Illinois Journal of Mathematics
Volume 48, Number 1, Spring 2004, Pages 353–356
S 0019-2082

A REMARK ON HECKE OPERATORS AND A THEOREM OF DWORK AND KOIKE

HOLLY SWISHER

ABSTRACT. Let $p \geq 5$ be prime, $\mathfrak{S}_p$ the set of all characteristic p supersingular j-invariants in $\mathbb{F}_p - \{0, 1728\}$, and $\mathfrak{M}_p$ the set of all monic irreducible quadratic polynomials in $\mathbb{F}_p[x]$ whose roots are supersingular j-invariants. A theorem of Dwork and Koike asserts that there are integers $A_p(\alpha), B_p(g), C_p(g)$, and a polynomial $D_p(x) \in \mathbb{F}_p[x]$ of degree $p-1$, for which

$$j(pz) \equiv j(z)^p + pD_p(j(z)) + p \sum_{\alpha \in \mathfrak{S}_p} \frac{A_p(\alpha)}{j(z) - \alpha} + p \sum_{g(x) \in \mathfrak{M}_p} \frac{B_p(g)j(z) + C_p(g)}{g(j(z))} \pmod{p^2}.$$

It is natural to seek a description of the polynomials $D_p(x)$. Here we provide such a description in terms of certain Hecke polynomials.

1. Introduction

Throughout this paper let $q := e^{2\pi iz}$, and let $j(z)$ be the usual elliptic modular function on $SL_2(\mathbb{Z})$:

$$j(z) = q^{-1} + 744 + 196884q + 21493760q^2 + \cdots$$

Losing the constant term, we define $J(z)$ to be the usual Hauptmodul

$$J(z) := j(z) - 744 = \sum_{n=-1}^{\infty} c(n)q^n = q^{-1} + 196884q + 21493760q^2 + \cdots .$$

We recall an infinite class of monic polynomials $j_m \in \mathbb{Z}[j(z)]$ of degree m. The j_m can be described in two ways. Let $j_0(z) = 1$, and for each positive integer m, let $j_m(z)$ be given by

$$j_m(z) = J(z) \mid T_0(m),$$

where $T_0(m)$ is the normalized mth Hecke operator of weight zero. Notice that for each m, $j_m(z)$ is the unique modular function that is holomorphic on

Received May 1, 2003; received in final form June 25, 2003.
2000 *Mathematics Subject Classification.* 11F33, 11F30.

the upper half plane $\mathcal{H}$ and has Fourier expansion of the form

$$j_m(z) = q^{-m} + \sum_{n=1}^{\infty} c_m(n) q^n \in \frac{1}{q^m}\mathbb{Z}[[q]].$$

Each $j_m(z)$ is a monic degree m polynomial in $\mathbb{Z}[j(z)]$. The first few $j_m(z)$ are:

$$\begin{aligned} j_0(z) &= 1 \\ j_1(z) &= J(z) = j(z) - 744 \\ j_2(z) &= j(z)^2 - 1488 j(z) + 159768. \end{aligned}$$

For a second description of the j_m and more about their importance see [Br-K-O].

Here we show that the $j_p(z)$ are also important for studying the p-adic properties of modular forms. For primes $p \geq 5$, let $\mathfrak{S}_p$ be the set of all characteristic p supersingular j-invariants in $\mathbb{F}_p - \{0, 1728\}$, and $\mathfrak{M}_p$ the set of all monic irreducible quadratic polynomials in $\mathbb{F}_p$ whose roots are supersingular j-invariants. As a special case of the work of Deligne and Dwork [D] on the p-adic rigidity of the map $j(z) \to j(pz)$, Koike [K] described the Fourier expansion of $j(pz) \pmod{p^2}$. Refining the simple fact that $j(pz) \equiv j(z)^p \pmod{p}$, Koike proved (see [K], [D]) that for primes $p \geq 5$ there exist integers $A_p(\alpha)$, $B_p(g)$, $C_p(g) \in \mathbb{Z}$ and a polynomial $D_p(x) \in \mathbb{F}_p[x]$ of degree $p-1$ such that

$$\begin{aligned} j(pz) \equiv j(z)^p \ + \ & p D_p(j(z)) \\ & + p \sum_{\alpha \in \mathfrak{S}_p} \frac{A_p(\alpha)}{j(z) - \alpha} + p \sum_{g(x) \in \mathfrak{M}_p} \frac{B_p(g) j(z) + C_p(g)}{g(j(z))} \pmod{p^2}. \end{aligned}$$

Here we provide an explicit description of the polynomials $D_p(x)$ in terms of the j_p. If $p \geq 5$ is prime, then in $\mathbb{F}_p[j]$ we show that

$$D_p(j) = \frac{1}{p}(j_p - j^p + 744).$$

In particular, we prove the following theorem.

THEOREM 1.1. *If $p \geq 5$ is prime, then there exist $A_p(\alpha)$, $B_p(g)$, $C_p(g) \in \mathbb{Z}$ such that*

$$j(pz) \equiv j_p(z) + 744 + p \sum_{\alpha \in \mathfrak{S}_p} \frac{A_p(\alpha)}{j(z) - \alpha} + p \sum_{g(x) \in \mathfrak{M}_p} \frac{B_p(g) j(z) + C_p(g)}{g(j(z))} \pmod{p^2}.$$

EXAMPLE. Consider the case where $p = 43$. Here we have $\mathfrak{S}_{43} = \{-2\}$ and $\mathfrak{M}_{43} = \{x^2 + 19x + 16\}$. In Koike's theorem we get that

$$j(43z) \equiv j(z)^{43} + 43(30j(z)^{42} + 36j(z)^{41} + 12j(z)^{40} + \cdots + 14j(z) + 9) + \frac{860}{j(z)+2} + \frac{43(11j(z)+40)}{j(z)^2 + 19j(z) + 16} \pmod{43^2},$$

which shows $D_{43}(x) = 30x^{42} + 36x^{41} + 12x^{40} + \cdots + 34x^2 + 14x + 9$ in $\mathbb{F}_{43}[x]$. Now consider

$$j_{43} - j^{43} + 744 = -31992j^{42} + 491376996j^{41} - 4825080706976j^{40} + \cdots$$
$$-123992487051810829159422312656870824123505391598393324723609239857834359623346157164874913016618601599 2.$$

Dividing by 43 gives

$$\frac{j_{43} - j^{43} + 744}{43} = -744j^{42} + 11427372j^{41} - 112211179232j^{40} + \cdots$$
$$- 2883546210507228585102844480392344747058264920892$$
$$8680168281218571589385958917710968575561166655488744,$$

which in $\mathbb{F}_{43}$ is equal to

$$30j^{42} + 36j^{41} + 12j^{40} + \cdots + 34j^2 + 14j + 9.$$

2. Proof of Theorem 1.1

We begin with a preliminary lemma.

LEMMA 2.1. *Suppose $f, g \in \mathbb{Z}[x]$ are polynomials with g monic, and $\deg g = m > \deg f = n$. Then the Fourier expansion of $\frac{f(j(z))}{g(j(z))}$ is of the form $\sum_{k=m-n}^{\infty} a(k)q^k$, where $a(k) \in \mathbb{Z}$ (i.e., there are only positive powers of q).*

Proof. By the hypotheses $q^n f(j(z))$ is in the ring of formal power series $\mathbb{Z}[[q]]$, and $q^m g(j(z))$ is a unit in $\mathbb{Z}[[q]]$. Thus

$$\frac{f(j(z))}{g(j(z))} = \frac{q^{m-n}q^n f(j(z))}{q^m g(j(z))} \in q^{m-n}\mathbb{Z}[[q]]. \qquad \square$$

Proof of Theorem 1.1. Define the polynomial $F_p(x) \in \mathbb{Z}[x]$ by $F_p(j(z)) = j_p(z) - j(z)^p + 744$. Then Koike's result implies that

$$j_p(z) - j(pz) + 744 \equiv F_p(j(z)) - pD_p(j(z)) - p\sum_{\alpha \in \mathfrak{S}_p} \frac{A_p(\alpha)}{j(z) - \alpha} - p\sum_{g(x) \in \mathfrak{M}_p} \frac{B_p(g)j(z) + C_p(g)}{g(j(z))} \pmod{p^2}.$$

Now looking at the q-expansions of $j_p(z)$ and $j(pz)$ we see that the left hand side has only positive powers of q. In particular,

$$\text{LHS} \equiv \sum_{n\geq 1} a(n)q^n \pmod{p^2} \Longrightarrow \text{RHS} \equiv \sum_{n\geq 1} a(n)q^n \pmod{p^2},$$

where $a(n) \in \mathbb{Z}$. Thus by Lemma 2.1 we deduce that $F_p(j(z))$ and $pD_p(j(z))$ have the same coefficients of q^n for $n \leq 0$ modulo p^2. As polynomials in $\mathbb{Z}[x]$ the coefficients of x are determined solely by these q-coefficients for nonpositive powers of q. So we have $F_p(x) \equiv pD_p(x) \pmod{p^2}$, and thus in $\mathbb{F}_p[x]$, $\frac{1}{p}F_p(x) = D_p(x)$. □

References

[Br-K-O] J. H. Bruinier, W. Kohnen, and K. Ono, *The arithmetic of the values of modular functions and the divisors of modular forms*, Comp. Math., accepted for publication.

[D] B. Dwork, *p-adic cycles*, Inst. Hautes Études Sci. Publ. Math. **37** (1969), 27–115. MR 45#3415

[K] M. Koike, *Congruences between modular forms and functions and applications to the conjecture of Atkin*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **20** (1973), 129–169. MR 55#10391

[S] J.-P. Serre *A course in arithmetic*, Springer-Verlag, New York, 1973. MR 49#8956

Department of Mathematics, University of Wisconsin, 480 Lincoln Drive, Madison, WI 53706, USA

E-mail address: swisher@math.wisc.edu