PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 141, Number 1, January 2013, Pages 41–53
S 0002-9939(2012)11434-0
Article electronically published on May 3, 2012

DIVISIBILITY PROPERTIES OF COEFFICIENTS OF LEVEL p MODULAR FUNCTIONS FOR GENUS ZERO PRIMES

NICKOLAS ANDERSEN AND PAUL JENKINS

(Communicated by Matthew A. Papanikolas)

Abstract. Lehner's 1949 results on the j-invariant showed high divisibility of the function's coefficients by the primes $p \in \{2, 3, 5, 7\}$. Expanding his results, we examine a canonical basis for the space of level p modular functions holomorphic at the cusp 0. We show that the Fourier coefficients of these functions are often highly divisible by these same primes.

1. Introduction and statement of results

A level p modular function $f(\tau)$ is a holomorphic function on the complex upper half-plane which satisfies

$$f\left(\frac{a\tau+b}{c\tau+d}\right) = f(\tau) \text{ for all } \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(p)$$

and is meromorphic at the cusps of $\Gamma_0(p)$. Equivalently, $f(\tau)$ is a weakly holomorphic modular form of weight 0 on $\Gamma_0(p)$. Such a function will necessarily have a q-expansion of the form $f(\tau) = \sum_{n=n_0}^{\infty} a(n)q^n$, where $q = e^{2\pi i\tau}$.

Of particular interest in the study of modular forms is the classical j-invariant, $j(\tau) = q^{-1} + 744 + \sum_{n=1}^{\infty} c(n)q^n$, which is a modular function of level 1. The coefficients $c(n)$ of the j-function, like the Fourier coefficients of many other modular forms, are of independent arithmetic interest; for instance, they appear as dimensions of a special graded representation of the Monster group.

In 1949 Lehner showed [7, 8] that

$$c(2^a 3^b 5^c 7^d n) \equiv 0 \pmod{2^{3a+8} 3^{2b+3} 5^{c+1} 7^d},$$

proving that the coefficients $c(n)$ are often highly divisible by small primes. Similar results have recently been proven for other modular functions in [6], and for modular forms of level 1 and small weight in [4], [3]. It is natural to ask whether such congruences hold for the Fourier coefficients of modular functions of higher level, such as those studied by Ahlgren [1] in his work on Ramanujan's θ-operator.

Lehner's results for $j(\tau)$ are in fact more general; in [8] he pointed out that for $p = 2, 3, 5, 7$, similar congruences hold for the coefficients of level p modular functions which have integral coefficients at both cusps and have poles of order less than p at the cusp at infinity.

Received by the editors June 6, 2011.
2010 *Mathematics Subject Classification.* Primary 11F03, 11F33.
The first author thanks the Brigham Young University Department of Mathematics for its generous support, as well as Dr. Darrin Doud for his instruction and guidance.

In this paper, for $p \in \{2,3,5,7\}$, we examine canonical bases for spaces of level p modular functions which are holomorphic at the cusp 0. To construct these bases, we introduce the level p modular function $\psi^{(p)}(\tau)$, defined as

$$\psi^{(p)}(\tau) = \left(\frac{\eta(\tau)}{\eta(p\tau)}\right)^{\frac{24}{p-1}} \quad \text{where } \eta(\tau) = q^{\frac{1}{24}} \prod_{n=1}^{\infty}(1-q^n).$$

The integer $\frac{24}{p-1}$ for $p = 2,3,5,7$ will appear frequently, so we will denote it by $\lambda^{(p)}$, or simply λ where no confusion arises. The function $\psi^{(p)}(\tau)$ is a modular function of level p with a simple pole at ∞ and a simple zero at 0. We will also use the modular function

$$\phi^{(p)}(\tau) = (\psi^{(p)}(\tau))^{-1}.$$

Following Ahlgren [1] and using the notation of Duke and Jenkins [5], for $p = 2,3,5,7$ we construct a basis $\{f_{0,m}^{(p)}(\tau)\}_{m=0}^{\infty}$ for the space of level p modular functions which are holomorphic at 0 as follows:

$$f_{0,0}^{(p)}(\tau) = 1, f_{0,m}^{(p)}(\tau) = q^{-m} + O(1) = \psi^{(p)}(\tau)^m - Q(\psi^{(p)}(\tau)),$$

where $Q(x)$ is a polynomial of degree $m-1$ with no constant term, chosen to eliminate all negative powers of q in $\psi^{(p)}(\tau)^m$ except for q^{-m}. Since $\psi^{(p)}(\tau)$ vanishes at 0 and the polynomial Q has no constant term, we see that the functions $f_{0,m}^{(p)}$ also vanish at 0 when $m > 0$. We write

$$f_{0,m}^{(p)} = q^{-m} + \sum_{n=0}^{\infty} a_0^{(p)}(m,n)q^n$$

so that for $n \geq 0$, the symbol $a_0^{(p)}(m,n)$ denotes the coefficient of q^n in the mth basis element of level p. Note that the function $f_{0,m}^{(p)}$ corresponds to Ahlgren's $j_m^{(p)}$.

For an example of some of these functions, consider the case $p = 2$:

$$\begin{aligned}
f_{0,1}^{(2)}(\tau) &= \psi^{(2)}(\tau) \\
&= q^{-1} - 24 + 276q - 2048q^2 + 11202q^3 - 49152q^4 + \dots, \\
f_{0,2}^{(2)}(\tau) &= \psi^{(2)}(\tau)^2 + 48\psi^{(2)}(\tau) \\
&= q^{-2} - 24 - 4096q + 98580q^2 - 1228800q^3 + 10745856q^4 + \dots, \\
f_{0,3}^{(2)}(\tau) &= \psi^{(2)}(\tau)^3 + 72\psi^{(2)}(\tau)^2 + 900\psi^{(2)}(\tau) \\
&= q^{-3} - 96 + 33606q - 1843200q^2 + 43434816q^3 - 648216576q^4 + \dots.
\end{aligned}$$

The function $f_{0,m}^{(p)}$ is a level p modular function that vanishes at 0 (if $m \neq 0$) and has a pole of order m at ∞. The conditions at the cusps determine this function uniquely; if two such functions exist, their difference is a holomorphic modular function, which must be a constant. Since both functions vanish at 0, this constant must be 0.

The functions composing these bases for $p = 2,3,5,7$ have divisibility properties which bear a striking resemblance to the divisibility properties of $j(\tau)$; in many cases they are identical. As an example of some of the divisibility properties we encounter with this basis, we experimentally examine the 2-adic valuation of the even-indexed coefficients of $f_{0,m}^{(2)}(\tau)$ for $m = 1,3,5,7$ in Table 1. As the data in the

table suggest, the 2-divisibility which $j(\tau)$ exhibits gives us a lower bound on the 2-divisibility of the odd-indexed $p = 2$ basis elements.

TABLE 1. 2-adic valuation of $a_0^{(2)}(m,n)$ compared to corresponding coefficients in $j(\tau)$

		$a_0^{(2)}(m,2)$	$a_0^{(2)}(m,4)$	$a_0^{(2)}(m,6)$	$a_0^{(2)}(m,8)$	$a_0^{(2)}(m,10)$	$a_0^{(2)}(m,12)$
m	1	11	14	13	17	12	16
	3	13	16	15	19	14	18
	5	12	15	14	18	13	17
	7	14	17	16	20	15	19
	min	11	14	13	17	12	16
$j(\tau)$		11	14	13	17	12	16

Note that these functions form a basis for $M_0^\infty(p)$, the space of modular forms of weight 0 and level p with poles allowed only at the cusp at ∞. A full basis for the space $M_0^!(p)$ of weakly holomorphic modular forms of weight 0 and level p is generated by the $f_{0,m}^{(p)}(\tau)$ and the functions $(\phi^{(p)}(\tau))^n$ for integers $n \geq 1$.

Recall that the concluding remarks of Lehner's second paper [8] state that the coefficients of certain level p modular functions having a pole of order less than p at ∞ have the same p-divisibility properties as the coefficients $c(n)$ of $j(\tau)$. More precisely, we have the following theorem.

Theorem 1 (Lehner)**.** *Let $p \in \{2,3,5,7\}$ and let $f(\tau)$ be a modular function on $\Gamma_0(p)$ having a pole at ∞ of order $< p$ and q-series of the form*

$$f(\tau) = \sum_{n=n_0}^{\infty} a(n)q^n,$$

$$f(-1/p\tau) = \sum_{m=m_0}^{\infty} b(n)q^n,$$

where $a(n), b(n) \in \mathbb{Z}$. Then the coefficients $a(n)$ satisfy the following congruence properties:

$$\begin{array}{lll} a(2^a n) \equiv 0 & \pmod{2^{3a+8}} & \text{if } p = 2, \\ a(3^a n) \equiv 0 & \pmod{3^{2a+3}} & \text{if } p = 3, \\ a(5^a n) \equiv 0 & \pmod{5^{a+1}} & \text{if } p = 5, \\ a(7^a n) \equiv 0 & \pmod{7^a} & \text{if } p = 7. \end{array}$$

Note that Lehner's original statement of this theorem mistakenly states that a function on $\Gamma_0(p)$ inherits the p-divisibility property for *every* prime in $\{2,3,5,7\}$, not just the prime matching the level.

A necessary condition in the statement of Lehner's theorem is that the function must have an integral q-expansion at 0. This condition is quite strong; in fact, neither the function $\phi^{(p)}(\tau)$ nor any of its powers satisfy it, although the functions $f_{0,m}^{(p)}(\tau)$ do.

Further, Lehner's theorem assumes that the order of the pole at ∞ must be less than p. In this paper, we remove this restriction on the order of the pole to show that every function in the $f_{0,m}^{(p)}$ basis has divisibility properties similar to those in Theorem 1. Specifically, we prove the following theorem.

Theorem 2. *Let $p \in \{2,3,5,7\}$, and let*

$$f_{0,m}^{(p)}(\tau) = q^{-m} + \sum_{n=0}^{\infty} a_0^{(p)}(m,n)q^n$$

be an element of the basis described above, with $m = p^\alpha m'$ and $(m',p) = 1$. Then, for $\beta > \alpha$,

$$\begin{aligned}
a_0^{(2)}(2^\alpha m', 2^\beta n) &\equiv 0 \pmod{2^{3(\beta-\alpha)+8}} && \text{if } p = 2,\\
a_0^{(3)}(3^\alpha m', 3^\beta n) &\equiv 0 \pmod{3^{2(\beta-\alpha)+3}} && \text{if } p = 3,\\
a_0^{(5)}(5^\alpha m', 5^\beta n) &\equiv 0 \pmod{5^{(\beta-\alpha)+1}} && \text{if } p = 5,\\
a_0^{(7)}(7^\alpha m', 7^\beta n) &\equiv 0 \pmod{7^{(\beta-\alpha)}} && \text{if } p = 7.
\end{aligned}$$

Note that for basis elements $f_{0,m}^{(p)}$ with $(m,p) = 1$, these divisibility properties match those in Theorem 1; in fact, Lehner's proof is easily extended to prove the congruences in these cases. For basis elements with $m = p^\alpha m'$ and $\alpha \geq 1$, the divisibility is "shifted". This shifting occurs in the $(\beta - \alpha)$ factor in the exponent of the modulus.

For the coefficients $a_0^{(p)}(p^\alpha m', p^\beta n)$ with $\alpha > \beta$, computations suggest that similar congruences should hold. Additionally, it appears that powers of the function $\phi^{(p)}(\tau)$ have Fourier coefficients with slightly weaker divisibility properties, despite the fact that their Fourier coefficients at 0 are not integral. It would be interesting to more fully understand these congruences.

2. Preliminary lemmas and definitions

In this section, we provide the necessary definitions and background for the proof of the main theorem.

For a prime p we define the level p Hecke operator U_p by

$$U_p f(\tau) = \frac{1}{p}\sum_{\ell=0}^{p-1} f\left(\frac{\tau+\ell}{p}\right),$$

using the notation $U_p^n f = U_p U_p \cdots U_p f$ for repeated applications of U_p. When f has the Fourier expansion $f(\tau) = \sum_{n=n_0}^{\infty} a(n)q^n$, this operator takes the form

$$U_p f(\tau) = \sum_{n=n_0}^{\infty} a(pn)q^n,$$

essentially "pulling out" all of the coefficients of f whose index is divisible by p. This operator preserves modularity: if f is a level p modular function, then $U_p f$ is also a level p modular function.

For the primes $p = 2,3,5,7$ the topological genus of $\Gamma_0(p)\backslash\mathcal{H}$ is zero, so the field of level p modular functions is generated by a single modular function called a Hauptmodul. For the primes under consideration, one such function is $\psi^{(p)}(\tau)$. Note that the modular function $\phi^{(p)}(\tau) = \psi^{(p)}(\tau)^{-1} = q + O(q^2)$ is also a Hauptmodul.

Further, for these primes, the fundamental domain for $\Gamma_0(p)$ has precisely two cusps, which may be taken to be at ∞ and at 0. Hence, we are most concerned with the behavior of these functions at ∞ and at 0. To switch between cusps, we make the substitution $\tau \mapsto -1/(p\tau)$. The following lemma gives relations for $\psi^{(p)}(\tau)$ and $\phi^{(p)}(\tau)$ at 0 and makes clear that powers of $\phi^{(p)}$ do not satisfy Lehner's integrality condition.

Lemma 3. *The functions $\psi^{(p)}(\tau)$ and $\phi^{(p)}(\tau)$ satisfy the relations*

$$\psi^{(p)}(-1/p\tau) = p^{\lambda/2}\phi^{(p)}(\tau), \tag{2.1}$$

$$\phi^{(p)}(-1/p\tau) = p^{-\lambda/2}\psi^{(p)}(\tau). \tag{2.2}$$

Proof. The functional equation for $\eta(\tau)$ is $\eta(-1/\tau) = \sqrt{-i\tau}\eta(\tau)$. Using this, we find that

$$\psi^{(p)}\left(\frac{-1}{p\tau}\right) = \left(\frac{\eta(-1/(p\tau)}{\eta(-1/\tau)}\right)^{\lambda} = \left(\frac{\sqrt{-ip\tau}\eta(p\tau)}{\sqrt{-i\tau}\eta(\tau)}\right)^{\lambda} = (\sqrt{p})^{\lambda}\left(\frac{\eta(p\tau)}{\eta(\tau)}\right)^{\lambda} = p^{\lambda/2}\phi^{(p)}(\tau).$$

The second statement follows after replacing τ by $-1/(p\tau)$ in the first statement. □

We next state a well-known lemma which gives a formula for determining the behavior of a modular function at 0 after U_p has been applied. A proof can be found in [2, p. 83].

Lemma 4. *Let p be prime and let $f(\tau)$ be a level p modular function. Then*

$$p(U_p f)(-1/(p\tau)) = p(U_p f)(p\tau) + f(-1/(p^2\tau)) - f(\tau). \tag{2.3}$$

Lehner's original papers included the following lemma and its proof, which gives two important equations. The first gives a formula for $U_p\phi^{(p)}$ as a polynomial with integral coefficients in $\phi^{(p)}$; the second gives an algebraic relation which is satisfied by $\phi^{(p)}(\tau/p)$.

Lemma 5. *Let $p \in \{2, 3, 5, 7\}$. Then there exist integers $b_j^{(p)}$ such that*

$$\textit{(a)} \quad U_p\phi^{(p)}(\tau) = p\sum_{j=1}^{p} b_j^{(p)}\phi^{(p)}(\tau)^j.$$

Further, let $h^{(p)}(\tau) = p^{\lambda/2}\phi^{(p)}(\tau/p)$. Then

$$\textit{(b)} \quad \left(h^{(p)}(\tau)\right)^p + \sum_{j=1}^{p}(-1)^j g_j(\tau)\left(h^{(p)}(\tau)\right)^{p-j} = 0,$$

where $g_j(\tau) = (-1)^{j+1}p^{\lambda/2+2}\sum_{\ell=j}^{p} b_\ell^{(p)}\phi^{(p)}(\tau)^{\ell-j+1}$.

Proof. (a) Since ϕ vanishes at ∞, $U_p\phi$ also vanishes at ∞; we will now consider its behavior at 0. Using (2.3) and replacing τ by $p\tau$ in (2.1) we obtain

$$\begin{aligned} U_p\phi(-1/(p\tau)) &= U_p\phi(p\tau) + p^{-1}\phi(-1/(p^2\tau)) - p^{-1}\phi(\tau) \\ &= U_p\phi(p\tau) + p^{-1}\psi(p\tau) - p^{-1}\phi(\tau) \\ &= O(q^p) + p^{-\lambda/2-1}q^{-p} + O(1) - p^{-1}q + O(q^2), \\ p^{\lambda/2+1}U_p\phi(-1/(p\tau)) &= q^{-p} + O(1). \end{aligned}$$

The right side of this equation is a level p modular function with integer coefficients, so we may write it as a polynomial in $\psi(\tau)$ with integer coefficients. The polynomial will not have a constant term since the left side vanishes at 0. Therefore,

$$p^{\lambda/2+1}U_p\phi(-1/(p\tau)) = \sum_{j=1}^{p} c_j\psi(\tau)^j.$$

Now, replacing τ by $-1/(p\tau)$, we find that

$$p^{\lambda/2+1}U_p\phi(\tau) = \sum_{j=1}^{p} c_j p^{\lambda j/2}\phi(\tau)^j.$$

After cancelling the $p^{\lambda/2+1}$, we find that $U_p\phi(\tau) = \sum_{j=1}^{p} c'_j\phi(\tau)^j$ and we compute the coefficients c'_j (the authors used MATHEMATICA). The computation is finite, and we find that each coefficient c'_j has a factor of p, so the coefficients $b_j^{(p)}$ are integral. A complete table of values of the $b_j^{(p)}$ is found in Table 2.

TABLE 2. Values of $b_j^{(p)}$

		p			
		2	3	5	7
j	1	$3\cdot 2^2$	$10\cdot 3^1$	$63\cdot 5^0$	$82\cdot 7^0$
	2	2^{10}	$4\cdot 3^6$	$52\cdot 5^3$	$176\cdot 7^2$
	3		3^{10}	$63\cdot 5^5$	$845\cdot 7^3$
	4			$6\cdot 5^8$	$272\cdot 7^5$
	5			5^{10}	$46\cdot 7^7$
	6				$4\cdot 7^9$
	7				7^{10}

(b) We again apply (2.3) to $\phi(\tau)$, this time using what we know from (a):

$$pU_p\phi(-1/(p\tau)) = pU_p\phi(p\tau) + \phi(-1/(p^2\tau)) - \phi(\tau),$$

$$p^2\sum_{j=1}^{p} b_j^{(p)}\phi(-1/(p\tau))^j = p^2\sum_{j=1}^{p} b_j^{(p)}\phi(p\tau)^j + \phi(-1/(p^2\tau)) - \phi(\tau).$$

We now use Lemma 3 with the knowledge that $\psi(\tau) = \phi(\tau)^{-1}$ to obtain

$$p^2\sum_{j=1}^{p} b_j^{(p)}p^{-\lambda j/2}\phi(\tau)^{-j} - p^2\sum_{j=1}^{p} b_j^{(p)}\phi(p\tau)^j + \phi(\tau) - p^{-\lambda/2}\phi(p\tau)^{-1} = 0.$$

After replacing τ by τ/p and multiplying by $p^{\lambda/2}$, we obtain

$$p^{\lambda/2+2}\sum_{j=1}^{p} b_j^{(p)}\big(h(\tau)^{-j} - \phi(\tau)^j\big) + h(\tau) - \phi(\tau)^{-1} = 0. \tag{2.4}$$

We now divide by $h^{-1} - \phi$. Note two facts:

$$h^{-j} - \phi^j = (h^{-1} - \phi) \sum_{\ell=0}^{j-1} h^{-\ell} \phi^{j-\ell-1},$$

$$\frac{h - \phi^{-1}}{h^{-1} - \phi} = \frac{h(h\phi - 1)}{\phi(1 - h\phi)} = -\frac{h}{\phi}.$$

So (2.4) becomes

$$p^{\lambda/2+2} \sum_{j=1}^{p} b_j^{(p)} \sum_{\ell=0}^{j-1} h^{-\ell} \phi^{j-\ell-1} - \phi^{-1} h = 0,$$

which, after multiplying by ϕh^{p-1}, becomes

$$p^{\lambda/2+2} \sum_{j=1}^{p} b_j^{(p)} \sum_{\ell=0}^{j-1} h^{p-\ell-1} \phi^{j-\ell} - h^p = 0.$$

We now change the order of summation and rearrange terms to obtain the desired formula:

$$h(\tau)^p = \sum_{j=1}^{p} \big(p^{\lambda/2+2} \sum_{\ell=j}^{p} b_\ell^{(p)} \phi(\tau)^{\ell-j+1}\big) h(\tau)^{p-j}. \qquad \square$$

The next lemma states that when you apply U_p to a certain type of polynomial in ϕ_p, you get a similar polynomial back which has picked up a power of p. The details of this lemma are found in both [7] and [8], scattered throughout the proofs of the main theorems. For our purposes, it will be more useful in the following form.

Lemma 6. *Let $p \in \{2, 3, 5, 7\}$ and let $R^{(p)}$ denote the set of polynomials in $\phi^{(p)}$ of the form*

$$d_1 \phi^{(p)}(\tau) + \sum_{n=2}^{N} d_n p^\gamma \phi^{(p)}(\tau)^n,$$

$$\text{where } \gamma = \begin{cases} 8(n-1) & \text{if } p = 2, \\ 4(n-1) & \text{if } p = 3, \\ n & \text{if } p = 5, \\ n & \text{if } p = 7. \end{cases}$$

Then U_p maps $R^{(p)}$ to $p^\delta R^{(p)}$ where $\delta = 3, 2, 1, 1$ for $p = 2, 3, 5, 7$, respectively. That is, applying U_p to a polynomial of the above form yields a polynomial of the same form with an extra factor of p^δ.

Proof. Consider the function

$$d_1 U_p \phi(\tau) + \sum_{n=2}^{r} d_n p^\gamma U_p \phi(\tau)^n.$$

For the first term, Lemma 5(a) shows that $U_p \phi(\tau) \in p^\delta R_p$ since, by inspection, the $b_j^{(p)}$ integers are divisible by sufficiently high powers of p.

For the remaining terms, we will prove that

$$p^{\gamma} U_p \phi^n = p^{\delta} r, \tag{2.5}$$

where $r \in R_p$. The result will immediately follow.

By the definition of U_p we have

$$U_p \phi^n = p^{-1} \sum_{\ell=0}^{p-1} \phi\left(\frac{\tau+\ell}{p}\right)^n = p^{-1-\lambda t/2} \sum_{\ell=0}^{p-1} h_\ell(\tau)^n, \tag{2.6}$$

where $h_\ell(\tau) = p^{\lambda/2}\phi\left(\frac{\tau+\ell}{p}\right)$ is related to h from Lemma 5(b). Let S_n be the sum of the nth powers of the h_ℓ so that

$$S_n = \sum_{\ell=0}^{p-1} h_\ell^n.$$

Define the polynomial $F(x) = \sum_{j=0}^{p}(-1)^j g_j(\tau) x^{p-j}$, where the $g_j(\tau)$ are as in Lemma 5. In the same lemma, if we replace τ with $\tau+\ell$, the $g_j(\tau)$ are unaffected since $\phi(\tau+1) = \phi(\tau)$. Therefore, that lemma tells us that the p roots of the polynomial $F(x)$ are precisely the h_ℓ. Using Newton's formula for the nth power sum of the roots of a polynomial, we obtain

$$S_n = \sum_{\ell=0}^{p-1} h_\ell^n = \sum_{j=1}^{n} (-1)^{j+1} g_j S_{n-j}, \tag{2.7}$$

where $g_j = 0$ for $j > p$ and $S_0 = n$.

We now proceed case-by-case. The $p = 2$ case illustrates the method, so we will only include the intermediate steps in the $p = 3, 5, 7$ cases.

Case 1. $p = 2$. Then, using (2.6), equation (2.5) is equivalent to

$$2^{8(n-1)}\left(2^{-1-12n} S_n\right) = 2^3 r \text{ or}$$

$$S_n = 2^{4n+12} r. \tag{2.8}$$

We now use (2.7) to calculate S_1 and S_2:

$$S_1 = g(1),$$

$$S_2 = g_1 S_1 - 2g_2 = g_1^2 - 2g_2.$$

From Lemma 5 we can compute the values of the g_j. Using the b_j values from the table in that lemma, we have

$$g_1 = 2^{14}(b_1\phi_2 + b_2\phi_2^2) = 2^{16}(3\phi_2 + 2^8\phi_2^2),$$

$$g_2 = -2^{14} b_2 \phi_2 = -2^{24}\phi_2.$$

We can now see that

$$S_1 = g_1 = 2^{16}(3\phi_2 + 2^8\phi_2^2),$$

$$S_2 = 2^{32}(3\phi_2 + 2^8\phi_2^2)^2 + 2^{25}\phi_2 = 2^{20}(2^5\phi_2 + 2^{12}3^2\phi_2^2 + 2^{21}3\phi_2^3 + 2^{28}\phi_2^4).$$

Thus (2.8) is satisfied for $n = 1, 2$. We proceed by induction. Assume (2.8) is satisfied for all integers $< n$. We show that it is satisfied for n. For ease of

computation, we introduce the set

$$R^* = 2^8 R^{(2)} = \left\{ \sum_{i=1}^{m} d_i 2^{8i} \phi_2^i \middle| d_i \in \mathbb{Z}, m \in \mathbb{Z}^+ \right\},$$

which, the reader will notice, is a ring without 1. From (2.7) we obtain

$$S_n = g_1 S_{n-1} - g_2 S_{n-2} = 2^8 r_1^* \cdot 2^{4n} r_2^* + 2^{16} r_3^* \cdot 2^{4(n-1)} r_4^* = 2^{4n+8} r_5^* = 2^{4n+16} r,$$

where $r_i^* \in R^*$ and $r \in R^{(2)}$.

Case 2. $p = 3$. We want to show that

$$S_n = 3^{2n+7} r, \tag{2.9}$$

where $r \in R^{(3)}$. We compute the g_j and S_n as follows, using the b_j from the table:

$$g_1 = 3^9(3^9\phi_3^3 + 3^5 4\phi_3^2 + 10\phi_3), \quad g_2 = 3^{14}(-3^4\phi_3^2 - 4\phi_3), \quad g_3 = 3^{18}\phi_3,$$
$$S_1 = g_1, \quad S_2 = g_1^2 - 2g_2, \quad S_3 = {g_1}^3 - 3g_1 g_2 + 3g_3.$$

From this, we obtain

$$\begin{aligned} S_1 &= 3^9(3^9\phi_3^3 + 3^5 4\phi_3^2 + 10\phi_3), \\ S_2 &= 3^{14}(8\phi_3 + 3^5 34\phi_3^2 + 3^9 80\phi_3^3 + 3^{13} 68\phi_3^4 + 3^{18} 8\phi_3^5 + 3^{25}\phi_3^6), \\ S_3 &= 3^{19}(\phi_3 + 3^5 40\phi_3^2 + 3^8 1174\phi_3^3 + 3^{15} 136\phi_3^4 + 3^{18} 581\phi_3^5 + 3^{25} 16\phi_3^6 \\ &\qquad + 3^{27} 58\phi_3^7 + 3^{32} 4\phi_3^8 + 3^{35}\phi_3^9) \end{aligned}$$

which proves (2.9) for $n = 1, 2, 3$. For the inductive step, let R^* be the ring without 1 given by $3^4 R^{(3)}$ so that

$$\begin{aligned} S_n &= g_1 S_{n-1} - g_2 S_{n-2} + g_3 S_{n-3} \\ &= 3^5 r_1^* 3^{2n+1} r_2^* + 3^{10} r_3^* 3^{2n-1} r_4^* + 3^{14} r_5^* 3^{2n-3} r_6^* \\ &= 3^{2n+6} r_7^* \\ &= 3^{2n+10} r, \end{aligned}$$

where $r_i^* \in R^*$ and $r \in R^{(3)}$.

Case 3. $p = 5$. We want

$$S_n = 5^{2n+2} r, \tag{2.10}$$

where $r \in R^{(5)}$. Computing the S_n we find

$$S_1 = 5^5 r_1, \quad S_2 = 5^8 r_2, \quad S_3 = 5^{10} r_3,$$
$$S_4 = 5^{13} r_4, \quad S_5 = 5^{16} r_5$$

for some $r_1, \ldots, r_5 \in R^{(5)}$. This proves (2.10) for $n = 1, \ldots, 5$. For the inductive step, let R^* be the ring without 1 given by $5R^{(5)}$ so that

$$\begin{aligned} S_n &= g_1 S_{n-1} - g_2 S_{n-2} + g_3 S_{n-3} - g_4 S_{n-4} + g_5 S_{n-5} \\ &= 5^4 r_1^* 5^{2n-1} r_2^* - \ldots + 5^{14} r_9^* 5^{2n-9} r_{10}^* \\ &= 5^{2n+3} r_{11}^* \\ &= 5^{2n+4} r, \end{aligned}$$

where $r_i^* \in R^*$ and $r \in R^{(5)}$.

Case 4. $p = 7$. We want

$$S_n = 7^{n+2} r, \tag{2.11}$$

where $r \in R^{(7)}$. Computing the S_n we find

$$S_1 = 7^4 r_1, \quad S_2 = 7^6 r_2, \quad S_3 = 7^7 r_3, \quad S_4 = 7^9 r_4,$$
$$S_5 = 7^{11} r_5, \quad S_6 = 7^{13} r_6, \quad S_7 = 7^{15} r_7$$

for some $r_1, \ldots, r_7 \in R^{(7)}$. This proves (2.11) for $n = 1, \ldots, 7$. For the inductive step, let R^* be the ring without 1 given by $7R^{(7)}$ so that

$$\begin{aligned} S_n &= \sum_{i=1}^{7} (-1)^{i+1} g_i S_{n-i} \\ &= 7^3 r_1^* 7^n r_2^* - \ldots + 7^{13} r_{13}^* 7^{n-6} r_{14}^* \\ &= 7^{n+3} r_{15}^* \\ &= 7^{n+4} r, \end{aligned}$$

where $r_i^* \in R^*$ and $r \in R^{(7)}$. □

3. Proof of the theorem

To remind the reader of the main result of the paper, we include it here.

Theorem. *Let $p \in \{2, 3, 5, 7\}$ and let $f_{0,m}^{(p)}(\tau) = q^{-m} + \sum a_0^{(p)}(m,n) q^n$ be an element of the basis described above, with $m = p^\alpha m'$ and $(m', p) = 1$. Then, for $\beta > \alpha$,*

$$\begin{array}{lll} a_0^{(2)}(2^\alpha m', 2^\beta n) \equiv 0 & \pmod{2^{3(\beta-\alpha)+8}} & \text{if } p = 2, \\ a_0^{(3)}(3^\alpha m', 3^\beta n) \equiv 0 & \pmod{3^{2(\beta-\alpha)+3}} & \text{if } p = 3, \\ a_0^{(5)}(5^\alpha m', 5^\beta n) \equiv 0 & \pmod{5^{(\beta-\alpha)+1}} & \text{if } p = 5, \\ a_0^{(7)}(7^\alpha m', 7^\beta n) \equiv 0 & \pmod{7^{(\beta-\alpha)}} & \text{if } p = 7. \end{array}$$

The proof is in three cases. The first illustrates the method for the simplest basis elements, namely those with $(m, p) = 1$. The second demonstrates the "shifting" property at its first occurrence, $f_{0,p}^{(p)}$. The third is the general case; it builds inductively upon the methods of the first two cases.

3.1. **Case 1:** $(m, p) = 1$.

Proof. This proof is almost identical to Lehner's proof of Theorem 3 in [8]; however, it applies not only to functions which have poles of order bounded by p but to all basis elements with $(m, p) = 1$. For ease of notation, let $f(\tau) = f_{0,m}^{(p)}(\tau)$.

We will demonstrate the method with $m = 1$, then generalize it to all m relatively prime to p. First, we will write $U_p f(\tau)$ as a polynomial in $\phi(\tau)$ with integral coefficients, all of which are divisible by the desired power of p. Since U_p isolates the coefficients whose index is divisible by p, we will have proven the theorem for $\beta = 1$. We will then apply U_p repeatedly to the polynomial, showing that the result is always another polynomial in ϕ with integral coefficients, all of which are divisible by the desired higher power of p.

Consider the level p modular function $g(\tau) = pU_p f(\tau) + p^{\lambda/2}\phi(\tau)$. Notice that $g(\tau)$ is holomorphic at ∞ since both $U_p f(\tau)$ and $\phi(\tau)$ are holomorphic there. The q-expansion at 0 for $g(\tau)$ is given by

$$g(-1/(p\tau)) = p(U_p f)(-1/(p\tau)) + p^{\lambda/2}\phi(-1/(p\tau)),$$

which, by Lemmas 3 and 4 becomes

$$g(-1/(p\tau)) = p(U_p f)(p\tau) + f(-1/(p^2\tau)) - f(\tau) + \psi(\tau).$$

When we notice that $f(\tau) = \psi(\tau)$ in this $m = 1$ case, we obtain

$$\begin{aligned} g(-1/(p\tau)) &= p(U_p f)(p\tau) + \psi(-1/(p^2\tau)) - \psi(\tau) + \psi(\tau) \\ &= p(U_p f)(p\tau) + p^{\lambda/2}\phi(p\tau), \end{aligned}$$

which is holomorphic at ∞. Hence, $g(\tau)$ is a holomorphic modular function on $\Gamma_0(p)$, so it must be constant. Therefore,

$$U_p f(\tau) = c_0 - p^{\lambda/2-1}\phi(\tau) \tag{3.1}$$

for some constant c_0. The proof is complete for $\beta = 1$.

Note: The prime 13, having genus zero, would work in this construction; however, in that case $\lambda = \frac{24}{13-1} = 2$, so $13^{\lambda/2-1} = 1$, and we gain no new information.

We now iterate the above process to prove the theorem for $\beta > 1$. Notice that

$$U_p(U_p f(\tau)) = c^{(p)} - p^{\lambda/2-1}U_p\phi(\tau).$$

We know from Lemma 5 that $U_p\phi$ is a polynomial in ϕ; in fact, by inspection of the $b_j^{(p)}$ values we see that we may write

$$\begin{aligned} U_2\phi^{(2)}(\tau) &= 2^3\big(d_1^{(2)}\phi^{(2)}(\tau) + \sum_{n=2}^{2} d_n^{(2)}2^{8(n-1)}\phi^{(2)}(\tau)^n\big), \\ U_3\phi^{(3)}(\tau) &= 3^2\big(d_1^{(3)}\phi^{(3)}(\tau) + \sum_{n=2}^{3} d_n^{(3)}3^{4(n-1)}\phi^{(3)}(\tau)^n\big), \\ U_5\phi^{(5)}(\tau) &= 5\big(d_1^{(5)}\phi^{(5)}(\tau) + \sum_{n=2}^{5} d_n^{(5)}5^n\phi^{(5)}(\tau)^n\big), \\ U_7\phi^{(7)}(\tau) &= 7\big(d_1^{(7)}\phi^{(7)}(\tau) + \sum_{n=2}^{7} d_n^{(7)}7^n\phi^{(7)}(\tau)^n\big) \end{aligned}$$

for some integers $d_n^{(p)}$. This shows that the second U_p iteration is divisible by the correct power of p. Further, it gives us a polynomial of a suitable form to iterate the process using Lemma 6. In each of the polynomials above, notice that $U_p\phi(\tau) = p^\delta r$ for some $r \in R^{(p)}$. Using Lemma 6, we find that

$$U_p(U_p\phi)(\tau) = p^{2\delta}r'$$

for some $r' \in R^{(p)}$, and further

$$U_p^\beta\phi(\tau) = p^{\beta\delta}r^{(\beta)}$$

for some $r_\beta \in R^{(p)}$. This completes the proof for $m = 1$.

Now, if $(m, p) = 1$, then $U_p f(\tau)$ is holomorphic at ∞, just as it was with $m = 1$. Moving to the cusp at 0 we find that $(U_p f)(-1/(p\tau))$ can be written as a polynomial

in $\psi(\tau)$ which appears as a polynomial in $\phi(\tau)$ when we return to ∞. Similar to (3.1), we obtain the equality

$$U_p f(\tau) = c_0 + \sum_{i=1}^{M} p^{\lambda i/2-1} c_i \phi(\tau)^i$$

for some $c_i \in \mathbb{Z}$ and $M \in \mathbb{Z}^+$. The only difference between this equation and (3.1) is that in this more general case, we find that $U_p f$ is a higher-degree polynomial in ϕ. This formula can easily be iterated as before to obtain the desired result. □

3.2. **Case 2:** $m = p$.

Proof. Again, for ease of notation, denote $f_{0,p}^{(p)}(\tau)$ by $f(\tau)$. For the $m = p$ case, we will proceed as before; however, we will find that $U_p f(\tau)$ has poles at both ∞ and 0 and that $U_p f(\tau)$ does not possess any interesting divisibility properties, but $U_p^2 f(\tau)$ does. This property will manifest itself as the "shifting" previously mentioned.

Notice first that $U_p f(\tau) = q^{-1} + O(1)$ has a simple pole at ∞. Therefore, we shall deal primarily with the function $U_p f(\tau) - \psi(\tau)$, which is holomorphic at ∞. We can use Lemmas 3 and 4 to view this function at 0:

$$\begin{aligned} p(U_p f)\left(\frac{-1}{p\tau}\right) - p\psi\left(\frac{-1}{p\tau}\right) &= p(U_p f)(p\tau) + f\left(\frac{-1}{p^2\tau}\right) - f(\tau) - p^{\lambda/2+1}\phi(\tau) \\ &= pq^{-p} + O(1) + O(1) - q^{-p} + O(1) + O(q) \\ &= c_0 + \sum_{i=1}^{p} c_i \psi(\tau)^i \end{aligned}$$

for some integers c_i. Replacing τ by $-1/(p\tau)$, we obtain

$$(U_p f)(\tau) = \frac{c_0}{p} + \psi(\tau) + \sum_{i=1}^{p} c_i p^{\lambda i/2-1} \phi(\tau)^i. \tag{3.2}$$

The $\psi(\tau)$ term in the equation makes any attempt at p-divisibility fail; for example, computation shows that the 7th coefficient of $\psi^{(2)}(\tau)$ is odd. However, $\psi(\tau)$ satisfies Lehner's divisibility properties, so $U_p f$ inherits its p-divisibility from $\psi(\tau)$. So the function

$$U_p^2 f(\tau) = c_0 + U_p\psi(\tau) + \sum_{i=1}^{p} c_i p^{\lambda i/2-1} U_p \phi(\tau)^i$$

has the same p-divisibility as $f_{0,1}^{(p)}$, hence, the shift. □

3.3. **Case 3:** $m = p^\alpha m'$.

Proof. We prove this case using induction on α. Case 1 showed that the theorem is true for all m' relatively prime to p, so the $\alpha = 0$ base case is complete. Assume Theorem 2 holds for all m of the form $m = p^\ell m'$ with $\ell < \alpha$. We will show that it holds for $m = p^\alpha m'$. To simplify notation, let $f_\alpha(\tau) = f_{0,p^\alpha m'}^{(p)}(\tau)$.

Since $f_\alpha(\tau) = q^{-p^\alpha m'} + O(1)$, we find that $U_p f_\alpha(\tau) = q^{-p^{\alpha-1} m'} + O(1)$ has a pole of order $p^{\alpha-1}m'$ at ∞. So we focus our attention on $U_p f_\alpha(\tau) - f_{\alpha-1}(\tau)$, which

is holomorphic at ∞. Using (2.3) we examine this function at 0:

$$\begin{aligned} p(U_p f_\alpha)\left(\frac{-1}{p\tau}\right) - p f_{\alpha-1}\left(\frac{-1}{p\tau}\right) &= p(U_p f_\alpha)(p\tau) + f_\alpha\left(\frac{-1}{p^2\tau}\right) - f_\alpha(\tau) - p f_{\alpha-1}\left(\frac{-1}{p\tau}\right) \\ &= pq^{-p^\alpha m'} + O(1) + O(1) - q^{-p^\alpha m'} - O(1) - O(1) \\ &= (p-1)q^{-p^\alpha m'} + O(1). \end{aligned}$$

As before, we write this function as a polynomial in $\psi(\tau)$ with integral coefficients c_i:

$$p(U_p f_\alpha)\left(\frac{-1}{p\tau}\right) - p f_{\alpha-1}\left(\frac{-1}{p\tau}\right) = c_0 + \sum_{i=1}^{p^\alpha m'} c_i \psi(\tau)^i,$$

which, after switching back to the q-expansion at ∞, becomes

$$U_p f_\alpha(\tau) = \frac{c_0}{p} + f_{\alpha-1}(\tau) + \frac{1}{p}\sum_{i=1}^{p^\alpha m'} c_i p^{\lambda i/2}\phi(\tau)^i. \tag{3.3}$$

Notice that (3.3) looks very similar to (3.2), where $\psi(\tau)$ is replaced by $f_{\alpha-1}(\tau)$, so $U_p f_\alpha(\tau)$ inherits whatever divisibility properties $f_{\alpha-1}(\tau)$ has. Our inductive hypothesis states that $f_{\alpha-1}(\tau)$ exhibits Lehner's divisibility properties only after U_p is applied $\alpha - 1$ times. Therefore, applying U_p to (3.3) $\alpha - 1$ times, we obtain

$$U_p^\alpha f_\alpha(\tau) = \frac{c_0}{p} + U_p^{\alpha-1} f_{\alpha-1}(\tau) + \frac{1}{p}\sum_{i=1}^{p^\alpha m'} c_i p^{\lambda i/2} U_p^{\alpha-1}\phi(\tau)^i,$$

showing that $U_p^\alpha f_\alpha(\tau)$ exhibits Lehner's divisibility properties. □

References

1. Scott Ahlgren. The theta-operator and the divisors of modular forms on genus zero subgroups. *Math. Res. Lett.*, 10(5-6):787–798, 2003. MR2024734 (2004m:11059)
2. Tom M. Apostol. *Modular functions and Dirichlet series in number theory*, volume 41 of Graduate Texts in Mathematics. Springer-Verlag, New York, second edition, 1990. MR1027834 (90j:11001)
3. D. Doud, P. Jenkins, and J. Lopez. Two-divisibility of the coefficients of certain weakly holomorphic modular forms. Ramanujan Journal, 2012, doi:10.1007/s11139-011-9331-0, arXiv:1105.0684v1 [math.NT].
4. Darrin Doud and Paul Jenkins. p-adic properties of coefficients of weakly holomorphic modular forms. *Int. Math. Res. Not. IMRN*, (16):3184–3206, 2010. MR2673723 (2011j:11081)
5. W. Duke and Paul Jenkins. On the zeros and coefficients of certain weakly holomorphic modular forms. *Pure Appl. Math. Q.*, 4(4), Special Issue: In honor of Jean-Pierre Serre. Part 1:1327–1340, 2008. MR2441704 (2010a:11068)
6. M. Griffin. Divisibility properties of coefficients of weight 0 weakly holomorphic modular forms. *International Journal of Number Theory*, 7(4):933–941, 2011, DOI 10.1142/S1793042111004599.
7. Joseph Lehner. Divisibility properties of the Fourier coefficients of the modular invariant $j(\tau)$. *Amer. J. Math.*, 71(1):136–148, Jan. 1949. MR0027801 (10:357a)
8. Joseph Lehner. Further congruence properties of the Fourier coefficients of the modular invariant $j(\tau)$. *Amer. J. Math.*, 71(2):373–386, April 1949. MR0027802 (10:357b)

Department of Mathematics, University of Illinois, Urbana, Illinois 61801
E-mail address: nickolasandersen@gmail.com

Department of Mathematics, Brigham Young University, Provo, Utah 84602
E-mail address: jenkins@math.byu.edu