3-3-2017

Integer Partitions and Why Counting Them is Hard

Jose A. Ortiz
Portland State University

Integer Partitions and Why Counting Them is Hard

by

Jose A. Ortiz

An Undergraduate Honors Thesis

submitted in partial fulfillment of

the requirements for the

degree of

Bachelor of Science

in

University Honors

and

Mathematics with Honors

Thesis Advisor

Derek Garton

Portland State University

2017

TABLE OF CONTENTS

Page

1 Preliminaries 1
1.1 Introduction 1
1.2 Generating Functions 2
1.3 Applications of Generating Functions to Partitions 10

2 Congruence Properties of Partition Functions 16
2.1 Previous Results 16
2.2 Congruence Properties of m-ary Partitions mod m 18

Bibliography 27

Chapter 1: Preliminaries

1.1 Introduction

Before we dive into a recent paper on the topic of congruence properties of integer partitions, we'll take some time to go over some mathematics we'll need in order to understand the arguments presented in a recent paper. We'll focus on learning about generating functions and their applications to integer partitions and we'll also touch upon some of their amusing combinatorial applications. Throughout this article, we'll assume the reader has some knowledge of advanced mathematics beyond introductory analysis, but the accessible nature of partition theory makes it so just about anyone with the desire can understand and keep up with the information as presented—at least that's the goal.

Generating functions can be thought of as a "clothesline from which to hang a sequence of numbers for display" [11]. Simply stated, a generating function is a power series whose coefficients are a sequence of numbers that we are interested in. But we can do much more than simply display them in a different form; suppose we have some infinite sequence of numbers and want to find a formula that generates it. It may be the case that the sequence can be generated by a closed form function such as Gauss' formula for the nth triangular number. But it could also be the case that there is no neat formula that can generate the sequence, or that such a

sequence is unknown. For these situations, generating functions can nonetheless be used to encode the sequence, or even to help discover a closed formula for its terms.

We can rely on generating functions as purely algebraic objects, with no consideration on whether or not the function converges; these are what we'll refer to as a formal power series. Other times, we'll rely on their analytic properties when the power series expansion of the generating function converges on the complex plane [2, 3]. Part of what makes generating functions so interesting to work with is that they work the same way either way; all we gain or lose are a handful of identities and methods. Regardless of which way you want to look at them, generating functions have many interesting uses but we'll begin by listing off some of their basic properties, then we'll dive into a few basic examples to gain some familiarity with them.

1.2 Generating Functions

Definition 1.1. A *generating function* for a sequence $A = \{a_0, a_1, a_2, ...\}$ is the formal power series $A(x) = \sum_{n=0}^{\infty} a_n x^n = a_0 + a_1 x + a_2 x^2 + \cdots$, whereby formal we mean that we don't require the series to converge.
We use the notation $[x^n]A(x)$ to denote the coefficient of the x^n term in the power series expansion of $A(x)$.

Definition 1.2. Let $A(x) := \sum_{n\geq 0} a_n x^n$ and $B(x) := \sum_{n\geq 0} b_n x^n$. Then:

i. Addition of generating functions is defined as:

$$A(x) + B(x) = \sum_{n\geq 0}(a_n + b_n)x^n$$

ii. Multiplication of generating functions is defined as:

$$A(x) \cdot B(x) = \sum_{n\geq 0}\left(\sum_{n\geq k\geq 0} a_k b_{n-k}x^n\right)$$

iii. We say $B(x)$ is the inverse of $A(x)$ if

$$A(x) \cdot B(x) = 1 + 0x + 0x^2 + \cdots = 1$$

Remark. Note that these properties combined with those of the usual addition and multiplication, make the set of formal power series into a ring. This allows us to define derivatives as formal identities [11].

Example 1.1. What sequence of coefficients does the generating function $\frac{x^{n+1}-1}{x-1}$ encode if $x \neq 1$?

Note that we can factor a term from the numerator and end up with an identity:

$$\frac{x^{n+1}-1}{x-1} = \frac{(x-1)(x^n + x^{n-1} + \cdots + 1)}{x-1} = x^n + x^{n-1} + \cdots + 1 = \sum_{i=0}^{n} x^i$$

Thus we say that the generating function for the sequence $\{\underbrace{1,1,\ldots,1}_{n+1 \text{ times}}, 0, 0, 0, ...\}$ is the polynomial $\frac{x^{n+1}-1}{x-1}$.

Furthermore, we can use polynomial long division to obtain a familiar identity:

$$\frac{1}{1-x} = 1 + x + x^2 + \cdots = \sum_{n=0}^{\infty} x^n$$

And if we substitute ax, we get

$$\frac{1}{1-ax} = 1 + ax + a^2x^2 + \cdots = \sum_{n=0}^{\infty} (ax)^n$$

In order to use generating functions to their full potential, we'll need to know how to find the nth coefficient in the power series expansion of a generating function. For long-winded calculations, using a computer algebra system such as SageMath or Mathematica is much more efficient. But for simple examples, all we'll need to know are these following properties and the occasional use of partial fraction decomposition.

Definition 1.3. If $A(x) = \sum_{n=0}^{\infty} a_n x^n$, $B(x) = \sum_{n=0}^{\infty} b_n x^n$, and $c \in \mathbb{Z}$ then:

i. Sum Rule:

$$[x^n](A(x) + B(x)) = [x^n]A(x) + [x^n]B(x)$$

ii. Product Rule:

$$[x^n](A(x) \cdot B(x)) = \sum_{k=0}^{n} \left([x^k]A(x) \cdot [x^{n-k}]B(x)\right)$$

iii. Power Rule:

$$[x^n]A(cx) = c^n[x^n]A(x)$$

iv. Reduction Rule:

$$[x^n]x^k A(x) = [x^{n-k}]A(x)$$

In addition to those basic definitions, the next two theorems are useful for generating functions that can be expressed as binomials. We'll include them here for the sake of convenience.

Theorem 1.1. *Binomial Theorem: Let $n, k \in \mathbb{Z}_{\geq 0}$, then*

$$[x^n](x+1)^k = \binom{k}{n} = \begin{cases} \frac{n!}{(k-n)!n!} & \text{if } n \leq k \\ 0 & \text{otherwise} \end{cases}$$

Theorem 1.2. *Extended Binomial Theorem: For $n, k \in \mathbb{Z}_{\geq 0}$, then*

$$[x^n](x+1)^{-k} = \binom{-k}{n} = (-1)^n \binom{k+n-1}{k-1} = (-1)^n \binom{k+n-1}{n}$$

Example 1.2. What is the 11th coefficient of
$(x^2 + x^4 + x^6)(1 + x + x^2 + \cdots)$?

If we factor $(x^2 + x^4 + x^6)$ and use the identity $\frac{1}{1-x} = 1 + x + x^2 + \cdots$, we

obtain:

$$\begin{aligned}[x^{11}]\left[x^2(1+x^2+x^4)\left(\frac{1}{1-x}\right)\right] =&[x^{11-2}]\left[(1+x^2+x^4)\frac{1}{1-x}\right]\\ =&[x^9]\frac{1}{1-x}+[x^9]\frac{x^2}{1-x}+[x^9]\frac{x^4}{1-x}\\ =&[x^9]\frac{1}{1-x}+[x^7]\frac{1}{1-x}+[x^5]\frac{1}{1-x}\\ =&3\end{aligned}$$

Theorems 1.1 and 1.2 lead us to a few more common identities which may be useful.

Example 1.3. Let $n, k \in \mathbb{Z}^{>0}$ and $a \in \mathbb{Z}$, then

i.
$$\left(\frac{1}{1-x}\right)^k = \sum_{n=0}^{\infty}\binom{n+k-1}{k-1}x^n$$

ii.
$$\left(\frac{1}{1-ax}\right)^k = \sum_{n=0}^{\infty}\binom{n+k-1}{k-1}a^n x^n$$

iii.
$$\left(\frac{1}{1+ax}\right)^k = \sum_{n=0}^{\infty}\binom{n+k-1}{k-1}(-1)^n a^n x^n$$

Proof. **(i)** We know that $\left(\frac{1}{1-x}\right)^k = (1+x+x^2+\cdots)^k$. Then each term of the form x^n is the product of k possible powers of x. That is, the coefficient of x^n represents the number of solutions to the equation $x_1 + x_2 + \cdots + x_k = n$ for $x_i \geq 0$. We can simply use the stars and bars technique to get $[x^n]\left(\frac{1}{1-x}\right)^k = \binom{n+k-1}{k-1}$.

(ii) The identity follows by substituting ax into **(i)**.

(iii) This identity follows by using the extended binomial theorem. □

Example 1.4. How many ways can you roll a twenty-sided die 3 times such that they sum to 42?

Here the question asks for the number of solutions to the equation $a_1+a_2+a_3 = 42$ such that $a_1, a_2, a_3 \in \{1, 2, 3, ..., 20\}$. But rather than dealing with the inclusion-exclusion principle from the start, we can simplify the problem by using generating functions first. What we're looking for is the coefficient for the term x^{42} in the power series expansion of $(x^1 + x^2 + x^3 + \cdots + x^{20})^3$. We can simplify this as:

$$\begin{aligned}
[x^{42}](x + x^2 + x^3 + \cdots + x^{20})^3 &= [x^{42}]x^3(1 + x + x^2 + \cdots + x^{19})^3 \\
&= [x^{39}]\left(\frac{1 - x^{20}}{1 - x}\right)^3 \\
&= [x^{39}](1 - x^{20})^3 \cdot (1 - x)^{-3}
\end{aligned}$$

Now here is where we'll have to use the inclusion-exclusion principle; in order to end up with a x^{39} term in the series expansion, we need to consider how many ways we can obtain x^{39} using multiples of $-x^{20}$ and $-x$. Luckily, the number of cases to consider has been minimized, so consider the case where we choose no multiples of $-x^{20}$, that means that we are forced to choose 39 multiples of $-x$ from the second term.

If we choose one multiple of $-x^{20}$, then we can only choose 19 multiples of $-x$ from the second term. Lastly, it doesn't make sense to choose two or more multiples of x^{20} since we'd end up with a term of degree greater than 39. So then

we get the solution

$$\begin{aligned}[x^{39}](1-x^{20})^3(1-x)^{-3} =& \binom{3}{0}\binom{-3}{39}(-1)^{39} + \binom{3}{1}\binom{-3}{19}(-1)^{19} \\ =& \binom{41}{39} + 3\binom{41}{19} \\ =& 733988011420\end{aligned}$$

Another useful application of generating functions in solving linear recurrence relations. The benefit of using generating functions to find closed-form solutions of linear recurrence relations is that the process stays the same regardless of how complicated the equations get; we'll begin by illustrating an example before stating the general process.

Example 1.5. Use generating functions to derive Gauss' formula for the nth triangular number.

As the legend goes, an eight-year-old Gauss was in his mathematics class when the instructor asked the class to add up all the integers from 1 to 100. Thinking this would occupy the class for quite some time, the instructor was baffled when Gauss quickly computed the answer—5050. Needless to say, his instructor didn't make further attempts to punish his students with similar busywork.

Although Gauss' derivation was much simpler and didn't use generating functions, it's still worthwhile to use different techniques to solve old problems since they can be insightful (or just plain entertaining).

We'll start by defining $T(x) = \sum_{n\geq 0} t_n x^n$ and noting that the nth triangular number is simply the sum of the integers between 1 and n. This gives us the

recurrence relation $t_n = t_{n-1} + n$ for $n \geq 1$ where t_0=0. Multiplying both sides of this relation by x^n, summing over n, and reducing gives:

$$\begin{aligned}
\sum_{n\geq 0} t_n x^n &= \sum_{n\geq 0} t_{n-1} x^n + \sum_{n\geq 0} n x^n \\
&= x \sum_{n\geq 0} t_n x^n + \sum_{n\geq 1} n x^n \\
T(x) &= xT(x) + x \sum_{n\geq 1} n x^{n-1} \\
\frac{T(x)}{x} &= T(x) + \frac{d}{dx} \sum_{n\geq 0} x^n \\
T(x)\left(\frac{1}{x} - 1\right) &= \frac{d}{dx} \frac{1}{1-x} \\
T(x) &= \frac{x}{(1-x)^3}
\end{aligned}$$

So then we use Example 3 to get:

$$[x^n]T(x) = [x^n]\frac{x}{(1-x)^3} = [x^{n-1}]\frac{1}{(1-x)^3} = \binom{n+1}{2} = \frac{n(n+1)}{2}$$

With the previous example in mind, we can now describe the general process of how to solve linear recurrence relations using generating functions.

1. Define a generating function, $A(x) = \sum_{n\geq 0} a_n x^n$ and multiply both sides of the recurrence relation by x^n.

2. Sum up both sides of the equation as power series summations.

3. Through power series manipulations, express both sides of the recurrence

relation in terms of $A(x)$ and solve for $A(x)$.

4. Use generating function identities and partial fraction decomposition (if needed) to find $[x^n]A(x)$, and simplify into a complete solution.

1.3 Applications of Generating Functions to Partitions

Definition 1.4. A partition of a positive integer n is a sequence of positive integers $\{n_1, n_2, ..., n_k\}$ such that $\sum_{i=1}^{k} n_i = n$ and the order is irrelevant. Each n_i is called a part of the partition $\{n_1, n_2, ..., n_k\}$.

Definition 1.5. The partition function $p(n)$ is the number of partitions of a positive integer n, where $p(-n) = 0$ and $p(0) = 1$.

Example 1.6. Here are a few partition numbers with their corresponding partitions.

$p(1) = 1: \quad 1 = 1$

$p(2) = 2: \quad 2 = 2, \quad 2 = 1 + 1$

$p(3) = 3: \quad 3 = 3, \quad 3 = 2 + 1, \quad 3 = 1 + 1 + 1$

$p(4) = 5: \quad 4 = 4, \quad 4 = 3 + 1, \quad 4 = 2 + 2, \quad 4 = 2 + 1 + 1, \quad 4 = 1 + 1 + 1 + 1$

$p(100) = 190569292:$ (I'm sure you get the idea...)

Suppose we wanted to figure out of the number of partitions consisting of odd and even parts such that each part is less than 9. Counting all of the possible partitions by hand would be far too inefficient (and tedious) for any mathematician, so instead we'll utilize generating functions to find them. Luckily, applying

generating functions to this problem is straightforward, as shown in the following example.

Example 1.7. What is the generating function for the number of partitions of a positive integer n where each partition consists of one odd part and one even part such that each part is less than 9?

We denote this kind of partition by $p(n \mid \text{ one odd and one even part} < 9)$. Note that these partitions naturally occur in the exponents of the product:

$$\begin{aligned}
&(x^1 + x^3 + x^5 + x^7)(x^2 + x^4 + x^6 + x^8) \\
&= x^{1+2} + x^{1+4} + x^{1+6} + x^{1+8} + x^{3+2} + x^{3+4} + x^{3+6} + x^{3+8} + \\
&\qquad x^{5+2} + x^{5+4} + x^{5+6} + x^{5+8} + x^{7+2} + x^{7+4} + x^{7+6} + x^{7+8} \\
&= x^3 + 2x^5 + 3x^7 + 4x^9 + 3x^{11} + 2x^{13} + x^{15}
\end{aligned}$$

Furthermore, if we treat these as generating functions as usual then we notice that the coefficient of x^n gives us the number of partitions of n in one odd and one even part with each less than 9. As another example, we can consider a set of positive integers $S = \{s_1, s_2, ..., s_k\}$. Then the generating function for partitions of n with distinct parts in S is given by:

$$\prod_{i=1}^{k}(1 + x^{s_i}) = \prod_{n \in S}(1 + x^n) = \sum_{n \geq 0} p(n \mid \text{ distinct parts in } S)x^n$$

Example 1.8. Suppose we wanted to allow parts of S to repeat; what is the generating function for partitions of a positive integer n with a finite number of

repeated parts?

Suppose for illustrative purposes that wanted to find the partitions of n with parts in $S = \{2, 3\}$ with up to three repeats allowed. We would use the reasoning from the previous example and expand the product

$$\begin{aligned}
&(1 + x^2 + x^{2+2} + x^{2+2+2})(1 + x^3 + x^{3+3} + x^{3+3+3}) \\
&= 1 + x^3 + x^{3+3} + x^{3+3+3} + x^2 + x^{2+3} + x^{2+3+3} + x^{2+3+3+3} \\
&\quad + x^{2+2} + x^{2+2+3} + x^{2+2+3+3} + x^{2+2+3+3+3} \\
&\quad + x^{2+2+2} + x^{2+2+2+3} + x^{2+2+2+3+3} + x^{2+2+2+3+3+3} \\
&= 1 + x^2 + x^3 + x^4 + x^5 + 2x^6 + x^7 + x^8 + 2x^9 + x^{10} + x^{11} + x^{12} + x^{13} + x^{15}
\end{aligned}$$

And once again, we can find each of the partitions of n in the exponents of x. With this observation in mind, we can now find that the generalized generating function for the partitions of n with parts in S such that each part is repeated up to k times is:

$$\begin{aligned}
\sum_{n \geq 0} p(n \mid \text{ parts in } S \text{ with up to } k \text{ repeats}) x^n &= \prod_{s \in S} (1 + x^s + x^{2s} + x^{3s} + \cdots + x^{ks}) \\
&= \prod_{s \in S} \frac{1 - x^{(k+1)s}}{1 - x^s}
\end{aligned}$$

Example 1.9. What if we wanted to have no restrictions on the number of times any given part of a set S could appear in any partition of a positive integer n? What would its generating function be?

Well, all we need to do is consider the infinite geometric series as opposed to

the finite geometric series and we get the following generating function:

$$\sum_{n\geq 0} p(n \mid \text{ parts in } S)x^n = \prod_{s\in S}(1 + x^s + x^{2s} + x^{3s} + \cdots)$$
$$= \prod_{s\in S} \frac{1}{1-x^s}$$

Although this method seems simplistic, it is rather powerful due to its ease of application to other sorts of partitions.

Definition 1.6. Given a fixed positive integer $m \geq 2$, an *m-ary partition* is a partition of a nonnegative integer n whose parts are nonnegative powers of m. We denote the *m-ary partition function* by $b_m(n)$.

Example 1.10. What is the generating function for the m-ary partition function?

If we stare at the page long enough, we quickly realize this is another case of the previous example; we're only considering parts that happen to be non-negative powers of a fixed integer m. So let $S = \{1, m, m^2, ...\}$, and we get:

$$\sum_{n\geq 0} b_m(n)x^n = \sum_{n\geq 0} p(n \mid \text{ parts in } S)x^n = \prod_{s\in S} \frac{1}{1-x^s} = \prod_{j\geq 0} \frac{1}{1-x^{m^j}}$$

Lastly, we'll end the section with a minor remark on the uniqueness of base-m representations of n. We're all familiar with base-10 representations of numbers, e.g. if $a \in \mathbb{R}$ and $b \in \mathbb{Z}_{\geq 0}$, then there exist $a_i, b_k \in \{0, 1, 2, ..., 9\}$ where $i \in \mathbb{Z}$,$k \in \mathbb{Z}_{\geq 0}$ such that

$$a = \cdots + \frac{a_{-2}}{10^2} + \frac{a_{-1}}{10^1} + a_0 + a_1 10^1 + a_2 10^2 + \cdots$$
$$b = b_0 + b_1 10^1 + b_2 10^2 + \cdots$$

For example, $325 = 5 \cdot 10^0 + 2 \cdot 10^1 + 3 \cdot 10^2$. Now consider the general case where m is any positive integer.

Note that for any given base-m representation of n, there can be at most $m - 1$ multiples of any non-negative power of m. With this in mind, we can use the previous techniques to come up with a generating function that shows us the number of base-m representations of n:

Example 1.11. Base-m representations of nonnegative integers n are unique for all positive integers m.

$$\begin{aligned}
&\sum_{n\geq 0} p(n \mid \text{ parts are powers of } m \text{ with up to } m-1 \text{ repeats}) x^n \\
&= \prod_{s\in S} \frac{1-x^{sm}}{1-x^s} \\
&= \prod_{j=0} \frac{1-x^{m^{j+1}}}{1-x^{m^j}} \\
&= \left(\frac{1}{1-x}\right)\left(\frac{\prod_{j=0} 1-x^{m^{j+1}}}{\prod_{j=1} 1-x^{m^j}}\right) \\
&= \left(\frac{1}{1-x}\right)\left(\frac{\prod_{j=0} 1-x^{m^{j+1}}}{\prod_{j=0} 1-x^{m^{j+1}}}\right) \\
&= \frac{1}{1-x}
\end{aligned}$$

We already know this generating function has 1 for every coefficient, meaning there's exactly one base-m representation of any positive integer.

Chapter 2: Congruence Properties of Partition Functions

2.1 Previous Results

Congruence properties of partition functions have been studied extensively since S. Ramanujan and G.H. Hardy studied the unrestricted partition function around 1919 [9]. Since this was before computers, large tables of values of $p(n)$ were used as references and P. MacMahon supplied the pair of mathematicians with one. Upon examining the table, Ramanujan noticed a couple of patterns, namely:

$$p(5n+4) \equiv 0 \pmod{5}$$

$$p(7n+5) \equiv 0 \pmod{7}$$

$$p(11n+6) \equiv 0 \pmod{11}$$

Soon after, Ramanujan was able to supply proofs of these conjectures. But oddly enough, there did not seem to be any proofs for a modulus of 2 or 3 (as it would later turn out, there are none). Ramanujan was a prolific mathematician and filled numerous notebooks with conjectures and musings. However, he had few proofs of his conjectures in those notebooks; leaving others to rediscover his findings after his death. Many of his conjectures are still without proof, so Ramanujan's notebooks continue to be a fruitful field of study.

More recently in 2012, Folsom, Kent, and Ono [6] were studying the ℓ-adic behavior of $p(n)$ and discovered that it displays fractal-like behavior, similar to the Mandelbrot set's behavior of self-similarity. This means that there exist infinitely many Ramanujan congruences with a prime modulus $\ell \geq 5$.

In 1969, R.F. Churchhouse [5] was investigating congruences of the binary partition function $b_2(n)$ and conjectured that for t odd and $k \geq 1$,
$b_2(2^{2k+2}t) \equiv b_2(2^{2k}t) \pmod{2^{3k+2}}$ and $b_2(2^{2k+1}t) \equiv b_2(b^{2k-1}t) \pmod{2^{3k}}$.
This conjecture was soon after proven by Gupta [7] and similar congruences were proven for other cases such as $b_p(n)$ for p prime [10]. This was later extended for $b_m(n)$ for all $m > 1$ [1, 8]. And in 2012, Fraenkel [4] made the following conjectures related to the m-ary partition function b_m, for the case where $m = 3$.

- For all $n \geq 0$, $b_3(3n) \equiv 0 \pmod{3}$ if and only if at least one $a_i = 2$ in the base-3 representation of $n = a_0 + a_1 \cdot 3^1 + a_2 \cdot 3^2 + \cdots + a_j \cdot 3^j$ for any $0 \leq i \leq j$.

- If $a_i \neq 2$ for all $0 \leq i \leq j$ in the base-3 representation of n, we have that $b_3(3n) \equiv (-1)^j \pmod{3}$.

What was interesting about this result is that it provided a complete characterization of the ternary partition function for all multiples of 3. Characterizations of partitions are difficult to come by, so finding any pattern in their distribution is noteworthy. Which leaves us at the starting point for the main result that we're studying in this project.

2.2 Congruence Properties of m-ary Partitions mod m

In 2015, Andrews et al. [4] went one step further and discovered a complete characterization of the m-ary partition function mod m. This discovery is what we will now focus on understanding using the results from the preliminaries section. We'll begin by stating the result that was discovered, then we'll continue by proving several lemmas which will make the proof of Theorem 2.1 more obvious.

Theorem 2.1. *For any fixed integer $m \geq 2$, if $n = a_0 + a_1 m + a_2 m^2 + \cdots + a_j m^j$ is the base m representation of n, so that $0 \leq a_i \leq m-1$ for each $0 \leq i \leq j$, then for $0 \leq k \leq m-1$,*

$$b_m(mn) = b_m(mn+k) \equiv \prod_{i=0}^{j}(a_i+1) \pmod{m}.$$

Lemma 2.1. *If $|x| < 1$, then*

$$\frac{1-x^m}{(1-x)^2} \equiv \sum_{k=1}^{m} k x^{k-1} \pmod{m}$$

i.e., the coefficients of the sequence of integers generated by the function on the left are congruent mod m to the coefficients of the sum on the right.

Proof. Recall that if $|x| < 1$, the geometric series converges and we get the following identity:

$$\sum_{k=0}^{\infty} x^k = \frac{1}{1-x}.$$

If we take the derivative we get

$$\sum_{k=1}^{\infty} kx^{k-1} = \frac{1}{(1-x)^2}$$

Multiplying both sides of the equality by $1 - x^m$ gives:

$$\begin{aligned}\frac{1-x^m}{(1-x)^2} &= \sum_{k=1}^{\infty} kx^{k-1} - x^m \cdot \sum_{k=1}^{\infty} kx^{k-1} \\ &= \sum_{k=1}^{\infty} kx^{k-1} - \sum_{k=1}^{\infty} kx^{k-1+m}\end{aligned}$$

Note that we can alter the starting index of the second sum to get:

$$\begin{aligned}\sum_{k=1}^{\infty} kx^{k-1} - \sum_{k=1}^{\infty} kx^{k-1+m} &= \sum_{k=1}^{\infty} kx^{k-1} - \sum_{k=m+1}^{\infty} (k-m)x^{k-1} \\ &= \left(\sum_{k=1}^{m} kx^{k-1} + \sum_{k=m+1}^{\infty} kx^{k-1}\right) - \sum_{k=m+1}^{\infty} kx^{k-1} + \sum_{k=m+1}^{\infty} mx^{k-1} \\ &= \sum_{k=1}^{m} kx^{k-1} + \sum_{k=m+1}^{\infty} mx^{k-1} \\ &\equiv \sum_{k=1}^{m} kx^{k-1} \pmod{m}\end{aligned}$$

□

Before continuing, we'll need an elementary property of roots of unity which allows us to use them as a sort of 'filter' in sums.

Fact 1. If $\zeta = e^{2\pi i/m}$, then

$$\frac{1}{m}\sum_{r=0}^{m-1}\zeta^r = \begin{cases} m & \text{if } m|r \\ 0 & \text{otherwise.} \end{cases}$$

Lemma 2.2. *If $\zeta = e^{2\pi i/m}$ is an mth root of unity and $q \in \mathbb{C}$ such that $|q| < 1$, then*

$$\sum_{r=0}^{m-1}\frac{1}{1-\zeta^k q} = m\left(\frac{1}{1-q^m}\right).$$

Proof. Recall that $\sum_{r=0}^{\infty} q^r$ converges absolutely for $|q| < 1$ so that

$$\frac{1}{1-q} = \sum_{r=0}^{\infty} q^r$$

Furthermore, note that $|q\zeta^k| = |qe^{(2\pi i/m)k}| \leq |q| < 1$ for $k \in \mathbb{Z}$.

So $\sum_{r=0}^{\infty}(q\zeta^k)^r$ also converges absolutely and

$$\sum_{r=0}^{\infty}(q\zeta^k)^r = \frac{1}{1-q\zeta^k}$$

Since the series are both absolutely convergent, we can freely alter the order of summation to obtain the following:

$$\begin{aligned}\frac{1}{1-q}+\frac{1}{1-\zeta q}+\cdots+\frac{1}{1-\zeta^{m-1}q} &= \sum_{r=0}^{\infty} q^r + \sum_{r=0}^{\infty}(\zeta q)^r + \cdots + \sum_{r=0}^{\infty}(\zeta^{m-1}q)^r \\ &= \sum_{k=0}^{m-1}\sum_{r=0}^{\infty}(\zeta^k q)^r \\ &= \sum_{k=0}^{m-1}\left(\sum_{m|r}(\zeta^k q)^r + \sum_{m\nmid r}(\zeta^k q)^r\right)\end{aligned}$$

Note that if $m|r$, then $r = mj$ for some $j \in \mathbb{Z}$.

$$\begin{aligned}\sum_{k=0}^{m-1}\left(\sum_{m|r}(\zeta^k q)^r + \sum_{m\nmid r}(\zeta^k q)^r\right) &= \sum_{k=0}^{m-1}\left(\sum_{j=0}^{\infty}(\zeta^k q)^{jm} + \sum_{m\nmid r}(\zeta^k q)^r\right) \\ &= \sum_{k=0}^{m-1}\sum_{j=0}^{\infty}\zeta^{jmk}q^{jm} + \sum_{k=0}^{m-1}\sum_{m\nmid r}(\zeta^k q)^r \\ &= \sum_{k=0}^{m-1}\sum_{j=0}^{\infty}q^{jm} + \sum_{m\nmid r}\sum_{k=0}^{m-1}(\zeta^k q)^r \\ &= \sum_{k=0}^{m-1}\sum_{j=0}^{\infty}q^{jm} + \sum_{m\nmid r}q^r(1+\zeta^r+\cdots+\zeta^{(m-1)r})\end{aligned}$$

Using the identity from Example 1.1 and the fact that ζ is an mth root of unity, we get

$$\left(1+\zeta^r+\cdots+\zeta^{(m-1)r}\right) = \frac{1-\zeta^{mr}}{1-\zeta} = \frac{1-1}{1-\zeta} = 0$$

Thus,

$$\sum_{k=0}^{m-1}\sum_{j=0}^{\infty} q^{jm} + \sum_{m\nmid r} q^r(1+\zeta^r+\cdots+\zeta^{(m-1)r}) = \sum_{k=0}^{m-1}\frac{1}{1-q^m} = m\left(\frac{1}{1-q^m}\right)$$

□

Recall that the generating function for $b_m(n)$ is given by

$$B_m(q) = \prod_{j=0}^{\infty}\frac{1}{1-q^{m^j}} = \sum_{n=0}^{\infty} b_m(n)q^n.$$

This function also satisfies the property that $(1-q)B_m(q) = B_m(q^m)$. Furthermore, Gupta [8] also showed that for $1 \leq i \leq m-1$, $b_m(mn) = b_m(mn+i)$ and we'll use this seemingly minor fact for great effect.

For Lemma 2.3, we'll need to use a type of "linear operator" U_m which for our purposes is a function defined on all functions of the form $f(q) = \sum_{n=-\infty}^{\infty} a_n q^n$ and where $U_m(f(q)) := \sum_{n=-\infty}^{\infty} a_{mn} q^n$ for $q \in \mathbb{C}$. However we'll avoid a deep discussion on properties of linear operators as it requires a significant amount of discourse on topics related to modular forms and complex analysis. All we'll need to use is an elementary property from Andrews [2].

Fact 2. If $\zeta = e^{2\pi i/m}$ and $f(q) = \sum_{n=-\infty}^{\infty} a_n q^n$ for $q \in \mathbb{C}$, then there exists a linear operator U_m such that

$$U_m(f(q)) = \frac{1}{m}\left(f(q^{1/m}) + f(\zeta q^{1/m}) + \cdots + f(\zeta^{m-1}q^{1/m})\right).$$

Lemma 2.3. *Define* $T_m(q) := U_m\left(B_m(q)\right) = \sum_{n\geq 0} b_m(mn)q^n$ *where* $U_m(q)$ *is a linear operator acting on the generating function* $B_m(q) = \sum_{n=0}^{\infty} b_m(n)q^n$ *where* $b_m(n)$ *is the* m*-ary partition function and* $q \in \mathbb{C}$ *where* $|q| < 1$, $q = q_0^m$, *then*

$$T_m(q) = \frac{1}{1-q}B_m(q).$$

Proof. Let $\zeta = e^{2\pi i/m}$ and we'll begin by utilizing the previous fact to get:

$$\begin{aligned}
T_m(q_0^m) &= \sum_{n=0}^{\infty} b_m(mn)q_0^{mn} \\
&= \frac{1}{m}\left[B_m(q_0) + B_m(\zeta q_0) + \cdots + B_m(\zeta^{m-1}q_0)\right] \text{ by Fact 2} \\
&= \frac{1}{m}\left[\prod_{j=0}^{\infty}\frac{1}{1-q_0^{mj}} + \prod_{j=0}^{\infty}\frac{1}{1-(\zeta q_0)^{mj}} + \cdots + \prod_{j=0}^{\infty}\frac{1}{1-(\zeta^{m-1}q_0)^{mj}}\right] \\
&= \frac{1}{m}\left[\left(\frac{1}{1-q_0}\right)\prod_{j=1}^{\infty}\frac{1}{1-q_0^{mj}} + \left(\frac{1}{1-\zeta q_0}\right)\prod_{j=1}^{\infty}\frac{1}{1-(\zeta q_0)^{mj}} + \cdots\right. \\
&\qquad \left. \cdots + \left(\frac{1}{1-\zeta^{m-1}q_0}\right)\prod_{j=1}^{\infty}\frac{1}{1-(\zeta^{m-1}q_0)^{mj}}\right] \\
&= \frac{1}{m}\left(\sum_{k=0}^{m-1}\frac{1}{1-\zeta^k q_0}\right)\cdot\prod_{j=1}^{\infty}\frac{1}{1-q_0^{mj}} \text{ since } (\zeta^k)^{m^j} = 1 \text{ for all } k \in \mathbb{Z}, j \in \mathbb{Z}_{>0} \\
&= \frac{1}{m}\left(m\cdot\frac{1}{1-q_0^m}\right)\cdot\prod_{j=1}^{\infty}\frac{1}{1-q_0^{mj}} \text{ by Lemma 2.2}
\end{aligned}$$

So then

$$T_m(q) = \left(\frac{1}{1-q}\right)\prod_{j=1}^{\infty}\frac{1}{1-q^j} = \frac{1}{1-q}B_m(q)$$

□

Next, we'll prove one last lemma which combines the previous results and will lead us to a surprisingly straightforward proof.

Lemma 2.4. *If* $S_m(q) := \prod_{j=0}^{\infty}\left(1+2q^{m^j}+3q^{2m^j}+\cdots+mq^{(m-1)m^j}\right)$ *is a generating function such that* $|q|<1$, *then* $T_m(q) \equiv S_m(q) \pmod m$ *i.e., the coefficients in* $T_m(q)$ *are congruent to the coefficients in* $S_m(q)$ *mod* m.

Proof. It suffices to show that $\frac{1}{T_m(q)} \cdot S_m(q) \equiv 1 \pmod m$, so we'll proceed by this route. By the previous lemma, we get:

$$\begin{aligned}
\frac{1}{T_m(q)} \cdot S_m(q) =& \frac{1-q}{B_m(q)} \cdot S_m(q) \\
=&(1-q)\cdot\prod_{j=0}^{\infty}\left(1-q^{m^j}\right)\cdot\prod_{j=0}^{\infty}\left(1+2q^{m^j}+3q^{2m^j}+\cdots+mq^{(m-1)m^j}\right) \\
=&(1-q)^2\cdot\prod_{j=1}^{\infty}\left(1-q^{m^j}\right)\cdot\prod_{j=0}^{\infty}\left(\sum_{k=1}^{m}k(q^{m^j})^{k-1}\right) \\
\equiv&(1-q)^2\cdot\prod_{j=1}^{\infty}\left(1-q^{m^j}\right)\cdot\prod_{j=0}^{\infty}\frac{1-q^{m^{j+1}}}{(1-q^{m^j})^2} \pmod m \text{ By Lemma 2.1} \\
\equiv&(1-q)^2\cdot\prod_{j=1}^{\infty}\left(1-q^{m^j}\right)\cdot\left[\frac{1-q^m}{(1-q)^2}\cdot\prod_{j=1}^{\infty}\frac{1-q^{m^{j+1}}}{(1-q^{m^j})^2}\right] \pmod m \\
\equiv&\prod_{j=1}^{\infty}\left(1-q^{m^j}\right)\cdot\left[(1-q^m)\cdot\frac{\prod_{j=1}^{\infty}1-q^{m^{j+1}}}{\prod_{j=1}^{\infty}(1-q^{m^j})^2}\right] \pmod m \\
\equiv&\frac{\prod_{j=0}^{\infty}\left(1-q^{m^{j+1}}\right)}{\prod_{j=1}^{\infty}\left(1-q^{m^j}\right)} \pmod m \\
\equiv&\frac{\prod_{j=1}^{\infty}\left(1-q^{m^j}\right)}{\prod_{j=1}^{\infty}\left(1-q^{m^j}\right)} \pmod m \\
\equiv&1 \pmod m
\end{aligned}$$

□

Now we have all of the tools we need to prove Theorem 2.1. Luckily, most of the work has already been done; all we need to do is put the pieces together.

Proof. Fix an integer $m \geq 2$ and suppose $n = a_0 + a_1 m + a_2 m^2 + \cdots + a_j m^j$ is the base-m representation of n. Using the previous lemma we get:

$$\sum_{n \geq 0} b_m(mn) q^n = T_m(q) \equiv S_m(q) \pmod{m}$$

If we expand the product

$$\begin{aligned} S_m(q) &\equiv \prod_{k=0}^{\infty} \left(1 + 2q^{m^k} + 3q^{2m^k} + \cdots + mq^{(m-1)m^k}\right) \\ &\equiv \prod_{k=0}^{\infty} \sum_{k'=0}^{m-1} (k'+1)(q^{m^k})^{k'} \end{aligned}$$

we obtain a power series of the form

$$c_0 + c_1 q + c_2 q^2 + \cdots + c_m q^m + \cdots + c_n q^n + \cdots \pmod{m}$$

But recall by Example 1.11 that the base-m expansion of n is unique and $q^n = q^{a_0 + a_1 m + a_2 m^2 + \cdots + a_j m^j}$ will only appear once in this power series in its base-m representation. Furthermore, for each value of k, $q^{a_k m^k}$ will also only appear once.

That is, $\left[q^{a_k m^k}\right] S_m(q) \equiv a_k + 1 \pmod{m}$ for each $0 \leq k \leq j$.

If we recall the simple fact that $q^n = q^{a_0} \cdot q^{a_1 m} \cdot q^{a_2 m^2} \cdots q^{a_j m^j}$, then all we need to

do is multiply the coefficients to get:

$$[q^n]\, S_m(q) \equiv \prod_{i=0}^{j}(a_i + 1) \pmod{m}$$

Then if we use Gupta's fact that $b_m(mn) = b_m(mn + i)$ for $1 \leq i \leq m - 1$, we get the final result:

$$b_m(mn) \equiv b_m(mn + i) \equiv \prod_{i=0}^{j}(a_i + 1) \pmod{m}$$

for all $0 \leq i \leq m - 1$. □

This result shows us some interesting patterns in the distribution of $b_m(n)$, namely that if any of the coefficients in the base-m expansion of n is $m - 1$, then $b_m(mn) \equiv b_m(mn + i) \equiv 0 \pmod{m}$ for $0 \leq i \leq m - 1$.

Bibliography

[1] George E. Andrews. Congruence properties of the m-ary partition function. *J. Number Theory*, 3:104–110, 1971.

[2] George E. Andrews. *The theory of partitions*. Cambridge Mathematical Library. Cambridge University Press, Cambridge, 1998. Reprint of the 1976 original.

[3] George E. Andrews and Kimmo Eriksson. *Integer partitions*. Cambridge University Press, Cambridge, 2004.

[4] George E. Andrews, Aviezri S. Fraenkel, and James A. Sellers. Characterizing the number of m-ary partitions modulo m. *Amer. Math. Monthly*, 122(9):880–885, 2015.

[5] R. F. Churchhouse. Congruence properties of the binary partition function. *Proc. Cambridge Philos. Soc.*, 66:371–376, 1969.

[6] Amanda Folsom, Zachary A. Kent, and Ken and Ono. ℓ-adic properties of the partition function. *Adv. Math.*, 229(3):1586–1609, 2012. Appendix A by Nick Ramsey.

[7] Hansraj Gupta. Proof of the Churchhouse conjecture concerning binary partitions. *Proc. Cambridge Philos. Soc.*, 70:53–56, 1971.

[8] Hansraj Gupta. On m-ary partitions. *Mathematical Proceedings of the Cambridge Philosophical Society*, 71(2):343–345, 003 1972.

[9] S. Ramanujan. Some properties of $p(n)$, the number of partitions of n [Proc. Cambridge Philos. Soc. **19** (1919), 207–210]. In *Collected papers of Srinivasa Ramanujan*, pages 210–213. AMS Chelsea Publ., Providence, RI, 2000.

[10] Öystein Rödseth. Some arithmetical properties of m-ary partitions. *Proc. Cambridge Philos. Soc.*, 68:447–453, 1970.

[11] Herbert S. Wilf. *generatingfunctionology*. A K Peters, Ltd., Wellesley, MA, third edition, 2006.