2020-03-01

# Congruences for Coefficients of Modular Functions in Levels 3, 5, and 7 with Poles at 0

Ryan Austin Keck
*Brigham Young University*

# Congruences for Coefficients of Modular Functions in Levels 3, 5, and 7 with Poles at 0

Ryan Austin Keck

A thesis submitted to the faculty of
Brigham Young University
in partial fulfillment of the requirements for the degree of

Master of Science

Paul Jenkins, Chair
Nick Andersen
Michael Griffin
Pace Nielsen

Department of Mathematics

Brigham Young University

# ABSTRACT

## Congruences for Coefficients of Modular Functions in Levels 3, 5, and 7 with Poles at 0

Ryan Austin Keck
Department of Mathematics, BYU
Master of Science

We give congruences modulo powers of $p \in \{3, 5, 7\}$ for the Fourier coefficients of certain modular functions in level $p$ with poles only at 0, answering a question posed by Andersen and Jenkins and continuing work done by the Jenkins, the author, and Moss. The congruences involve a modulus that depends on the base $p$ expansion of the modular form's order of vanishing at $\infty$.

Keywords: modular forms, congruences, Fourier coefficients

# Contents

# List of Tables

# Chapter 1. Introduction

A modular form $f(z)$ of level $N$ and weight $k$ is a complex valued function which is holomorphic on the upper half plane, satisfies the equation

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z) \text{ for all } \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N),$$

and is holomorphic at the cusps of $\Gamma_0(N)$. Letting $q = e^{2\pi i z}$, modular forms have a Fourier expansion $f(z) = \sum_{n\geq 0} a(n)q^n$ with Fourier coefficients $a(n)$. A *weakly holomorphic* modular form is a modular form that is allowed to be meromorphic at the cusps; we define $M_k^\sharp(N)$ to be the space of weakly holomorphic modular forms of weight $k$ and level $N$ that are holomorphic away from the cusp at $\infty$, and in the same notation as [7], we use $M_k^\flat(N)$ to denote forms holomorphic away from the cusp at 0. For prime $N$, these are the only cusps. Modular forms in both of these spaces also have Fourier expansions at infinity, where the constraint $n \geq 0$ is relaxed to $n \gg -\infty$ if the form has a pole at infinity.

The Fourier coefficients of modular forms often satisfy interesting congruences. For the $j$-invariant $j(z) = q^{-1} + 744 + \sum_{n=1}^{\infty} c(n)q^n \in M_0^\sharp(1)$, Lehner [11, 12] proved that the $c(n)$ satisfy the congruence

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

Kolberg [9, 10], Aas [1], and Allatt and Slater [2] strengthened Lehner's congruences for $j(z)$. Furthermore, Griffin [6] gave a canonical basis for $M_0^\sharp(1)$ and extended Kolberg's and Aas's results to the basis elements. Similarly, Jenkins, Andersen, and Thornton [3, 8] proved congruences for the Fourier coefficients of elements of canonical bases for $M_0^\sharp(p)$ with $p = 2, 3, 5, 7$. Jenkins, the author, and Moss [7] proved congruences for the Fourier coefficients of elements of a canonical basis for $M_0^\flat(2)$. It is natural to wonder whether a similar result holds for bases of $M_0^\flat(p)$ for the other genus zero primes, mirroring the results of $M_0^\sharp(p)$.

Let $p \in \{2,3,5,7,13\}$. Taking $\eta(z) = q^{\frac{1}{24}} \prod_{n=1}^\infty (1-q^n)$ to be the Dedekind eta function, a Hauptmodul for $\Gamma_0(p)$ is

$$\phi^{(p)}(z) = \left(\frac{\eta(pz)}{\eta(z)}\right)^{24/(p-1)} = q + \frac{24}{p-1}q^2 + \cdots,$$

which vanishes at $\infty$ and has a pole only at 0. The functions $(\phi^{(p)}(z))^m$ for $m \geq 0$ are a basis for $M_0^\flat(p)$. Andersen and the Jenkins used powers of $\phi^{(p)}(z)$ to prove congruences involving $\psi^{(p)} = \frac{1}{\phi^{(p)}} = q^{-1} - \frac{24}{p-1} + \cdots \in M_0^\sharp(p)$ in [3], and made the following remark: "Additionally, it appears that powers of the function $[\phi^{(p)}(z)]$ have Fourier coefficients with slightly weaker divisibility properties... It would be interesting to more fully understand these congruences." The Jenkins, the author, and Moss in [7] proved congruences for the Fourier coefficients of $\phi^{(2)}(z)$ and its powers. In this paper, we use similar techniques to obtain congruences for $\phi^{(p)}(z)$ and its powers for $p = 3, 5, 7$.

Write $\phi^{(p)}(z)^m = \sum_{n=m}^\infty a^{(p)}(m,n)q^n$. Let $\chi_S$ be the characteristic function on $S$, which outputs 1 when the input is an element of $S$ and 0 otherwise. The main result of this paper is the following theorem.

**Theorem 1.1.** *Let $p \in \{3,5,7\}$. Let $n = p^\alpha n'$ where $p \nmid n'$. Express the base $p$ expansion of $m$ as $a = \sum_{i=1}^\infty a_i p^{i-1}$, where $a_i = 0$ for all sufficiently large $i$. Consider the rightmost $\alpha$ digits $a_\alpha \ldots a_2 a_1$. Let $i'$ be the index of the rightmost nonzero digit, or $i' = -1$ if $a_1 = a_2 = \cdots = a_\alpha = 0$. Let*

$$\gamma_3(m,\alpha) = \begin{cases} 3 - a_{i'} + 2\#\{\, i \mid a_i = 0, i > i' \,\} + \#\{\, i \mid a_i = 1, i > i' \,\} & \textit{if } i' \geq 0, \\ 0 & \textit{otherwise.} \end{cases}$$

$$\gamma_5(m,\alpha) = \gamma_7(m,\alpha) = \begin{cases} \chi_{\{1,2\}}(a_{i'}) + \#\{\, i \mid a_i \in \{0,1\}, i > i' \,\} & \textit{if } i' \geq 0, \\ 0 & \textit{otherwise.} \end{cases}$$

*Then*

$$a^{(p)}(m, p^{\alpha}n') \equiv 0 \pmod{p^{\gamma_p(m,\alpha)}}.$$

The power of $p$ in the congruence includes a count of the number of digits in the base $p$ expansion of $m$ that are 0, 1, or 2. This result is similar to the one found for $\phi^{(2)}$, but it is more complicated to state because there are more digits in bases $3, 5, 7$. We note that this congruence is not sharp. For $m = 1$, Allatt and Slater in [2] proved a stronger result that provides an exact congruence for many $n$.

As an example, the base 3 expansion for $m = 102$ is $m = \cdots 00010210$. Table 1 gives values of $\gamma_3$.

| $\alpha$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | $\cdots$ | $\alpha$ | $\cdots$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\gamma(40, \alpha)$ | 0 | 0 | 2 | 2 | 4 | 5 | 7 | 9 | 11 | 13 | $\cdots$ | $2(\alpha - 5) + 5$ | $\cdots$ |

Table 1.1: Values of $\gamma_3(m, \alpha)$ for $m = 102$

Notice that once $\alpha$ surpasses 5—the leftmost nonzero digit in the base 3 expansion of $m$ occurs in the 5th place—$\gamma_3$ always increases by 2 as $\alpha$ increases by 1. This illustrates that $\gamma_3(m, \alpha)$ is unbounded for a fixed $m$. Similar examples can be constructed for $\gamma_5$ and $\gamma_7$.

Chapter 2 contains the machinery and definitions we use for proving Theorem 1.1, and the proof itself is in Chapter 3. In Chapter 4 we discuss the $p = 13$ case; although 13 is also a genus zero prime we do not obtain congruences modulo 13.

# Chapter 2. Preliminary Lemmas

We prove Theorem 1.1 by first proving several facts about $\phi^{(p)}$, which is where we begin in this chapter. Most importantly, $U_p(\phi^{(p)})$ is a polynomial with integer coefficients in $\phi^{(p)}$ for the Hecke operator $U_p$, which acts on a Fourier expansion by dividing the power of $q$ by $p$ and throwing away non-integer powers. This means that if $U_p(\phi^{(p)})$, as a polynomial in $\phi^{(p)}$, has all coefficients divisible by some number, then every $p$th coefficient of $\phi^{(p)}$ is divisible by that number. The same holds true for applying $U_p$ to any power of $\phi^{(p)}$ as well.

One can also consider $U_p$ as a sum of Möbius transformations of a given function. We find a polynomial with functions as its coefficients such that when we evaluate it at the proper Möbius transformations of $\phi^{(p)}$, we get zero.

The operator $U_p$ on a function $f(z)$ is given by

$$U_p f(z) = \frac{1}{p} \sum_{j=0}^{p-1} f\left(\frac{z+j}{p}\right).$$

Let $M_k^!(N)$ be the space of weakly holomorphic modular forms of weight $k$ and level $N$, meaning we allow poles at any cusp. We have $U_p : M_k^!(N) \to M_k^!(N)$ if $p$ divides $N$. If $f(z)$ has the Fourier expansion $\sum_{n=n_0}^{\infty} a(n)q^n$, then the effect of $U_p$ is given by $U_p f(z) = \sum_{n=n_0}^{\infty} a(pn)q^n$.

The following result describes how $U_p$ applied to a modular function behaves under the Fricke involution. This will help us in Lemma 2.4 to write $U_p(\phi^{(p)})^m$ as a polynomial in $\phi^{(p)}$.

**Lemma 2.1** ([4, Theorem 4.6])**.** *Let $p$ be prime and let $f(z)$ be a level $p$ modular function. Then*

$$p(U_p f)\left(\frac{-1}{pz}\right) = p(U_p f)(pz) + f\left(\frac{-1}{p^2 z}\right) - f(z).$$

The Fricke involution $\left(\begin{smallmatrix} 0 & -1 \\ p & 0 \end{smallmatrix}\right)$ swaps the cusps of $\Gamma_0(p)$, which are 0 and $\infty$. We will use this fact in the proof of Lemma 2.4, and the following relations between $\phi^{(p)}(z)$ and $\psi^{(p)}(z)$ will help us compute this involution.

**Lemma 2.2** ([3, Lemma 3])**.** *The functions $\phi(z)$ and $\psi(z)$ satisfy the relations*

$$\begin{aligned} \phi^{(p)}\left(\frac{-1}{pz}\right) &= p^{-12/(p-1)}\psi^{(p)}(z), \\ \psi^{(p)}\left(\frac{-1}{pz}\right) &= p^{12/(p-1)}\phi^{(p)}(z). \end{aligned}$$

The following lemma is a special case of a result of Lehner [12]. It provides a polynomial with functions as its coefficients whose roots are modular forms used in the proof of Theorem 3.1, meaning that evaluating the polynomial at those modular forms yields the zero function.

**Lemma 2.3** ([12, Theorem 2])**.** *There exist integers $b_j^{(p)}$ such that*

$$U_p\phi^{(p)}(z) = p\sum_{j=1}^{p} b_j^{(p)}\phi^{(p)}(z)^j.$$

*Furthermore, let $h^{(p)}(z) = p^{12/(p-1)}\phi^{(p)}(z/p)$. Then*

$$(h^{(p)}(z))^p + \sum_{j=1}^{p}(-1)^j g_j(z)(h^{(p)}(z))^{p-j} = 0$$

*where*

$$g_j(z) = (-1)^{j+1}p^{12/(p-1)+2}\sum_{\ell=j}^{p} b_\ell^{(p)}\phi^{(p)}(z)^{\ell-j+1}.$$

In the following lemma, we extend the result from the first part of Lemma 2.3, writing $U_p(\phi^{(p)})^m$ as an integer polynomial in $\phi^{(p)}$. In particular, we give the degree of that polynomial. An alternative approach can be seen in [5, Lemma 4.1.1].

**Lemma 2.4.** *For all $m \geq 1$, $U_p(\phi^{(p)})^m \in \mathbb{Z}[\phi^{(p)}]$. In particular,*

$$U_p(\phi^{(p)})^m = \sum_{j=\lceil m/p\rceil}^{pm} d(m,j)(\phi^{(p)})^j$$

*where $d(m,j) \in \mathbb{Z}$, and $d(m,pm)$ is not 0.*

*Proof.* We proceed as in [7, Lemma 5]; this is a straightforward generalization from 2 to $p$. Using Lemmas 2.1 and 2.2, we have that

$$\begin{aligned}
U_p\phi^{(p)}(-1/pz)^m &= U_p\phi^{(p)}(pz)^m + p^{-1}\phi^{(p)}(-1/p^2z)^m - p^{-1}\phi^{(p)}(z)^m \\
&= U_p\phi^{(p)}(pz)^m + p^{-1-12m/(p-1)}\psi^{(p)}(pz)^m - p^{-1}\phi^{(p)}(z)^m \\
&= p^{-1-12m/(p-1)}q^{-pm} + O(q^{-pm+p}).
\end{aligned}$$

Thus,

$$p^{1+12m/(p-1)}U_p\phi^{(p)}(-1/pz)^m = q^{-pm} + O(q^{-pm+p}).$$

Because $\phi^{(p)}(z)^m$ is holomorphic at $\infty$, $U_p\phi^{(p)}(z)^m$ is holomorphic at $\infty$. So $U_p\phi(-1/pz)^m$ is holomorphic at 0 and, since the Fourier expansion starts with $q^{-pm}$, it must be a polynomial of degree $pm$ in $\psi^{(p)}(z)$. Let $b(m,j) \in \mathbb{Z}$ such that

$$p^{1+12m/(p-1)}U_p\phi^{(p)}(-1/pz)^m = \sum_{j=0}^{pm} b(m,j)\psi^{(p)}(z)^j,$$

and we note that $b(m,pm)$ is not 0. Now replace $z$ with $-1/pz$ and use Lemma 2.2 to get

$$p^{1+12m/(p-1)}U_p\phi^{(p)}(z)^m = \sum_{j=0}^{pm} b(m,j)p^{12j/(p-1)}\phi^{(p)}(z)^j,$$

which gives

$$U_p\left(\phi^{(p)}(z)^m\right) = \sum_{j=0}^{pm} b(m,j)p^{12(j-m)/(p-1)-1}\phi^{(p)}(z)^j.$$

Because $\left(\phi^{(p)}(z)\right)^m = q^m + \cdots$, if $m$ is divisible by $p$, the leading term of the above sum is $q^{m/p}$, and otherwise the smallest power of $q$ present in the polynomial is at least $\lceil m/p \rceil$, so the sum starts with $j = \lceil m/p \rceil$ as desired. Notice that $b(m,j)p^{12(j-m)/(p-1)-1}$ is an integer because the coefficients of $\phi^{(p)}(z)^m$ are integers. □

We may repeatedly use Lemma 2.4 to write $U_p^\alpha(\phi^{(p)})^m$ as a polynomial in $\phi^{(p)}$. Let

$$f_{(p)}(\ell) = \lceil \ell/p \rceil\,,\ f_{(p)}^0(\ell) = \ell,\ \text{and}\ f_{(p)}^\alpha(\ell) = f_{(p)}(f_{(p)}^{\alpha-1}(\ell)) \qquad \text{for } \alpha \geq 1. \tag{2.1}$$

Using Lemma 2.4, the smallest exponent of $q$ appearing in $U_p^\alpha(\phi^{(p)})^m$ is $f_{(p)}^\alpha(m)$.

Lemma 2.5 provides a connection between $\gamma_p(m,\alpha)$ and the integers $f_{(p)}^\alpha(m)$: $\gamma_p$ is counting the number of 0s and 1s to the left of the first nonzero digit in the base $p$ expansion of $m$. The key difference between the following lemma and its corresponding lemma in [7] is that there are more digits in bases $3, 5, 7$.

**Lemma 2.5.** *The number of* $0$*s to the left of the rightmost nonzero digit in the first* $\alpha$ *digits of the base* $p$ *expansion of* $m$ *is equal to the number of integers congruent to* $1$ *modulo* $p$ *in the list*

$$m, f_{(p)}(m), f_{(p)}^2(m), \ldots, f_{(p)}^{\alpha-1}(m),$$

*except when the rightmost nonzero digit is* $1$ *(in which case there is exactly one more in the list). Similarly, the number of* $1$*s to the left of the rightmost nonzero digit in the base* $p$ *expansion of* $m$ *is equal to the number of integers congruent to* $2$ *modulo* $p$ *in the above list, again with the exception of when the rightmost nonzero digit is* $2$.

*Proof.* Write the base $p$ expansion of $m$ as $a_r \ldots a_2 a_1$, and consider its first $\alpha$ digits, $a_\alpha \ldots a_2 a_1$, where $a_i = 0$ for $i > r$ if $\alpha > r$. If $a_i = 0$ for $1 \leq i \leq \alpha$, then all of the integers in the list are zero modulo $p$. Otherwise, suppose that $a_i = 0$ for $1 \leq i < i'$ and $a_{i'} \neq 0$. Apply $f_{(p)}$ repeatedly to $m$. Each application of $f_{(p)}$ deletes the rightmost $0$ from the expansion, until $a_{i'}$ is the rightmost remaining digit; that is, $f_{(p)}^{i'-1}(m) = a_\alpha \ldots a_{i'-1} a_{i'}$. In particular, the rightmost digit is nonzero. Having reduced to this case, we now treat only the case where $m$ is not divisible by $p$.

If $m$ is not divisible by $p$, and $a_1 \in \{1, 2\}$, then at least one number in the list, namely $m$, is congruent to either $1$ or $2$ modulo $p$. Also, $f_{(p)}(m) = \lceil m/p \rceil = (m + a)/p$ for some $a \neq 0$. Applied to the base $p$ expansion of $m$, $f_{(p)}$ deletes $a_1$ and propagates a 1 leftward through the base $p$ expansion, replacing any digit that was previously equal to $p - 1$ with zero. This is essentially the operation of carrying in addition. This process then terminates upon encountering the rightmost digit less than $p-1$ (if it exists), which becomes one greater. As in the case where $p$ divides $m$, we apply $f$ repeatedly to delete the new leading 0s. But if the first nonzero digit to the left was either a 0 or a 1 before we propagated a 1 leftward, it is now a 1 or a 2 respectively. So now when we repeat this process until all digits are accounted for, we notice that any digit that was either a 0 or a 1 becomes a 1 or a 2 respectively (with the exception of the first nonzero digit), which proves the lemma. □

# Chapter 3. Proof of the Main Theorem

Using the polynomial whose roots are the proper Möbius transformations of $\phi^{(p)}$, any result that works for enough powers of $\phi^{(p)}$ can be extended to all higher powers of $\phi^{(p)}$ using Newton's formulas for sums of powers of roots of a polynomial. In this chapter, we use this idea to prove Theorem 1.1.

Then, in order to find congruences for the coefficient of $n = p^{\alpha}n'$, we use the $U_p$ operator $\alpha$ times, showing that each successive time we hit $(\phi^{(p)})^m$ with $U_p$, we get a polynomial in $\phi^{(p)}$ of the same form we would expect if we just applied it to the lowest power of $\phi^{(p)}$ in the previous polynomial we had, with every coefficient divisible by some positive power of $p$ if there is a nontrivial congruence. The previously defined $\gamma_p$ functions are simply a method of quickly determining that power of $p$.

Theorem 1.1 will follow from the next theorem.

**Theorem 3.1.** *Let $f_{(p)}^{\alpha}(m)$ be as in (2.1). Let $\gamma_p(m, \alpha)$ be as in Theorem 1.1, and let $\alpha \geq 1$. Define $P^{(p)}(\ell, a)$ to be the set of polynomials in $\phi^{(p)}$ with lowest power $\ell$ having coefficient $d_\ell$ divisible by $p^a$ and each subsequent coefficient $d_k$ being divisible by at least $p^{\delta_p(k-\ell)+a}$, where $\delta_3 = 4$ and $\delta_5 = \delta_7 = 1$. Then*

$$U_p^{\alpha}(\phi^{(p)})^m \in P^{(p)}(f_{(p)}^{\alpha}(m), \gamma_p(m, \alpha)). \tag{3.1}$$

Because our methods use the $U_p$ operator, they do not give meaningful congruences for the case when $\alpha = 0$. Theorem 3.1 is an improvement on the following result by Lehner [12] for $p = 3$.

**Theorem 3.2.** *[12, Equation 3.24] Write $U_3^{\alpha}(\phi^{(3)})^m$ as $\sum d(m, j, \alpha)(\phi^{(3)})^j \in \mathbb{Z}[\phi^{(3)}]$. For any integer $k$, let $\nu_3(k)$ be the highest power of 3 dividing $k$. Then*

$$\nu_3(d(m, j, \alpha)) \geq 4(j - 1) + \alpha(2 - 4(1 - m)).$$

In particular, Lehner's bound sometimes only gives the trivial result that the 3-adic valuation of $d(m, j, \alpha)$ is greater than some negative integer. Lehner also proved congruences for $p = 5, 7$, but they experience similar issues [11].

We prove Theorem 3.1 by first letting $\alpha = 1$, which we refer to as the single term case, and showing the theorem holds there. The single term case is similar to Lemma 6 from [3], which gives a subring of $\mathbb{Z}[\phi]$ which is closed under the $U_p$ operator. Here, we employ a similar technique to prove divisibility properties of the polynomial coefficients in Lemma 2.4. We then show that applying $U_p$ to a polynomial in the set $P^{(p)}(f_{(p)}^{\alpha}(m), \gamma_p(m, \alpha))$ will carry it to the set $P^{(p)}(f_{(p)}^{\alpha+1}(m), \gamma_p(m, \alpha+1))$, which we refer to as the polynomial step. Implicitly, this proves the result by induction. This structure differs from [7] because it allows us to prove the polynomial step in a much cleaner way. Another approach to proving the base case can be found in [5, Lemma 4.1.1].

*Proof of Theorem 3.1.* For the base case, we let $\alpha = 1$, and seek to prove the statement

$$U_p(\phi^{(p)})^m = \sum_{j=\lceil m/p \rceil}^{pm} d_{m,j} (\phi^{(p)})^j$$

with

$$p^{\delta_p(j - \lceil m/p \rceil) + c_m^{(p)}} \mid d_{m,j} \tag{3.2}$$

where

$$c_m^{(3)} = \begin{cases} 2 & m \equiv 1 \pmod 3, \\ 1 & m \equiv 2 \pmod 3, \\ 0 & \text{otherwise}, \end{cases}$$

$$c_m^{(5)} = c_m^{(7)} = \begin{cases} 1 & m \equiv 1, 2 \pmod p, \\ 0 & \text{otherwise}. \end{cases}$$

We prove (3.2) by induction on $m$. We follow the proof techniques used in Lemmas 5 and 6 of [3]. From the definition of $U_p$, we have

$$U_p\phi^{(p)}(z)^m = p^{-1}\sum_{j=1}^{p}\phi^{(p)}\left(\frac{z+j}{p}\right)^m \tag{3.3}$$

where $h_\ell^{(p)}(z) = p^{12/(p-1)}\phi^{(p)}\left(\frac{z+\ell}{p}\right)$. We will construct polynomials whose roots are the functions $h_\ell^{(p)}(z)$, depending on $p$. The construction will be done in accordance with Lemma 2.3.

Consider the polynomials

$$F^{(p)}(x) = x^p + \sum_{j=1}^{p-1}(-1)^j g_j(z)x^{p-j}.$$

We claim that $F^{(p)}(x)$ has the $h_\ell^{(p)}(z)$ as roots. By Lemma 2.3, we know that $h_0^{(p)}(z)$ is a root; the others are roots because the $g_j(z)$ are fixed under $z \mapsto z+1$, but for this transformation of $z$, $h_\ell^{(p)}(z)$ gets sent to $h_{\ell+1}^{(p)}(z)$. Note that the coefficients of $F^{(p)}(x)$ are the $g_j(z)$ functions. Now since $F^{(p)}$ has the functions $h_\ell^{(p)}(z)$ as its roots, the coefficients, namely the functions $g_j(z)$, are the symmetric polynomials in the roots. Recall Newton's identities for the sum of powers of roots of a polynomial. Writing $F^{(p)}(x) = \prod_{i=1}^n (x - x_i)$, let $S_\ell = x_1^\ell + \cdots + x_n^\ell$. Then it follows that

$$S_\ell = g_1 S_{\ell-1} - g_2 S_{\ell-2} + \cdots + (-1)^{\ell+1}\ell g_\ell.$$

Let $R^{(p)}$ be the set of polynomials of the form $\sum_{n=1}^N d_n\phi^{(p)}(z)^n$ where $d_n \in \mathbb{Z}$ and where for $n \geq 2$, $\nu_p(d_n) \geq \delta_p(n-1)$, where $\delta_p$ is as in Theorem 3.1.

**Lemma 3.3.** *($R^{(p)}$ product lemma) If $f, g \in R^{(p)}$, then $p^{\delta_p} fg \in R^{(p)}$.*

*Proof.* To prove the lemma, we only need prove it for the product

$$p^{\delta_p}\left(p^{\delta_p(i-1)}d_i\phi^i(z)\right)\left(p^{\delta_p(j-1)}d'_j\phi^j(z)\right),$$

and then the lemma will hold for the product of any two polynomials by linearity, since the sum of any two elements in $R^{(p)}$ is clearly also an element of $R^{(p)}$. Observe that

$$\begin{aligned} p^{\delta_p}\left(p^{\delta_p(i-1)}d_i\phi^{(p)}(z)^i\right)\left(p^{\delta_p(j-1)}d'_j\phi^{(p)}(z)^j\right) &= p^{\delta_p(i-1+j-1+1)}d_id'_j\phi^{(p)}(z)^{i+j} \\ &= p^{\delta_p((i+j)-1)}(d_id'_j)\phi^{(p)}(z)^{i+j}, \end{aligned}$$

which is clearly an element of $R^{(p)}$. So the desired result holds. □

We call this the $R^{(p)}$ *product lemma*, as it implies that when multiplying two polynomials in $R^{(p)}$, we must multiply in $\delta_p$ extra copies of $p$ for the product to be in $R^{(p)}$.

We now continue in cases. Note that for brevity, we take $\phi = \phi^{(p)}$, where $p$ is determined by the case. The following three cases together make up the "single term case," since we are showing that the theorem holds for $U_p$ of a single $\phi^m$ term.

*Case 1.* Let $p = 3$. Given Lemma 2.3 and the statement we are trying to prove, we see that what we want depends on $m$ as follows:

$$\begin{aligned} m &\equiv 0 \pmod 3 : \exists\, r \in R^{(3)},\ U_3\phi^m = 3^{-4(\lceil m/3\rceil - 1)}r, \\ m &\equiv 1 \pmod 3 : \exists\, r \in R^{(3)},\ U_3\phi^m = 3^{-4(\lceil m/3\rceil - 1)+2}r, \\ m &\equiv 2 \pmod 3 : \exists\, r \in R^{(3)},\ U_3\phi^m = 3^{-4(\lceil m/3\rceil - 1)+1}r. \end{aligned}$$

Furthermore, by Equation 3.3 and considering the functions $h_\ell^{(3)}$, we see that $U_3\phi^m = 3^{-1-6m}S_m$. Let $c_m = 0, 2, 1$ if $m$ is congruent to $0, 1, 2$ modulo 3 respectively. Then for our theorem to be true, we require

$$S_m = 3^{6m+5-4\lceil m/3\rceil + c_m} r \tag{3.4}$$

for some $r \in R^{(3)}$. We will prove this by induction.

Our base case will be $m = 1, 2, 3$. Observe that

$$\begin{aligned} g_1(z) &= 10 \cdot 3^9 \phi(z) + 4 \cdot 3^{14} \phi^2(z) + 3^{18} \phi^3(z), \\ g_2(z) &= -4 \cdot 3^{14} \phi(z) - 3^{18} \phi^2(z), \\ g_3(z) &= 3^{18} \phi(z). \end{aligned}$$

We find $S_1, S_2$, and $S_3$ as follows:

$$\begin{aligned} S_1 &= g_1 = 3^9(Q_1(\phi)), \\ S_2 &= g_1 S_1 - 2g_2 = 3^{14}(Q_2(\phi)), \\ S_3 &= g_1 S_2 - S_1 g_2 + 3g_3 = 3^{19}(Q_3(\phi)), \end{aligned}$$

where $Q_1, Q_2, Q_3 \in R^{(3)}$. Note that since $g_1$ and $S_1$ each are of the form $3^9 r$ for some $r \in R^{(3)}$, we use the $R^{(p)}$ product lemma to quickly deduce that their product is of the form $3^{18-4} r = 3^{14} r$ for some $r \in R^{(3)}$, from which we easily see $S_2 = 3^{14}(Q_2(\phi))$. Similarly, $3^{23}$ divides both $g_1 S_2$ and $S_1 g_2$, which means that to keep $g_1 S_2$ and $S_1 g_2$ in $R^{(p)}$, we lose $3^4$ and get $S_3 = 3^{19}(Q_3(\phi))$ using the same lemma. Comparing with (3.4), we see that the base case is proved.

Suppose that for some $M \geq 4, i \in \{1, 2, 3\}$ we have

$$S_{M-i} = r_i 3^{6(M-i)+5-4\lceil (M-i)/3 \rceil + c_{M-i}}$$

for some $r_i \in R^{(3)}$. We want to show that $S_M = 3^{6M+5-4\lceil M/3 \rceil + c_M} r_0$ for some $r_0 \in R^{(3)}$. Recall that for $M \geq 4$,

$$S_M = g_1 S_{M-1} - g_2 S_{M-2} + g_3 S_{M-3}.$$

If each of the terms is of the form $3^{6M+5-4\lceil M/3 \rceil + c_M} r_0$ for some $r_0 \in R^{(3)}$, then we are done.

We will check each term.

Using the $R^{(p)}$ product lemma, the power of 3 that we get from $g_1S_{M-1}$ is

$$\begin{aligned}&9+6(M-1)+5-4\lceil (M-1)/3\rceil + c_{M-1}-4\\&=6M+4-4\lceil (M-1)/3\rceil + c_{M-1},\end{aligned}$$

which we want to be greater than $6M+5-4\lceil M/3\rceil + c_M$. In other words, we want to check whether

$$-1-4\lceil (M-1)/3\rceil + c_{M-1} \geq -4\lceil M/3\rceil + c_M,$$

i.e.

$$-1+c_{M-1} \geq -4(\lceil M/3\rceil - \lceil (M-1)/3\rceil) + c_M. \tag{3.5}$$

Now we will evaluate both sides three different ways, depending on the parity of $M$:

$$\begin{aligned}M &\equiv 0 \pmod 3 : -1+1 \geq 0,\\M &\equiv 1 \pmod 3 : -1+0 \geq -4+2,\\M &\equiv 2 \pmod 3 : -1+2 \geq 1,\end{aligned}$$

so we see that Equation 3.5 is true.

The power of 3 that divides $g_2S_{M-2}$ is

$$\begin{aligned}&14+6(M-2)+5-4\lceil (M-2)/3\rceil + c_{M-2}-4\\&=6M+3-4\lceil (M-2)/3\rceil + c_{M-2},\end{aligned}$$

which we want to be greater than $6M+5-4\lceil M/3\rceil + c_M$. In other words, we want to check

whether

$$
\begin{aligned}
-2-4\lceil (M-2)/3\rceil + c_{M-2} &\geq -4\lceil M/3\rceil + c_M && (3.6)\\
-2 + c_{M-2} &\geq -4(\lceil M/3\rceil - \lceil (M-2)/3\rceil) + c_M. && (3.7)
\end{aligned}
$$

Now we will evaluate both sides three different ways, depending on the parity of $M$:

$$
\begin{aligned}
M &\equiv 0 \pmod 3 : -2+2 \geq 0,\\
M &\equiv 1 \pmod 3 : -2+1 \geq -4+2,\\
M &\equiv 2 \pmod 3 : -2+0 \geq -4+1,
\end{aligned}
$$

so we see that Equation 3.6 is true.

In the final term, the power of 3 that divides $g_3 S_{M-3}$ is

$$
\begin{aligned}
&19 + 6(M-3) + 5 - 4\lceil (M-3)/3\rceil + c_{M-3} - 4\\
&= 6M + 2 - 4\lceil (M-3)/3\rceil + c_{M-3},
\end{aligned}
$$

which we want to be greater than $6M + 5 - 4\lceil M/3\rceil + c_M$. In other words, we want to check whether

$$
-4 - 4\lceil (M-3)/3\rceil + c_{M-3} \geq -4\lceil M/3\rceil + c_M,
$$

i.e.

$$
-4 \geq -4(\lceil M/3\rceil - \lceil (M-3)/3\rceil). \qquad (3.8)
$$

Now we will evaluate both sides three different ways, depending on the parity of $M$:

$$\begin{aligned} M &\equiv 0 \pmod 3 : -4 \geq -4, \\ M &\equiv 1 \pmod 3 : -4 \geq -4, \\ M &\equiv 2 \pmod 3 : -4 \geq -4, \end{aligned}$$

so we see that Equation 3.8 is true. This concludes the case where $p = 3$.

*Case 2.* Let $p = 5$. Given Lemma 2.3 and the statement we are trying to prove, we see that what we want depends on $m$ as follows:

$$\begin{aligned} m \equiv 1, 2 \pmod 5 &: \exists\, r \in R^{(5)},\ U_5\phi^m = 5^{-(\lceil m/5 \rceil - 1) + 1} r \\ m \equiv 0, 3, 4 \pmod 5 &: \exists\, r \in R^{(5)},\ U_5\phi^m = 5^{-(\lceil m/5 \rceil - 1)} r. \end{aligned}$$

Furthermore, by Equation 3.3 and considering the functions $h_\ell^{(5)}$, we see that $U_5\phi^m = 5^{-1-3m} S_m$. Let $c_m = 1$ if $m$ is congruent to $1, 2$ modulo 5, and $c_m = 0$ otherwise. Then for our theorem to be true, we require

$$S_m = 5^{3m+2-\lceil m/5 \rceil + c_m} r \tag{3.9}$$

for some $r \in R^{(5)}$. We will prove this by induction.

Our base cases are $m = 1, 2, 3, 4, 5$. From Lemma 2.3,

$$\begin{aligned} g_1(z) &= 63 \cdot 5^5 \phi(z) + 52 \cdot 5^8 \phi^2(z) + 63 \cdot 5^{10} \phi^3(z) + 6 \cdot 5^{13} \phi^4(z) + 5^{15} \phi^5(z), \\ g_2(z) &= -52 \cdot 5^8 \phi(z) - 63 \cdot 5^{10} \phi^2(z) - 6 \cdot 5^{13} \phi^3(z) - 5^{15} \phi^4(z), \\ g_3(z) &= 63 \cdot 5^{10} \phi(z) + 6 \cdot 5^{13} \phi^2(z) + 5^{15} \phi^3(z), \\ g_4(z) &= -6 \cdot 5^{13} \phi(z) - 5^{15} \phi^2(z), \\ g_5(z) &= 5^{15} \phi(z). \end{aligned}$$

We find $S_1, S_2, S_3, S_4$ and $S_5$ as follows:

$$\begin{aligned}
&S_1 = g_1 = 5^5(Q_1(\phi)),\\
&S_2 = g_1S_1 - 2g_2 = 5^8(Q_2(\phi)),\\
&S_3 = g_1S_2 - g_2S_1 + 3g_3 = 5^{10}(Q_3(\phi)),\\
&S_4 = g_1S_3 - g_2S_2 + g_3S_1 - 4g_4 = 5^{13}(Q_4(\phi)),\\
&S_5 = g_1S_4 - g_2S_3 + g_3S_2 - g_4S_1 + 5g_5 = 5^{16}(Q_5(\phi)),
\end{aligned}$$

where $Q_1, Q_2, Q_3, Q_4, Q_5 \in R^{(5)}$, again using the $R^{(p)}$ product lemma in the same way as the previous part. Comparing with (3.9), we see that the base case is proved.

So suppose for some $M \geq 6, i \in \{1, 2, 3, 4, 5\}$ we have

$$S_{M-i} = r_i 5^{3(M-i)+2-\lceil (M-i)/5 \rceil + c_{M-i}}$$

for some $r_i \in R^{(5)}$. We want to show that $S_M = 5^{5M+2-\lceil M/5 \rceil + c_M} r_0$ for some $r_0 \in R^{(5)}$. Recall that for $M \geq 6$,

$$S_M = g_1S_{M-1} - g_2S_{M-2} + g_3S_{M-3} - g_4S_{M-4} + g_5S_{M-5}.$$

If each of the terms is of the form $5^{3M+2-\lceil M/5 \rceil + c_M} r_0$ for some $r_0 \in R^{(5)}$, then we are done. We will check each term.

Using the $R^{(p)}$ product lemma, the power of 5 that we get from $g_1S_{M-1}$ is

$$\begin{aligned}
&5 + 3(M-1) + 2 - \lceil (M-1)/5 \rceil + c_{M-1} - 1\\
&= 3M + 4 - \lceil (M-1)/5 \rceil + c_{M-1} - 1\\
&= 3M + 3 - \lceil (M-1)/5 \rceil + c_{M-1},
\end{aligned}$$

which we want to be greater than $3M + 2 - \lceil M/5 \rceil + c_M$. In other words, we want to check

whether

$$1 - \lceil (M-1)/5 \rceil + c_{M-1} \geq -\lceil M/5 \rceil + c_M,$$

i.e.

$$1 + c_{M-1} \geq -(\lceil M/5 \rceil - \lceil (M-1)/5 \rceil) + c_M.$$

Considering the possibilities modulo 5, this always holds true.

Moving on to the next term, the power of 5 that we get from $g_2 S_{M-2}$ is

$$\begin{aligned}
&8 + 3(M-2) + 2 - \lceil (M-2)/5 \rceil + c_{M-2} - 1 \\
&= 3M + 4 - \lceil (M-2)/3 \rceil + c_{M-2} - 1 \\
&= 3M + 3 - \lceil (M-2)/3 \rceil + c_{M-2},
\end{aligned}$$

which we want to be greater than $3M + 2 - \lceil M/5 \rceil + c_M$. In other words, we want to check whether

$$1 + c_{M-2} \geq -(\lceil M/5 \rceil - \lceil (M-2)/5 \rceil) + c_M.$$

Considering the possibilities modulo 5, this always holds true.

In the next term, the power of 5 that we get from $g_3 S_{M-3}$ is

$$\begin{aligned}
&10 + 3(M-3) + 2 - \lceil (M-3)/5 \rceil + c_{M-3} - 1 \\
&= 3M + 3 - \lceil (M-3)/5 \rceil + c_{M-3} - 1 \\
&= 3M + 2 - \lceil (M-3)/5 \rceil + c_{M-3},
\end{aligned}$$

which we want to be greater than $3M + 2 - \lceil M/5 \rceil + c_M$. In other words, we want to check

whether

$$c_{M-3} \geq -(\lceil M/5 \rceil - \lceil (M-3)/5 \rceil) + c_M.$$

Considering the possibilities modulo 5, this always holds true.

In the next term, the power of 5 that we get from $g_4 S_{M-4}$ is

$$\begin{aligned}
&13 + 3(M-4) + 2 - \lceil (M-4)/5 \rceil + c_{M-4} - 1 \\
&= 3M + 3 - \lceil (M-4)/5 \rceil + c_{M-4} - 1 \\
&= 3M + 2 - \lceil (M-4)/5 \rceil + c_{M-4},
\end{aligned}$$

which we want to be greater than $3M + 2 - \lceil M/5 \rceil + c_M$. In other words, we want to check whether

$$c_{M-4} \geq -(\lceil M/5 \rceil - \lceil (M-4)/5 \rceil) + c_M.$$

Considering the possibilities modulo 5, this always holds true.

In the last term, the power of 5 that we get from $g_5 S_{M-5}$ is

$$\begin{aligned}
&15 + 3(M-5) + 2 - \lceil (M-5)/5 \rceil + c_{M-5} - 1 \\
&= 3M + 2 - \lceil (M-5)/5 \rceil + c_{M-5} - 1 \\
&= 3M + 1 - \lceil (M-5)/5 \rceil + c_{M-5},
\end{aligned}$$

which we want to be greater than $3M + 2 - \lceil M/5 \rceil + c_M$. In other words, we want to check whether

$$-1 + c_{M-5} \geq -(\lceil M/5 \rceil - \lceil (M-5)/5 \rceil) + c_M.$$

Considering the possibilities modulo 5, this always holds true. This concludes the case where

$p = 5$.

*Case 3.* Let $p = 7$. Given Lemma 2.3 and the statement we are trying to prove, we see that what we want depends on $m$ as follows:

$$m \equiv 1, 2 \pmod 7 : \exists\, r \in R^{(7)},\ U_7\phi^m = 7^{-(\lceil m/7 \rceil - 1)+1} r,$$
$$m \equiv 0, 3, 4 \pmod 7 : \exists\, r \in R^{(5)},\ U_7\phi^m = 7^{-(\lceil m/7 \rceil - 1)} r.$$

Furthermore, by Equation 3.3 and considering the functions $h_\ell^{(7)}$, we see that $U_7\phi^m = 7^{-1-2m} S_m$. Let $c_m = 1$ if $m$ is congruent to $1, 2$ modulo 7, and $c_m = 0$ otherwise. Then for our theorem to be true, we require

$$S_m = 5^{2m+2-\lceil m/7 \rceil + c_m} r \tag{3.10}$$

for some $r \in R^{(7)}$. We will prove this by induction.

Our base cases are $m = 1, 2, 3, 4, 5, 6, 7$. From Lemma 2.3,

$$g_1(z) = 82 \cdot 7^4\phi + 176 \cdot 7^6\phi^2 + 845 \cdot 7^7\phi^3 + 272 \cdot 7^9\phi^4 + 46 \cdot 7^{11}\phi^5 + 4 \cdot 7^{13}\phi^6 + 7^{14}\phi^7,$$
$$g_2(z) = -176 \cdot 7^6\phi - 845 \cdot 7^7\phi^2 - 272 \cdot 7^9\phi^3 - 46 \cdot 7^{11}\phi^4 - 4 \cdot 7^{13}\phi^5 - 7^{14}\phi^6,$$
$$g_3(z) = 845 \cdot 7^7\phi + 272 \cdot 7^9\phi^2 + 46 \cdot 7^{11}\phi^3 + 4 \cdot 7^{13}\phi^4 + 7^{14}\phi^5,$$
$$g_4(z) = -272 \cdot 7^9\phi - 46 \cdot 7^{11}\phi^2 - 4 \cdot 7^{13}\phi^3 - 7^{14}\phi^4,$$
$$g_5(z) = 46 \cdot 7^{11}\phi + 4 \cdot 7^{13}\phi^2 + 7^{14}\phi^3,$$
$$g_6(z) = -4 \cdot 7^{13}\phi - 7^{14}\phi^2,$$
$$g_7(z) = 7^{14}\phi.$$

We find $S_1, S_2, S_3, S_4, S_5, S_6$ and $S_7$ as follows:

$$\begin{aligned}
&S_1 = g_1 = 7^4(Q_1(\phi)),\\
&S_2 = g_1S_1 - 2g_2 = 7^6(Q_2(\phi)),\\
&S_3 = g_1S_2 - g_2S_1 + 3g_3 = 7^7(Q_3(\phi)),\\
&S_4 = g_1S_3 - g_2S_2 + g_3S_1 - 4g_4 = 7^9(Q_4(\phi)),\\
&S_5 = g_1S_4 - g_2S_3 + g_3S_2 - g_4S_1 + 5g_5 = 7^{11}(Q_5(\phi)),\\
&S_6 = g_1S_5 - g_2S_4 + g_3S_3 - g_4S_2 + g_5S_1 - 6g_6 = 7^{13}(Q_6(\phi)),\\
&S_7 = g_1S_6 - g_2S_5 + g_3S_4 - g_4S_3 + g_5S_2 - g_6S_1 + 7g_7 = 7^{15}(Q_7(\phi)).
\end{aligned}$$

where $Q_1, Q_2, Q_3, Q_4, Q_5, Q_6, Q_7 \in R^{(7)}$, again using the $R^{(p)}$ product lemma in the same way as the previous part. Comparing with (3.10), we see that the base case is proved.

So suppose for some $M \geq 8, i \in \{1, 2, 3, 4, 5, 6, 7\}$ we have

$$S_{M-i} = r_i 7^{2(M-i)+2-\lceil (M-i)/7 \rceil + c_{M-i}}$$

for some $r_i \in R^{(7)}$. We want to show that $S_M = 7^{2M+2-\lceil M/7 \rceil + c_M} r_0$ for some $r_0 \in R^{(7)}$. Recall that for $M \geq 8$,

$$S_M = g_1S_{M-1} - g_2S_{M-2} + g_3S_{M-3} - g_4S_{M-4} + g_5S_{M-5} - g_6S_{M-6} + g_7S_{M-7}.$$

If each of the terms is of the form $7^{2M+2-\lceil M/7 \rceil + c_M} r_0$ for some $r_0 \in R^{(7)}$, then we are done. We will check each term.

Using the $R^{(p)}$ product lemma, the power of 7 that we get from $g_1 S_{M-1}$ is

$$\begin{aligned}
&4 + 2(M-1) + 2 - \lceil (M-1)/7 \rceil + c_{M-1} - 1 \\
&= 2M + 4 - \lceil (M-1)/7 \rceil + c_{M-1} - 1 \\
&= 2M + 3 - \lceil (M-1)/7 \rceil + c_{M-1},
\end{aligned}$$

which we want to be greater than $2M + 2 - \lceil M/7 \rceil + c_M$. In other words, we want to check whether

$$1 - \lceil (M-1)/7 \rceil + c_{M-1} \geq -\lceil M/7 \rceil + c_M,$$

i.e.

$$1 + c_{M-1} \geq -(\lceil M/7 \rceil - \lceil (M-1)/7 \rceil) + c_M.$$

Considering the possibilities modulo 7, this always holds true.

Moving on to the next term, the power of 7 that we get from $g_2 S_{M-2}$ is

$$\begin{aligned}
&6 + 2(M-2) + 2 - \lceil (M-2)/7 \rceil + c_{M-2} - 1 \\
&= 2M + 4 - \lceil (M-2)/7 \rceil + c_{M-2} - 1 \\
&= 2M + 4 - \lceil (M-2)/7 \rceil + c_{M-2},
\end{aligned}$$

which we want to be greater than $2M + 2 - \lceil M/7 \rceil + c_M$. In other words, we want to check whether

$$1 + c_{M-2} \geq -(\lceil M/7 \rceil - \lceil (M-2)/7 \rceil) + c_M.$$

Considering the possibilities modulo 7, this always holds true.

In the next term, the power of 7 that we get from $g_3S_{M-3}$ is

$$\begin{aligned}
&7+2(M-3)+2-\lceil (M-3)/7\rceil + c_{M-3}-1\\
&=2M+3-\lceil (M-3)/7\rceil + c_{M-3}-1\\
&=2M+2-\lceil (M-3)/7\rceil + c_{M-3},
\end{aligned}$$

which we want to be greater than $2M+2-\lceil M/7\rceil + c_M$. In other words, we want to check whether

$$c_{M-3} \geq -(\lceil M/7\rceil - \lceil (M-3)/7\rceil) + c_M.$$

Considering the possibilities modulo 7, this always holds true.

In the next term, the power of 7 that we get from $g_4S_{M-4}$ is

$$\begin{aligned}
&9+2(M-4)+2-\lceil (M-4)/7\rceil + c_{M-4}-1\\
&=2M+3-\lceil (M-4)/7\rceil + c_{M-4}-1\\
&=2M+2-\lceil (M-4)/7\rceil + c_{M-4},
\end{aligned}$$

which we want to be greater than $2M+2-\lceil M/7\rceil + c_M$. In other words, we want to check whether

$$c_{M-4} \geq -(\lceil M/7\rceil - \lceil (M-4)/7\rceil) + c_M.$$

Considering the possibilities modulo 7, this always holds true.

In the next term, the power of 7 that we get from $g_5 S_{M-5}$ is

$$\begin{aligned} & 11 + 2(M-5) + 2 - \lceil (M-5)/7 \rceil + c_{M-5} - 1 \\ & = 2M + 3 - \lceil (M-5)/7 \rceil + c_{M-5} - 1 \\ & = 2M + 2 - \lceil (M-5)/7 \rceil + c_{M-5}, \end{aligned}$$

which we want to be greater than $2M + 2 - \lceil M/7 \rceil + c_M$. In other words, we want to check whether

$$c_{M-5} \geq -(\lceil M/7 \rceil - \lceil (M-5)/7 \rceil) + c_M.$$

Considering the possibilities modulo 7, this always holds true.

In the next term, the power of 7 that we get from $g_6 S_{M-6}$ is

$$\begin{aligned} & 13 + 2(M-6) + 2 - \lceil (M-6)/7 \rceil + c_{M-6} - 1 \\ & = 2M + 3 - \lceil (M-6)/7 \rceil + c_{M-6} - 1 \\ & = 2M + 2 - \lceil (M-6)/7 \rceil + c_{M-6}, \end{aligned}$$

which we want to be greater than $2M + 2 - \lceil M/7 \rceil + c_M$. In other words, we want to check whether

$$c_{M-6} \geq -(\lceil M/7 \rceil - \lceil (M-6)/7 \rceil) + c_M.$$

Considering the possibilities modulo 7, this always holds true.

In the last term, the power of 7 that we get from $g_7 S_{M-7}$ is

$$\begin{aligned} &14 + 2(M-7) + 2 - \lceil (M-7)/7 \rceil + c_{M-7} - 1 \\ &= 2M + 2 - \lceil (M-7)/7 \rceil + c_{M-7} - 1 \\ &= 2M + 1 - \lceil (M-7)/7 \rceil + c_{M-7}, \end{aligned}$$

which we want to be greater than $2M + 2 - \lceil M/7 \rceil + c_M$. In other words, we want to check whether

$$-1 + c_{M-7} \geq -(\lceil M/7 \rceil - \lceil (M-7)/7 \rceil) + c_M.$$

Considering the possibilities modulo 7, this always holds true. This concludes the case where $p = 7$.

We will also do the polynomial step by cases.

*Case 1.* For the case $p = 3$, our single term case says that

$$U_3(\phi(z)^m) = \sum_{n=i}^{3m} d_n (\phi(z))^n,$$

where $i = \lceil \frac{m}{3} \rceil$, and $3^2 \mid d_i$ if $m \equiv 1 \pmod 3$, or $3 \mid d_i$ if $m \equiv 2 \pmod 3$. Furthermore, $\nu_3(d_n) \geq 4 + \nu_3(d_{n-1})$, where $n \neq i$. To take into account the equivalence class of $m$ modulo 3, we can rewrite this as

$$U_3(\phi(z)^m) = 3^{c_m} \sum_{n=i}^{3m} d'_n (\phi(z))^n,$$

where $c_m$ is as it was in the single term case. Since this is a constant, it factors out of $U_3$ and we treat the polynomial step as follows:

Suppose that

$$\sum_{n=i}^{j} d_n (\phi(z))^n$$

is a polynomial where $\nu_3(d_n) \geq 4 + \nu_3(d_{n-1})$, for $n > i$. We will show that

$$U_3\left(\sum_{n=i}^{j} d_n \phi(z)^n\right) = 3^{c_i} \sum_{n=i'}^{3j} d'_n \phi(z)^n,$$

where $3^{c_i}$ is $3^2, 3$, or 1 if $i$ is $1, 2$, or 0 modulo 3 respectively, and $\nu_3(d'_n) \geq 4 + \nu_3(d'_{n-1})$, for $n > i'$.

First of all, we have already shown that $i' = \lceil \frac{i}{3} \rceil$ and that the degree of the resulting polynomial is $3j$, so it is of the correct form. The only question is whether or not the $3^{c_i}$ term appears and whether the $d'_n$ satisfy the appropriate relative divisibility by increasing powers of 3.

For this purpose, we use the sets $P^{(3)}(\ell, a)$ as defined in Theorem 3.1. Note that in a trivial sense, we take $\nu_3(0) = \infty$, so if any coefficient of $(\phi^{(3)})^m$ is zero, it may still be an element of $P^{(3)}(\ell, a)$ as long as the divisibility holds for the nonzero coefficients. Now since $U_3$ is linear over the sum, we can use the single term case to find the sets to which each single term belongs, and then show that each of the sets is contained in $P^{(3)}(i', c_i + \nu_3(d_i))$, which is the set that $U_3((\phi^{(3)})^i)$ belongs to. Note that any element of this set is a polynomial of the form we are trying to obtain. We do this by showing the containments

$$\begin{aligned} P^{(3)}\left(i', \gamma_i + \nu_3(d_i)\right) &\supseteq P^{(3)}\left(\left\lceil \frac{i+1}{3} \right\rceil, \gamma_{i+1} + \nu_3(d_{i+1})\right) \\ &\supseteq \cdots \\ &\supseteq P^{(3)}\left(\left\lceil \frac{j}{3} \right\rceil, \gamma_j + \nu_3(d_j)\right). \end{aligned}$$

In order to show all of these containments, we only need show consecutive set inclusions. So we will show that for a particular $m$, $P^{(3)}(\lceil \frac{m}{3} \rceil, c_m + \nu_3(d_m)) \subseteq P^{(3)}(\lceil \frac{m-1}{3} \rceil, c_{m-1} + \nu_3(d_{m-1}))$. Now we move to subcases.

*Subcase 1.* If $m \equiv 0 \pmod 3$, then $\lceil \frac{m-1}{3} \rceil = \lceil \frac{m}{3} \rceil$, and we want to show $P^{(3)}(\lceil \frac{m}{3} \rceil, \nu_3(d_m)) \subseteq$

$P^{(3)}(\lceil\frac{m-1}{3}\rceil, 1+\nu_3(d_{m-1}))$. Observe that

$$\begin{aligned}P^{(3)}\left(\left\lceil\frac{m}{3}\right\rceil, \nu_3(d_m)\right) &\subseteq P^{(3)}\left(\left\lceil\frac{m-1}{3}\right\rceil, 4+\nu_3(d_{m-1})\right)\\ &\subseteq P^{(3)}\left(\left\lceil\frac{m-1}{3}\right\rceil, 1+\nu_3(d_{m-1})\right),\end{aligned}$$

as desired.

*Subcase 2.* If $m \equiv 1 \pmod 3$, then $\lceil\frac{m-1}{3}\rceil = \lceil\frac{m}{3}\rceil - 1$, and we want to show $P^{(3)}(\lceil\frac{m}{3}\rceil, 2+\nu_3(d_m)) \subseteq P^{(3)}(\lceil\frac{m-1}{3}\rceil, \nu_3(d_{m-1}))$. Observe that

$$\begin{aligned}P^{(3)}\left(\left\lceil\frac{m}{3}\right\rceil, 2+\nu_3(d_m)\right) &\subseteq P^{(3)}\left(\left\lceil\frac{m-1}{3}\right\rceil+1, 4+2+\nu_3(d_{m-1})\right)\\ &\subseteq P^{(3)}\left(\left\lceil\frac{m-1}{3}\right\rceil, 2+\nu_3(d_{m-1})\right)\\ &\subseteq P^{(3)}\left(\left\lceil\frac{m-1}{3}\right\rceil, \nu_3(d_{m-1})\right),\end{aligned}$$

as desired.

*Subcase 3.* If $m \equiv 2 \pmod 3$, then $\lceil\frac{m-1}{3}\rceil = \lceil\frac{m}{3}\rceil$, and we want to show $P^{(3)}(\lceil\frac{m}{3}\rceil, 1+\nu_3(d_m)) \subseteq P^{(3)}(\lceil\frac{m-1}{3}\rceil, 2+\nu_3(d_{m-1}))$. Observe that

$$\begin{aligned}P^{(3)}\left(\left\lceil\frac{m}{3}\right\rceil, 1+\nu_3(d_m)\right) &\subseteq P^{(3)}\left(\left\lceil\frac{m-1}{3}\right\rceil, 4+1+\nu_3(d_{m-1})\right)\\ &\subseteq P^{(3)}\left(\left\lceil\frac{m-1}{3}\right\rceil, 2+\nu_3(d_{m-1})\right),\end{aligned}$$

as desired.

As explained, this shows that the result holds for $p = 3$.

*Case 2.* We will handle the cases $p = 5, 7$ together. For these cases, our single term case says that

$$U_p((\phi^{(p)}(z))^m) = \sum_{n=i}^{pm} d_n(\phi^{(p)}(z))^n,$$

where $i = \lceil\frac{m}{p}\rceil$, and $p \mid d_i$ if $m \equiv 1, 2 \pmod p$. Furthermore, $\nu_p(d_n) \geq 1 + \nu_p(d_{n-1})$, where

$n \neq i$. To take into account the equivalence class of $m$ modulo $p$, we can rewrite this as

$$U_p((\phi^{(p)}(z))^m) = p^{c_m} \sum_{n=i}^{pm} d'_n (\phi^{(p)}(z))^n,$$

where $c_m$ is as it was in the single term case. Since this is a constant, it factors out of $U_p$ and we treat the polynomial step as follows:

Suppose that

$$\sum_{n=i}^{j} d_n (\phi^{(p)}(z))^n$$

is a polynomial where $\nu_p(d_n) \geq 1 + \nu_p(d_{n-1})$, for $n \neq i$. Then we will show that

$$U_p\left(\sum_{n=i}^{j} d_n (\phi^{(p)}(z))^n\right) = p^{c_i} \sum_{n=i'}^{pj} d'_n (\phi^{(p)}(z))^n,$$

where $p^{c_i}$ is $p$ or 1 depending on $i$ modulo $p$, and $\nu_p(d'_n) \geq 1 + \nu_p(d'_{n-1})$, for $n \neq i'$.

First of all, we have already shown that $i' = \lceil \frac{i}{p} \rceil$ and that the degree of the resulting polynomial is $pj$, so it is of the correct form. The only question is then whether or not the $p^{c_i}$ term appears and whether the $d'_n$ satisfy the appropriate relative divisibility by increasing powers of $p$.

For this purpose, we use the sets $P^{(p)}(\ell, a)$ as defined in Theorem 3.1. Now since $U_p$ is linear over the sum, we can use the single term case to find the sets to which each single term belongs, and then show that each of the sets is contained in $P^{(p)}(i', c_i + \nu_p(d_i))$, which is the set that $U_p((\phi^{(p)})^i)$ belongs to. Note that any element of this set is a polynomial of the form we are trying to obtain. We do this by showing the containments

$$\begin{aligned} P^{(p)}(i', \gamma_i + \nu_p(d_i)) &\supseteq P^{(p)}\left(\left\lceil \frac{i+1}{p} \right\rceil, \gamma_{i+1} + \nu_p(d_{i+1})\right) \\ &\supseteq \cdots \\ &\supseteq P^{(p)}\left(\left\lceil \frac{j}{p} \right\rceil, \gamma_j + \nu_p(d_j)\right). \end{aligned}$$

In order to show all of these containments, we only need show consecutive set inclusions. So we will show that for a particular $m$,

$$P^{(p)}\left(\left\lceil\frac{m}{p}\right\rceil, \gamma_m + \nu_p(d_m)\right) \subseteq P^{(p)}\left(\left\lceil\frac{m-1}{p}\right\rceil, \gamma_{m-1} + \nu_p(d_{m-1})\right).$$

Now we move to subcases.

*Subcase 1.* If $m \equiv 1 \pmod p$, then $\lceil\frac{m-1}{p}\rceil = \lceil\frac{m}{p}\rceil - 1$, and we want to show $P^{(p)}\left(\left\lceil\frac{m}{p}\right\rceil, 1 + \nu_p(d_m)\right) \subseteq P^{(p)}\left(\left\lceil\frac{m-1}{p}\right\rceil, \nu_p(d_{m-1})\right)$. Observe that

$$\begin{aligned} P^{(p)}\left(\left\lceil\frac{m}{p}\right\rceil, 1 + \nu_p(d_m)\right) &\subseteq P^{(p)}\left(\left\lceil\frac{m-1}{p}\right\rceil, \nu_p(d_m)\right) \\ &\subseteq P^{(p)}\left(\left\lceil\frac{m-1}{p}\right\rceil, \nu_p(d_{m-1})\right), \end{aligned}$$

as desired.

*Subcase 2.* If $m \equiv 2 \pmod p$, then $\lceil\frac{m-1}{p}\rceil = \lceil\frac{m}{p}\rceil$, and we want to show $P^{(p)}\left(\left\lceil\frac{m}{p}\right\rceil, 1 + \nu_p(d_m)\right) \subseteq P^{(p)}\left(\left\lceil\frac{m-1}{p}\right\rceil, 1 + \nu_p(d_{m-1})\right)$. Observe that

$$\begin{aligned} P^{(p)}\left(\left\lceil\frac{m}{p}\right\rceil, 1 + \nu_p(d_m)\right) &\subseteq P^{(p)}\left(\left\lceil\frac{m-1}{p}\right\rceil, 1 + 1 + \nu_p(d_{m-1})\right) \\ &\subseteq P^{(p)}\left(\left\lceil\frac{m-1}{p}\right\rceil, 1 + \nu_p(d_{m-1})\right), \end{aligned}$$

as desired.

*Subcase 3.* If $m \equiv 3 \pmod p$, then $\lceil\frac{m-1}{p}\rceil = \lceil\frac{m}{p}\rceil$, and we want to show $P^{(p)}\left(\left\lceil\frac{m}{p}\right\rceil, \nu_p(d_m)\right) \subseteq P^{(p)}\left(\left\lceil\frac{m-1}{p}\right\rceil, 1 + \nu_p(d_{m-1})\right)$. Observe that

$$\begin{aligned} P^{(p)}\left(\left\lceil\frac{m}{p}\right\rceil, \nu_p(d_m)\right) &\subseteq P^{(p)}\left(\left\lceil\frac{m-1}{p}\right\rceil, 1 + \nu_p(d_{m-1})\right) \\ &\subseteq P^{(p)}\left(\left\lceil\frac{m-1}{p}\right\rceil, 1 + \nu_p(d_{m-1})\right), \end{aligned}$$

as desired.

*Subcase 4.* If $m \not\equiv 1, 2, 3 \pmod{p}$, then $\lceil \frac{m-1}{p} \rceil = \lceil \frac{m}{p} \rceil$, and we want to show $P^{(p)}\left(\left\lceil \frac{m}{p} \right\rceil, \nu_p(d_m)\right) \subseteq P^{(p)}\left(\left\lceil \frac{m-1}{p} \right\rceil, \nu_p(d_{m-1})\right)$. Observe that

$$\begin{aligned} P^{(p)}\left(\left\lceil \frac{m}{p} \right\rceil, \nu_p(d_m)\right) &\subseteq P^{(p)}\left(\left\lceil \frac{m-1}{p} \right\rceil, 1 + \nu_p(d_{m-1})\right) \\ &\subseteq P^{(p)}\left(\left\lceil \frac{m-1}{p} \right\rceil, \nu_p(d_{m-1})\right), \end{aligned}$$

as desired.

As explained, this shows that the result holds for $p = 5, 7$. □

This method of proving the polynomial step could be used to create a similar proof for $p = 2$, simplifying the argument in [7].

Now Theorem 1.1 follows easily from Theorem 3.1.

**Theorem 1.1.** *Let $p \in \{3, 5, 7\}$. Let $n = p^\alpha n'$ where $p \nmid n'$. Express the base $p$ expansion of $m$ as $a = \sum_{i=1}^{\infty} a_i p^{i-1}$, where $a_i = 0$ for all sufficiently large $i$. Consider the rightmost $\alpha$ digits $a_\alpha \ldots a_2 a_1$. Let $i'$ be the index of the rightmost nonzero digit, or $i' = -1$ if $a_1 = a_2 = \cdots = a_\alpha = 0$. Let*

$$\gamma_3(m, \alpha) = \begin{cases} 3 - a_{i'} + 2\#\{\, i \mid a_i = 0, i > i' \,\} + \#\{\, i \mid a_i = 1, i > i' \,\} & \text{if } i' \geq 0, \\ 0 & \text{otherwise.} \end{cases}$$

$$\gamma_5(m, \alpha) = \gamma_7(m, \alpha) = \begin{cases} \chi_{\{\,1,2\,\}}(a_{i'}) + \#\{\, i \mid a_i \in \{\,0, 1\,\}, i > i' \,\} & \text{if } i' \geq 0, \\ 0 & \text{otherwise.} \end{cases}$$

*Then*

$$a^{(p)}(m, p^\alpha n') \equiv 0 \pmod{p^{\gamma_p(m,\alpha)}}.$$

*Proof.* The leading coefficient of a polynomial in the set $P^{(p)}(f^\alpha(m), \gamma_p(m, \alpha))$ is divisible by $p^{\gamma_p(m,\alpha)}$. On the other hand, by Theorem 3.1, $U_{(p)}^\alpha \phi^m$ is an element of that set, so every

$p^\alpha$th coefficient is divisible by $p^{\gamma_p(m,\alpha)}$. □

# Chapter 4. The Case p = 13

Since 13 is also a genus zero prime, it is natural to consider whether any congruences hold for $\phi^{(13)}(z)$ or its powers. Computationally, it appears that unless $m \equiv 5 \pmod{13}$, expressing $U_{13}\phi^{(13)}(z)^m$ as a polynomial in $\phi^{(13)}(z)$ gives a coefficient not divisible by 13. Furthermore, in the case of $m \equiv 5 \pmod{13}$, it appears that there are two coefficients of that polynomial that are exactly divisible by 13. If we attempt to use the methods in this paper, this prevents us from chaining properly in the polynomial step. There may be some way around this issue, but it will take a slightly different approach. Computationally, for any prime $p$ less than 1000, it appears that the Fourier coefficient of $q^p$ in $\phi^{(13)}(z)$ is divisible by 13 precisely when $\tau(p)$ is divisible by 13, but no further congruences of the style given in this paper are immediately apparent.

# Bibliography

[1] H.-F. Aas. Congruences for the coefficients of the modular invariant $j(\tau)$. *Math. Scand.*, 15:64–68, 1964.

[2] P. Allatt and J. B. Slater. Congruences on some special modular forms. *J. London Math. Soc. (2)*, 17(3):380–392, 1978.

[3] N. Andersen and P. Jenkins. Divisibility properties of coefficients of level $p$ modular functions for genus zero primes. *Proc. Amer. Math. Soc.*, 141(1):41–53, 2013.

[4] T. M. Apostol. *Modular functions and Dirichlet series in number theory*, volume 41 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1990.

[5] F. Calegari. Congruences between modular forms. Arizona Winter School notes, http://swc.math.arizona.edu/aws/2013/2013CalegariLectureNotes.pdf, 2013.

[6] M. Griffin. Divisibility properties of coefficients of weight 0 weakly holomorphic modular forms. *Int. J. Number Theory*, 7(4):933–941, 2011.

[7] P. Jenkins, R. Keck, and E. Moss. Congruences for coefficients of level 2 modular functions with poles at 0. *Archiv der Mathematik*, 111(4):369–378, 2018.

[8] P. Jenkins and D. J. Thornton. Congruences for coefficients of modular functions. *Ramanujan J.*, 38(3):619–628, 2015.

[9] O. Kolberg. The coefficients of $j(\tau)$ modulo powers of 3. *Arbok Univ. Bergen Mat.-Natur. Ser.*, 1962(16):7, 1962.

[10] O. Kolberg. Congruences for the coefficients of the modular invariant $j(\tau)$. *Math. Scand.*, 10:173–181, 1962.

[11] J. Lehner. Divisibility properties of the Fourier coefficients of the modular invariant $j(\tau)$. *Amer. J. Math.*, 71:136–148, 1949.

[12] J. Lehner. Further congruence properties of the Fourier coefficients of the modular invariant $j(\tau)$. *Amer. J. Math.*, 71:373–386, 1949.