Congruences modulo primes of the Romik sequence related to the Taylor expansion of the Jacobi theta constant θ_3

Robert Scherer

April 10, 2019

Abstract

Recently, Romik determined in [9] the Taylor expansion of the Jacobi theta constant θ_3, around the point $x = 1$. He discovered a new integer sequence, $(d(n))_{n=0}^{\infty} = 1, 1, -1, 51, 849, -26199, \dots$, from which the Taylor coefficients are built, and conjectured that the numbers $d(n)$ satisfy certain congruences modulo various primes. In this paper, we prove some of these conjectures, for example that $d(n) \equiv (-1)^{n+1} \pmod 5$ for all $n \geq 1$, and that for any prime $p \equiv 3 \pmod 4$, $d(n)$ vanishes modulo p for all large enough n.

1 Introduction

1.1 The sequence $(d(n))_{n=0}^{\infty}$ and the main result

In this paper we will prove a list of congruences, modulo certain prime numbers, satisfied by the integer-valued Romik sequence, which is defined below and whose first several terms are given by

$$(d(n))_{n=0}^{\infty} = 1, 1, -1, 51, 849, -26199, 1341999, 82018251, 18703396449, \dots$$

(see also [11]). Specifically, we will show:

Theorem 1. *(i) $d(n) \equiv 1$ (mod 2) for all $n \geq 0$,*

(ii) $d(n) \equiv (-1)^{n+1}$ (mod 5) for all $n \geq 1$, and

(iii) if $p \equiv 3$ *(mod 4), then* $d(n) \equiv 0$ *(mod p) for all* $n > \frac{p^2-1}{2}$.

This proves half of Conjecture 13 (b) in [9], where the sequence $(d(n))$ was first introduced. (The half of the statement that we don't prove is that for primes $p = 4k+1$, the sequence $(d(n))_{n=0}^{\infty}$ mod p is periodic, although Theorem 1 is a specific example of this phenomenon in the case $p = 5$.)

The sequence $(d(n))$ is defined in terms of the Jacobi theta constant θ_3, which is the holomorphic function defined on the right half-plane by

$$\theta_3(x) = 1 + 2\sum_{n=1}^{\infty} e^{-\pi n^2 x} \qquad (\mathrm{Re}(x) > 0). \tag{1}$$

θ_3 satisfies the modular transformation identity

$$\theta_3\left(\frac{1}{x}\right) = \sqrt{x}\,\theta_3(x), \tag{2}$$

which implies that the function ϑ defined on the upper half-plane by $\vartheta(\tau) = \theta_3(-i\tau)$ is a weight $\frac{1}{2}$ modular form with respect to a certain subgroup of $\mathrm{SL}_2(\mathbb{Z})$ (see [10, Ch. 4] and [3, p. 100]). The numbers $d(n)$ arise in the following way.

Definition 2 (Romik [9])**.** *Define the function* σ *on the unit disk by*

$$\sigma(z) = \frac{1}{\sqrt{1+z}}\theta_3\left(\frac{1-z}{1+z}\right), \tag{3}$$

and define the sequence $(d(n))_{n=0}^{\infty}$ *by*

$$d(n) = \frac{\sigma^{(2n)}(0)}{A\Phi^n},$$

where $\Phi = \frac{\Gamma(\frac{1}{4})^8}{128\pi^4}$, *and* $A = \theta_3(1) = \frac{\Gamma(\frac{1}{4})}{\sqrt{2}\pi^{3/4}}$.

Thus the numbers $(d(n))_{n=0}^{\infty}$ are the Taylor coefficients, modulo trivial factors, of σ at 0. It's not at all clear from the definition that the numbers $d(n)$ are integers, but this is shown to be true in [9]. Furthermore, the connection of the sequence $(d(n))$ to the derivatives of θ_3 at 0 can be made explicit:

Theorem 3 (Romik [9])**.** *For all* $n \geq 0$,

$$\theta_3^{(n)}(1) = A \cdot \frac{(-1)^n}{4^n} \sum_{k=0}^{\lfloor n/2 \rfloor} \frac{(2n)!(4\Phi)^k}{2^{n-2k}(4k)!(n-2k)!} d(k). \tag{4}$$

1.2 Fourier and Taylor coefficients of modular forms

While the study of congruences of derivatives of modular forms is relatively recent, congruence properties of the Fourier coefficients of modular forms have been well-studied since the work of Ramanujan. He famously proved, for example, that $\tau(n) \equiv \sigma_{11}(n) \pmod{691}$, where $\sigma_{11}(n)$ is the sum of the 11^{th} powers of the positive divisors of n, and $\tau(n)$ denotes the n^{th} Fourier coefficient of the modular discriminant, Δ (see [10, Ch.2]). Similar results for τ with respect to other moduli are discussed in [8]. Another well-known example is the modular function $j = \frac{E_4^3}{\Delta}$, and various vanishings of the Fourier coefficients of j modulo powers of primes are discussed in [2, Ch.4].

In this paper we contribute to a more recent focus on the arithmetic properties of the Taylor coefficients of modular forms. Theorem 1 (iii) is related to a result in [6], which gives a sufficient condition for the vanishing modulo p^m (p prime, $m \geq 0$) of the Taylor coefficients, with respect to a certain differential operator, of a certain class of modular forms, not containing θ_3. We discuss not only the vanishings mod p of Taylor coefficients of θ_3, but also the result Theorem 1 (ii) regarding the periodicity of congruences mod 5. The periodicity of Taylor coefficients of modular forms does not appear to be well-studied, and as it was further conjectured in [9] that $d(n)$ has periodic congruences mod p for all primes $p \equiv 1 \pmod 4$, it is our hope that the result given here for $p = 5$ will eventually give way to a proof of that broader conjecture.

1.3 An auxiliary matrix and a recurrence for $d(n)$

In this subsection we recall from [9] a recurrence relation for $(d(n))$ in terms of a certain infinite matrix.

Definition 4. *Define the sequences $(u(n))_{n=0}^{\infty}$ and $(v(n))_{n=0}^{\infty}$ by $u(0) = v(0) = 1$ and the following recurrence relations for $n \geq 1$:*

$$u(n) = (3 \cdot 7 \cdots (4n-1))^2 - \sum_{m=0}^{n-1} \binom{2n+1}{2m+1} (1 \cdot 5 \cdots (4(n-m)-3))^2 \, u(m) \tag{5}$$

$$v(n) = 2^{n-1} (1 \cdot 5 \cdots (4n-3))^2 - \frac{1}{2} \sum_{m=1}^{n-1} \binom{2n}{2m} v(m) v(n-m). \tag{6}$$

Definition 5. *Define the array* $(s(n,k))_{1\leq k\leq n}$, *by*

$$s(n,k)=\frac{(2n)!}{(2k)!}[z^{2n}]\left(\sum_{j=0}^{\infty}\frac{u(j)}{(2j+1)!}z^{2j+1}\right)^{2k}, \tag{7}$$

where $[z^n]f(z)=[z^n]\sum_{n=0}^{\infty}c_nz^n$ *denotes the* n'^{th} *coefficient* c_n *in a power series expansion for* f. *Also for* $1\leq k\leq n$, *define* $r(n,k):=2^{n-k}s(n,k)$

Remark: The integers $r(n,k)$ were originally defined in [9] in a different manner and shown to be equivalent to 2^{n-k} times the right-hand-side of (7). The notation $s(n,k)$ is new.

The importance of the preceding definition is in the following recurrence relation for $d(n)$ (which is used in [9] to prove that $d(n)\in\mathbb{Z}$).

Theorem 6 (Romik [9])**.** *For all pairs* (n,k), $1\leq k\leq n$, *both* $r(n,k)$ *and* $s(n,k)$ *are integers. Furthermore, with* $d(0)=1$, *the following recurrence relation holds for all* $n\geq 1$*:*

$$d(n)=v(n)-\sum_{k=1}^{n-1}r(n,k)d(k). \tag{8}$$

The proof of Theorem 1 will be based on (8) and a new formula for $s(n,k)$, given in Theorem 8 below. This formula will provide, among other things, an argument different from the one in [9] that $s(n,k)\in\mathbb{Z}$.

1.4 Structure of the paper

In the next section we will derive a formula for $s(n,k)$ mod p that will be an important tool in the rest of the paper. In Section 3, we prove Theorem 1, part (i). In Sections 4 and 5 we will give proofs of parts (ii) and (iii), respectively, based on the expression for $s(n,k)$ mod p derived in Section 2, the recursive definition (8) for $d(n)$, and a few more facts about the congruences of $(u(n))$ and $(v(n))$.

2 A formula for $s(n,k)$ mod p

Before we derive the formula, we briefly recall some standard definitions regarding partitions.

Let n and k be positive integers. By an *unordered partition* λ *(of n with k parts)* we mean, as usual, a tuple of positive integers, $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_k)$, with $\lambda_i \leq \lambda_{i+1}$ for $1 \leq i < k$, such that $\sum_{i=1}^{k} \lambda_i = n$. The numbers λ_i are the *parts*. We let $\mathcal{P}_{n,k}$ denote the set of ordered partition of n with k parts, and we let $\mathcal{P}'_{n,k} \subset \mathcal{P}_{n,k}$ be the set of such partitions whose parts are odd numbers. For a given $\lambda \in \mathcal{P}_{n,k}$, we will let c_i denote the number (possibly 0) of parts of λ whose value is i, for $1 \leq i \leq n$. Thus, the tuple $c(\lambda) = (c_1, c_2, \ldots, c_n)$ gives an alternative description of λ, which we will use freely. (Although each c_i depends on λ, we choose not to reflect this dependence in the notation, in order to keep it simple, and since it will always be clear from context.) Finally, observe that $\sum_{i=1}^{n} ic_i = n$, and $\sum_{i=1}^{n} c_i = k$, for each $\lambda \in \mathcal{P}_{n,k}$.

Lemma 7 ([1, pp. 215-216])**.** *For any pair (n, k) of positive integers such that $n \geq k$, and any partition $\lambda \in \mathcal{P}_{n,k}$, the number $N(\lambda)$ defined by*

$$N(\lambda) = \frac{n!}{\prod_{i=1}^{n} i!^{c_i} c_i!}$$

is an integer.

Remark: The theorem in [1] proves the stronger statement that if S is a set with n elements, then $N(\lambda)$ is the number of set partitions of S into k blocks B_i, with $|B_i| \leq |B_{i+1}|$ for $1 \leq i < k$, such that $|B_i| = \lambda_i$.

Theorem 8. *For any pair (n, k) of positive integers such that $n \geq k$, we have*

$$s(n,k) = \sum_{\lambda \in \mathcal{P}'_{2n,2k}} \left[\frac{(2n)! \prod_{i=1}^{2n} u\left(\frac{i-1}{2}\right)^{c_i}}{\prod_{i=1}^{2n} i!^{c_i} c_i!} \right]. \tag{9}$$

If $\mathcal{P}'_{2n,2k}$ is empty, then $s(n, k) = 0$.

Proof. From (7) we see that

$$\begin{aligned} s(n,k) &= \frac{(2n)!}{(2k)!}[z^{2n}] \left(\sum_{\substack{j \geq 1 \\ j \text{ odd}}} \frac{u\left(\frac{j-1}{2}\right)}{j!} z^j \right)^{2k} \\ &= \frac{(2n)!}{(2k)!} \sum_{(j_1, j_2, \ldots, j_{2k})} \prod_{i=1}^{2k} \frac{u\left(\frac{j_i - 1}{2}\right)}{j_i!}, \end{aligned} \tag{10}$$

where the sum runs over all tuples $j = (j_1, j_2 \ldots, j_{2k})$ of positive odd integers such that $\sum_{i=1}^{2k} j_i = 2n$ (in other words, over all *ordered partitions* of $2n$ into $2k$ odd parts). Call the set of such tuples Λ. To each $j \in \Lambda$ we associate the unique unordered partition $\lambda \in \mathcal{P}'_{2n,2k}$ obtained by ordering the j_i's in non-decreasing order, and we also associate the tuple $c(\lambda)$. We can define an equivalence relation on Λ by calling j and j' equivalent if they map to the same $c(\lambda)$ under this association. If j maps to $c(\lambda) = (c_1, \ldots, c_{2n}) \in \mathcal{P}'_{2n,2k}$, then it is elementary to count that the size of the equivalence class of j is $\frac{(2k)!}{\prod_{i=1}^{2n} c_i!}$. Furthermore, the product $\prod_{i=1}^{2k} \frac{u\left(\frac{j_i-1}{2}\right)}{j_i!}$ in (10), as a function of $(j_1, \ldots, j_{2k})$, is constant on equivalence classes, and the equivalence classes are indexed by $\mathcal{P}'_{2n,2k}$ in the obvious way. Thus, we may rewrite (10) as

$$s(n,k) = \frac{(2n)!}{(2k)!} \sum_{\lambda \in \mathcal{P}'_{2n,2k}} \left(\frac{(2k)!}{\prod_{i=1}^{2n} c_i!} \prod_{i=1}^{2n} \frac{u\left(\frac{i-1}{2}\right)^{c_i}}{i!^{c_i}} \right),$$

which simplifies to (9). □

In light of Lemma 7 and the fact that each $u(n)$ is an integer, we see explicitly that $s(n,k)$ is always an integer. Furthermore, we may reduce mod p in (9) to immediately obtain the following formula for $s(n,k)$ mod p. Henceforth, if $x \in \mathbb{Z}$, and $p \geq 2$ is prime, we let x_p denote the congruence class of x modulo p.

Corollary 9. *For any pair (n,k) of positive integers such that $n \geq k$, and any prime number p, we have*

$$s(n,k)_p = \sum_{\lambda \in \mathcal{P}'_{2n,2k}} \left(\left[\frac{(2n)!}{\prod_{i=1}^{2n} i!^{c_i} c_i!} \right]_p \prod_{i=1}^{2n} \left[u\left(\frac{i-1}{2} \right)^{c_i} \right]_p \right), \qquad (11)$$

where the multiplication in parentheses is of congruence classes, as is the summation over $\mathcal{P}'_{2n,2k}$.

3 Proof of Theorem 1 (i)

In the previous section we saw that $s(n,k) = \frac{r(n,k)}{2^{n-k}}$ is an integer for all $1 \leq k \leq n$, which immediately implies that $r(n,k)$ is even. Thus, (8) implies that in order to show that $d(n)$ is odd for all n, it suffices to show that $v(n)$ is odd for all n. We will prove this by induction. The first few values of $v(n)$ are given by $(v(n))_{n=0}^{\infty} = 1, 1, 47, 7395, \ldots$, which can easily be computed. This establishes the base case.

Before proceeding with the induction step, we recall the following formula of Legendre [7, p. 10]. For p a prime number, and n a positive integer, let $\omega_p(n)$ denote the p-adic valuation of n, meaning that $\omega_p(n)$ is the largest natural number α such that p^{α} divides n.

Theorem 10 (Legendre)**.** *For any positive integer n,*

$$\omega_p(n!) = \frac{n - s_p(n)}{p-1},$$

where $s_p(n)$ is the sum of the digits in the base-p expansion of n.

Assume now the induction hypothesis that $v(m)$ is odd for all $m < n$. We first consider the case that n is odd. Throughout the proof we will use the notation $A \equiv B$, for $A, B \in \mathbb{Z}$, to mean that A and B have the same parity. We apply the induction hypothesis to simplify the expression in (6), obtaining

$$v(n) \equiv \frac{1}{2} \sum_{m=1}^{n-1} \binom{2n}{2m} = \sum_{m=1}^{\frac{n-1}{2}} \binom{2n}{2m}.$$

Then we apply twice the famous identity of Pascal, which says that for $1 \leq k \leq n$, $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$. Thus we obtain

$$\begin{aligned} v(n) &\equiv \sum_{m=1}^{\frac{n-1}{2}} \left[\binom{2n-2}{2m} + 2\binom{2n-2}{2m-1} + \binom{2n-2}{2m-2} \right] \\ &\equiv \left[\sum_{m=1}^{\frac{n-1}{2}} \binom{2n-2}{2m} \right] + \left[\sum_{m=1}^{\frac{n-1}{2}} \binom{2n-2}{2m-2} \right] \\ &= \binom{2n-2}{n-1} + \left[\sum_{m=1}^{\frac{n-1}{2}} \binom{2n-2}{2m} \right] + 1 + \left[\sum_{k=1}^{\frac{n-1}{2}} \binom{2n-2}{2k} \right] \\ &\equiv \binom{2n-2}{n-1} + 1, \end{aligned}$$

which is odd, since $\binom{2k}{k}$ is even for all $k \geq 1$. Now assume that n is even. Similarly to the odd case, we have

$$\begin{aligned}
v(n) &\equiv \sum_{m=1}^{\frac{n}{2}-1} \binom{2n}{2m} + \frac{1}{2}\binom{2n}{n} \\
&= \left[\sum_{m=1}^{\frac{n}{2}-1} \left[\binom{2n-2}{2m} + 2\binom{2n-2}{2m-1} + \binom{2n-2}{2m-2}\right]\right] + \frac{1}{2}\binom{2n}{n} \\
&\equiv \binom{2n-2}{n-2} + 2\left[\sum_{m=1}^{\frac{n}{2}-2} \binom{2n-2}{2m}\right] + 1 + \frac{1}{2}\binom{2n}{n} \\
&\equiv 1 + \frac{1}{2}\binom{2n}{n} + \binom{2n-2}{n-2}.
\end{aligned}$$

So to complete the proof we must show that

$$\frac{1}{2}\binom{2n}{n} \equiv \binom{2n-2}{n-2},$$

for all $n \geq 1$. We do this by checking separately the parity of each term. First we claim that $\frac{1}{2}\binom{2n}{n}$ is odd iff n is a power of 2. Indeed, by Theorem 10 we have

$$\begin{aligned}
\omega_2\left(\frac{1}{2}\binom{2k}{k}\right) &= \omega_2((2k)!) - 2\omega_2(k!) - 1 \\
&= s(k) - 1 \geq 0,
\end{aligned}$$

with equality iff $s_2(k) = 1$, iff k is a power of 2, as claimed.

Next, observe that $\binom{2n-2}{n-2}$ is odd iff $\omega_2\binom{2n-2}{n-2} = 0$. From Theorem 10 we see that

$$\omega_2\binom{2n-2}{n-2} = s_2(n) + s_2(n-2) - s_2(2n-2),$$

which is 0 iff n and $n-2$ don't both have a 1 digit in the same place in their binary expansions. This certainly occurs when n is a power of 2. On the other hand, if n is not a power of 2, write the binary expansion of n as $n = \sum_{i=0}^{\infty} a_i 2^i$, and let i_1 and i_2 be the indices at which the first and second 1 occur in the expansion, i.e.

$$n = 2^{i_1} + 2^{i_2} + r,$$

where either $r = 0$ or r is divisible by 2^j, for some $j > i_2 \geq i_1$. Then $n-2 = \left(\sum_{i=0}^{i_1-1} 2^i\right) + 2^{i_2} + r$, and we see that n and $n-2$ share a 1 for their i_2'th digit; hence $\binom{2n-2}{n-2}$ is even. This completes the proof.

4 The behavior of $d(n)$ modulo $p = 5$

4.1 A formula for $r(n,k)$ mod 5

Corollary 9 provides a flexible way to reduce $s(n,k)$ (and hence $r(n,k)$) modulo p, and will be our main tool, along with the recurrence relation (8), in studying the congruences of $d(n)$ modulo primes $p \neq 2$. In the case $p = 5$, the reduction (11) is particularly simple. Throughout this section the notation $A \equiv B$ will be shorthand for $A \equiv B \pmod 5$.

Theorem 11 (Formula for $r(n,k)$ mod 5)**.** *For $1 \leq k \leq n \leq 5k$ the following congruences hold mod 5:*

$$r(n,k) \equiv \begin{cases} \frac{(2n)!}{\left(\frac{5k-n}{2}\right)!\left(\frac{n-k}{2}\right)!5^{\frac{n-k}{2}}} & \text{if } n-k \text{ is even} \\ \\ \frac{2(2n)!}{\left(\frac{5k-n-1}{2}\right)!\left(\frac{n-k-1}{2}\right)!5^{\frac{n-k-1}{2}}} & \text{if } n-k \text{ is odd} \end{cases} \tag{12}$$

If $n > 5k$, then $r(n,k) \equiv 0$.

A graphical plot of Theorem 11 shows a compelling fractal pattern (see Figure 1 below).

Before we begin the proof, we need another lemma about the sequences $(u(n))$ and $(v(n))$.

Lemma 12. *The sequences u and v satisfy the following congruences mod 5:*

$$(i) \qquad (v(n))_{n=0}^{\infty} \equiv (1,1,2,0,0,0,0,\dots)$$

$$(ii) \qquad (u(n))_{n=0}^{\infty} \equiv (1,1,1,0,0,0,0,\dots)$$

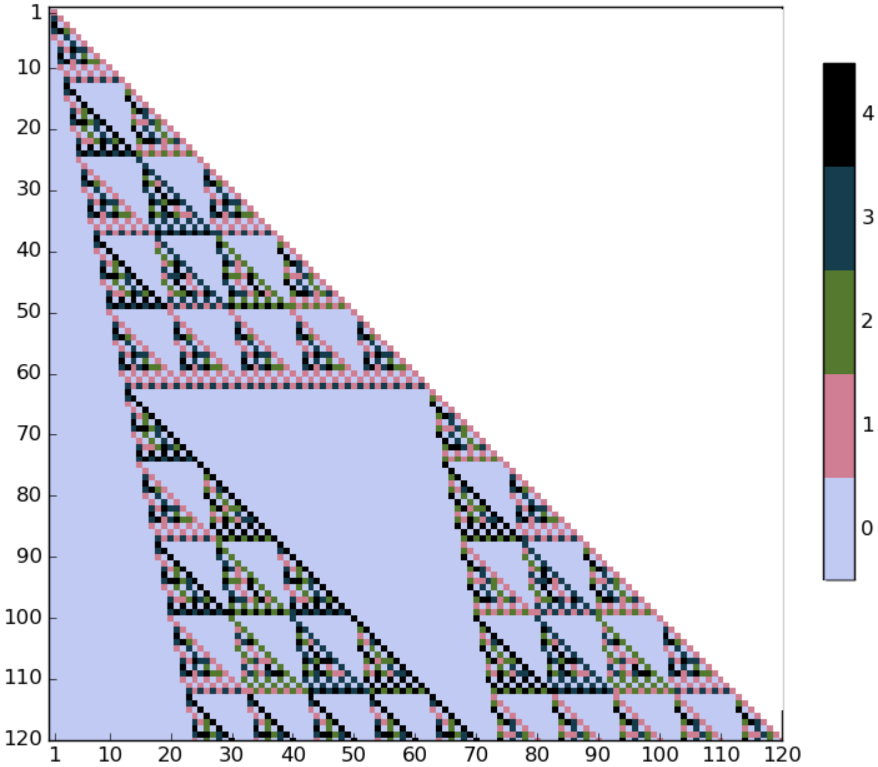

Figure 1: Congruences of $r(n,k)$ mod 5, $1 \le k \le n < 120$. The rows are indexed by n, the columns are indexed by k, and the colors indicate residue classes of $r(n,k)$ mod 5, according to the colorbar.

Proof. From Definition 4, one can calculate by hand or with a computer that the first few terms of the sequence $(u(n))_{n=0}^{\infty}$ are $1, 6, 256, 28560, 6071040$. Furthermore, it is clear from (5) that if $n \ge 4$, we have the simplified recursion

$$u(n) \equiv \binom{2n+1}{2n-1} u(n-1)$$

since the term $(3 \cdot 7 \cdot 11 \cdots (4n-1))^2)$ vanishes, as do all of the terms in the summation except for the term corresponding to $m = n-1$. Then by induction we see that $u(n) \equiv 0$ for all $n \ge 4$.

Similarly the initial terms of the sequence $(v(n))_{n=0}^{\infty}$ are $1, 1, 47, 7395,$

$2453425, 1399055625$. For $n \geq 2$ the following relation holds

$$v(n) \equiv -\frac{1}{2}\sum_{m=1}^{n-1}\binom{2n}{2m}v(m)v(n-m)$$

so if we assume that $v(k) \equiv 0$ for $2 \leq k \leq n$, then it is clear that $v(n+1) \equiv 0$, and the lemma follows by induction. □

Remark: Whereas Theorem 8 is general for all primes, the lemma we just proved was stated for $p = 5$. In fact, experimental evidence suggests that this lemma can be generalized to the statement that $u(n)$ and $v(n)$ are both congruent to 0 mod p for all $n \geq \frac{p+1}{2}$, when p is a prime congruent to 1 mod 4. Indeed our proof in the case $p = 5$ is rather ad hoc and in particular makes no use of the binomial coefficients appearing in the recursions for u and v. In Section 4 we will prove a similar lemma for u and v in the case $p \equiv 3 \pmod 4$.

Proof of Theorem 11. In view of Lemma 12, we may restrict the class of partitions that need to be considered in the summation appearing in (11). More specifically, let $\mathcal{P}^3_{n,k} \subset \mathcal{P}'_{n,k}$ be the set of partitions of n into k parts among the first three odd positive integers, $1, 3, 5$. Since $u(n)$ vanishes mod 5 for $n > 2$, and therefore $u\left(\frac{i-1}{2}\right)$ vanishes mod 5 for $i > 5$, summands in (11) that are indexed by partitions not in $\mathcal{P}^3_{2n,2k}$ have a residue of 0 mod 5. Thus we obtain an equivalent definition of $s(n,k)_5$ to that in (11) if we replace the indexing set with $\mathcal{P}^3_{2n,2k}$ and adopt the convention that $s(n,k)_5 = 0$ for pairs (n,k) such that $\mathcal{P}^3_{2n,2k}$ is empty.

Furthermore, for $n = 0, 1, 2$, $u(n) \equiv 1$. Hence, $u\left(\frac{i-1}{2}\right) \equiv 1$ for $i = 1, 3, 5$, and if we substitute these values of $u\left(\frac{i-1}{2}\right)_5$ into (11), we obtain

$$s(n,k)_5 = \sum_{\lambda \in \mathcal{P}^3_{2n,2k}} \left[\frac{(2n)!}{c_1! 3!^{c_3} c_3! 5!^{c_5} c_5!}\right]_5, \tag{13}$$

with the convention that $s(n,k)_5 = 0$ if $\mathcal{P}^3_{2n,2k} = \emptyset$. The expression is already interesting. One immediate implication is that if $5k < n$, then $r(n,k)_5 = s(n,k)_5 = 0$, since $\mathcal{P}^3_{2n,2k}$ is clearly empty (see Figure 1).

To reduce the sum in (13) further, we recall that in the field of residues modulo 5, nonzero elements are invertible; therefore, since we've shown that each summand in (13) is an integer, we can replace 3! in the denominator with 1 and replace $5! = 5 \cdot 4!$ with $5 \cdot (-1)$ without changing the value of the summand's residue mod 5. Thus, we have

$$s(n,k)_5 = \sum_{\lambda \in P^3_{2n,2k}} \left[\frac{(2n)!(-1)^{c_5}}{c_1! c_3! c_5!} \right]_5 . \tag{14}$$

Next, identify elements of $P^3_{2n,2k}$ in the obvious way with triples (c_1, c_3, c_5) of non-negative integers satisfying the pair of equations

$$\begin{cases} \sum_{i=1}^3 ic_i & = 2n \\ \sum_{i=1}^3 c_i & = 2k. \end{cases}$$

For a given pair (n,k), if we fix c_5 to be some integer c, then this becomes an invertible linear system with

$$c_1 = 3k - n + c \,, \quad c_3 = n - k - 2c.$$

There exists $(c_1, c_3, c) \in P^3_{2n,2k}$ satisfying the system if and only if $n \leq 5k$ and

$$\max(0, n-3k) \leq c \leq \left\lfloor \frac{n-k}{2} \right\rfloor .$$

This allows us to rewrite (14) as a summation over a single index parameter:

$$s(n,k)_5 = \begin{cases} \displaystyle\sum_{c=\max(0,n-3k)}^{\lfloor \frac{n-k}{2} \rfloor} \left[\tfrac{(2n)!(-1)^c}{(3k-n+c)!(n-k-2c)!c!5^c} \right]_5 & \text{if } n \leq 5k \\ 0 & \text{if } n > 5k. \end{cases} \tag{15}$$

Our next step in the proof is to simplify (15) further by showing that the summation depends only on the term corresponding to the largest value of the index parameter, namely $c = \lfloor \frac{n-k}{2} \rfloor$, because all other terms are congruent to 0. This is the content of the next lemma.

Lemma 13. *For integers $0 < k \leq n \leq 5k$, the quantity*

$$V(c) := \omega_5 \left(\frac{(2n)!(-1)^c}{(3k-n+c)!(n-k-2c)!c!5^c} \right),$$

as a function of $c \in \mathbb{Z}$, is minimized over max$(0, n-3k) \leq c \leq \lfloor \frac{n-k}{2} \rfloor$ when $c = \lfloor \frac{n-k}{2} \rfloor$ and for no other values of c.

Proof. Assume $n > k$, as otherwise there is nothing to check. Let $c \in \{\max(0, n-3k), \cdots, \lfloor \frac{n-k}{2} \rfloor - 1\}$, and let $\delta = \lfloor \frac{n-k}{2} \rfloor - c > 0$. Then,

$$\begin{aligned} V(c) - V\left(\left\lfloor \frac{n-k}{2} \right\rfloor\right) &= V(c) - V(c+\delta) \\ &= \omega_5((3k-n+c+\delta)!) - \omega_5((3k-n+c)!) \\ &\ + \omega_5((n-k-2(c+\delta))!) - \omega_5((n-k-2c)!) \\ &\ + \omega_5((c+\delta)!) - \omega_5(c!) \\ &\ + \omega_5(5^{c+\delta}) - \omega_5(5^c). \end{aligned} \tag{16}$$

Each line of the summation contains a difference that we would like to estimate from below. To do that, we note the general fact that if a and b are positive integers, then

$$\begin{aligned} \omega_5((a+b)!) &= \omega_5(a!) + \omega_5(b!) + \omega_5\left(\binom{a+b}{a}\right); \text{ hence,} \\ \omega_5((a+b)!) - \omega_5(a!) &\geq \omega_5(b!). \end{aligned}$$

We also note that $n-k-2(c+\delta) = n-k-2\lfloor \frac{n-k}{2} \rfloor \in \{0,1\}$ and $n-k-2c \in \{2\delta, 2\delta+1\}$. Therefore, we can bound from below each line in (16) to obtain the estimate

$$V(c) - V\left(\left\lfloor \frac{n-k}{2} \right\rfloor\right) \geq 2\omega_5(\delta!) - \omega_5((2\delta+1)!) + \delta.$$

An application of Theorem 10 now yields

$$\begin{aligned} V(c) - V\left(\left\lfloor \frac{n-k}{2} \right\rfloor\right) &\geq 2\frac{\delta - s_5(\delta)}{4} - \frac{2\delta+1-s_5(2\delta+1)}{4} + \delta \\ &= \delta - \frac{s_5(\delta)}{2} + \frac{1}{4}(s_5(2\delta+1) - 1) \\ &> \delta - s_5(\delta) \\ &\geq 0, \end{aligned}$$

where the last two inequalities amount to the simple fact that for p prime, any integer $k \geq 1$ satisfies $1 \leq s_p(k) \leq k$. We've shown that $V(c)$ assumes its smallest value uniquely at $c = \lfloor \frac{n-k}{2} \rfloor$. □

Proof of Theorem 11, continued. By the lemma, all of the summands in (15), except the one indexed by $c = \lfloor \frac{n-k}{2} \rfloor$, must vanish mod 5, since they have positive valuation. The remaining summand may or may not vanish. In any case, we have the following simplified formula for $s(n,k)_5$, $1 \leq k \leq n \leq 5k$.

$$s(n,k) \equiv \begin{cases} \frac{(2n)!(-1)^{\frac{n-k}{2}}}{\left(\frac{5k-n}{2}\right)!\left(\frac{n-k}{2}\right)!5^{\frac{n-k}{2}}} & \text{if } n-k \text{ is even} \\ \\ \frac{(2n)!(-1)^{\frac{n-k-1}{2}}}{\left(\frac{5k-n-1}{2}\right)!\left(\frac{n-k-1}{2}\right)!5^{\frac{n-k-1}{2}}} & \text{if } n-k \text{ is odd} \end{cases} \tag{17}$$

Now we want to translate this into a formula for $r(n,k)_5 = 2_5^{n-k} s(n,k)_5$. The congruence of $(n-k)$ modulo 4 determines the congruence of 2^{n-k} modulo 5, as well as the sign of $(-1)^{\frac{n-k}{2}}$ (respectively $(-1)^{\frac{n-k-1}{2}}$) in the case $n-k$ is even (respectively odd). However, it turns out that we need only consider parity, since one can check routinely that

$$\begin{aligned} 2^{n-k}(-1)^{\frac{n-k}{2}} &\equiv 1 \pmod 5 \text{ if } n-k \text{ is even, and} \\ 2^{n-k}(-1)^{\frac{n-k-1}{2}} &\equiv 2 \pmod 5 \text{ if } n-k \text{ is odd.} \end{aligned}$$

Combined with (17), this completes the proof of Theorem 11. □

4.2 Proof of Theorem 1 (ii)

Now that we have a nice expression for $r(n,k)_5$, we return to the main objective of this section, proving Theorem 1 (ii).

Lemma 14. *In order to prove Theorem 1 (ii), it suffices to prove the following: For $n \geq 3$,*

$$\sum_{\substack{\frac{n}{5} \leq k \leq n \\ k \text{ even}}} r(n,k) \equiv \sum_{\substack{\frac{n}{5} \leq k \leq n \\ k \text{ odd}}} r(n,k) \equiv 0. \tag{18}$$

Proof. Assume that (18) holds. Then

$$\sum_{\frac{n}{5} \leq k \leq n} r(n,k)(-1)^k = \sum_{\substack{\frac{n}{5} \leq k \leq n \\ k \text{ even}}} r(n,k) - \sum_{\substack{\frac{n}{5} \leq k \leq n \\ k \text{ odd}}} r(n,k) \equiv 0.$$

Subtracting $r(n,n)(-1)^n$ from the left and right sides, we obtain

$$\sum_{\frac{n}{5}\leq k\leq n-1} r(n,k)(-1)^k \equiv r(n,n)(-1)^{n+1}. \tag{19}$$

Now a quick application of Theorem 11 shows that $r(n,n) \equiv 1$ for all n (in fact, it's not hard to deduce from (7) and the fact that $u(1) = 1$ that $r(n,n) = 1$ for all n), and we have also observed above that $r(n,k) \equiv 0$ when $5k < n$. Therefore, from (19) we obtain

$$\sum_{k=1}^{n-1} r(n,k)(-1)^k \equiv (-1)^{n+1}. \tag{20}$$

We will now prove by induction that $d(n) \equiv (-1)^{n+1}$ for $n \geq 1$. The cases $n = 1$ and $n = 2$ can be checked directly, since $d(1) = -1$ and $d(2) = 51$. Also from (8) and Lemma 12, we see that when $n \geq 3$, the following holds:

$$d(n) \equiv -\sum_{k=1}^{n-1} r(n,k)d(k).$$

Thus, if $n \geq 3$ and we assume the induction hypothesis that $d(k) \equiv (-1)^{k+1}$ for all $1 \leq k < n$, it follows that

$$d(n) \equiv -\sum_{k=1}^{n-1} r(n,k)(-1)^{k+1} \equiv \sum_{k=1}^{n-1} r(n,k)(-1)^k.$$

But the right-hand-side is congruent to $(-1)^{n+1}$, by (20). This verifies the induction step. Thus, the truth of (18) implies Theorem 1 (ii). □

We will now use some concepts from group theory to verify (18). For n a positive integer, let S_n denote the symmetric group on n letters, and recall that every element of S_n has a unique decomposition as a product of disjoint cycles. Let X_n be the set of elements $x \in S_n$ such that $x^5 = 1$. For any non-negative integer $k \leq n$, let X_n^k denote the set of elements $x \in S_n$ such that x can be written as a disjoint product of k five-cycles and $n - 5k$ one-cycles. Then

$$X_n = \bigcup_{k=0}^{\lfloor \frac{n}{5} \rfloor} X_n^k\ . \tag{21}$$

The connection to Theorem 11 is the following:

Lemma 15. *For $n \geq 3$,*

$$(a.) \qquad |X_{2n}| = \sum_{\substack{\frac{n}{5} \leq k \leq n \\ n-k \ even}} \frac{(2n)!}{\left(\frac{5k-n}{2}\right)! \left(\frac{n-k}{2}\right)! 5^{\frac{n-k}{2}}} \ ,$$

$$(b.) \quad 2(2n)(2n-1)(2n-2) \cdot |X_{2n-3}| = \sum_{\substack{\frac{n}{5} \leq k < n \\ n-k \ odd}} \frac{2(2n)!}{\left(\frac{5k-n-1}{2}\right)! \left(\frac{n-k-1}{2}\right)! 5^{\frac{n-k-1}{2}}} \ .$$

Proof. First we observe that X_n^k is a conjugacy class in S_n with cardinality

$$|X_n^k| = \frac{n!}{(n-5k)!k!5^k} \tag{22}$$

(see e.g. [4, Prop. 11 and Exercise 33 in Sec. 4.3]).

Fix $n \geq 3$. Observe from (22) that if $n-k$ is even, then the expression on the right-hand-side of (12) is precisely $\left|X_{2n}^{\frac{n-k}{2}}\right|$. Also, from (21) we see that

$$|X_{2n}| = \sum_{0 \leq k \leq \frac{2n}{5}} |X_{2n}^k|.$$

Therefore, to prove part (a.) of the lemma, we must show that the quantity $\frac{n-k}{2}$ assumes every value in the set $T_1 = \{0, 1, \cdots, \lfloor \frac{2n}{5} \rfloor\}$ exactly once as k ranges over the set $T_2 = \{k : \lceil \frac{n}{5} \rceil \leq k \leq n, \, n-k \text{ even}\}$. This is not hard to see, since the change of variable $k \mapsto \frac{n-k}{2}$ maps n to 0, and is linear with first difference -2, while both T_1 and T_2 have the same cardinality, as one can deduce from a simple analysis of the cases of the congruence mod 5 of n.

Similarly, if $n-k$ is odd, then the expression on the right-hand-side of (12) is $2(2n)(2n-1)(2n-2) \cdot \left|X_{2n-3}^{\frac{n-k-1}{2}}\right|$, and

$$|X_{2n-3}| = \sum_{0 \leq k \leq \frac{2n-3}{5}} |X_{2n-3}^k|.$$

So to prove part (b.) we must show that the quantity $\frac{n-k-1}{2}$ assumes every value in the set $\{0, 1, \cdots, \lfloor \frac{2n-3}{5} \rfloor\}$ exactly once as k ranges over $\{k : \lceil \frac{n}{5} \rceil \leq k \leq n-1, \, n-k \text{ odd}\}$. This can be deduced from the change of variables $k \mapsto \frac{n-k-1}{2}$ and the same type of argument as before. □

We see from Lemma 15 that if $n > 3$ is even, then $|X_{2n}|$ is congruent to $\sum_{\substack{\frac{n}{5} \leq k \leq n \\ k \text{ even}}} r(n,k)$, and an integer multiple of $|X_{2n-3}|$ is congruent to $\sum_{\substack{\frac{n}{5} \leq k \leq n \\ k \text{ odd}}} r(n,k)$. Therefore, in order to verify that (18) holds for all even n, it suffices to show that $|X_{2n}|$ and $|X_{2n-3}|$ are both congruent to 0, when $n > 3$. This follows from a theorem of Frobenius (see e.g. [5]).

Theorem 16 (Frobenius)**.** *Let G be a finite group whose order is divisible by a positive integer m. Then m divides the cardinality of the set of solutions x in G to the equation $x^m = 1$.*

Since X_n is precisely the set of solutions to the equation $x^5 = 1$ in S_n, the theorem implies that $|X_{2n}| \equiv |X_{2n-3}| \equiv 0$ for even $n > 3$. Similarly, if $n > 3$ is odd, then $|X_{2n}|$ is congruent to $\sum_{\substack{\frac{n}{5} \leq k \leq n \\ k \text{ odd}}} r(n,k)$, and an integer multiple of $|X_{2n-3}|$ is congruent to $\sum_{\substack{\frac{n}{5} \leq k \leq n \\ k \text{ even}}} r(n,k)$, and we again apply Theoerem 16. Finally, if $n = 3$ we can check the validity of (18) by directly computing from (12) that $r(3,1)_5 = 4_5, r(3,2) = 0_5$, and $r(3,3) = 1_5$. This verifies (18) for all $n \geq 3$ and finishes the proof of Theorem 1 (ii).

5 Vanishing of $d(n)$ modulo primes $p = 4k + 3$

5.1 A vanishing theorem for $u(n)$ and $v(n)$

Throughout Section 5, p will always denote a prime congruent to 3 mod 4, $A \equiv B$ will be shorthand for $A \equiv B \pmod{p}$, and we define $n_0 := \frac{p^2-1}{2}$. We begin with a theorem about the congruences of $(u(n))$ and $(v(n))$ modulo p, similar to Lemma 12 above.

Theorem 17. *The sequences $(u(n))_{n=0}^{\infty}$ and $(v(n))_{n=0}^{\infty}$ satisfy*

(i)

$$u\left(\frac{p-1}{2}\right) \equiv 0,$$

(ii)

$$u(n) \equiv 0 \textit{ for } n \geq n_0,$$

(iii)

$$v(n) \equiv 0 \text{ for } n > n_0.$$

We first prove a lemma that will be used repeatedly, then we prove the theorem in three parts.

Lemma 18. *If $a, b \in \mathbb{Z}$ and $p^2 \leq a \leq b + p^2 - 1 \leq 2p^2 - 2$, then $\binom{a}{b} \equiv 0$.*

Proof. The hypothesis implies that $b \leq p^2 - 1$ and $a - b \leq p^2 - 1$. It follows that

$$\omega_p(b!(a-b)!) = \left\lfloor \frac{b}{p} \right\rfloor + \left\lfloor \frac{a-b}{p} \right\rfloor \leq \frac{a}{p}.$$

Meanwhile, since $a \geq p^2$

$$\omega_p(a!) \geq \left\lfloor \frac{a}{p} \right\rfloor + 1 > \frac{a}{p},$$

and therefore $\omega_p\left(\binom{a}{b}\right) > 0$. □

Proof of Theorem 17 (i). By (5), we have

$$\begin{aligned} u\left(\frac{p-1}{2}\right) &= (3 \cdot 7 \cdots (2p-3))^2 \\ &\quad - \sum_{m=0}^{\frac{p-1}{2}-1} \binom{p}{2m+1} \left[1 \cdot 5 \cdots \left(4\left(\frac{p-1}{2} - m\right) - 3\right)\right]^2 u(m). \end{aligned} \tag{23}$$

The product $(3 \cdot 7 \cdots (2p-3))^2$ contains as factors all positive integers that are congruent to 3 mod 4 and less than $2p+1$, and p is such a number. Furthermore $\binom{p}{m} \equiv 0$ for $1 \leq m < p$, so the sum in (23) also vanishes mod p. □

Proof of Theorem 17 (ii). Set $n_1 = \frac{3(p+1)}{4} < n_0$. Referring to (5), observe that $3 \cdot 7 \cdots (4n-1))^2 \equiv 0$ for $n \geq \frac{p+1}{4}$, so in particular for $n \geq n_0$. Observe also that $0 \equiv 1 \cdot 5 \cdots (4(n-m)-3)$ if $n - m \geq n_1$. It follows that if $n \geq n_0$, we have the following truncated summation for $u(n)$:

$$u(n) \equiv \sum_{m=n-n_1+1}^{n-1} \binom{2n+1}{2m+1} (1 \cdot 5 \cdots (4(n-m)-3))^2 u(m). \tag{24}$$

We will also use the fact that

$$\binom{2n+1}{2m+1} \equiv 0 \tag{25}$$

for $n_0 \leq n \leq n_0 + n_1 - 2$ and $n_0 - n_1 + 1 \leq m \leq n_0 - 1$, which follows from Lemma 18. Indeed, the assumptions on n in (25) imply that

$$p^2 = 2n_0 + 1 \leq 2n + 1 \leq 2n_0 + 2n_1 - 3 \leq 2p^2 - 2,$$

and hence

$$p^2 + \frac{3}{2}(p+1) + 2 = 2n_0 - 2n_1 + 3 \leq 2m + 1 \leq 2n_0 - 1 = p^2 - 2.$$

But $p^2 + \frac{3}{2}(p+1) + 2 \geq (2n+1) - p^2 + 1$, for $n \leq n_0 + n_1 - 2$. In brief, Lemma 18 applies with $a = 2n + 1$ and $b = 2m + 1$, verifying (25).

It follows that $u(n_0) \equiv 0$, since (25) implies that all of the binomial coefficients in (24) vanish mod p when $n = n_0$. Now suppose that

$$u(n_0) \equiv u(n_0 + 1) \equiv \cdots \equiv u(n_0 + k - 1) \equiv 0,$$

for some k such that $1 \leq k \leq n_1 - 2$. This supposition, along with (24) implies that

$$\begin{aligned} u(n_0 + k) &= \sum_{m=n_0+k-n_1+1}^{n_0+k-1} \binom{2(n_0+k)+1}{2m+1} (1 \cdot 5 \cdots (4(n_0 + k - m) - 3))^2 \\ &= \sum_{m=n_0+k-n_1+1}^{n_0-1} \binom{2(n_0+k)+1}{2m+1} (1 \cdot 5 \cdots (4(n_0 + k - m) - 3))^2. \end{aligned}$$

By (25) all the binomial coefficients in the sum vanish; hence $u(n_0 + k) \equiv 0$. Since k was arbitrary, we can conclude that $u(n) \equiv 0$ when $n_0 \leq n \leq n_0 + n_1 - 2$.

Finally, observe that (24) shows that $u(n)_p$ is a sum involving only those values of u evaluated at integers in $[n - n_1 + 1, n - 1]$; if these values of u vanish mod p, then so does $u(n)$. Therefore, if one can show that $u(n)$ vanishes mod p for $n_1 - 1$ consecutive values of n, then by induction $u(n)$ must vanish mod p for all larger n. But we've already shown above that $u(n)$ vanishes for $n \in [n_0, n_0 + n_1 - 2]$, so it follows that $u(n)$ vanishes for all $n \geq n_0$. □

Proof of Theorem 17 (iii). Referring to the recursive definition for $v(n)$ in (6), observe that $1 \cdot 5 \cdots (4n-3) \equiv 0$ for $n \geq \frac{3p+3}{4}$ and hence for $n \geq n_0$. Furthermore, if $n = n_0 + 1$ and $1 \leq m \leq n_0$, then Lemma 18 applies with $a = 2n$ and $b = 2m$ and hence $\binom{2n}{2m} \equiv 0$. Therefore, $v(n_0 + 1) \equiv 0$.

Now let $n > n_0$ be arbitrary, and assume as an induction hypothesis that $v(k) \equiv 0$ for all $n_0 < k < n$. Then

$$v(n) \equiv -\frac{1}{2} \sum_{m=1}^{n-1} \binom{2n}{2m} v(m) v(n-m). \tag{26}$$

If $n \geq 2n_0$, then $n - m > n_0$ for all values of the summation index m, so by the induction hypothesis $v(n-m)$ vanishes mod p and so does the sum. So assume that $n \leq 2n_0$. Then we may restrict the sum in (26) to index values $m \in [n - n_0, n_0]$, since for other values of m either $m > n_0$ or $n - m > n_0$. However, for any such m, we can apply Lemma 18 with $a = 2n$ and $b = 2m$, since $p^2 \leq 2n$ and $2n - p^2 + 1 \leq 2m \leq 2n_0 = p^2 - 1$. It follows that every binomial coefficient in (26) vanishes mod p and so does $v(n)$. Induction on $n > n_0$ completes the proof. □

5.2 Proof of Theorem 1 (iii)

We begin with a lemma that provides a means for proving the theorem.

Lemma 19. *If $r(n,k) \equiv 0$ for all pairs (n,k) such that $1 \leq k \leq n_0 < n$, then Theorem 1 (iii) is true.*

Figure 2 below gives an illustration of the lemma's hypothesis in the case $p = 7$.

Proof. Equation (8) and Theorem 17 imply that if $n > n_0$ then

$$d(n) \equiv -\sum_{k=1}^{n-1} r(n,k) d(k).$$

If we assume the hypothesis of the lemma, then

$$d(n_0 + 1) \equiv -\sum_{k=1}^{n_0} r(n_0 + 1, k) d(k) \equiv 0,$$

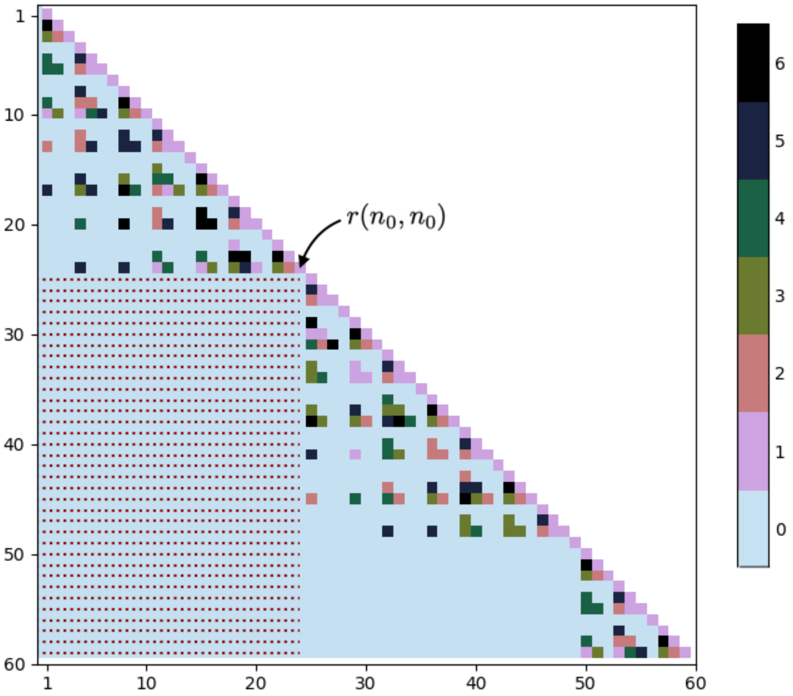

Figure 2: Congruences of $r(n, k)$ mod 7, $1 \leq k \leq n < 60$. The rows are indexed by n, and the colors indicate residue classes of $r(n, k)$ mod 7, according to the colorbar. Note that $n_0 = \frac{p^2-1}{2} = 24$ for $p = 7$. The submatrix $(r(n, k))_{1 \leq k \leq n_0 < n}$, where $r(n, k)$ vanishes by Theorem 20, is emphasized.

since all the summands vanish mod p; moreover for general $n > n_0$,

$$d(n+1) \equiv -\sum_{k=n_0+1}^{n} r(n, k)d(k).$$

Therefore, if we assume that $d(k) \equiv 0$ for all k such that $n_0 + 1 \leq k \leq n$, then $d(n+1) \equiv 0$. It follows by induction that $d(n) \equiv 0$ for all $n > n_0$, which is the statement of Theorem 1 (iii). □

As we did in Section 4, for $p = 5$, we would now like to restrict the class of partitions that we need to consider in (11), for $p \equiv 3 \pmod 4$. Let

$\mathcal{P}^*_{2n,2k} \subset \mathcal{P}'_{2n,2k}$ denote the set of partitions λ whose parts are all less than p^2, and such that no part of λ is equal to p, i.e. $c_p = 0$. Theorem 17 implies that we may replace the index set in the summation (11) with $\mathcal{P}^*_{2n,2k}$, since any partition $\lambda \in \mathcal{P}'_{2n,2k} \setminus \mathcal{P}^*_{2n,2k}$ must contain a part λ_i such that $u\left(\frac{\lambda_i - 1}{2}\right)_p = 0$ and hence will contribute 0 to the sum. In other words,

$$s(n,k)_p = \sum_{\lambda \in \mathcal{P}^*_{2n,2k}} \left(\left[\frac{(2n)!}{\prod_{i=1}^{2n} i!^{c_i} c_i!} \right]_p \prod_{i=1}^{2n} \left[u\left(\frac{i-1}{2}\right)^{c_i} \right]_p \right). \tag{27}$$

The key to using formula (27) is the following theorem.

Theorem 20. *Let (n,k) be such that $1 \leq k \leq n_0 < n$. Let $\lambda = (c_1, c_2, \ldots, c_{2n})$ be a partition in $\mathcal{P}^*_{2n,2k}$. Then,*

$$\omega_p \left(\frac{(2n)!}{\prod_{i=1}^{2n} i!^{c_i} c_i!} \right) > 0. \tag{28}$$

The theorem implies, by (27), that $r(n,k) = 2^{n-k} s(n,k)$ vanishes mod p for $1 \leq k \leq n_0 < n$, and in view of Lemma 19 will complete the proof of Theorem 1 (iii). We record as a lemma a few facts about arithmetic that will be used freely in the proof of Theorem 20.

Lemma 21. *Let r and s be positive integers with base-p expansions*

$$r = \sum_{i=1}^{\infty} r_i p^i \quad \textit{and} \quad s = \sum_{i=1}^{\infty} s_i p^i.$$

Then the following are true:

(i) $s_p(r+s) \leq s_p(r) + s_p(s)$, *with equality iff there are no carries when r is added to s in base p, iff $r_i + s_i \leq p-1$ for all i.*

(ii) $\displaystyle\sum_{i=1}^{\infty}(r_i + s_i) \geq s_p \left[\sum_{i=1}^{\infty} (r_i + p s_i) \right]$

(iii) $s_p(rp) = s_p(r)$ *always, and* $s_p(r) = r$ *iff* $r \leq p-1$.

Proof. Statements (i) and (iii) are trivial. We use them to verify (ii).

$$\begin{aligned}\sum_{i=1}^{\infty}(r_i+s_i) &\geq s_p\left(\sum_{i=1}^{\infty} r_i\right)+s_p\left(\sum_{i=1}^{\infty} s_i\right)\\ &= s_p\left(\sum_{i=1}^{\infty} r_i\right)+s_p\left(p\sum_{i=1}^{\infty} s_i\right)\\ &\geq s_p\left(\sum_{i=1}^{\infty} r_i+p\sum_{i=1}^{\infty} s_i\right)\\ &= s_p\left[\sum_{i=1}^{\infty}(r_i+ps_i)\right].\end{aligned}$$

□

Proof of Theorem 20. Let $\lambda=(c_1,c_2,\ldots,c_{2n})\in\mathcal{P}^*_{2n,2k}$. For each i, $1\leq i\leq 2n$, let $c_i=a_0^i+a_1^i p$ be the base-p expansion of c_i, and let $i=b_0^i+b_1^i p$ be the base-p expansion of i. (The exponents are indices, and the fact that there are at most two digits in each expansion follows from the conditions $k\leq n_0$ and $\lambda_i<p^2$ for all i.)

By Theorem 10,

$$\begin{aligned}\omega_p\left(\frac{(2n)!}{\prod_{i=1}^{2n} i!^{c_i}c_i!}\right)(p-1) &= 2n-s_p(2n)-\sum_{i=1}^{2n}[c_i(i-s_p(i))+(c_i-s_p(c_i))]\\ &= \sum_{i=1}^{2n} s_p(i)c_i+\left[\sum_{i=1}^{2n}(s_p(c_i)-c_i)\right]-s_p(2n),\end{aligned}$$

where the last equality comes from the fact that $2n=\sum_{i=1}^{2n} ic_i$. We expand all the terms in the last line base-p, obtaining

$$\begin{aligned}&\omega_p\left(\frac{(2n)!}{\prod_{i=1}^{2n} i!^{c_i}c_i!}\right)(p-1)\\ &=\sum_{i=1}^{2n}(b_0^i+b_1^i)(a_0^i+a_1^i p)+\sum_{i=1}^{2n} a_1^i(1-p)-s_p\left(\sum_{i=1}^{2n}(b_0^i+b_1^i p)(a_0^i+a_1^i p)\right)\end{aligned}$$

$$
\begin{align*}
&= \sum_{i=1}^{2n}(b_0^i + b_1^i)a_1^i p + \sum_{i=1}^{2n}(b_0^i + b_1^i)a_0^i + \sum_{i=1}^{2n} a_1^i(1-p) \\
&\qquad\qquad\qquad - s_p\left(\sum_{i=1}^{2n}(b_0^i + b_1^i p)a_0^i + \sum_{i=1}^{2n}(b_0^i + b_1^i p)a_1^i p\right) \tag{29} \\
&\geq \sum_{i=1}^{2n}(b_0^i + b_1^i)a_1^i p - s_p\left(\sum_{i=1}^{2n}(b_0^i + b_1^i p)a_1^i p\right) + \sum_{i=1}^{2n} a_1^i(1-p) \tag{30} \\
&\qquad\qquad\qquad + \sum_{i=1}^{2n}(b_0^i + b_1^i)a_0^i - s_p\left(\sum_{i=1}^{2n}(b_0^i + b_1^i p)a_0^i\right) \tag{31} \\
&\geq 0,
\end{align*}
$$

where we justify the last inequality as follows. The quantity in (31) is non-negative by Lemma 21 (ii), and we claim that the quantity in (30) is also non-negative. To show that, write the quantity as

$$
\left\{\left[\sum_{i=1}^{2n}(b_0^i + b_1^i)a_1^i\right] - s_p\left(\sum_{i=1}^{2n}(b_0^i + b_1^i p)a_1^i p\right)\right\}
$$
$$
+\left\{\left[\sum_{i=1}^{2n}(b_0^i + b_1^i)a_1^i(p-1)\right] + \left[\sum_{i=1}^{2n} a_1^i(1-p)\right]\right\}.
$$

The first bracketed term is non-negative by Lemma 21, and the second bracketed term is non-negative since $b_0^i + b_1^i \geq 1$ for all i.

Suppose now that $\omega_p\left(\frac{(2n)!}{\prod_{i=1}^{2n} i!^{c_i} c_i!}\right) = 0$. Then the inequality that we used to transition from (29) to (30) and (31) must be an equality, and the quantity in (31) and the bracketed quantities above must all vanish. These facts have a number of consequences. First, from the second bracketed quantity, observe that for all i,

$$
a_1^i(b_0^i + b_1^i) = a_1^i,
$$

so either $a_1^i = 0$ or $(b_0, b_1) = (1, 0)$ or $(b_0, b_1) = (0, 1)$. Since no part of λ is equal to p, by the definition of $\mathcal{P}^*_{2n,2k}$, the last option is not possible. We conclude that $a_1^i = 0$ for all $i \geq 2$. In view of this, the identity

$$\begin{aligned}
&s_p\left(\sum_{i=1}^{2n}(b_0^i + b_1^i p)a_0^i + \sum_{i=1}^{2n}(b_0^i + b_1^i p)a_1^i p\right) \\
&\quad = s_p\left(\sum_{i=1}^{2n}(b_0^i + b_1^i p)a_0^i\right) + s_p\left(\sum_{i=1}^{2n}(b_0^i + b_1^i p)a_1^i p\right)
\end{aligned}$$

(from the transition from (29) to (30) and (31)), can be simplified to

$$s_p\left(\sum_{i=1}^{2n}(b_0^i + b_1^i p)a_0^i + a_1^1 p\right) = s_p\left(\sum_{i=1}^{2n}(b_0^i + b_1^i p)a_0^i\right) + a_1^1. \tag{32}$$

Furthermore, the fact that the quantity in (31) vanishes implies that (32) can be written as

$$s_p\left(\sum_{i=1}^{2n}(b_0^i + b_1^i p)a_0^i + a_1^1 p\right) = \left[\sum_{i=1}^{2n}(b_0^i + b_1^i)a_0^i\right] + a_1^1. \tag{33}$$

Since we can estimate the left-hand-side by

$$\begin{aligned}
s_p\left(\sum_{i=1}^{2n}(b_0^i + b_1^i p)a_0^i + a_1^1 p\right) &\leq s_p\left(\sum_{i=1}^{2n} b_0^i a_0^i\right) + s_p\left(p\left[\sum_{i=1}^{2n} b_1^i a_0^i\right] + a_1^1 p\right) \\
&= s_p\left(\sum_{i=1}^{2n} b_0^i a_0^i\right) + s_p\left(\left[\sum_{i=1}^{2n} b_1^i a_0^i\right] + a_1^1\right) \\
&\leq \left[\sum_{i=1}^{2n} b_0^i a_0^i\right] + \left[\sum_{i=1}^{2n} b_1^i a_0^i\right] + a_1^1,
\end{aligned} \tag{34}$$

which is the right-hand-side of (33), we must have equality throughout (34). It follows that

$$s_p\left(\sum_{i=1}^{2n} b_0^i a_0^i\right) + s_p\left(\left[\sum_{i=1}^{2n} b_1^i a_0^i\right] + a_1^1\right) = \left[\sum_{i=1}^{2n} b_0^i a_0^i\right] + \left[\sum_{i=1}^{2n} b_1^i a_0^i\right] + a_1^1,$$

and hence, by Lemma 21 (iii), we see that

$$\left[\sum_{i=1}^{2n} b_0^i a_0^i\right] \leq p - 1 \quad \text{and} \quad \left[\sum_{i=1}^{2n} b_1^i a_0^i\right] + a_1^1 \leq p - 1. \tag{35}$$

Recalling that $2n = \sum_{i=1}^{2n} ic_i$, we see from (35) that

$$\begin{aligned} 2n &= a_1^1 p + \sum_{i=1}^{2n} (b_0^i + b_1^i p) a_0^i \\ &= \sum_{i=1}^{2n} b_0^i a_0^i + p \left[\left(\sum_{i=1}^{2n} b_1^i a_0^i \right) + a_1^1 \right] \\ &\leq (p-1) + p(p-1) \\ &= p^2 - 1. \end{aligned}$$

In conclusion, the supposition above that $\omega_p \left(\frac{(2n)!}{\prod_{i=1}^{2n} i!^{c_i} c_i!} \right) = 0$ led us to the statement that $2n \leq p^2 - 1$. But the theorem assumed $n > n_0$, and hence $2n > p^2 - 1$. This contradiction completes the proof of Theorem 20. □

The theorem, along with Lemma 19 and (27), proves Theorem 1 (iii).

5.3 Closing remarks

The inspiration for the proof above was supplied by Figure 2, from which the statement of Theorem 20 in the case $p = 7$ seems obvious. It is now interesting and natural to ask why the results for $p = 5$ and $p = 4k + 3$ are so different. Surely the difference should be reflected somewhere in the proofs of the respective statements. The most important difference is that $u(2)_5 = u\left(\frac{5-1}{2}\right)_5 = 1$, whereas $u\left(\frac{p-1}{2}\right)_p = 0$ for $p = 4k = 3$. Consequently, there exist partitions in $\mathcal{P}^3_{2n,2k}$ that index non-vanishing summands in (11), and indeed those partitions with the largest possible number of 5's are the important ones. On the other hand, when $p = 4k+3$, partitions in $\mathcal{P}'_{2n,2k}$ with parts equal to p do not contribute to the sum in (11) at all. It seems plausible, then, that a statement similar to Theorem 17 that is general for powers p^α of primes $p = 4k + 3$ would exist and be useful in proving the experimentally evident conjecture from [9] that $d(n)$ eventually vanishes mod p^α.

Acknowledgments

The author would like to thank Dan Romik for suggesting the topic of this paper and for many helpful discussions. This material is based upon work supported by the National Science Foundation under Grant No. DMS-1800725.

References

[1] G.E.. Andrews. The Theory of Partitions. Addison-Wesley Publishing Company, 1976.

[2] T. Apostol. Modular Functions and Dirichlet Series in Number Theory (Second Ed.). Springer-Verlag, 1990.

[3] R. Bellman. A Brief Introduction to Theta Functions. Holt, Rinehart and Winston, Inc., 1961.

[4] D. S. Dummit and R.M. Foote. Abstract Algebra (Third Ed.). John Wiley and Sons, Inc., 2004

[5] H. Finkelstein. Solving equations in groups: a survey of Frobenius' theorem. *Periodica Mathematica Hungarica* **9.3** (1978), 187-204

[6] H. Larson and G. Smith. Congruence properties of Taylor coefficients of modular forms. *Int. J. Number Theory* **10** (2014), 1501 - 1518.

[7] A. M. Legendre. Essai sur la théorie des nombres (Second Ed.). Courcier, Paris, 1808.

[8] B.C. Berndt and K. Ono. Ramanujans Unpublished Manuscript on the Partition and Tau Functions with Proofs and Commentary. In: The Andrews Festschrift, eds. D. Foata, GN. Han, Springer, 2001, pp. 39-110.

[9] D. Romik (2019). The Taylor coefficients of the Jacobi theta constant θ_3. *Ramanujan Journal* https://doi.org/10.1007/s11139-018-0109-5.

[10] D. Zagier. Elliptic Modular Forms and Their Applications. In: The 1-2-3 of Modular Forms, ed. K. Ranestad, Springer, 2008, pp. 1103.

[11] OEIS Foundation Inc. (2019), http://oeis.org/A317651.

Robert Scherer
Department of Mathematics
University of California, Davis
One Shields Ave.
Davis, CA 95616, USA
E-mail: `rscherer@math.ucdavis.edu`