ILLINOIS JOURNAL OF MATHEMATICS
Volume 24, Number 1, Spring 1980

THE U_p-OPERATOR OF ATKIN ON MODULAR FUNCTIONS OF LEVEL THREE

BY

ALAN ADOLPHSON

1. Introduction

In [7] Dwork determines the number of p-adic unit eigenvalues of Atkin's U_p-operator on modular functions of level 2. He applies these techniques in [8] to modular functions of level 3. After lengthy calculation, he obtains an answer when $p \equiv 1 \pmod 3$ but leaves unsettled the case $p \equiv -1 \pmod 3$. In [2], we gave a new proof of Dwork's result in the level 2 case. In this work, we extend this method to the level 3 case. We determine the number of unit eigenvalues when $p \equiv 1 \pmod 3$ (Corollary 1 to the main theorem) and give an upper bound for this number when $p \equiv -1 \pmod 3$ (Corollary 1 to Proposition 1).

In Section 2, we discuss the Hasse invariant and compute its values at certain points. The computation is based on the fact that after a change of variable the Hasse invariant satisfies a hypergeometric differential equation (see [8]). Theorem 1 is in [8], but we offer a different proof based on Lemma 1 and the infinite product for det $(I - tU_p)$. This avoids the need for an a priori upper bound on the degree of det $(I - tU_p) \pmod p$. Our Main Theorem (the principal result of [8]) is deduced as a corollary of Theorem 2, rather than by a computation involving differential operators as in [8]. For the final step, however, we still rely on a result of Dwork (Lemma 3). In fact, we feel our approach reveals the significance of Dwork's lemma.

I am indebted to B. Dwork for providing me with a copy of his manuscript [8] and for suggesting improvements to the original version of this work. I would also like to thank B. Dwork and S. Sperber for pointing out errors in the original version.

Throughout this paper, p is a prime $p \geq 5$. We let $\mathbf{F}_p$ denote the prime field of p elements, $\bar{\mathbf{F}}_p$ its algebraic closure, $\mathbf{Q}_p$ the field of p-adic numbers, $\mathbf{Z}_p$ the ring of p-adic integers. If f is a polynomial with coefficients in $\mathbf{Z}_p$, we write $\bar{f}$ for the polynomial with coefficients in $\mathbf{F}_p$ which are the reductions mod $p\mathbf{Z}_p$ of the coefficients of f. If $\alpha, \beta \in \mathbf{Z}_p[[t]]$ are such that $(\alpha - \beta) \in p\mathbf{Z}_p[[t]]$ we will write $\alpha \equiv \beta \pmod p$. We use the standard notation for hypergeometric functions [9, p. 162]:

$$F(a, b; c; \lambda) = \sum_{j=0}^{\infty} ((a)_j(b)_j/(c)_j\, j!)\lambda^j$$

Received May 31, 1977.

where for any non-negative integer j and $a \in \mathbf{Q}_p$, $(a)_0 = 1$, $(a)_j = \prod_{s=0}^{j-1} (a+s)$ for $j > 0$.

2. The level three Hasse invariant

Consider the family of elliptic curves given by the projective equation

$$X_1^3 + X_2^3 + X_3^3 - 3\mu X_1 X_2 X_3 = 0, \tag{2.1}$$

where $\mu \in \bar{\mathbf{F}}_p$, $\mu^3 \neq 1$. An explicit formula for the Hasse invariant of this family has been given by Katz [11, equ. (2.3.7.20)]. Define $h(\mu) \in \mathbf{Z}_p(\mu)$ by

$$h(\mu) = \mu^{p-1} \sum_{j=0}^{[(p-1)/3]} ((1/3)_j(2/3)_j/j!\,j!)\mu^{-3j} \tag{2.2}$$

where [ ] denotes the greatest integer function. Then $\bar{h}(\mu)$ is the Hasse invariant of (2.1). We have

$$h(\mu) = \begin{cases} \displaystyle\sum_{j=0}^{(p-1)/3} ((1/3)_j(2/3)_j/j!\,j!)\mu^{p-1-3j} & \text{if } p \equiv 1 \pmod 3 \\ \displaystyle\sum_{j=0}^{(p-2)/3} ((1/3)_j(2/3)_j/j!\,j!)\mu^{p-1-3j} & \text{if } p \equiv -1 \pmod 3). \end{cases} \tag{2.3}$$

Thus in either case $\deg h(\mu) = p - 1$, and $\mu \mid h(\mu)$ iff $p \equiv -1 \pmod 3$.

For later use, we calculate $\bar{h}(\omega)$, where $\omega^3 = 1$. From [5, (8.4)], it follows that the periods of the differential of the first kind on (2.1) satisfy the differential equation

$$(\mu^3 - 1)y'' + 3\mu^2 y' + \mu y = 0. \tag{2.4}$$

By [13], the polynomial $h(\mu)$ satisfies eq. (2.4). Making the change of variable $\lambda = \mu^3$ and multiplying by a constant transforms (2.4) into

$$\lambda(1-\lambda)y'' + ((2-5\lambda)/3)y' - y/9 = 0 \tag{2.5}$$

(where y', y'' now denote derivatives with respect to λ). The point is that (2.5) is a classical hypergeometric equation [9, p. 161] and its properties are well known. It is satisfied by $F(1/3, 1/3; 1; 1-\lambda)$.

Suppose first $p \equiv 1 \pmod 3$. Put

$$B(\lambda) = \sum_{j=0}^{p-1} ((1/3)_j/j!)^2 \lambda^j \in \mathbf{Z}_p[\lambda].$$

Then by [6, Cor. 1 to Lemma 1 and (3.2′)],

$$B(\lambda) \equiv F(1/3, 1/3; 1; \lambda)/F(1/3, 1/3; 1; \lambda^p) \pmod p.$$

Hence $\bar{B}(1-\lambda)$ satisfies (2.5). It is easily seen that $\deg \bar{B} = (p-1)/3$. Thus $\bar{B}(1-\mu^3)$ satisfies (2.4) and has degree $p-1$ in μ. Since $\bar{h}(\mu)$ has these same properties, and since -1 is the unique root of the indicial equation of equ. (2.4), it follows that $\bar{B}(1-\mu^3)$ is a constant multiple of $\bar{h}(\mu)$. Comparing coefficients of μ^{p-1} we conclude (since $(-1)^{(p-1)/3}=1$) that $\bar{h}(\mu)=\bar{B}(1-\mu^3)$, hence if $\omega^3=1$, $\bar{h}(\omega)=\bar{B}(0)=1$.

Now suppose $p\equiv -1 \pmod 3$. Put

$$C(\lambda)=\lambda^{(2p-1)/3}\sum_{j=0}^{p-1}((1/3)_j(2/3)_j/j!\,j!)\lambda^{-j}.$$

Note that $(1/3)_j(2/3)_j/j!\,j!$ is a p-adic integer and is divisible by p for $(p-2)/3<j\le p-1$. Hence $\bar{C}(\lambda)$ is a polynomial of degree $(2p-1)/3$. By [6, Cor. 2 to Lemma 1 and equ. (3.2′) with $s=0$],

$$C(\lambda)/\lambda^{(2p-1)/3}\equiv F(1/3,2/3;1;\lambda^{-1})/F(1/3,2/3;1;\lambda^{-p}) \pmod p.$$

Thus $\bar{C}(\lambda)$ is a solution of (2.5), since it is well known that $\lambda^{-1/3}F(1/3,2/3;1;\lambda^{-1})$ satisfies (2.5). Again applying [6], we have

$$\sum_{j=0}^{(2p-1)/3}((1/3)_j/j!)^2\lambda^j\equiv F(1/3,1/3;1;\lambda)/F(2/3,2/3;1;\lambda^p) \pmod p.$$

Thus the polynomial $\bar{D}(\lambda)\in \mathbf{F}_p[\lambda]$ defined by

$$\bar{D}(\lambda)=\sum_{j=0}^{(2p-1)/3}((1/3)_j/j!)^2(1-\lambda)^j$$

is a solution of (2.5) (since $F(1/3,1/3;1;1-\lambda)$ is). Since $-1/3$ is the unique root of the indicial equation of (2.5), it follows that $\bar{D}(\lambda)$ is a constant multiple of $\bar{C}(\lambda)$. Comparing coefficients of $\lambda^{(2p-1)/3}$ we conclude (since $(-1)^{(2p-1)/3}=-1$) that $\bar{D}(\lambda)=-\bar{C}(\lambda)$. It is clear from the definitions of $h(\mu)$ and $C(\mu)$ that $\bar{h}(\mu)=\mu^{-p}\bar{C}(\mu^3)$, hence $\bar{h}(\mu)=-\mu^{-p}\bar{D}(\mu^3)$. Thus if $\omega^3=1$, we have $\bar{h}(\omega)=-\omega^{-p}\bar{D}(1)=-\omega^{-p}$.

3. Reduction mod p of characteristic polynomial of Atkin's operator

For the definition of Atkin's operator, denoted here by U_p, we refer the reader to [3], [7], or [10]. We recall the identity [10, A3. 1.5].

$$\det(I-tU_p)=\prod_{r=0}^{\infty}\prod_{\{\mu\}}{}'(1-\pi_1(\mu)^{-2(r+1)}(p^rt)^{\deg\mu})^{-1}, \tag{3.1}$$

where $\prod'_{\{\mu\}}$ indicates the product is taken over all $\mathbf{F}_p$-conjugacy classes of elements of $\bar{\mathbf{F}}_p$, excluding the supersingular classes and the cube roots of unity, and $\pi_1(\mu)$ is the unit reciprocal root of the numerator of the zeta function of (2.1).

For any field K, define an endomorphism ψ of $K[\mu]$ by linearity and the condition

$$\psi(\mu^n)=\begin{cases}\mu^{n/p} & \text{if } p\mid n,\\ 0 & \text{if } p\nmid n.\end{cases}$$

Let $A(\mu) \in K[\mu]$. For k a non-negative integer, $\xi \to \psi(A^k\xi)$ is an endomorphism of $K[\mu]$, denoted $\psi \circ A^k$. Let V_n be the subspace of $K[\mu]$ of polynomials of degree $\leq n$. As observed in [4], if we put $n = [\deg A^k/(p-1)]$, then $\psi \circ A^k$ is stable on V_n and the eigenspaces corresponding to non-zero eigenvalues are contained in V_n.

THEOREM 1. *Let $h(\mu)$ be defined by* (2.3) *and consider $\psi \circ h^{p-3}$ as endomorphism of $\mathbf{Q}_p[\mu]$. If $p \equiv 1 \pmod 3$, then*

$$\det(I - tU_p) \equiv (1-t)^3 \det(I - t(\psi \circ h^{p-3}) \mid V_{p-3})/(1 - h(0)^{p-3}t) \pmod p.$$

If $p \equiv -1 \pmod 3$, then

$$\det(I - tU_p) \equiv (1-t)(1-t^2) \det(I - t(\psi \circ h^{p-3}) \mid V_{p-3}) \pmod p.$$

Before beginning the proof, we need a lemma. If $\mu \in \bar{\mathbf{F}}_p$ let μ_T denote its Teichmüller representative, i.e. μ_T is the unique lifting of μ to characteristic zero satisfying $\mu_T^{p^N-1} = 1$, where $N = [\mathbf{F}_p(\mu)\colon \mathbf{F}_p]$. (We take $0_T = 0$. Let A be a polynomial with coefficients in $\mathbf{Q}_p$ and put

$$\pi_A(\mu) = \prod_{i=0}^{N-1} A(\mu_T^{p^i}).$$

Note that $\pi_A(\mu) \in \mathbf{Q}_p$ (since $\pi_A(\mu) = \mathrm{Norm}_{\mathbf{Q}_p(\mu_T)/\mathbf{Q}_p} A(\mu_T)$) and depends only on the $\mathbf{F}_p$-conjugacy class of μ.

LEMMA 1. *Considering $\psi \circ A^k$ as endomorphism of the space of polynomials with coefficients in $\mathbf{Q}_p$, we have*

$$\det(I - t(\psi \circ A^k) \mid V_n) = \prod_{r=0}^{\infty} \prod_{\{\mu\}}'' (1 - \pi_A(\mu)^k (p^r t)^{\deg \mu})^{-1},$$

where $n = [\deg A^k/(p-1)]$ and $\prod''_{\{\mu\}}$ indicates a product extended over all $\mathbf{F}_p$-conjugacy classes of elements of $\bar{\mathbf{F}}_p$ excluding $\bar{\mu} = 0$.

Proof. This follows easily from the trace formula [4]

$$\mathrm{Tr}\,(\psi \circ A^k)^n = (p^n - 1)^{-1} \sum_{\mu_T{}^{p-1} = 1} A(\mu_T)^k A(\mu_T^p)^k \cdots A(\mu_T^{p^{n-1}})^k.$$

We obtain

$$(3.2) \quad -\sum_{n=1}^{\infty} \mathrm{Tr}\,(\psi \circ A^k)^n t^n/n = \sum_{n=1}^{\infty} (t^n/n) \sum_{r=0}^{\infty} p^{nr} \sum_{\mu^{p^n-1} = 1} \pi_A(\mu)^{nk/\deg \mu}$$
$$= \sum_{r=0}^{\infty} \sum_{\{\mu\}}'' \sum_{s=1}^{\infty} (\pi_A(\mu)^k (p^r t)^{\deg \mu})^s/s,$$

where $\sum''_{\{\mu\}}$ denotes a sum over all $\mathbf{F}_p$-conjugacy classes of elements of $\bar{\mathbf{F}}_p$ excluding $\mu = 0$. Taking exponentials in (3.2) gives the lemma. Q.E.D.

Proof of Theorem 1. From (3.1) we deduce

$$(3.3)\qquad \det(I - tU_p) \equiv \prod_{\{\mu\}}{}' (1 - \pi_1(\mu)^{-2} t^{\deg \mu})^{-1} \pmod p$$
$$\equiv \prod_{\{\mu\}}{}' (1 - \pi_1(\mu)^{p-3} t^{\deg \mu})^{-1} \pmod p,$$

since $\pi_1(\mu)$ is a unit in $\mathbf{Z}_p$ hence satisfies $\pi_1(\mu)^{p-1} \equiv 1 \pmod p$. From Lemma 1, taking for A the Hasse invariant h of equ. (2.3), we get

$$(3.4)\quad \det(I - t(\psi \circ h^{p-3}) \mid V_{p-3}) \equiv \prod_{\{\mu\}}{}''(1 - \pi_h(\mu)^{p-3} t^{\deg \mu})^{-1} \pmod p.$$

But it follows from [13] that if μ is not supersingular, then $\pi_h(\mu) \equiv \pi_1(\mu) \pmod p$. If μ is supersingular, then $\pi_h(\mu) \equiv 0 \pmod p$. Thus modulo p,

$$\det(I - tU_p)$$
$$\equiv (1 - \pi_h(0)^{p-3} t)^{-1} \det(I - t(\psi \circ h^{p-3}) \mid V_{p-3}) \prod_{\mu^3 = 1} (1 - \pi_h(\mu)^{p-3} t^{\deg \mu})^{1/\deg \mu}$$

Note that $\pi_h(0) = h(0)$, which is zero when $p \equiv -1 \pmod 3$.

Suppose that $p \equiv 1 \pmod 3$. In this case $\mu^3 = 1$ implies $\deg \mu = 1$. Thus

$$\pi_h(\mu) = h(\mu_T) \equiv 1 \pmod p$$

by the discussion in Section 2.

Suppose that $p \equiv -1 \pmod 3$. Let $1, \omega, \omega^2$ be the three cube roots of unity over $\mathbf{Q}_p$, and let $1, \bar{\omega}, \bar{\omega}^2$ be the their reductions mod p in $\bar{\mathbf{F}}_p$. In this case, we have $\deg \bar{\omega} = \deg \bar{\omega}^2 = 2$. Then

$$\pi_h(1) = h(1) \equiv -1 \pmod p$$
$$\pi_h(\bar{\omega}) = h(\omega) h(\omega^p) \equiv (-\bar{\omega}^{-p})(-\bar{\omega}^{-p^2}) \equiv 1 \pmod p$$
$$\pi_h(\bar{\omega}^2) = h(\omega^2) h(\omega^{2p}) \equiv (-\bar{\omega}^{-2p})(-\bar{\omega}^{-2p^2}) \equiv 1 \pmod p$$

by the results of Section 2. Q.E.D.

4. Main theorem and corollaries

Suppose $p \equiv 1 \pmod 3$. Consider the matrix (in the usual monomial basis) of $\psi \circ h^{p-3}$ on V_{p-3}. The first entry of the first row is $h(0)^{p-3}$, the other entries in the first row are zero. The last entry in the last row is 1, the other entries in the last row are zero. Thus

$$\det(I - t(\psi \circ h^{p-3}) \mid V_{p-3}) = (1 - h(0)^{p-3} t)(1 - t) \det(I - t(\psi \circ h^{p-3}) \mid W),$$

where W is the space of polynomials with coefficients in $\mathbf{Q}_p$ of degree $\leq p - 4$ with no constant term. From Theorem 1, we obtain

$$(4.1)\qquad \det(I - tU_p) \equiv (1 - t)^4 \det(I - t(\psi \circ h^{p-3}) \mid W) \pmod p$$

MAIN THEOREM. *Suppose* $p \equiv 1 \pmod 3$. *Then*

$$\deg [\det (I - t(\psi \circ h^{p-3}) \,|\, W) \pmod p] = p - 4,$$

i.e., as an operator on W, $\psi \circ h^{p-3}$ *has no eigenvalues divisible by* p.

The proof of the Main Theorem will be given in Section 5. By (4.1), we have:

COROLLARY 1. *For* $p \equiv 1 \pmod 3$, *Atkin's operator* U_p *has* p *eigenvalues (counting multiplicities) which are* p*-adic units.*

Comparing (4.1) with [10, (A3.3.3)], we see that

$$\det (I - t(\psi \circ h^{p-3}) \,|\, W) \equiv \det (I - tT_{p-1}(p)) \pmod p,$$

where $T_{p-1}(p)$ is the *pth* Hecke operator acting on cusp forms of weight $p - 1$ and level three. But the dimension of the space of cusp forms of weight $p - 1$ and level three is $p - 4$ [12], so by the Main Theorem we have:

COROLLARY 2. *For* $p \equiv 1 \pmod 3$, *all eigenvalues of the Hecke operator* $T_{p-1}(p)$ *are* p*-adic units.*

For the connection with the Cartier operator, see [10, (A3.3.3)].

Now suppose $p \equiv -1 \pmod 3$. Examining the matrix of $\psi \circ h^{p-3}$ as before (and keeping in mind that h has no constant term in this case) we see that

$$\det (I - t(\psi \circ h^{p-3}) \,|\, V_{p-3}) = (1 - t) \det (I - t(\psi \circ h^{p-3}) \,|\, W).$$

Comparing this with Theorem 1, we obtain

$$\det (I - tU_p) \equiv (1 - t)^2(1 - t^2) \det (I - t(\psi \circ h^{p-3}) \,|\, W) \pmod p. \tag{4.2}$$

The conclusion of the Main Theorem is false when $p \equiv -1 \pmod 3$. One has instead:

PROPOSITION 1. *If* $p \equiv -1 \pmod 3$, *then*

$$\deg [\det (I - t(\psi \circ h^{p-3}) \,|\, W) \pmod p] \leq p - 5.$$

The proof of Proposition 1 will be given in Section 6. By (4.2), we have:

COROLLARY 1. *For* $p \equiv -1 \pmod 3$, *Atkin's operator* U_p *has no more than* $p - 1$ *eigenvalues which are* p*-adic units.*

Combining (4.2) with [10, A3.3.3] gives

$$\det (I - t(\psi \circ h^{p-3}) \,|\, W) \equiv \det (I - tT_{p-1}(p)) \pmod p,$$

hence by Proposition 1:

COROLLARY 2. *For* $p \equiv -1 \pmod 3$, *the Hecke operator* $T_{p-1}(p)$ *has at least one eigenvalue which is a* p*-adic non-unit.*

5. Proof of main theorem

LEMMA 2. *Let k and n be positive integers. If $n > 1$, let α be the unique positive integer such that*

$$(\alpha - 1)(p - 1)/(n - 1) < k \leq \alpha(p - 1)/(n - 1).$$

If $n = 1$, let $\alpha = 0$. Then $[k(p - n)/(p - 1)] = k - \alpha$.

Proof. The assertion is clear if $n = 1$. If $n > 1$ define ε by the equation

$$k = ((\alpha - 1)(p - 1)/(n - 1)) + \varepsilon \tag{5.1}$$

so that

$$0 < \varepsilon \leq (p - 1)/(n - 1). \tag{5.2}$$

Using (5.1) to express k we compute

$$(k(p - n)/(p - 1) - (k - \alpha) = 1 - \varepsilon(n - 1)/(p - 1),$$

and by (5.2), $0 \leq 1 - \varepsilon(n - 1)/(p - 1) < 1$. Q.E.D.

Denote by $\bar{V}_m$ the space of polynomials in $\mathbf{F}_p[\mu]$ of degree $\leq m$.

COROLLARY. *Let $f \in \mathbf{F}_p[\mu]$ and put $k = \deg f$. Let n be an integer, $1 \leq n \leq p$. Then $\psi \circ f^{p-n}$ is stable on $\bar{V}_{k-\alpha}$*

Consider now the operator $\psi \circ f^{n-1}$ on $\mathbf{F}_p[\mu]$, where f and n are as defined in the corollary. From (5.1) and (5.2), we have

$$[k(n - 1)/(p - 1)] = \begin{cases} \alpha & \text{if } \varepsilon = (p - 1)/(n - 1) \text{ or } n = 1 \\ \alpha - 1 & \text{if } \varepsilon \neq (p - 1)/(n - 1), \end{cases} \tag{5.3}$$

where α is defined in Lemma 2. If $\varepsilon = (p - 1)/(n - 1)$, we have $k = \alpha(p - 1)/(n - 1)$ and

$$\psi(f^{n-1}\mu^\alpha) = c\mu^\alpha + \text{lower order terms} \tag{5.4}$$

where $c \in \mathbf{F}_p^\times$ is the coefficient of $\mu^{k(n-1)}$ in f^{n-1}. Thus by (5.3), $\psi \circ f^{n-1}$ is stable on either $\bar{V}_\alpha$ or $\bar{V}_{\alpha-1}$, and by (5.4) the kernel of $\psi \circ f^{n-1}$ is contained in $\bar{V}_{\alpha-1}$ in either case (in particular, taking $n = 1$, $\ker(\psi) = \{0\} = V_{-1}$).

The Main Theorem will be a corollary of the next theorem.

THEOREM 2. *Let $f \in \mathbf{F}_p[\mu]$ and put $k = \deg f$. Suppose n is integral, $1 \leq n \leq p$, and let α, ε be defined by lemma 2 and* equ. (5.1) (*thus ε is defined only if $n > 1$). We assume the following:*

(i) $f(0) \neq 0$,
(ii) *f is relatively prime to its derivative,*
(iii) $k \leq p(p - 1)/(n - 1)$ (*if* $n > 1$),
(iv) $\varepsilon(n - 1) \geq \alpha - 1$ (*if* $n > 1$).

Then the kernel of $\psi \circ f^{p-n}$ on $\bar{V}_{k-\alpha}$ is isomorphic to the kernel of $\psi \circ f^{n-1}$ on $\bar{V}_{\alpha-1}$.

Proof. The theorem is trivial if $k = 0$, so we suppose $k \geq 1$. Let $\xi \in \mathbf{F}_p[\mu]$ be such that $\psi(\xi f^{p-n}) = 0$. Then we must have $\xi = \mu\eta$ with $\eta \in \mathbf{F}_p[\mu]$, so

$$\psi(\mu\eta f^{p-n}) = f\psi(\mu\eta/f^n) = 0.$$

Thus $\psi(\mu\eta/f^n) = 0$. This implies $\eta/f^n \in d/d\mu(\mathbf{F}_p(\mu))$. We can then write $\eta = f^n\rho'$ with $\rho \in \mathbf{F}_p(\mu)$ where $\rho' = d\rho/d\mu$), and can assume without loss of generality that ρ has poles only at zeros of f. We will have $\xi \in \bar{V}_{k-\alpha}$ if and only if ρ produces a polynomial η with $\deg \eta \leq k - \alpha - 1$. The proof is divided into several cases.

Case 1. Assume $\rho \in \mathbf{F}_p[\mu]$. Then $\eta = f^n\rho'$ implies $\eta = 0$ or $\deg \eta \geq nk > k - \alpha - 1$. Hence $\xi \notin \bar{V}_{k-\alpha}$.

If $\rho \notin \mathbf{F}_p[\mu]$ we may write $\rho = \tau/f^r$ where $r > 0$ and $\tau \in \mathbf{F}_p[\mu]$. We assume $f \nmid \tau$, which determines r uniquely. Further, we can assume without loss of generality that $p \nmid r$: for if $p \mid r$ (by looking at the principal part expansion of $\rho = \tau/f^r$) one can find $\rho_1 = \sigma/f^s$ such that $\rho_1' = \rho'$, $\sigma \in \mathbf{F}_p[\mu]$, and either $p \nmid s$ or $s = 0$. Since we are really concerned with $\eta = f^n\rho'$, we may then replace ρ by ρ_1.

Case 2. Assume $r > n - 1$. We have $\eta = f^n\rho' = (f\tau' - rf'\tau)/f^{r+1-n}$ with $r + 1 - n > 0$. For η to be a polynomial f must divide $f'\tau$ (since $r \not\equiv 0 \pmod p$). But $(f, f') = 1$ so $f \mid \tau$, contradicting the assumption made after case 1. Thus η cannot be a polynomial in this case.

Taking $n = 1$ in the theorem, this shows that $\psi \circ f^{p-1}$ has trivial kernel on $\bar{V}_k$, since $r > n - 1$ is the only case that occurs. As already observed, ψ has trivial kernel on $\bar{V}_{-1}$. This proves the theorem when $n = 1$ and when $n = p$ (since $n = p$ determines the same pair of operators ψ and $\psi \circ f^{p-1}$). From now on, we assume $1 < n < p$.

Case 3. Assume $r < n - 1$. Then $\eta = f^{n-r-1}(f\tau' - rf'\tau)$. Since $n - r - 1 > 0$, it follows that either $\eta = 0$ or $\deg \eta \geq k > k - \alpha - 1$.

Thus none of the first three cases produces an η with $\deg \eta \leq k - \alpha - 1$ (other than $\eta = 0$).

Case 4. Assume $r = n - 1$. Then $\eta = f\tau' - (n - 1)f'\tau$. Put $l(\tau) = f\tau' - (n - 1)f'\tau$. If $\deg \tau = j$, it follows that (since $n > 1$ implies $\alpha \geq 1$) $\deg \eta = j + k - 1 > k - \alpha - 1$ unless $j \equiv k(n - 1) \pmod p$.

Suppose $\alpha = 1$. From the definition of α (Lemma 2) this implies

$$\deg f^{n-1} = k(n - 1) < p. \tag{5.5}$$

In this case, $\psi \circ f^{p-n}$ has non-trivial kernel on $\bar{V}_{k-\alpha}$ if and only if there exists a polynomial τ with $\deg \tau \equiv k(n - 1) \pmod p$ such that $\eta = l(\tau)$ is non-trivial and satisfies $\deg \eta \leq k - 2$. Let τ_0 be the polynomial of least degree having these properties. By (5.5), there exist $c \in \mathbf{F}_p$ and a non-negative integer m such that $\deg(\tau_0 - c\mu^{mp}f^{n-1}) < \deg \tau_0$. But $l(f^{n-1}) = 0$ implies

$$l(\tau_0 - c\mu^{mp}f^{n-1}) = l(\tau_0),$$

contradicting the minimality of $\deg \tau_0$. Hence $\psi \circ f^{p-n}$ has trivial kernel on $\bar{V}_{k-1}$. Since we are assuming $f(0) \neq 0$, $\psi \circ f^{n-1}$ has trivial kernel on $\bar{V}_0$. This proves the theorem when $\alpha = 1$. From now on, we assume $\alpha \geq 2$.

By (5.1), $k(n-1)/p = \alpha - 1 + (\varepsilon(n-1) - (\alpha - 1))/p$. Using (5.2) and our hypothesis that $\varepsilon(n-1) \geq \alpha - 1$ we see that $[k(n-1)/p] = \alpha - 1$. Thus we can write

$$f^{n-1} = f_0 + \mu^p f_1 + \mu^{2p} f_2 + \cdots + \mu^{(\alpha-1)p} f_{\alpha-1}, \quad f_{\alpha-1} \neq 0,$$

where $f_0, f_1, \ldots, f_{\alpha-1} \in \mathbf{F}_p[\mu]$, $\deg f_0, \deg f_1, \ldots, \deg f_{\alpha-2} \leq p-1$, and $\deg f_{\alpha-1} \equiv k(n-1) \pmod p$. For $m = 1, 2, \ldots, \alpha - 1$ set

$$B_m = \mu^{-mp}\left(f^{n-1} - \sum_{i=0}^{m-1} \mu^{ip} f_i\right).$$

Then $B_m \in \mathbf{F}_p[\mu]$ and $\deg B_m = k(n-1) - mp$. Since $l(f^{n-1}) = 0$, the degree of $l(B_m)$ is $\leq k-2$. The operator $\psi \circ f^{p-n}$ on $\bar{V}_{k-\alpha}$ has a non-trivial kernel if and only if there exists $\tau \in \mathbf{F}_p[\mu]$ with $\deg \tau \equiv k(n-1) \pmod p$ such that $\eta = l(\tau)$ is non-trivial and satisfies $\deg \eta \leq k - \alpha - 1$.

Suppose $\tau \in \mathbf{F}_p[\mu]$ is such that $\deg \tau \equiv k(n-1) \pmod p$ and $\deg l(\tau) \leq k-2$. Then

$$\deg \tau \equiv \deg f^{n-1} \equiv \deg B_m \pmod p \quad \text{for } m = 1, 2, \ldots, \alpha - 1,$$

and since $(\alpha - 1 - m)p \leq \deg B_m \leq (\alpha - m)p$, we see that τ can be expressed in the form

$$\tau = g(\mu^p) f^{n-1} + \sum_{m=1}^{\alpha-1} c_m B_m,$$

where $g(\mu) \in \mathbf{F}_p[\mu]$, $c_1, c_2, \ldots, c_{\alpha-1} \in \mathbf{F}_p$. Hence

$$l(\tau) = l\left(\sum_{m=1}^{\alpha-1} c_m B_m\right). \tag{5.6}$$

Put

$$\sigma_1 = \left(\sum_{m=1}^{\alpha-1} c_m \mu^{-mp}\right) f^{n-1}.$$

For $i = 0, 1, \ldots, \alpha - 2$, put $f_i = \sum_{j=0}^{p-1} a_{i,j}\mu^j$. Set

$$\sigma_2 = \sum_{m=1}^{\alpha-1} c_m \mu^{-p}\left(\sum_{j=p+1-\alpha}^{p-1} a_{m-1,j}\mu^j\right).$$

Define σ_3 by

$$\sigma_3 = \left(\sum_{m=1}^{\alpha-1} c_m B_m\right) - \sigma_1 - \sigma_2.$$

From the definition of B_m it is clear that σ_3 consists of terms of degree $\leq -\alpha$. Hence deg $l(\sigma_3) \leq k - \alpha - 1$. Furthermore, $l(\sigma_1) = 0$. Thus

$$\deg l\left(\sum_{m=1}^{\alpha-1} c_m B_m\right) \leq k - \alpha - 1 \leftrightarrow \deg l(\sigma_2) \leq k - \alpha - 1.$$

Write $\sigma_2 = \sum_{j=1}^{\alpha-1} d_j/\mu^j$. From (5.1), we have

$$k(n-1) = (\alpha - 1)(p - 1) + \varepsilon(n - 1),$$

which implies $k(n-1) \equiv \varepsilon(n-1) - (\alpha - 1) \pmod p$. By (5.2) and hypothesis (iv), $p - 1 \geq \varepsilon(n-1) \geq \alpha - 1$; hence $k(n-1)$ is congruent modulo p to one of the numbers $0, 1, \ldots, p - \alpha$. Thus for $j = 1, 2, \ldots, \alpha - 1$,

$$\deg l(1/\mu^j) = k - j - 1 > k - \alpha - 1.$$

Therefore,

$$\deg l(\sigma_2) \leq k - \alpha - 1 \leftrightarrow d_1 = d_2 = \cdots = d_{\alpha-1} = 0.$$

In matrix terms, if we put

$$b_{ij} = a_{j-1,p-i}, \quad i, j = 1, 2, \ldots, \alpha - 1,$$

then $(b_{ij})(c_1, \ldots, c_{\alpha-1})^t = (d_1, \ldots, d_{\alpha-1})^t$. Hence

$$\deg l(\sigma_2) \leq k - \alpha - 1 \leftrightarrow (c_1, \ldots, c_{\alpha-1})^t \in \ker (b_{ij}),$$

where (b_{ij}) is considered as acting on $\mathbf{F}_p^{\alpha-1}$.

Summarizing, we have shown that the map

$$(c_1, \ldots, c_{\alpha-1})^t \mapsto \mu l\left(\sum_{m=1}^{\alpha-1} c_m B_m\right)$$

is a surjection of ker (b_{ij}) onto ker $(\psi \circ f^{p-n})$. It is easy to see that this map is actually an isomorphism: if it were not injective, l would have a polynomial solution of degree $< k(n-1)$, which is impossible.

The kernel of $\psi \circ f^{n-1}$ on $\bar{V}_{\alpha-1}$ is contained in the space spanned by $\{\mu, \mu^2, \ldots, \mu^{\alpha-1}\}$ (since f has a non-zero constant term). Its matrix in this basis in (b_{ji}). Thus ker $(\psi \circ f^{n-1})$ and ker $(\psi \circ f^{p-n})$ have the same dimension. Q.E.D.

Proof of Main Theorem. The Hasse invariant $\bar{h}(\mu)$ satisfies the hypotheses of Theorem 2: that $\bar{h}(0) \neq 0$ follows from (2.3), and $\bar{h}$ is relatively prime to its derivative since it is a non-trivial solution of a second order differential equation. Hypotheses (iii) and (iv) are easily checked. Note that $\alpha = n - 1$. Furthermore, letting $\bar{W}$ denote the space of polynomials in $\mathbf{F}_p[\mu]$ of degree $\leq p-4$ which are divisible by μ, we have

$$\det(I - t(\psi \circ h^{p-3})|W) \equiv \det(I - t(\psi \circ \bar{h}^{p-3})|\bar{W}) \pmod{p}.$$

Thus the Main Theorem asserts that $\psi \circ \bar{h}^{p-3}$ has trivial kernel on $\bar{W}$. Applying Theorem 2 with $n = 3$ (and hence $\alpha = 2$), we see that this will be the case provided $\psi \circ \bar{h}^2$ has trivial kernel on $\bar{V}_1$. Since $\bar{h}$ has non-zero constant term, it is clear that $\psi \circ \bar{h}^2$ has non-trivial kernel if and only if $\psi(\mu\bar{h}^2) = 0$, i.e. if and only if the coefficient of μ^{p-1} in $\bar{h}^2$ is zero. The proof is concluded by the following:

LEMMA 3 (Dwork [8]). *For $p \equiv 1 \pmod 3$, the coefficient of μ^{p-1} in $\bar{h}^2$ is non-zero.*

Proof. The Hasse invariant $\bar{h}$ satisfies the differential equation (2.4). Its square $\bar{h}^2$ satisfies the second symmetric power L of (2.4). A straightforward calculation shows that

$$(\mu^3 - 1)^2 L = (\mu^3 - 1)^2 (d/d\mu)^3 + 9\mu^2(\mu^3 - 1)(d/d\mu)^2 + (19\mu^4 - 10\mu)(d/d\mu) + (8\mu^3 - 2).$$

Writing $\bar{h}^2 = \sum_{n=0}^{2p-2} a_n \mu^n$ and putting $a_n = 0$ for $n < 0$ or $n > 2p-2$, we have

$$\begin{aligned} (5.7) \qquad 0 &= (\mu^3 - 1)^2 L(\bar{h}^2) \\ &= \sum_{n=0}^{2p+1} [(n-1)^3 a_{n-3} + (-2n^3 - 3n^2 - 5n - 2)a_n \\ &\quad + (n+3)(n+2)(n+1)a_{n+3}]\mu^n. \end{aligned}$$

Putting $n = p-1$ in this sum gives $(p-2)^3 a_{p-4} + 2a_{p-1} = 0$. If $a_{p-1} = 0$, then $a_{p-4} = 0$. Putting $n = p-4$ in this sum now gives $(p-5)^3 a_{p-7} = 0$. Hence $a_{p-7} = 0$. Continuing this procedure we arrive at $a_0 = 0$. But as already observed $\bar{h}(0) \neq 0$. This contradiction shows $a_{p-1} \neq 0$. Q.E.D.

6. Proof of Proposition 1

LEMMA 4. *Let $f \in \mathbf{F}_p[\mu]$ with $\deg f = p-1$ and $f(0) = 0$. Write*

$$(6.1) \qquad \mu f^2 = f_0 + \mu^p f_1$$

(where $\deg f_1 = p-1$, $\deg f_0 \leq p-1$) and put $\sigma = \mu f^3 (f_1/\mu f^2)'$. Then $\sigma \in \mathbf{F}_p[\mu]$, $\deg \sigma \leq p-4$, and $\sigma \in \ker(\psi \circ f^{p-3})$

Proof. An easy calculation shows $\sigma = ff'_1 - 2f_1 f' - \mu^{-1} f_1 f$. Hence $\sigma \in \mathbf{F}_p[\mu]$ since $\mu | f$. Next we have $\psi(f^{p-3}\sigma) = f\psi(\mu(f_1/\mu f^2)') = 0$ since

$(f_1/\mu f^2)'$ has no terms of degree congruent to -1 modulo p. Finally, using (6.1), we can write

$$\sigma = (\mu f)^{-1}(f_0 f_1' - f_1 f_0'). \tag{6.2}$$

Hence $\deg \sigma \leq p - 4$. Q.E.D.

Proof of Proposition 1. Let $\bar{W}$ again denote the space of polynomials in $\mathbf{F}_p[\mu]$ of degree $\leq p - 4$ which are divisible by μ. Then

$$\det(I - t(\psi \circ h^{p-3})W) \equiv \det(I - t(\psi \circ \bar{h}^{p-3}) \,|\, \bar{W}) \pmod p$$

Thus Proposition 1 is equivalent to the assertion that $\psi \circ \bar{h}^{p-3}$ has non-trivial kernel on $\bar{W}$.

Write $\mu\bar{h}^2 = h_0 + \mu^p h_1$. Then by Lemma 4, $\sigma = \mu\bar{h}^3(h_1/\bar{h}^2)'$ lies in the kernel of $\psi \circ \bar{h}^{p-3}$ on $\bar{W}$. Furthermore, $\sigma \neq 0$: if not, then by (6.2), we have $h_0 = \alpha h_1$ for some constant α; so $\bar{h}^2 = (\alpha + \mu^p)h_1$. But this implies $\bar{h}$ has a multiple root, contradicting the fact that $\bar{h}$ is a non-trivial solution of a second order linear differential equation. Q.E.D.

Added in proof. Hypothesis (iii) of Theorem 2 is implied by hypothesis (iv). The proof can be streamlined somewhat by replacing (iii) and (iv) by the equivalent hypothesis that $[k(n-1)/p] = \alpha - 1$.

References

1. A. Adolphson, *A p-adic theory of Hecke polynomials*, Duke Math. J., vol. 43 (1976), pp. 115–145.
2. ———, *On the mod p eigenvalues of Hecke operators*, Duke Math. J., vol. 43 (1976), pp. 109–114.
3. A. O. Atkin, *Congruence Hecke operators*, Proc. Symp. Pure Math., vol. 12 (1969), pp. 33–40.
4. B. Dwork, *On the rationality of the zeta function of an algebraic variety*, Amer. J. Math., vol. 82 (1960), pp. 631–647.
5. ———, *On the zeta function of a hypersurface II*, Ann. of Math., vol. 80 (1964), pp. 227–299.
6. ———, *p-adic cycles*, Publ. Math. IHES, vol. 37 (1969), pp. 327–415.
7. ———, *The U_p-operator of Atkin on modular functions of level two with growth conditions*, Lecture Notes in Mathematics, No. 350, Springer-Verlag, New York, 1973, pp. 57–67.
8. ———, *The action of Atkin's U_p-operator on modular functions of level three*, (unpublished manuscript).
9. E. L. Ince, *Ordinary differential equations*, Dover, New York, 1956.
10. N. Katz, *p-adic properties of modular schemes and modular forms*, Lecture Notes in Mathematics, No. 350, Springer-Verlag, New York, 1973, pp. 69–190.
11. ———, *Algebraic solutions of differential equations (p-curvature and the Hodge filtration)*, Invent. Math., vol. 18 (1972), pp. 1–118.
12. R. Gunning, *Lectures on modular forms*, Ann. of Math. Studies, No. 48, Princeton University Press, Princeton, 1962.
13. J. Manin, *The Hasse-Witt matrix of an algebraic curve*, Amer. Math. Soc. Translations, ser. 2, vol. 45 (1965), pp. 245–264.

University of Washington
Seattle, Washington