M. Koike
Nagoya Math. J.
Vol. 64 (1976), 87-96

ON p-ADIC PROPERTIES OF THE EICHLER-SELBERG TRACE FORMULA II

M. KOIKE

Introduction

Let $\mathfrak{S}_k$ be the space of cusp forms of weight k with respect to $SL(2, \boldsymbol{Z})$. Let p be a prime number and let $T_k(p)$ be the Hecke operator of degree p acting on $\mathfrak{S}_k$ as a linear endomorphism. Put $H_k(X) = \det(I - T_k(p)X + p^{k-1}X^2I)$, where I is the identity operator on $\mathfrak{S}_k$. $H_k(X)$ is a polynomial with coefficients of rational integers, which is called the Hecke polynomial.

In this paper, we shall prove the congruences between Hecke polynomials:

THEOREM. *Let $p \geq 5$ be a prime number and let α be a positive integer. Let k be an even positive integer such that $k \geq 2\alpha + 2$ and $\dim_C \mathfrak{S}_{k+p^\alpha-p^{\alpha-1}} < p^{k-\alpha-1}$. Then we have*

$$H_{k'}(X) \equiv H_k(X) \qquad (\mathrm{mod}\, p^\alpha \boldsymbol{Z}[X])$$

for every even positive integer $k' > k$ satisfying $k' \equiv k \,(\mathrm{mod}\, p^\alpha - p^{\alpha-1})$.

In the case of $\alpha = 1$, our theorem is a weaker version of the property of contraction of U_p, which was proved by Serre. The proof of our theorem makes essential use of the p-adic properties of the Eichler-Selberg trace formula which is finer than what was proved in our previous paper [2].

§ 1. Congruences between traces of Hecke operators.

We fix a prime number p once and for all. For each positive integer n, let $T_k(n)$ be the Hecke operator of degree n acting on $\mathfrak{S}_k$ as a linear endomorphism. The Eichler-Selberg trace formula for $T_k(n)$ reads as follows:

Received May 12, 1976.

https://doi.org/10.1017/S0027763000017566 Published online by Cambridge University Press

$$\text{(1)}\quad \begin{aligned} \operatorname{tr} T_k(n) = & \sum_{\{\rho,\rho'\}} \sum_{\mathfrak{o}\ni\rho} -\frac{h_{\mathfrak{o}}}{w_{\mathfrak{o}}} F^{(k-2)}(\rho,\rho') - \sum_{\substack{d\mid n \\ d>0,\, d\le\sqrt{n}}}{}' d^{k-1} \\ & + \delta(\sqrt{n})\frac{k-1}{12} n^{k/2-1} + \begin{cases} 0 & (k>2)\,, \\ \sum_{\substack{d\mid n\\ d>0}} d & (k=2)\,, \end{cases} \end{aligned}$$

where we use the same notations as in [2].

We shall prove finer congruences between traces of Hecke operators than what was proved in our previous paper [2]. Our result is as follows:

PROPOSITION. *We assume* $p \geq 5$. *Let* m *and* α *be positive integers. Put* $\operatorname{ord}_p m = \beta$. *Let* k' *and* k *be even positive integers satisfying* (1) $k' \equiv k \pmod{p^\alpha - p^{\alpha-1}}$ *and* (2) $k' > k \geq \operatorname{Max}\{2\alpha+2, \alpha+\beta+2\}$. *Then we have*

$$\operatorname{tr} T_{k'}(p^m) \equiv \operatorname{tr} T_k(p^m) \qquad (\operatorname{mod} p^{\alpha+\beta}) \, .$$

Remark. In order to prove congruences between traces of Hecke operators in our previous paper, we made use of the property that $h_{\mathfrak{o}}$ is merely a rational integer. On the other hand, the proof of Proposition makes essential use of the fact that $h_{\mathfrak{o}}$ is the number of proper $\mathfrak{o}$-ideal classes.

Proof. We consider the trace formula for $T_k(p^m) \bmod p^{\alpha+\beta}$. Since $k \geq 4$, the fourth summand is equal to zero. By the condition (2), the second (resp. third) summand is proved to be congruent to one (resp. zero) mod $p^{\alpha+\beta}$. Let us deal with the first summand. Let K be an imaginary quadratic field which contains ρ and ρ' and let $\left(\frac{K}{p}\right)$ denote Kronecker's symbol. In the case of $\left(\frac{K}{p}\right) = -1$ or 0, $F^{(k-2)}(\rho,\rho')$ is easily proved to be congruent to zero mod $p^{\alpha+\beta}$. So we may assume $\left(\frac{K}{p}\right) = 1$, $p = \mathfrak{p}\cdot\mathfrak{p}'$ with two prime ideals in K. If the conductor of $\mathfrak{o}$ is divisible by p, $F^{(k-2)}(\rho,\rho')$ is congruent to zero mod $p^{\alpha+\beta}$. Hence we may assume the conductor of $\mathfrak{o}$ is not divisible by p. Put $\mathfrak{p}_{\mathfrak{o}} = \mathfrak{p} \cap \mathfrak{o}$ and $\mathfrak{p}'_{\mathfrak{o}} = \mathfrak{p}' \cap \mathfrak{o}$. Let d be the smallest positive integer such that $\mathfrak{p}_{\mathfrak{o}}^d$ is principal. Put $\gamma = \operatorname{ord}_p d$. We may put $\mathfrak{p}_{\mathfrak{o}}^d = \pi\mathfrak{o}$ with $\pi \in \mathfrak{o}$, or what is the same as $\mathfrak{p}^d = \pi\mathfrak{o}_1$, $\mathfrak{o}_1$ being the maximal order of K. If ρ is not primitive, $F^{(k-2)}(\rho,\rho')$ is congruent to zero mod $p^{\alpha+\beta}$. So we may also assume that

ρ is primitive and that $\rho' \equiv 0 \pmod{\mathfrak{p}}$. Since $\rho \cdot \rho' = p^m$, we have $(\rho) = \mathfrak{p}'^m$. Hence $\mathfrak{p}'^{mp\gamma-\beta}$ is principal and it is proved that there exists an imaginary quadratic integer ρ_1 such that $\rho_1^{p\beta-\gamma} = \rho$. Therefore we have

$$F^{(k'-2)}(\rho, \rho') \equiv \frac{1}{\rho - \rho'} \cdot \rho^{k-1} \cdot \rho_1^{(k'-k)p\beta-\gamma} \qquad (\mathrm{mod}\ \mathfrak{p}^{\alpha+\beta-\gamma}) ,$$

$$\equiv \frac{\rho^{k-1}}{\rho - \rho'} \qquad (\mathrm{mod}\ \mathfrak{p}^{\alpha+\beta-\gamma}) ,$$

$$\equiv F^{(k-2)}(\rho, \rho') \qquad (\mathrm{mod}\ \mathfrak{p}^{\alpha+\beta-\gamma}) .$$

Since h_0 is divisible by d, we have $\mathrm{ord}_p h_0 \geq \gamma$. Hence we have $\dfrac{h_0}{w_0} F^{(k'-2)}(\rho, \rho') \equiv \dfrac{h_0}{w_0} F^{(k-2)}(\rho, \rho') \pmod{p^{\alpha+\beta}}$. Thus Proposition is completely proved. Q.E.D.

In cases of $p = 2, 3$, we can prove following propositions by the same arguments as above:

PROPOSITION. (Case of $p = 2$.) *Let m and α be positive integers. Put* $\mathrm{ord}_2 m = \beta$. *Let k' and k be even positive integers satisfying* (1) $k' \equiv k \pmod{2^\alpha}$ *and* (2) $k' > k \geq \mathrm{Max}\{2\alpha + 6, \alpha + \beta + 4\}$. *Then we have*

$$\mathrm{tr}\ T_{k'}(2^m) \equiv \mathrm{tr}\ T_k(2^m) \qquad (\mathrm{mod}\ 2^{\alpha+\beta}) .$$

PROPOSITION. (case of $p = 3$.) *Let m and α be positive integers. Put* $\mathrm{ord}_3 m = \beta$. *Let k' and k be even positive integers satisfying* (1) $k' \equiv k \pmod{3^\alpha - 3^{\alpha-1}}$ *and* (2) $k' > k \geq \mathrm{Max}\{2\alpha + 4, \alpha + \beta + 3\}$. *Then we have*

$$\mathrm{tr}\ T_{k'}(3^m) \equiv \mathrm{tr}\ T_k(3^m) \qquad (\mathrm{mod}\ 3^{\alpha+\beta}).$$

§ 2. Preliminary lemmas

Let $x_1, \cdots, x_N$ be indeterminates. For each positive integer n, we define $S_n(x_1, \cdots, x_N) = \sum_{i=1}^{N} x_i^n$ and $F_n(x_1, \cdots, x_N) = (-1)^n \sum_{1 \leq i_1 < \cdots < i_n \leq N} x_{i_1} \cdots x_{i_n}$. We simply write S_n and F_n instead of $S_n(x_1, \cdots, x_N)$ and $F_n(x_1, \cdots, x_N)$. It is obvious that $F_n = 0$ if n is greater than N. It is well known that there exist following relations between two functions S_n and F_n, which are called Newton's formulae;

$$S_n + S_{n-1}F_1 + \cdots + S_1 F_{n-1} + nF_n = 0 .$$

https://doi.org/10.1017/S0027763000017566 Published online by Cambridge University Press

By means of Newton's formulae, F_n (resp. S_n) can be described as a polynomial of S_i (resp. F_i) with $1 \leq i \leq n$ as follows:

$$F_n = \sum_{r=1}^{n} \sum_{\substack{1 \leq i_1 < \cdots < i_r \leq n \\ 1 \leq j_s \\ \sum_{s=1}^{r} i_s j_s = n}} a^{(n)}_{\binom{i_1, \cdots, i_r}{j_1, \cdots, j_r}} S_{i_1}^{j_1} \cdots S_{i_r}^{j_r} ,$$

$$S_n = \sum_{r=1}^{n} \sum_{\substack{1 \leq i_1 < \cdots < i_r \leq n \\ 1 \leq j_s \\ \sum_{s=1}^{r} i_s j_s = n}} b^{(n)}_{\binom{i_1, \cdots, i_r}{j_1, \cdots, j_r}} F_{i_1}^{j_1} \cdots F_{i_r}^{j_r} ,$$

where $a^{(n)}$ and $b^{(n)}$ are rational numbers. All these coefficients can be calculated as follows:

LEMMA 1. *We have*

$$a^{(n)}_{\binom{i_1, \cdots, i_r}{j_1, \cdots, j_r}} = \left((-1)^{\sum_{s=1}^{r} j_s} \prod_{s=1}^{r} j_s ! \, i_s^{j_s} \right)^{-1} , \tag{2}$$

and

$$b^{(n)}_{\binom{i_1, \cdots, i_r}{j_1, \cdots, j_r}} = (-1)^{\sum_{s=1}^{r} j_s} \frac{\left(\left(\sum_{s=1}^{r} j_s \right) - 1 \right) !}{\prod_{s=1}^{r} j_s !} n . \tag{3}$$

Proof. We use induction on n. It is obvious that (2) is valid for $n = 1$. Suppose that (2) is valid for all $a^{(\ell)}$ with $1 \leq \ell \leq n-1$. By Newton's formulae, we have $F_n = -\frac{1}{n}\left(S_n + \sum_{k=1}^{n-1} S_{n-k} F_k \right)$. If $i_1 = n$, (2) is obviously valid. So we may assume $i_1 < n$. Then we have

$$\begin{aligned} a^{(n)}_{\binom{i_1, \cdots, i_r}{j_1, \cdots, j_r}} &= -\frac{1}{n}\left((-1)^{\left(\sum_{s=1}^{r} j_s \right) - 1} \left[\sum_{s=1}^{r} \left\{ (j_s - 1) ! \, i_s^{j_s - 1} \prod_{k \neq s} j_k ! \, i_k^{j_k} \right\}^{-1} \right] \right) , \\ &= (-1)^{\sum_{s=1}^{r} j_s} \left(\prod_{s=1}^{r} j_s ! \, i_s^{j_s} \right)^{-1} \frac{1}{n} \sum_{s=1}^{r} i_s j_s , \\ &= (-1)^{\sum_{s=1}^{r} j_s} \left(\sum_{s=1}^{r} j_s ! \, i_s^{j_s} \right)^{-1} . \end{aligned}$$

Hence (2) is proved to be valid. Let us prove that (3) is valid. We also use induction on n. It is obvious that (3) is valid for $n = 1$. Suppose that (3) is valid for all $b^{(\ell)}$ with $1 \leq \ell \leq n-1$. By Newton's

https://doi.org/10.1017/S0027763000017566 Published online by Cambridge University Press

formulae, we have $S_n = -\left(nF_n + \sum_{k=1}^{n-1} S_{n-k}F_k\right)$. If $i_1 = n$, it is obvious that (3) is valid. So we may assume $i_1 < n$. Then we have

$$\begin{aligned} b^{(n)}_{\binom{i_1,\cdots,i_r}{j_1,\cdots,j_r}} &= -\sum_{s=1}^{r} (-1)^{\left(\sum_{s=1}^{r} j_s\right)-1} \frac{\left(\left(\sum_{s=1}^{r} j_s\right) - 2\right)!}{(j_s - 1)!\prod_{k \neq s} j_k!}(n - i_s) , \\ &= (-1)^{\sum_{s=1}^{r} j_s} \frac{\left(\left(\sum_{s=1}^{r} j_s\right) - 2\right)!}{\prod_{s=1}^{r} j_s!} \left(\sum_{s=1}^{r} j_s n - j_s i_s\right) , \\ &= (-1)^{\sum_{s=1}^{r} j_s} \frac{\left(\left(\sum_{s=1}^{r} j_s\right) - 1\right)!}{\sum_{s=1}^{r} j_s!} n . \end{aligned}$$

Therefore (3) is proved to be valid. Q.E.D.

By making use of Lemma 1, we can prove the following lemma:

LEMMA 2. *Let* $G(X) = \prod_{i=1}^{k} (1 - a_i X)$ *and* $H(X) = \prod_{j=1}^{\ell} (1 - b_j X)$ *be polynomials with coefficients of rational integers. Put* $s_n = S_n(a_1, \cdots, a_k)$, $t_n = S_n(b_1, \cdots, b_\ell)$, $\sigma_n = F_n(a_1, \cdots, a_k)$ *and* $\tau_n = F_n(b_1, \cdots, b_\ell)$. *Let* α *be a positive integer. Then the following statements are equivalent*:

(1) $s_n \equiv t_n \pmod{p^{\alpha + \mathrm{ord}_p n}}$ *for every* $n \geq 1$,

(2) $\sigma_n \equiv \tau_n \pmod{p^\alpha}$ *for every* n *with* $1 \leq n \leq \mathrm{Max}\,\{k, \ell\}$,

(3) $F(X) \equiv G(X) \pmod{p^\alpha \boldsymbol{Z}[X]}$.

Proof. It is obvious that the statements (2) and (3) are equivalent. So we shall show that the statements (1) and (2) are equivalent. Let N be any positive integer. We assume that $(1)_{N-1}$: $s_n \equiv t_n \pmod{p^{\alpha + \mathrm{ord}_p n}}$ for every $n \leq N - 1$ and $(2)_{N-1}$: $\sigma_n \equiv \tau_n \pmod{p^\alpha}$ for every $n \leq N - 1$. Under this assumption, we show that the following statements are equivalent:

$(1)_N$ $s_n \equiv t_n \pmod{p^{\alpha + \mathrm{ord}_p n}}$ for every $n \leq N$,

$(2)_N$ $\sigma_n \equiv \tau_n \pmod{p^\alpha}$ for every $n \leq N$.

By making use of (3) in Lemma 1, we have

$$s_N = -N\sigma_N + \sum_{r=1}^{N} \sum_{\substack{1 \leq i_1 < \cdots < i_r \leq N \\ 1 \leq j_s \\ \sum_{s=1}^{r} i_s j_s = N}} b^{(N)}_{\binom{i_1,\cdots,i_r}{j_1,\cdots,j_r}} \sigma_{i_1}^{j_1} \cdots \sigma_{i_r}^{j_r} ,$$

$$t_N = -N\tau_N + \sum_{r=1}^{N} \sum_{\substack{1 \le i_1 < \cdots < i_r \le N \\ 1 \le j_s \\ \sum_{s=1}^{r} i_s j_s = N}} b^{(N)}_{\binom{i_1, \cdots, i_r}{j_1, \cdots, j_r}} \tau_{i_1}^{j_1} \cdots \tau_{i_r}^{j_r} .$$

Since $\dfrac{\left(\sum_{s=1}^{r} j_s\right)!}{\prod_{s=1}^{r} j_s!}$ is a rational integer, $\dfrac{j_s}{N} b^{(N)}_{\binom{i_1, \cdots, i_r}{j_1, \cdots, j_r}}$ and $\dfrac{\left(\sum_{s=1}^{r} j_s\right)}{N} b^{(N)}_{\binom{i_1, \cdots, i_r}{j_1, \cdots, j_r}}$ are rational integers. Put $\beta = \mathrm{ord}_p N$ and $\gamma = \mathrm{Min}\left\{\mathrm{ord}_p j_1, \cdots, \mathrm{ord}_p j_s, \mathrm{ord}_p \sum_{s=1}^{r} j_s\right\}$. Then we have $\mathrm{ord}_p b^{(N)}_{\binom{i_1, \cdots, i_r}{j_1, \cdots, j_r}} \ge \beta - \gamma$. By the condition $(2)_{N-1}$, we have $\sigma_{i_s} \equiv \tau_{i_s} \pmod{p^\alpha}$ for every i_s with $1 \le i_s \le N-1$. Hence we have $\sigma_{i_s}^{j_s} \equiv \tau_{i_s}^{j_s} \pmod{p^{\alpha + \mathrm{ord}_p j_s}}$ for every i_s with $1 \le i_s \le N-1$. Therefore we have $s_N - N\sigma_N \equiv t_N - N\tau_N \pmod{p^{\alpha + \mathrm{ord}_p N}}$, so $s_N - t_N \equiv N(\sigma_N - \tau_N) \pmod{p^{\alpha + \mathrm{ord}_p N}}$. From this, it follows immediately that $(1)_N$ and $(2)_N$ are equivalent under the assumption that $(1)_{N-1}$ and $(2)_{N-1}$ are valid. Hence it is proved that (1) and (2) are equivalent. Q.E.D.

§ 3. Congruences between Hecke polynomials

For any even positive integer k, we put $C_k(X) = \det(I - T_k(p)X)$ and $H_k(X) = \det(I - T_k(p)X + p^{k-1}X^2 I)$ where I is the identity operator on $\mathfrak{S}_k$. $C_k(X)$ and $H_k(X)$ are polynomials with coefficients of rational integers. $H_k(X)$ is usually called the Hecke polynomial.

Combining results in § 1 and 2, we can prove the following:

THEOREM 1. *We assume $p \ge 5$. Let α be a positive integer. Let k be an even positive integer such that* (1) $k \ge 2\alpha + 2$ *and* (2) $\dim_C \mathfrak{S}_{k+p^\alpha - p^{\alpha-1}} < p^{k-\alpha-1}$. *Then we have*

$$H_{k'}(X) \equiv H_k(X) \qquad (\mathrm{mod}\ p^\alpha \boldsymbol{Z}[X]) ,$$
$$C_{k'}(X) \equiv C_k(X) \qquad (\mathrm{mod}\ p^\alpha \boldsymbol{Z}[X]) ,$$

for every even positive integer $k' > k$ satisfying $k' \equiv k$ $(\mathrm{mod}\ p^\alpha - p^{\alpha-1})$.

Proof. Since $k \ge 2\alpha + 2$, we have $H_k(X) \equiv C_k(X)$ $(\mathrm{mod}\ p^\alpha \boldsymbol{Z}[X])$. So we shall prove only $C_{k'}(X) \equiv C_k(X)$ $(\mathrm{mod}\ p^\alpha \boldsymbol{Z}[X])$. By the dimension formula for $\mathfrak{S}_k$, it is easily proved that $k + p^\alpha - p^{\alpha-1}$ also satisfies the condition (2) if k satisfies it. Hence we may prove our theorem only in case of $k' = k + p^\alpha - p^{\alpha-1}$. Let m be any positive integer such that

$m < \dim_C \mathfrak{S}_{k'}$, and put $\beta = \operatorname{ord}_p m$. By the condition (2), we have $\beta < k - \alpha - 1$, so we have $\alpha + \beta + 2 \leq k$. Hence, making use of Proposition 1, we have $\operatorname{tr} T_{k'}(p^m) \equiv \operatorname{tr} T_k(p^m) \pmod{p^{\alpha+\beta}}$. On the other hand, by the recursion formula for $T_k(p^m)$, we have $\operatorname{tr} T_k(p^m) \equiv \operatorname{tr} T_k(p)^m \pmod{p^{k-1}}$. Therefore we have $\operatorname{tr} T_{k'}(p)^m \equiv \operatorname{tr} T_k(p)^m \pmod{p^{\alpha+\beta}}$. Combining these congruences with Lemma 2, we obtain the proof of Theorem 1.

Q.E.D.

In cases of $p = 2, 3$, we can prove following theorems by the same arguments as above:

THEOREM 1 (Case of $p = 2$). *Let α be a positive integer. Let k be an even positive integer such that $k \geq 2\alpha + 6$ and $\dim_C \mathfrak{S}_{k+2^\alpha} < 2^{k-\alpha-3}$. Then we have*

$$H_{k'}(X) \equiv H_k(X) \qquad (\operatorname{mod} 2^\alpha \boldsymbol{Z}[X]) ,$$

for every even positive integer $k' > k$ satisfying $k' \equiv k \pmod{2^\alpha}$.

THEOREM 1 (Case of $p = 3$). *Let α be a positive integer. Let k be an even positive integer such that $k \geq 2\alpha + 4$ and $\dim_C \mathfrak{S}_{k+3^\alpha-3^{\alpha-1}} < 3^{k-\alpha-2}$. Then we have*

$$H_{k'}(X) \equiv H_k(X) \qquad (\operatorname{mod} 3^\alpha \boldsymbol{Z}[X]) ,$$

for every even positive integer $k' > k$ satisfying $k' \equiv k \pmod{3^\alpha - 3^{\alpha-1}}$.

We give an application of Theorem 1. In the rest of this section, we assume $p \geq 5$ for the sake of simplicity. Let $k' > k$ be even positive integers such that $k' \equiv k \pmod{p-1}$ and $k \geq 4$. Then, it is obvious that k satisfies the condition (2) in Theorem 1 for $\alpha = 1$. Put $n = \dim_C \mathfrak{S}_k$ and $n' = \dim_C \mathfrak{S}_{k'}$. It is clear that $\det(XI - T_k(p)) = X^n \det\left(I - \frac{1}{X} T_k(p)\right)$, where I is the identity operator on $\mathfrak{S}_k$. Therefore, from Theorem 1 follows

COROLLARY. *Under the above conditions, we have*

$$\det(XI_{k'} - T_{k'}(p)) \equiv X^{n'-n} \det(XI_k - T_k(p)) \qquad (\operatorname{mod} p\boldsymbol{Z}[X]) .$$

This result is equivalent to Serre's result [3, (i), Corollary to Theorem 6].

§ 4. p-adic Hecke polynomials

Let α be a positive integer. Put $X_\alpha = Z/(p^\alpha - p^{\alpha-1})Z$ if $p \neq 2$, and $X_\alpha = Z/2^{\alpha-2}Z$ if $p = 2$. $\{X_\alpha\}$ forms a projective system naturally. We have

$$X = \lim_{\leftarrow} X_\alpha = \begin{cases} Z_p \times Z/(p-1)Z & \text{if } p \neq 2\,, \\ Z_2 & \text{if } p = 2\,, \end{cases}$$

where Z_p is the ring of p-adic integers. The canonical homomorphism $Z \to X$ is injective. We identify Z with a dense subgroup of X through this homomorphism.

Let $\mathfrak{O}$ denote the ring of formal power series in X with coefficients in Z_p. Let $\mathfrak{m}$ be the maximal ideal of $\mathfrak{O}$. The powers of $\mathfrak{m}, \mathfrak{m}^n$, $n \geq 0$ define the $\mathfrak{m}$-adic topology on $\mathfrak{O}$.

We assume $p \geq 5$. Let $\{k_\alpha\}_{\alpha=1}^\infty$ be a sequence of monotonically increasing, even positive integers satisfying $k_\alpha \equiv k_{\alpha'} \pmod{p^\alpha - p^{\alpha-1}}$ if $\alpha' > \alpha$, $k_\alpha \geq 2^\alpha + 2$ and $\dim_C \mathfrak{S}_{k_\alpha + p^\alpha - p^{\alpha-1}} < p^{k_\alpha - \alpha - 1}$. Then $\{k_\alpha\}_{\alpha=1}^\infty$ has a limit in X, which is denoted by $\tilde{k}$. By means of Theorem 1, there exists a common $\mathfrak{m}$-adic limit of $\{H_{k_\alpha}(X)\}$ and of $\{C_{k_\alpha}(X)\}$ in $\mathfrak{O}$. Put $\tilde{H}_{\tilde{k}}(X) = \lim_{\alpha\to\infty} H_{k_\alpha}(X)$. It is clear that $\tilde{H}_{\tilde{k}}(X)$ depends only on $\tilde{k}$, but not on the choice of sequences $\{k_\alpha\}$ with $\lim k_\alpha = \tilde{k}$. We call $\tilde{H}_{\tilde{k}}(X)$ the p-adic Hecke polynomial.

In the case where $\tilde{k}$ belongs to $2Z$, we shall show that $\tilde{H}_{\tilde{k}}(X)$ coincides with the Fredholm determinant of the p-adic Hecke operator $\tilde{U}_{\tilde{k}}(p)$ and that $\tilde{H}_{\tilde{k}}(X)$ is an entire function.

Before this, we extend Lemma 1 as follows:

LEMMA 3. *Let* $G(X) = 1 + \sum_{n\geq 1} \sigma_n X^n$ *be a formal power series in* X *with coefficients* σ_n *in a field* K, *so that* $\log G(X) = \sum_{n\geq 1} (-1)^n \frac{(G(X)-1)^n}{n}$ *is also a formal power series in* X *with coefficients in* K, *which we write* $-\sum_{n\geq 1} \frac{s_n}{n} X^n$, *with* $s_n \in K$. *Then there exist following relations between* σ_n *and* s_n;

$$S_n = \sum_{r=1}^{n} \sum_{\substack{1\leq i_1 < \cdots < i_r \leq n \\ 1 \leq j_s \\ \sum_{s=1}^{r} i_s j_s = n}} b^{(n)}_{\binom{i_1,\cdots,i_r}{j_1,\cdots,j_r}} \sigma_{i_1}^{j_1} \cdots \sigma_{i_r}^{j_r}\,,$$

(4)

https://doi.org/10.1017/S0027763000017566 Published online by Cambridge University Press

$$\sigma_n = \sum_{r=1}^{n} \sum_{\substack{1\leq i_1<\cdots<i_r\leq n \\ 1\leq j_s \\ \sum_{s=1}^{r} i_s j_s = n}} a^{(n)}_{\binom{i_1,\cdots,i_r}{j_1,\cdots,j_r}} s_{i_1}^{j_1} \cdots s_{i_r}^{j_r} ,$$

where $a^{(n)}$ *and* $b^{(n)}$ *are the same as in Lemma* 1.

Proof. If $G(X)$ is a polynomial in X with coefficients in K, (4) is equal to (2) and (3) in Lemma 1. Put $G_n(X) = 1 + \sum_{i=1}^{n} \sigma_i X^i$ and $\log G_n(X) = (-1) \sum_{i\geq 1} \frac{s_i^{(n)}}{i} X^i$. Then it is clear that $s_i^{(n)} = s_i$ for all i with $i \leq n$. Hence, from Lemma 1, (4) follows immediately. Q.E.D.

Let $\tilde{k}$ be an even integer and let $D_{\tilde{k}}^{(p)}(X)$ be the Fredholm determinant of the p-adic Hecke operator $\tilde{U}_{\tilde{k}}(p)$ which is defined in [2].

THEOREM 2. *We have*

$$\tilde{H}_{\tilde{k}}(X) = D_{\tilde{k}}^{(p)}(X) , \qquad \text{for } \tilde{k} \in 2\boldsymbol{Z} .$$

Proof. Let $\{k_\alpha\}$ be a sequence of monotonically increasing, even positive integers satisfying $k_\alpha \equiv k_{\alpha'} \pmod{p^\alpha - p^{\alpha-1}}$ for every $\alpha' \geq \alpha$, $k_\alpha \leq 2\alpha + 2$, $\dim_C \mathfrak{S}_{k_\alpha + p^\alpha - p^{\alpha-1}} < p^{k_\alpha - \alpha - 1}$ and $\lim k_\alpha = \tilde{k}$. Put $H_{k_\alpha}(X) = 1 + \sum_{n\geq 1} \sigma_n^{(\alpha)} X^n$ and $\log H_{k_\alpha}(X) = -\sum_{n\geq 1} \frac{s_n^{(\alpha)}}{n} X_n$ with $\sigma_n^{(\alpha)}$ and $s_n^{(\alpha)}$ in $\boldsymbol{Z}$. When $\alpha \to \infty$, $\{\sigma_n^{(\alpha)}\}$ and $\{s_n^{(\alpha)}\}$ have p-adic limits which we deonte by σ_n and s_n respectively. Then we have $\tilde{H}_{\tilde{k}}(X) = 1 + \sum_{n\geq 1} \sigma_n X^n$. Since $\sigma_n^{(\alpha)}$ and $s_n^{(\alpha)}$ satisfy the relations (4), σ_n and s_n also satisfy the relations (4). Hence we have $\log H_{\tilde{k}}(X) = -\sum_{n\geq 1} \frac{s_n}{n} X^n$. On the other hand, we have $s_n^{(\alpha)} = \operatorname{tr} U_{k_\alpha}(p^n)$ by (41) in [1]. Hence, from Theorem 1 in [2], it follows that $s_n = \operatorname{tr} \tilde{U}_{\tilde{k}}(p)^n$. Therefore we have $\tilde{H}_{\tilde{k}}(X) = D_{\tilde{k}}^{(p)}(X)$. Q.E.D.

Since $D_{\tilde{k}}^{(p)}(X)$ is a p-adic entire function, we have the following:

COROLLARY. $\tilde{H}_{\tilde{k}}(X)$ *is a p-adic entire function for* $\tilde{k} \in 2\boldsymbol{Z}$.

Remark. It is obvious that the p-adic Hecke polynomials converge for all $x \in \boldsymbol{Z}_p$.

Remark. In cases of $p = 2, 3$, the same argument as above can be applied.

Remark. Recently, Prof. B. Dwork kindly let me know a direct proof of Theorem is obtained from Adolphson's thesis and, at the same time, the condition on $\dim_C \mathfrak{S}_{k+p^\alpha-p^{\alpha-1}}$ can be discarded.

REFERENCES

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

[2] M. Koike, On some p-adic properties of the Eichler-Selberg trace formula, Nagoya Math. J., vol. **56** (1974), 45–52.

[3] J.-P. Serre, Formes modulaires et fonctions zeta p-adiques, Modular functions of one variable III, Lecture note in math., Springer, Berlin-Heidelberg-New York, 1973.

Nagoya University