Hecke polynomials $H_k^{(p)}(u)$ ($p=2$ *or* 3)

Dedicated to Prof. Shôkichi Iyanaga on his 60th birthday

By Yasuo MORITA

(Comm. by Y. Kawada)

Introduction

Y. Ihara has shown in his paper "Hecke polynomials as congruence ζ functions in elliptic modular case" Ann. of Math. **85** (1967) that the Hecke polynomials $H_k^{(p)}(u)$ can be expressed by the congruence ζ functions $Z_r(u)$ of some algebraic varieties V_r defined over the prime field F_p of characteristic p. But in his paper the case of $p=2$ or 3 was not treated explicitly, and the purpose of this paper is to give the expression explicitly in this case. All the methods and results of this paper are similar to those of his paper. Later we shall often refer to his paper and call it in short [HP]. Finally, since the purpose of this paper is to supplement his work, the readers are assumed to have read [HP] and it is explained what is pertinent here.

§1. Deuring's works on elliptic curves and ζ functions of certain fibre varieties.

1-1. *Notations.* Let $p=2$ or 3 and Ω be a fixed universal domain, of characteristic p. For any positive power $q=p^d$ of p, we shall denote by F_q ($\subset\Omega$) and $\overline{F_q}$ ($\subset\Omega$) the finite field with q elements and its algebraic closure in Ω respectively. For any field k ($\subset\Omega$) a k-isomorphism class of one dimensional abelian variety defined over k will be called a k-elliptic curve. For any elliptic curve E let $j(E)$ be its modulus in the sense of Deuring [1], [2], and $\mathfrak{o}(E)$ be its endomorphism ring. We denote by Z, Q, K and $\mathfrak{o}_1$, respectively, the ring of rational integers, the rational number field, and imaginary quadratic number field, and its maximal order. For any order $\mathfrak{o}=Z+Zf\omega$ ($f\in Z$) of K where $\omega\in K$ satisfies $\mathfrak{o}_1=Z+Z\omega$, we shall call $f\mathfrak{o}_1$ its conductor. An $\mathfrak{o}$-ideal $\mathfrak{A}$ will be called a proper $\mathfrak{o}$-ideal if it satisfies $\mathfrak{o}=\{a\in K \mid a\mathfrak{A}\subset\mathfrak{A}\}$. We denote by $G_\mathfrak{o}$ the group of all proper $\mathfrak{o}$-ideal classes, by $h_\mathfrak{o}$ the number of proper $\mathfrak{o}$-ideal classes and by $w_\mathfrak{o}$ the number of $\mathfrak{o}$-units. We shall denote by $\mathfrak{S}_p$ the set of all orders $\mathfrak{o}$ of all imaginary quadratic fields K such that $\left(\frac{K}{p}\right)=1$ (where $\left(\frac{K}{p}\right)$ denotes the Legendre symbol) and that the conductors of $\mathfrak{o}$ are not divisible by p. For each $\mathfrak{o}\in\mathfrak{S}_p$, let $\mathfrak{p}$ be

a prime divisor of p in K. Put $\mathfrak{p}_{\mathfrak{o}}=\mathfrak{p}\cap\mathfrak{o}$, and denote by $d_{\mathfrak{o}}$ the order in $G_{\mathfrak{o}}$ of the proper $\mathfrak{o}$-ideal class represented by $\mathfrak{p}_{\mathfrak{o}}$.

REMARK 1. In our case we can check

$$\left(\frac{Q(\sqrt{-1})}{2}\right)=0,\ \left(\frac{Q(\sqrt{-3})}{2}\right)=-1,\ \left(\frac{Q(\sqrt{-1})}{3}\right)=-1,\ \left(\frac{Q(\sqrt{-3})}{3}\right)=0,$$

so in every $\mathfrak{o}\in\mathfrak{J}_p$, there are only two units, i.e. ±1.

1-2. *Endomorphism rings of elliptic curves.* Now we shall summarize Deuring's works on the endomorphism rings $\mathfrak{o}(E)$ of elliptic curves for our case $p=2$ or 3.

THEOREM D. (Deuring [1] p. 199-200 and §10). *For any j ($\neq0$, $\in\Omega$) let E_j be any elliptic curve with modulus j. Then $\mathfrak{o}(E_j)\in\mathfrak{J}_p$ if and only if $j\in\bar{F}_p$, and $\mathfrak{o}(E_j)\cong Z$ if and only if $j\notin\bar{F}_p$. For any given $\mathfrak{o}\in\mathfrak{J}_p$ there exist precisely $h_{\mathfrak{o}}$ distinct $j\in\bar{F}_p$ ($j\neq0$) such that $\mathfrak{o}(E_j)\cong\mathfrak{o}$, and the degree of such j over the prime field F_p is equal to $d_{\mathfrak{o}}$. They constitute $h_{\mathfrak{o}}/d_{\mathfrak{o}}$ distinct complete sets of conjugates over F_p.*

REMARK 2. (Deuring [1]). In our case of $p=2$ or 3, $\mathfrak{o}(E)$ is non-commutative if and only if its modulus $j=0$.

1-3. *Congruence ζ functions of elliptic curves.*

PROPOSITION 1. ([HP] p. 277). *Let $j\in\bar{F}_p$ ($j\neq0$), E be an $F_p(j)$-elliptic curve with modulus j, $\mathfrak{o}=\mathfrak{o}(E)\in\mathfrak{J}_p$ and $d_{\mathfrak{o}}$ be as before. Then the congruence ζ function $Z(u)$ of E over $F_p(j)$ has the form*

$$Z(u)=\frac{(1-\pi_{\mathfrak{o}}u)(1-\pi'_{\mathfrak{o}}u)}{(1-u)(1-p^{d}\mathfrak{o}u)} \tag{1}$$

where $\pi_{\mathfrak{o}}$ is an integer of K satisfying $\mathfrak{p}_{\mathfrak{o}}{}^{d}\mathfrak{o}=\pi_{\mathfrak{o}}\mathfrak{o}$, and $'$ denotes the conjugation of K over Q.

1-4. Now we shall define a canonical family of elliptic curves. For $j\in\Omega$ ($j\neq0$) let E_j be the locus of the following equation in the projective space $P^2(\Omega)$:

$$Y^2Z=X^3-X^2Z+j^{-1}Z^3 \qquad \text{for } p=3,$$

and

$$XY^2-XYZ=jX^3+j^{-1}Z^3 \qquad \text{for } p=2.$$

We can easily see that the assignment $\Omega-\{0\}\ni j\mapsto E_j$ satisfies the following two conditions:

(i) E_j is an $F_p(j)$-elliptic curve with modulus j,

(ii) the assignment $\Omega-\{0\}\ni j\mapsto E_j$ is compatible with specializations of j.

We shall later use only these two properties of the canonical family.

REMARK 3. (Igusa [4] p. 472). In our case we can see that the two defects $j=0,12^3$ for $p\neq 2,3$ come together to $j=0$ so that the canonical family has only two defects at $j=0$ and $j=\infty$.

1-5. *Fibre varieties.* The cannonical family $j\mapsto E_j$ being as above, let r be a non-negative integer, and put

$$V_r=\bigcup_{0\neq j\in\Omega}(j\times\overbrace{E_j\times\cdots\times E_j}^{r\text{ copies}})\subset S^1\times\overbrace{P^2\times\cdots\times P^2}^{r\text{ copies}}$$

where S^1 is the affine line and P^2 is the projective space $P^2(\Omega)$. By the properties of the canonical family this point set can be regarded as a fibre variety defined over the prime field F_p whose base is $S^1-\{0\}$ and whose fibre at a base point j is $E_j\times\cdots\times E_j$ (r copies). Let $Z_r(u)$ be the congruence ζ function of V_r over the prime field F_p, and for each positive integer $m\geqq 1$, let $N_m^{(r)}$ be the number of F_{p^m} rational points of V_r. Then we have

$$\log Z_r(u)=\sum_{m=1}^{\infty}\frac{1}{m}N_m^{(r)}u^m.$$

For each $j\in\overline{F}_p$ ($j\neq 0$) with $d_j\mid m$, the number of F_{p^m} rational points of E_j is equal to

$$1+p^m-\pi_j{}^{m/d_j}-\pi_j'{}^{m/d_j}=(1-\pi_j{}^{m/d_j})(1-\pi_j'{}^{m/d_j}),$$

where $d_j=[F_p(j):F_p]$, π_j and π_j' are the roots of the numerator of the ζ functions of E_j(cf. Lang [6] p. 164), so we have

$$N_m^{(r)}=\sum_{\substack{0\neq j\in F_p\\ d_j\mid m}}\{(1-\pi_j{}^{m/d_j})(1-\pi_j'{}^{m/d_j})\}^r. \tag{2}$$

For any non-negative integer r put

$$N^{(r)}(X,\ Y)=\{(1-X)(1-Y)\}^r,$$

$$F^{(r)}(X,\ Y)=\frac{X^{r+1}-Y^{r+1}}{X-Y},$$

and define the polynomials $A_{r,l}(T)\in Z[T]$ ($0\leqq l\leqq r$) inductively by

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

where $A_{r,l}(T)$ should be replaced by 0 whenever $0\leqq l\leqq r$ is not satisfied. We can prove by induction on r that

$$F^{(r)}(X,\ Y)=\sum_{l=0}^{r}A_{r,l}(XY)N^{(l)}(X,\ Y)\ . \tag{3}$$

We have by Theorem D, Proposition 1 and Remark 1

$$d_j=d_{\mathcal{O}},\quad \{\pi_j,\ \pi_j'\}=\pm\{\pi_{\mathcal{O}},\ \pi_{\mathcal{O}}'\}\ .$$

Now, for any even integer $r\geqq 0$, we have by Theorem D

$$\sum_{\substack{0\neq j\in F_p\\ d_j\mid m}}F^{(r)}(\pi_j^{m/d_j},\ \pi_j'^{m/d_j})=\sum_{\substack{\mathcal{O}\in\mathfrak{F}_p\\ d_{\mathcal{O}}\mid m}}h_{\mathcal{O}}F^{(r)}(\pi_{\mathcal{O}}^{m/d_{\mathcal{O}}},\ \pi_{\mathcal{O}}'^{m/d_{\mathcal{O}}}). \tag{4}$$

By (2), (3) and (4), we obtain

MAIN LEMMA 1. *For any even integer $r\geqq 0$ we have*

$$\sum_{l=0}^{r}A_{r,l}(p^m)N_m^{(l)}=\sum_{\substack{\mathcal{O}\in\mathfrak{F}_p\\ d_{\mathcal{O}}\mid m}}h_{\mathcal{O}}F^{(r)}(\pi_{\mathcal{O}}^{m/d_{\mathcal{O}}},\ \pi_{\mathcal{O}}'^{m/d_{\mathcal{O}}})\ . \tag{5}$$

§2. Hecke polynomials and their expressions by $Z_r(u)$.

2.1 Let $T_k(n)(n\geqq 1)$ be the Hecke operators acting on the space of cusp forms of negative even weight $-k$ with respect to $SL(2,\ Z)$. We shall define

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

and call them the Hecke polynomials, where u denotes an indeterminate and I denotes the identity map. Put

$$\begin{cases}U_k(p)=T_k(p)\\ U_k(p^m)=T_k(p^m)-p^{k-1}T_k(p^{m-2})\qquad (m\geqq 2)\ .\end{cases} \tag{6}$$

Using the well-known fact that the operators $T_k(p^m)$ can be represented simultaneously by diagonal matrices, we get

$$\log\ H_k^{(p)}(u)=-\sum_{m=1}^{\infty}\frac{1}{m}\ \mathrm{Tr}\ U_k(p^m)u^m\ . \tag{7}$$

(For details, see [HP] p. 285).

2-2. We have by the Eichler-Selberg trace formula (cf. [3] p. 229)

$$\begin{aligned}\mathrm{Tr}\ T_k(n)=&\sum_{\{\rho,\ \rho'\}}\sum_{\rho\in\mathcal{O}}\left\{-\frac{h_{\mathcal{O}}}{w_{\mathcal{O}}}F^{(k-2)}\{\rho,\ \rho'\}\right\}-\sum_{\substack{d\mid n\\ d\leqq\sqrt{n}}}{}'\ d^{k-1}\\ &+\delta(\sqrt{n})\cdot\frac{1}{12}\cdot(k-1)\cdot n^{\frac{1}{2}(k-2)}+\begin{cases}0 & \cdots\ k>2\\ \sum_{d\mid n}d & \cdots\ k=2\ .\end{cases}\end{aligned} \tag{8}$$

Here $\{\rho, \rho'\}$ runs over all pairs of mutually conjugate irrational quadratic integers with norm n, $\mathcal{O}$ runs over all orders of imaginary quadratic fields such that $\mathcal{O} \ni \rho$; $F^{(k-2)}(X, Y)$, $h_{\mathcal{O}}$ and $w_{\mathcal{O}}$ are as before; and in the second term $\sum'$, d^{k-1} should be replaced by $\frac{1}{2} \cdot d^{k-1}$ when $d=\sqrt{n}$ is a rational integer, and finally, $\delta(\sqrt{n})$ represents 1 resp. 0 when $\sqrt{n}$ is rational resp. irrational.

Using this trace formula (8) , we obtain

MAIN LEMMA 2 (cf. [HP] Lemma 6). *In our case of* $p=2$ *or* 3, *the trace of the operators* $U_k(p^m)$ $(m \geqq 1, k=2, 4, 6, \cdots)$ *can be witten as follows*:

$$\text{Tr } U_k(p^m) = \sum_{\substack{\mathcal{O} \in \mathcal{J}_p \\ d_{\mathcal{O}} \mid m}} \{-h_{\mathcal{O}} F^{(k-2)}(\pi_{\mathcal{O}}^{m/d_{\mathcal{O}}}, \pi_{\mathcal{O}}'^{m/d_{\mathcal{O}}})\} \tag{9}$$
$$-c(k, m) p^{\frac{1}{2} m(k-2)} - \begin{cases} 1 \cdots k>2 \\ -p^m \cdots k=2 \end{cases}$$

with $\quad c(k, m)=e(k, p) \cdot (-1)^{\frac{1}{2}(k-2)} \cdots m$ *odd*,

$$c(k, m)=\frac{1}{12}(k-1)(p-1)+\frac{1}{4}\left\{1-\left(\frac{-1}{p}\right)\right\} \cdot (-1)^{\frac{1}{2}(k-2)}$$
$$+\frac{1}{3}\left\{1-\left(\frac{-3}{p}\right)\right\}\begin{cases} 0 \cdots k \equiv 1 \pmod 3 \\ 1 \cdots k \equiv -1 \pmod 3 \\ -1 \cdots k \equiv 0 \pmod 3 \end{cases}$$

$$\cdots m \text{ even},$$

$$e(k, p)=\begin{cases} 1 \cdots k \equiv 0, 2 \pmod 8,\ p=2 \text{ or } k \not\equiv 1 \pmod 3 \text{ and } p=3 \\ 0 \cdots k \equiv 4, 6 \pmod 8,\ p=2 \text{ or } k \equiv 1 \pmod 3 \text{ and } p=3, \end{cases}$$

$$\left(\frac{-1}{p}\right)=\left(\frac{Q(\sqrt{-1})}{p}\right) \text{ and } \left(\frac{-3}{p}\right)=\left(\frac{Q(\sqrt{-3})}{p}\right).$$

SKETCH OF THE PROOF. We shall call a quadratic integer ρ primitive if $p^{-1}\rho$ is not an integer. Put $\mu=\frac{1+\sqrt{-1}}{\sqrt{2}}$, $\omega=\frac{-1+\sqrt{-3}}{2}$ and

$$I_1(m)=\left\{ \{\rho, \rho'\} \;\middle|\; \rho\rho'=p^m,\ \rho \text{ primitive}, \left(\frac{Q(\rho)}{p}\right)=1 \right\},$$

$$I_2(m)=\left\{ \{\rho, \rho'\} \;\middle|\; m \text{ odd}, \rho=(-p)^{\frac{1}{2}m} \text{ or } \begin{cases} (-2)^{\frac{1}{2}m}\mu \text{ or } -(-2)^{\frac{1}{2}m}\mu \cdots p=2 \\ (-3)^{\frac{1}{2}m}\omega \text{ or } -(-3)^{\frac{1}{2}m}\omega \cdots p=3 \end{cases} \right\},$$

$$I_3(m)=\left\{ \{\rho, \rho'\} \;\middle|\; m \text{ even}, \rho(-p)^{-\frac{1}{2}m} = \text{root of unity in } Q(\rho) \text{ other than } \pm 1 \right\},$$

$$I_4(m)=\left\{\{\rho,\ \rho'\}\ \middle|\ \rho\rho'=p^m,\ \rho\neq\text{primitive},\left(\frac{Q(\rho)}{p}\right)=1\right\}.$$

Now we can decompose the first summation term on the right-hand side of the trace formula as below (cf. Remark 1):

$$\sum_{\{\rho,\rho'\}}\sum_{\rho\in\mathcal{O}}\left\{-\frac{h_{\mathcal{O}}}{w_{\mathcal{O}}}F^{(k-2)}(\rho,\ \rho')\right\}=\sum_{\{\rho,\rho'\}\in I_1(m)}\sum_{\rho\in\mathcal{O}}+\sum_{\{\rho,\rho'\}\in I_2(m)}\sum_{\rho\in\mathcal{O}}$$
$$+\sum_{\{\rho,\rho'\}\in I_3(m)}\sum_{\rho\in\mathcal{O}}+\sum_{\{\rho,\rho'\}\in I_4(m)}\sum_{\rho\in\mathcal{O}}.$$

As to the first, third and fourth terms of the right-hand side of this equation, the results are similar to the corresponding terms of [HP] (cf. [HP] §5 (54), (56) and (67)). As to the second term (cf. [HP] p. 292 (62)),

$$\delta_1(m)=\sum_{\{\rho,\rho'\}\in I_2(m)}\sum_{\rho\in\mathcal{O}}\left\{-\frac{h_{\mathcal{O}}}{w_{\mathcal{O}}}F^{(k-2)}(\rho,\ \rho')\right\}$$
$$=\begin{cases}-(-p)^{\frac{1}{2}m(k-2)}(1+p+\cdots+p^{\frac{1}{2}(m-1)})\times e(k,\ p) & \cdots m\text{ odd}\\ 0 & \cdots m\text{ even}.\end{cases}$$

This term appears in the trace of $U_k(p^m)$ as

$$-p^{k-1}\delta_1(m-2)+\delta_1(m)=\begin{cases}-(-p)^{\frac{1}{2}m(k-2)}\times e(k,\ p) & \cdots m\text{ odd}\\ 0 & \cdots m\text{ even}.\end{cases}$$

So, by comparing this term to the corresponding term of [HP], we can prove Main Lamma 2 (cf. [HP] p. 294 (71)).

REMARK 4. In [HP] p. 287, the term $\frac{p-1}{12}-H-\Delta$ in c_k is mistaken and should be replaced by $\frac{p-1}{12}-H+\Delta$.

2-3. By Main Lemma 1 and Main Lemma 2, we have

$$-\operatorname{Tr}U_k(p^m)=\sum_{l=0}^{k-2}A_{k-2,\,l}(p^m)N_m^{(l)}$$
$$+\begin{cases}c(k,\ 1)p^{\frac{1}{2}m(k-2)} & \cdots m\text{ odd}\\ c(k,\ 2)p^{\frac{1}{2}m(k-2)} & \cdots m\text{ even}\end{cases}+\begin{cases}1 & \cdots k>2\\ -p^m & \cdots k=2.\end{cases}\tag{10}$$

Now for any polynomials $A(T)=\sum_{n\geq 0}a_nT^n\in Z[T]$ and for any non-negative integer r, we shall define

$$Z_r(A, u) = \prod_{n \geq 0} Z_r(p^n u)^{a_n}, \tag{11}$$

where $Z_r(u)$ are the congruence ζ functions of the fibre varieties V_r over the prime field F_p. Since the Hecke polynomials can be written as

$$H_k^{(p)}(u) = \exp\left\{ -\sum_{m=1}^{\infty} \frac{1}{m} \operatorname{Tr} U_k(p^m) u^m \right\}, \tag{12}$$

so from (10), (11) and (12) we obtain by simple computations the following Theorem.

MAIN THEOREM. *In our case of $p=2$ or 3 the Hecke polynomials $H_k^{(p)}(u)$ $(k=2, 4, 6 \cdots)$ can be written by means of the congruence ζ functions of the fibre varieties V_r as*

$$H_k^{(p)}(u) = \prod_{l=0}^{k-2} Z_l(A_{k-2,l}, u) \times \Delta_k(u), \tag{13}$$

where

$$\Delta_k(u) = (1 - p^{\frac{1}{2}(k-2)} u)^{-\frac{1}{2}\{c(k,1)+c(k,2)\}} \times (1 + p^{\frac{1}{2}(k-2)} u)^{-\frac{1}{2}\{-c(k,1)+c(k,2)\}} \times \begin{cases} (1-u)^{-1} \cdots & k>2 \\ (1-pu) \quad \cdots & k=2 . \end{cases}$$

REMARK 5. We can easily see that $c(k, 1) \pm c(k, 2) \equiv 0 \pmod 2$, so the first two factors of $\Delta_k(u)$ are rational functions of u.

REMARK 6. In [HP], the factor of $\Delta_k(u)$ which contains c_k is not correct because c_k depends on m; it should be corrected as above.

University of Tokyo

References

[1] M. Deuring, Die Typen der Multipikatorenringe elliptischer Funktionenkörper, Abh. Math. Sem. Hamburg **14** (1941), 197-272.

[2] ———, Zur Theorie der elliptischen Funktionenkörper, Abh. Math. Sem. Hamburg **15** (1947), 211-261.

[3] M. Eichler, Quadratische Formen und Modulfunktionen, Acta Arith. **4** (1958), 217-239.

[4] J. Igusa, Fibre system of Jacobian varieties III, Amer. J. Math. **81** (1959), 453-476.

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

[6] S. Lang, Abelian varieties, Tracts in Math. No. 7.

(Received March 15, 1968)