e_P = e \neq 1$ and $l \neq 0$ in a similar way. We see that

$$(44) \quad -\deg P \cdot \frac{1}{2} \cdot \frac{1}{e} \sum_{l=1}^{e-1} \left[\left[p\left\{1 - \frac{1}{p}\left(\frac{Q(\zeta_P)}{p}\right)\right\} + \cdots + p^m\left\{1 - \frac{1}{p}\left(\frac{Q(\zeta_P)}{p}\right)\right\}\right] \times \frac{\zeta_P^{l(k-1)} - \zeta_P^{\prime l(k-1)}}{\zeta_P^l - \zeta_P^{\prime l}} \right] \cdot p^{m(k-2)}$$

comes from $E(P) = \bigcup_{l=1}^{e-1} \{\varepsilon_P^l\}_{\Delta}$ to the trace of $T(m)$. Therefore

$$(45) \quad -\deg P \cdot \frac{1}{2} \cdot \frac{1}{e} \cdot \left\{p - \left(\frac{Q(\zeta_P)}{p}\right)\right\} \cdot p^{m(k-2)} \cdot \sum_{l=1}^{e-1} \frac{\zeta_P^{l(k-1)} - \zeta_P^{\prime l(k-1)}}{\zeta_P^l - \zeta_P^{\prime l}}$$

comes from $E(P)$ to the trace of $U(m)$. Consequently, from torsions, there comes

$$(46) \quad -\frac{1}{3} \sum_{j=1}^{\nu_\omega} f_1(j)\left\{p - \left(\frac{-3}{p}\right)\right\} \begin{cases} 0 & \cdots k \equiv 1 \mod 3 \\ 1 & \cdots k \equiv -1 \mod 3 \\ -1 & \cdots k \equiv 0 \mod 3 \end{cases}$$
$$-\frac{1}{4} \sum_{j=1}^{\nu_i} f_2(j)\left\{p - \left(\frac{-1}{p}\right)\right\} p^{m(k-2)} (-1)^{\frac{k-2}{2}}$$

to the trace of $U(m)$.

(ii) The terms which come from the parabolic points.

Let $f_0(i) = d$ and $m = rd + \mu$. From Lemma 1 and from the definition of $\mathfrak{T}(\Delta, m)$, we know that $p^{\mu}\begin{pmatrix} 1 & p^{-\mu} \cdot l \\ 0 & p^{2rd} \end{pmatrix}$ $(0 \leqq l \leqq p^{m+rd} - 1)$ constitute the representatives of the left Δ^0-cosets contained in $\varphi^{(i)}\mathfrak{T}(\Delta, m)\varphi^{(i)-1} \cap \left\{\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}\right\}$. Therefore,

$$(47) \quad \begin{cases} 0 & \cdots r < 0 \\ -\frac{1}{2}(p^m - 1)p^{m(k-2)} & \cdots r = 0 \\ -p^{m-rd}p^{m(k-2)} & \cdots r > 0 \end{cases}$$

comes to the trace of $T(m)$. Therefore, summing up these terms,

$$(48) \quad -\frac{1}{2}(p^m - 1)p^{m(k-2)} - \sum_{0 < r \leqq m/d} p^{m-rd}p^{m(k-2)}$$

comes from the cuspidal points contained in $P_0(i)$ to the trace of $T(m)$. Therefore,

$$(49) \quad \begin{cases} -\frac{1}{2}p^{m(k-2)}(p-1) & \cdots f_0(i) \nmid m \\ -p^{m(k-2)} - \frac{1}{2}p^{m(k-2)}(p-1) & \cdots f_0(i) \mid m \end{cases}$$

comes to the trace of $U(m) = T(m) - p^{k-1}T(m-1)$. Consequently

$$(50)\qquad -p^{m(k-2)}\sum_{f_0(i)\mid m} f_0(i)-\frac{1}{2}(p-1)p^{m(k-1)}\sum_{i=1}^{g_0} f_0(i)$$

comes from the cuspidal points to the trace of $U(m)$.

(iii) The term which appears only in the case of $k=2$.

From Corollary 4 of Proposition 1, we see that $\mathfrak{T}(\Delta, m)$ contains just $p^{2m}+p^{2m-1}+\cdots+p^2+p$ right Δ^0-cosets and $p^{2m}+p^{2m-1}+\cdots+p^2+p$ left Δ^0-cosets. Therefore $p^{2m}+p^{2m-1}+\cdots+p^2+p$ comes to the trace of $T(m)$ only in the case of $k=2$. Therefore

$$(51)\qquad \begin{cases} 1 & \cdots\ k>2 \\ p^{2m}+p & \cdots\ k=2 \end{cases}$$

comes to the trace of $U(m)=T(m)-p^{k-1}T(m-1)$.

(iv) The term which comes from the identity operator.

From $p^m\Delta^0$, there comes $p^{m(k-2)}\dim \mathfrak{S}_k(\Delta)$ to the trace of $T(m)$. Therefore $-\dim \mathfrak{S}_k(\Delta)(p-1)p^{m(k-2)}$ comes to the trace of $U(m)=T(m)-p^{k-1}T(m-1)$. Well, by Lemma 2, this term is equal to

$$(52)\qquad -\frac{1}{12}(k-1)(p-1)[\Gamma:\Delta]p^{m(k-2)}+\frac{1}{2}(p-1)p^{m(k-2)}\sum_{i=1}^{g_0} f_0(i)$$
$$-(p-1)p^{m(k-2)}\Big[\frac{1}{3}\sum_{j=1}^{\nu_\omega} f_1(j)-\Big\{\Big\{\frac{k}{3}\sum_{j=1}^{\nu_\omega} f_1(j)\Big\}\Big\}\Big]$$
$$-(p-1)p^{m(k-2)}\Big[\frac{1}{4}\sum_{j=1}^{\nu_i} f_2(j)-\Big\{\Big\{\frac{k}{4}\sum_{j=1}^{\nu_i} f_2(j)\Big\}\Big\}\Big]-p^{m(k-2)}\begin{cases} 0 & \cdots\ k>2 \\ p-1 & \cdots\ k=2. \end{cases}$$

Now we add these five terms and prove the equation (39) (cf. Corollary 1 of Proposition 1). Q. E. D.

§ 3. Congruence zeta functions of fibre varieties.

3-1. *Quotations.* Let F_{p^2} be the finite field with p^2 elements and $\bar{F}_{p^2}$ be its algebraic closure. Let $j\in\bar{F}_{p^2}$, E_j be an elliptic curve with modulus j and $\mathcal{A}_j$ be the endomorphism ring of E_j. Now the following results are due to Deuring:

There may occur only two cases.

(i) $\mathcal{A}_j$ is isomorphic to an order of an imaginary quadratic number field K, where the conductor of $\mathcal{A}_j$ is prime to p and p decomposes in K. Moreover, $\mathcal{A}_j$ contains some units other than ±1 if and only if $j=0$ or 12^3. In this case, we call the modulus j a *singular modulus.*

(ii) $\mathcal{A}_j$ is isomorphic to a maximal order of the quaternion algebra D over Q in which only p and the infinite place ramify. Further, such a modulus j is contained in F_{p^2}. In this case, we call the modulus j a *supersingular modulus.* Hereafter we denote by S the set of all the supersingular moduli.

Now we shall cite a theorem from [*CMP*], Vol. 2, Chap. 5 on which our subsequent arguments rest.

THEOREM *CM. Let p be a prime number and Δ be a subgroup of finite index of $\Gamma = PSL(2, Z^{(p)})$. Then there is a finite algebraic extension L over the rational functional field $K = F_{p^2}(j)$ whose constant field is F_{p^2}, and there is a following commutative diagram;*

(53)
$$\begin{array}{ccc} \mathfrak{P}(\Delta) & \xrightarrow{\mathcal{J}_L} & \mathfrak{P}(L) \\ \Big\downarrow i & \circlearrowright & \Big\downarrow \pi \\ \mathfrak{P}(\Gamma) & \xrightarrow[\mathcal{J}_K]{} & \mathfrak{P}(K). \end{array}$$

Here $\mathfrak{P}(K)$ denotes the set of all the prime divisors of K which do not correspond to supersingular moduli or the infinite point ∞ and $\mathfrak{P}(L)$ denotes the set of all the prime divisors of L which lie on elements of $\mathfrak{P}(K)$. Moreover, horizontal maps $\mathcal{J}_L$ and $\mathcal{J}_K$ are degree preserving bijections, perpendicular maps i and π are induced by the natural injection and by the natural projection respectively. Still more closely, $\mathcal{J}_K$ is induced by the map

(54)
$$\mathfrak{P}(\Gamma) \ni P = \{z\}_\Gamma \longmapsto J(z) \bmod \mathfrak{P} \in \mathfrak{P}(K),$$

where $J(z)$ denotes the elliptic modular function, $\mathfrak{P}$ denotes a fixed prime divisor in the algebraic closure of Q which divides p, and in the right hand side we have identified $\mathfrak{P}(K)$ and the set $\{F_{p^2}$-conjugacy classes of all the singular moduli$\}$. Moreover, all the prime divisors belonging to $S-\{0, 12^3\}$ decompose completely in L.

REMARK 4. We see that $P_1 = \left\{\frac{-1+\sqrt{-3}}{2}\right\}_\Gamma$ and $P_2 = \{\sqrt{-1}\}_\Gamma$ correspond to $\{0\}_{F_{p^2}}$ and $\{12^3\}_{F_{p^2}}$ respectively by $\mathcal{J}_K$ (cf. [*CMP*], Vol. 2, Chap. 5).

REMARK 5. This theorem implies that the decomposition law of prime divisors in L/K can be described by means of "the decomposition law of prime divisors" in Γ/Δ. I remark that I have not described the decomposition law of the prime divisors $\{0\}_{F_{p^2}}$, $\{12^3\}_{F_{p^2}}$ and $\{\infty\}_{F_{p^2}}$ only because of the simplicity.

REMARK 6. Since $\mathcal{J}_L$ and $\mathcal{J}_K$ are degree preserving, we see easily $[\Gamma : \Delta] = [L : K]$.

3-2. *Construction of fibre varieties V_r and their congruence zeta functions.*

Let Ω be the universal domain of the characteristic p and $U_0 = \Omega - \{0, 12^3\}$. Let $\{E_j\}_{j \in U_0}$ be the family of elliptic curves defined by Tate's equation

(55)
$$Y^2Z + XYZ = X^3 - \frac{36}{j-12^3}XZ^2 - \frac{1}{j-12^3}Z^3 \quad \text{in} \quad P^2(\Omega).$$

Then this family has the following properties;

(i) E_j is an elliptic curve with modulus j which is defined over $F_{p^2}(j)$ and contained in the projective space $P^2(\Omega)$.

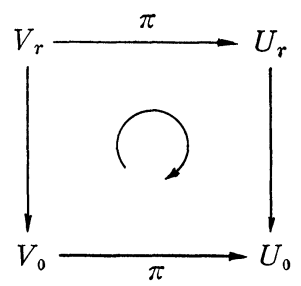
(ii) The correspondence $j \longmapsto E_j$ commutes with every specializations of j over F_{p^2}.

Now, for any integer $r \geqq 0$ we put

$$U_r = \bigcup_{j \in U_0} j \times \underbrace{E_j \times \cdots \times E_j}_{r \text{ copies}} \subset P^1(\Omega) \times \underbrace{P^2(\Omega) \times \cdots \times P^2(\Omega)}_{r \text{ copies}} . \tag{56}$$

Then U_r makes a fibre variety defined over F_{p^2} whose basic variety is U_0 and whose fibre at j is $E_j \times \cdots \times E_j$ (r copies).

By the way, since L is a finite algebraic extension of K, the complete non-singular model V of L over F_{p^2} makes a covering curve over $P^1(\Omega)$, which is a complete non-singular model of K over F_{p^2}. We identify U_0 with a subvariety of $P^1(\Omega)$ defined over F_{p^2} and denote by V_0 the subvariety of V which is made of all the points that are mapped into U_0 by the covering map. Then the covering map π induces a finite surjective algebraic morphism from V_0 to U_0 which is defined over F_{p^2}. We denote by V_r the fibre variety over V_0 which is induced from U_r by π. We note that V_r is a (non-complete) non-singular algebraic variety defined over F_{p^2} and that its fibre at $x \in V_0$ is $E_{\pi(x)} \times \cdots \times E_{\pi(x)}$ (r copies).



PROPOSITION 4. *We can calculate the number of $F_{p^{2m}}$-rational points on $x \times E_{\pi(x)} \times \cdots \times E_{\pi(x)} \subset V_r$ as*

$$N_r(L, x, m) = \begin{cases} 0 & \cdots\cdots \text{if } x \text{ is not rational over } F_{p^{2m}} \\ \{(\rho_x^{m/\deg(x)} - 1)(\rho_x'^{m/\deg(x)} - 1)\}^r & \\ & \cdots\cdots \text{if } x \text{ is rational over } F_{p^{2m}} . \end{cases} \tag{57}$$

Here we denote by $\{\rho_x, \rho_x'\}$ the characteristic roots of the Frobenius endomorphism of the elliptic curve $E_{\pi(x)}$ over $F_{p^2}(x)$ and $\deg(x) = [F_{p^2}(x) : F_{p^2}]$. We see that $\{\rho_x, \rho_x'\}$ is equal to $\pm\{p, p\}$ if $\pi(x)$ is supersingular and other than 0 and 12^3.

PROOF. Since $E_{\pi(x)}$ has $(\rho_x^{m/\deg(x)} - 1)(\rho_x'^{m/\deg(x)} - 1)$ $F_{p^{2m}}$-rational points if $\deg(x) \mid m$, we have immediately the first assertion. Now we assume that $\pi(x)$ is supersingular. Then $\deg(x) = 1$ (cf. Theorem *CM*). Moreover it is known that every supersingular elliptic curve over F_{p^2} whose modulus is other than 0 and 12^3 has $\pm\{p, p\}$ as its characteristic roots of the Frobenius endomorphism over F_{p^2} (cf. Proposition 5 of [*HP*]). Therefore we have the second assertion. Q. E. D.

Now let V_0^m ($m = 1, 2, 3, \cdots$) (resp. V_0^∞) be the set of all the $F_{p^{2m}}$-rational points on V_0 (resp. the set of all the $\bar{F}_{p^2}$-rational points on V_0). Then above

Proposition shows that the *congruence zeta function* $Z^c(u)=Z_r^c(L\,;u)$ of the fibre variety V_r over F_{p^2} can be written as

$$\log Z_r^c(L\,;u)=\sum_{m=1}^{\infty}\Big[\sum_{x\in V_0^m}\{(\rho_x^{m/\deg(x)}-1)(\rho_x'^{m/\deg(x)}-1)\}^r\Big]\frac{u^m}{m}. \tag{58}$$

LEMMA 4 (Lemma 3 of [*HP*]). *Let* $A_{k,r}(T)\in Z[T]$ $(0\leqq r\leqq k)$ *be the polynomials defined inductively by*

$$\begin{cases} A_{0,0}(T)=1 \\ A_{k+1,r}(T)=(T+1)A_{k,r}(T)-A_{k,r-1}(T)-TA_{k-1,r}(T)\,, \end{cases} \tag{59}$$

where $A_{k,r}(T)$ *should be replaced by* 0 *whenever* $0\leqq r\leqq k$ *is not satisfied. Then we have*

$$(X^{k-1}-Y^{k-1})/(X-Y)=\sum_{r=0}^{k-2}A_{k-2,r}(XY)\{(X-1)(Y-1)\}^r. \tag{60}$$

PROOF. Immediately by induction on r.

COROLLARY 1. *Let the notations be as in Proposition* 4. *Let* $\pi(x)$ *be a singular modulus, then we have*

$$\begin{aligned}(\rho_x^{\frac{m(k-1)}{\deg(x)}}-\rho_x'^{\frac{m(k-1)}{\deg(x)}})/(\rho_x^{m/\deg(x)}-\rho_x'^{m/\deg(x)}) \\ =\sum_{r=0}^{k-2}A_{k-2,r}(p^{2m})\{(\rho_x^{m/\deg(x)}-1)(\rho_x'^{m/\deg(x)}-1)\}^r\,.\end{aligned} \tag{61}$$

PROOF. Because $\rho_x\rho_x'=p^{2\deg(x)}$. Q. E. D.

COROLLARY 2.

$$(k-1)p^{m(k-2)}=\sum_{r=0}^{k-2}A_{k-2,r}(p^{2m})\{((\pm p)^m-1)((\pm p)^m-1)\}^r. \tag{62}$$

Now, for any polynomial $A(T)=\sum_{n=0}^{\infty}a_nT^n$ with integral coefficients, we put

$$Z^c(A\,;u)=Z_r^c(L,\,A\,;u)=\prod_{n=0}^{\infty}Z_r^c(L\,;p^nu)^{a_n}. \tag{63}$$

Then the corollaries of Lemma 4 show

PROPOSITION 5. *We have*

$$\begin{aligned}&\log\prod_{r=0}^{k-2}Z_r^c(L,\,A_{k-2,r}\,;u) \\ &=\sum_{m=1}^{\infty}\Big[\sum_{x\in V_0^m-\pi^{-1}(s)}\frac{\rho_x^{\frac{m(k-1)}{\deg(x)}}-\rho_x'^{\frac{m(k-1)}{\deg(x)}}}{\rho^{m/\deg(x)}-\rho'^{m/\deg(x)}}+\sum_{x\in\pi^{-1}(s-\{0,12^3\})}(k-1)p^{m(k-2)}\Big]\frac{u^m}{m}.\end{aligned} \tag{64}$$

PROOF. Because every element of $\pi^{-1}(s-\{0,12^3\})$ is rational over F_{p^2}. Q. E. D.

3-3. *The second equality.* Now we shall study the right hand side of (64) and show that they are equal to $\log Z_k^H(\Delta\,;u)$ up to correcting terms.

PROPOSITION 6. *We assume that a Δ-conjugacy class of Δ-fixed points $P=\{z\}_\Delta \in \mathfrak{P}(\Delta)$ and a prime rational cycle $P'=\{x\}_{F_{p^2}}$ on V_0 over F_{p^2} correspond by the map $\mathfrak{I}_L$ in Theorem CM. We denote, as before, a generator of Δ_z by δ_P, characteristic roots of δ_P by $\pm\{\rho_P, \rho'_P\}$ and the characteristic roots of the Frobenius endomorphism of $E_{\pi(x)}$ over $F_{p^2}(x)$ by $\{\rho_x, \rho'_x\}$. Then we have at first*

(i) *All the F_{p^2}-conjugate points $x \in \{x\}_{F_{p^2}}=P'$ have the same $\{\rho_x, \rho'_x\}$. So we define $\{\rho_{P'}, \rho'_{P'}\}=\{\rho_x, \rho'_x\}$ and $\deg P'=\deg(x)$. Then we have*

(ii) *$\{\rho_{P'}, \rho'_{P'}\}$ is equal to $p^{\deg P}\{\rho_P, \rho'_P\}$ up to the sign ± 1.*

PROOF. At first, we shall reduce it to the case of $\Delta=\Gamma$. Let P and P' be as above. Then Theorem *CM* shows that $\deg P=\deg P'$ and $\deg i(P)=\deg \pi(P')$. By the way, it is clear that $\rho_P=\rho_{i(P)}^{\deg P/\deg i(P)}$ and $\rho_x=\rho_{\pi(x)}^{\deg P'/\deg \pi(P')}$. Therefore we may assume $\Delta=\Gamma$.

Now we shall prove Proposition 6 in this case. Let j and j' be algebraic and conjugate over F_{p^2}. Then we have $j=j^{p^{2d}}$ with some positive integer d. We see that the Frobenius correspondence of degree p^{2d} on U_1, i. e.,

$$U_1 \ni (j, X, Y, Z) \longmapsto (j^{p^{2d}}, X^{p^{2d}}, Y^{p^{2d}}, Z^{p^{2d}}) \in U_1 \tag{65}$$

induces an $F_{p^2}(j)$-isogeny from E_j to $E_{j'}$. Therefore, by the result of Tate [**13**], E_j and $E_{j'}$ have the same characteristic roots of the Frobenius endomorphism over $F_{p^2}(j)$. Consequently we have $\{\rho_j, \rho'_j\}=\{\rho_{j'}, \rho'_{j'}\}$ and have proved the first assertion.

For the second assertion, let $E_{J(z)}$ be an elliptic curve with modulus $J(z)$ and $\mathfrak{P}$ be the prime divisor of p in $\bar{Q}$ which was fixed in Theorem *CM*. Then $E_{J(z)}$ has non-trivial complex multiplications because z is a fixed point of $PSL(2, Z^{(p)})$. Therefore $J(z)$ is integral and $E_{J(z)}$ has no defect at $\mathfrak{P}$. Let $J(z) \bmod \mathfrak{P}=j$, $\mathcal{O}_{J(z)}$ be the endomorphism ring of $E_{J(z)}$ and $\mathcal{O}_j$ be the endomorphism ring of E_j. Then it is well known that

$$\mathcal{O}_{J(z)} \cong \{k \in M_2(Z) \mid k[1, z]_Z \subset [1, z]_Z\}, \tag{66}$$

where $[1, z]_Z$ is the Z-lattice $Z+Zz \subset C$. Moreover $\mathcal{O}_j$ contains $\mathcal{O}_{J(z)}$ because E_j is $\bar{F}_{p^2}$-isomorphic to the reduction modulo $\mathfrak{P}$ of the elliptic curve $E_{J(z)}$ (cf. Shimura and Taniyama [**12**] p. 94). Since j is singular, we know that the imaginary quadratic number field $K=\mathcal{O}_{J(z)} \otimes_Z Q$ is isomorphic to $\mathcal{O}_j \otimes_Z Q$ and that p decomposes in K. We denote by $\mathcal{O}_1$ the maximal order of K and by $\mathfrak{p}$ and $\bar{\mathfrak{p}}$ the prime divisors of p in K.

Now let γ be a generator of Γ_z. Here, we may assume that $p^{\deg P}\gamma$ is contained in the matrix ring $M_2(Z)$ because the assertion (ii) does not change if we replace γ by a Γ-conjugate element (cf. Lemma 1). Then $p^{\deg P}\gamma$ is contained in $\mathcal{O}_{J(z)}$ because γ fixes z. Therefore its characteristic root $p^{\deg P}\rho_P$ is contained in $\mathcal{O}_{J(z)}$.

Since γ is contained in $PSL(2, Z^{(p)})$, $p^{\deg P}\rho_P$ is divisible only by primes

of K which divide p. Moreover, we may assume that $p^{\deg P}\rho_P\mathcal{O}_1$ is equal to $\mathfrak{p}^{2\deg P}$ from the definition of the degree of P. Consequently we have proved

$$\mathfrak{p}^{2\deg P}=p^{\deg P}\rho_P\mathcal{O}_1 \tag{67}$$

and

$$p^{\deg P}\rho_P\in\mathcal{O}_{J(z)}\subset\mathcal{O}_j\,. \tag{68}$$

By the way, we have from Proposition 4 of [*HP*]

$$\mathfrak{p}^{2\deg P'}=\rho_{P'}\mathcal{O}_1 \tag{69}$$

and

$$\rho_{P'}\in\mathcal{O}_j\,. \tag{70}$$

Therefore, since $\deg P=\deg P'$ from Theorem *CM* and $\mathcal{O}_j$ contains no other units than ±1 (because $j\neq0,\ 12^3$), we have $\pm p^{\deg P}\rho_P=\pm\rho_{P'}$. Q. E. D.

Now we can prove *the second equality:*

THEOREM 2. *Let p be a prime number, Δ be a subgroup of finite index of $PSL(2, Z^{(p)})$. Then we have the following relations between the zeta functions $Z_k^H(\Delta\,;u)$ $(k=2,4,6,\cdots)$ of the group Δ and the congruence zeta functions $Z_r^c(L\,;u)$ $(r=0,1,2,\cdots)$ of the fibre varieties V_r over F_{p^2};*

$$Z_k^H(\Delta\,;u)=\prod_{r=0}^{k-2}Z_r^c(L,\,A_{k-2,r}\,;u)\times c''(u)\,, \tag{71}$$

where $A_{k-2,r}(T)=\sum_{n=0}^{\infty}a_{n,k-2,r}T^n\in Z[T]$ denote the polynomials which were defined in Lemma 4,

$$Z_r^c(L,\,A_{k-2,r}\,;u)=\prod_{n=0}^{\infty}Z_r(L\,;p^nu)^{a_{n,k-2,r}}\,, \tag{72}$$

$$c''(u)=c_0''(u)c_1''(u)c_2''(u)c_3''(u)\,, \tag{73}$$

$$c_0''(u)=\prod_{i=1}^{g_0}(1-p^{f_0(i)(k-2)}u^{f_0(i)})^{-1}\,, \tag{74}$$

$$c_1''(u)=\begin{cases}1 & \cdots\ p\equiv-1 \bmod 3 \text{ or } p=2 \text{ or } 3\\ \displaystyle\prod_{j=1}^{\nu_\omega}\prod_{r=0}^{k-2}\prod_{l=0}^{2}\{1-p^{f_1(j)(k-2)}(\rho_1(j)^{f_1(j)}\omega^l)^r(\rho_1(j)''^{f_1(j)}\omega'^l)^{(k-2-r)}u^{f_1(j)}\}^{-1} & \\ \times\displaystyle\prod_{j=\nu_\omega+1}^{g_1}\prod_{r=0}^{k-2}\{1-p^{f_1(j)(k-2)}\rho_1(j)^{f_1(j)r}\rho_1(j)'^{f_1(j)(k-2-r)}u^{f_1(j)}\}^{-1} & \\ \cdots\ p\equiv1 \bmod 3\,,\end{cases} \tag{75}$$

$$(76)\qquad c_2''(u)=\begin{cases}1 & \cdots\ p\equiv -1 \bmod 4 \text{ or } p=2 \text{ or } 3\\ \prod_{j=1}^{\nu_i}\prod_{r=0}^{k-2}\prod_{l=0}^{1}\{1-p^{f_2(j)(k-2)}(\rho_2(j)^{f_2(j)}i^l)^r(\rho_2(j)'^{f_2(j)}i'^l)^{(k-2-r)}u^{f_2(j)}\}^{-1} & \\ \times\prod_{j=\nu_i+1}^{g_2}\prod_{r=0}^{k-2}\{1-p^{f_2(j)(k-2)}\rho_2(j)^{f_2(j)r}\rho_2(j)'^{f_2(j)(k-2-r)}u^{f_2(j)}\}^{-1} & \\ & \cdots\ p\equiv 1 \bmod 4,\end{cases}$$

$$(77)\qquad c_3''(u)=(1-p^{k-2}u)^{(H-I)[\Gamma:\Delta](k-1)}.$$

Here, H denotes the number $\#(S)$ of supersingular moduli and I denotes the number of supersingular moduli which are contained in $\{0, 12^3\}$.

We note that the correcting terms $c_0''(u)$, $c_1''(u)$ and $c_2''(u)$ are caused by the defects of V_0 at $\pi^{-1}(\infty)$, $\pi^{-1}(0)$ and $\pi^{-1}(12^3)$ respectively, and that the correcting term $c_3''(u)$ is caused by the fact that every element of $\pi^{-1}(S)$ corresponds to no Δ-fixed point.

REMARK 7. $j=0$ (resp. $j=12^3$) is supersingular if and only if $p\equiv -1$ (mod 3) or $p=2$ or 3 (resp. $p\equiv -1$ (mod 4) or $p=2$ or 3). Moreover

$$(78)\qquad H=\frac{1}{12}(p-1)+\frac{1}{3}\left\{1-\left(\frac{-3}{p}\right)\right\}+\frac{1}{4}\left\{1-\left(\frac{-1}{p}\right)\right\}.$$

PROOF. Since $S-\{0, 12^3\}$ contains $H-I$ elements and every element of $S-\{0, 12^3\}$ decomposes completely in L/K, $\pi^{-1}(S-\{0, 12^3\})$ contains $(H-I)[L:K]=(H-I)[\Gamma:\Delta]$ elements. Therefore, in view of Proposition 5, we need only to prove

$$(79)\qquad \sum_{\substack{\mathfrak{P}(\Delta)\ni P\\ \deg P\mid m\\ \pi(P)\neq P_1,P_2}}\deg P\,\frac{\rho_P^{\frac{m(k-1)}{\deg P}}-\rho_P'^{\frac{m(k-1)}{\deg P}}}{\rho_P^{\frac{m}{\deg P}}-\rho_P'^{\frac{m}{\deg P}}}=\sum_{x\in V_0^m-\pi^{-1}(s)}\frac{\rho_x^{\frac{m(k-1)}{\deg(x)}}-\rho_x'^{\frac{m(k-1)}{\deg(x)}}}{\rho_x^{\frac{m}{\deg(x)}}-\rho_x'^{\frac{m}{\deg(x)}}}.$$

By the definition of $\mathfrak{P}(L)$, we can rewrite the right side of (79) as

$$(80)\qquad \sum_{\substack{P'\in\mathfrak{P}(L)\\ \deg P'\mid m\\ \pi(P')\neq\{0\}_{F_{p^2}},\{12^3\}_{F_{p^2}}}}\ \sum_{x\in P'}\frac{\rho_x^{\frac{m(k-1)}{\deg(x)}}-\rho_x'^{\frac{m(k-1)}{\deg(x)}}}{\rho_x^{\frac{m}{\deg(x)}}-\rho_x'^{\frac{m}{\deg(x)}}}.$$

By the way, since P' contains $\deg P'=\deg(x)$ points and they have the same $\{\rho_{P'}, \rho_{P'}'\}=\{\rho_x, \rho_x'\}$ (cf. Proposition 6), we have

$$(81)\qquad \sum_{x\in P'}\frac{\rho_x^{\frac{m(k-1)}{\deg(x)}}-\rho_x'^{\frac{m(k-1)}{\deg(x)}}}{\rho_x^{\frac{m}{\deg(x)}}-\rho_x'^{\frac{m}{\deg(x)}}}=\deg P'\,\frac{\rho_{P'}^{\frac{m(k-1)}{\deg P'}}-\rho_{P'}'^{\frac{m(k-1)}{\deg P'}}}{\rho_{P'}^{\frac{m}{\deg P'}}-\rho_{P'}'^{\frac{m}{\deg P'}}}.$$

Now let $\mathfrak{I}_L(P)=P'$, then we have from Theorem *CM* and Proposition 6

$$(82)\qquad \deg P=\deg P',$$

$$(83)\qquad \pm p^{\deg P}\{\rho_P, \rho_P'\}=\pm\{\rho_{P'}, \rho_{P'}'\}.$$

Therefore the bijectivity of $\mathcal{J}_L$ implies (79). Q. E. D.

As a corollary of Theorem 1 and Theorem 2, we have

THEOREM 3. *We have*

$$H_k(\Delta\,;\,u)=\prod_{r=0}^{k-2} Z_r^c(L,\,A_{k-2,r}\,;\,u)\times\varepsilon(u)\,, \tag{84}$$

where

$$\varepsilon(u)=c_1'(u)c_2'(u)c_0''(u)c_1''(u)c_2''(u)c_3''(u) \tag{85}$$

is a correcting term.

University of Tokyo

References

[1] M. Deuring, Die Typen der Multiplicatorenringe elliptischer Funktionenkörper, Abh. Math. Sem. Univ. Hamburg, 14 (1941), 197–272.

[2] M. Deuring, Invarianten und Normalformen elliptischer Funktionenkörper, Math. Z., 47 (1941), 47–56.

[3] M. Deuring, Die Struktur der elliptischen Funktionenkörper und die Klassenkörper der imaginären quadratische Zahlkörper, Math. Ann., 124 (1952), 393–426.

[4] M. Eichler, Eine Verallgemeinerung der Abelschen Integral, Math. Z., 67 (1957), 267–298.

[5] Y. Ihara, Hecke polynomials as congruence ζ functions in elliptic modular case, Ann. of Math., 85 (1967), 267–295 (cited [HP]).

[6] Y. Ihara, On Congruence Monodromy Problems, Vol. 1, Lecture note at University of Tokyo, 1968 (cited [CMP] Vol. 1).

[7] Y. Ihara, On Congruence Monodromy Problems, Vol. 2, Lecture note at University of Tokyo, 1969 (cited [CMP] Vol. 2).

[8] M. Kuga and G. Shimura, On the zeta function of fibre variety whose fibres are abelian varieties, Ann. of Math., 82 (1965), 478–539.

[9] M. Mennicke, On Ihara's modular group, Invent. Math., 4 (1967), 202–228.

[10] A. Selberg, Harmonic analysis and discontinuous groups on weakly symmetric Riemannian spaces with applications to Dirichlet series, J. Indian Math. Soc., 20 (1956), 47–87.

[11] G. Shimura, Construction of class fields and zeta functions of algebraic curves, Ann. of Math., 85 (1967), 58–159.

[12] G. Shimura and Y. Taniyama, Complex multiplication of abelian varieties and its applications to number theory, Publ. Math. Soc. Japan, 1961.

[13] J. Tate, Endomorphisms of Abelian Varieties over Finite Fields, Invent. Math., 2 (1966), 134–144.