A GENERALIZATION OF CONGRUENCE PROPERTIES FOR A RESTRICTED PARTITION FUNCTION

Brandt Kronholm
Dept. of Mathematics, University of Texas Rio Grande Valley, Edinburg, Texas
brandt.kronholm@utrgv.edu

Jonathan Rehmert
Department of Mathematics, Kansas State University, Manhattan, Kansas
rehmert@math.ksu.edu

Received: 1/10/17, Revised: 10/11/17, Accepted: 3/14/18, Published: 3/20/18

Abstract

A 1989 result of Y. H. H. Kwong established periodicity of the sequence of values of the restricted partition function $p(n, m)$ modulo any natural number where $p(n, m)$ enumerates partitions of n into at most m parts. In this paper we re-visit this result and establish several new and general theorems on infinite families of partition congruences.

1. Introduction

A partition of an integer n is a finite sequence of non-increasing natural numbers $\lambda_1, \lambda_2, ..., \lambda_k$ such that $\lambda_1 + \lambda_2 + ... + \lambda_k = n$. Each λ_i is called a part of the partition. The general partition function is denoted by $p(n)$. In 1919, Ramanujan [12] observed and proved several congruence properties for the general partition function. The most most basic of these are

$$p(5n + 4) \equiv 0 \pmod 5, \quad p(7n + 5) \equiv 0 \pmod 7$$

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

In 2000 Ono [11] proved that for any prime $\ell \geq 5$, there exist infinitely many partition congruences with the form $p(An + B) \equiv 0 \pmod{\ell}$. With the assistance of Rhiannon Weaver [3], an undergraduate student at the time, they were able top compute many examples of Ono's results. Here is one example:

$$p(4063467631n + 30064597) \equiv 0 \pmod{31}.$$

Ono's partition divisibility results were extended by Ahlgren [1] to any prime power ℓ^a later in that year. Recent work of Yifan Yang [13] continues in this vein.

The restricted partition function, $p(n, m)$, defined as the number of partitions of n into at most m parts, was studied by Euler as an auxiliary partition function in his investigation into the general partition function. It was also a focus of J. J. Sylvester's work on invariant theory in the 19th century [4].

For $m \geq n$, we have the relation $p(n, m) = p(n)$. If n is negative, we define $p(n, m) = 0$, and $p(0, m) = 1$. Kronholm [5, 6, 7] and Larsen [8] have proven Ramanujan-style divisibility properties similar to those proved by Ono and Ahlgren for this restricted partition function. Here are several specific examples of congruences for $p(n, m)$.

Example 1. For $k \geq 0$ one has

$$p(54k - 3, 3) \equiv 0 \pmod{27} \tag{1}$$

$$p(60k - 5, 5) \equiv p(60k - 10, 5) \equiv 0 \pmod{5}. \tag{2}$$

and

$$p(2940k - 7, 7) \equiv 0 \pmod{49}. \tag{3}$$

In order to state such results in their full generality in Theorem 1 we require the following definition.

Definition 1 ([6]). For any natural number a, we denote by $lcm(a)$ the least common multiple of the natural numbers from 1 to a.

Theorem 1 ([7]). *For ℓ an odd prime, $k \geq 0$, $1 \leq j \leq \frac{\ell - 1}{2}$, and $\alpha \geq 1$,*

$$p(\mathrm{lcm}(\ell)\ell^{\alpha-1}k - j\ell, \ell) \equiv 0 \pmod{\ell^{\alpha}}.$$

We note that the congruence results of Theorem 1 are dependent on a prime number of parts ℓ and confined to some power of that same prime. The main goal of this paper is to establish results similar to Theorem 1 without any restrictions on the number of parts or the modulus. In order to do this we will make use of Theorem 2 and Theorem 3 which describe the periodicity of sequences of integer partitions of the form $\{p(n, m) \pmod{j}\}_{n \geq 0}$. Indeed, such periodicity results can be recast as divisibility patterns. However, we obtain several infinite families of partition congruences of the form $p(Ak + B, m) \equiv 0 \pmod{j}$ that, while dependent on established periodicity results, they are by no means immediate and overt. Moreover, the results of this paper are different than those displayed in Example 1 and Theorem 1 in that there are no restrictions on the number of parts m or the modulus j.

2. Background

It is well known that the generating function for $p(n, m)$ is given by

$$\sum_{n=0}^{\infty} p(n, m) q^n = \frac{1}{(1 - q)(1 - q^2) \ldots (1 - q^m)}. \tag{4}$$

Definition 2. A sequence $\{a_n\}_{n\geq 0}$ is *purely periodic* modulo a positive integer M if there exists a positive integer μ such that $a_{n+\mu} \equiv a_n \pmod{M}$ for $n \geq 0$. The smallest such μ is called the minimum period.

Nijenhuis and Wilf [10] described the periodicity of $p(n,m)$ modulo a prime. In 1989, Kwong [9] extended these results by proving that for fixed m, the restricted partition function is purely periodic modulo a power of a prime.

Theorem 2 (Kwong). *[9] Let ℓ, m, N and $b \geq 1$ be integers with ℓ prime and b the least integer such that $\ell^b \geq \sum_{\delta\geq 0} \phi(\ell^\delta)\left\lfloor \frac{m}{\ell^\delta}\right\rfloor$ where ϕ is Euler's totient function. Furthermore, let L be the ℓ-free part of $\operatorname{lcm}(m)$ as in Definition 1. Then $\{p(n,m) \pmod{\ell^N}\}_{n\geq 0}$ is purely periodic with minimum period $\ell^{N+b-1}L$.*

Kwong also proved a result that allows us to extend this to modulo any positive integer j.

Theorem 3 (Kwong). *[9] Let $\mu(M)$ be the minimum period of an infinite integer sequence modulo any positive integer $M > 1$. If $M = \ell_1^{e_1}\ell_2^{e_2}...\ell_s^{e_s}$ is the prime factorization of M, then $\mu(M) = \operatorname{lcm}(\mu(\ell_1^{e_1}), \mu(\ell_2^{e_2}), ..., \mu(\ell_s^{e_s}))$.*

Kwong's two theorems enable us to compute the minimum period of the restricted partition function modulo j given a fixed number of parts m. We denote this period as $\mu(m,j)$.

Remark 1. Statements of periodicity modulo j can be readily translated into infinite families of divisibility properties in the following way: For $0 \leq s < \mu(m,j)$ and integers t and k, whenever $p(s,m) \equiv t \pmod{j}$, then, for all $k \geq 0$, one has $p(\mu(m,j)k + s, m) \equiv t \pmod{j}$.

Some of the tools we will use in establishing our results are reciprocal polynomials and anti-reciprocal polynomials which we now define.

Definition 3. [2] A polynomial $P(q) = a_0 + a_1q + ... + a_dq^d$ is called *reciprocal* if for each $i, a_i = a_{d-i}$; equivalently, $q^dP\left(\frac{1}{q}\right) = P(q)$.

Definition 4. [5] A polynomial $P(q) = a_0 + a_1q + ... + a_dq^d$ is called *anti-reciprocal* if for each $i, a_i = -a_{d-i}$; equivalently, $q^dP\left(\frac{1}{q}\right) = -P(q)$.

The remainder of this paper investigates the instances of s, with $0 \leq s < \mu(m,j)$, for which $p(s,m) \equiv 0 \pmod{j}$ and thereby establishing several new infinite families of partition congruences overlooked by the periodicity results of Kwong. It is important to note that the minimum period $\mu(m,j)$ is describing "pure periodicity" whereas $\operatorname{lcm}(m)$, as it is used in Theorem 1, is describing a different and shorter *sub*-period.

3. Results

3.1. Congruences in an Arithmetic Progression for a Fixed Number of Parts

Theorem 4. *Modulo j, $\sum_{n=0}^{\infty}[p(n,m)-p(n-\mu(m,j),m)]q^n$ is a polynomial of degree $\mu(m,j)-\binom{m+1}{2}$. If m is even, it is an anti-reciprocal polynomial; if m is odd, it is a reciprocal polynomial.*

Proof. From Equation (4) we have

$$\sum_{n=0}^{\infty}[p(n,m)-p(n-\mu(m,j),m)]q^n = \frac{1-q^{\mu(m,j)}}{(1-q)(1-q^2)...(1-q^m)}. \tag{5}$$

Theorem 2 guarantees that modulo j, (5) is a polynomial.

We will use definitions 3 and 4 to show that modulo j, the right-hand side of (5) is either a reciproccal or antireciprocal polynomial of degree $d=\mu(m,j)-\binom{m+1}{2}$. We begin by setting

$$P(q) \equiv \frac{1-q^{\mu(m,j)}}{(1-q)(1-q^2)...(1-q^m)} \pmod{j}$$

for $P(q)$ the polynomial in question of degree $d=\mu(m,j)-\binom{m+1}{2}$.

$$q^dP\left(\frac{1}{q}\right) \equiv \frac{q^{\mu(m,j)-\binom{m+1}{2}}\left(1-q^{-\mu(m,j)}\right)}{\left(1-\frac{1}{q}\right)\left(1-\frac{1}{q^2}\right)...\left(1-\frac{1}{q^m}\right)} \equiv \frac{q^{\mu(m,j)}-1}{q^{\binom{m+1}{2}}\left(\frac{q-1}{q}\right)\left(\frac{q^2-1}{q^2}\right)...\left(\frac{q^m-1}{q^m}\right)}$$

$$\equiv \frac{q^{\mu(m,j)}-1}{(q-1)(q^2-1)...(q^m-1)} \equiv (-1)^{m+1}\frac{1-q^{\mu(m,j)}}{(1-q)(1-q^2)...(1-q^m)} \equiv \pm P(q) \pmod{j}.$$

The sign on the final equivalence depends on m even or odd. $\square$

Corollary 1. *For $\mu(m,j)-\binom{m+1}{2} < s < \mu(m,j)$ one has $p(\mu(m,j)k+s,m) \equiv 0 \pmod{j}$.*

Proof. Observe that

$$P(q) \equiv p(0,m)+p(1,m)q+...+p(\mu(m,j)-1,m)q^{\mu(m,j)-1} \pmod{j}. \tag{4}$$

Since it is an (anti)reciprocal polynomial of degree $\mu(m,j)-\binom{m+1}{2}$ we can rewrite (4) as

$$P(q) \equiv p(0,m)+p(1,m)q+...+p\left(\mu(m,j)-\binom{m+1}{2},m\right)q^{\mu(m,j)-\binom{m+1}{2}} \pmod{j}.$$

Note that $\mu(m,j) - \binom{m+1}{2} < \mu(m,j) - 1$, so each coefficient on the terms q with exponents between $\mu(m,j) - \binom{m+1}{2}$ and $\mu(m,j) - 1$ must be $0 \pmod{j}$. Hence, we have

$$p\left(\mu(m,j)k - \binom{m+1}{2} + 1, m\right) \equiv p\left(\mu(m,j)k - \binom{m+1}{2} + 2, m\right) \equiv \ldots$$
$$\ldots \equiv p(\mu(m,j)k - 1, m) \equiv 0 \pmod{j},$$

which proves the corollary. □

Here are some examples to illustrate Corollary 1.

Example 2. For $m = 6$ and $j = 4$, $\mu(m,j) = \mu(6,4) = 480$ and $\binom{m+1}{2} = \binom{7}{2} = 21$; hence,

$$p(480k - 20, 6) \equiv p(480k - 19, 6) \equiv \ldots \equiv p(480k - 1, 6) \equiv 0 \pmod{4}.$$

For $m = 5$ and $j = 5$, $\mu(m,j) = \mu(5,5) = 300$ and $\binom{m+1}{2} = \binom{6}{2} = 15$; hence,

$$p(300k - 14, 5) \equiv p(300k - 13, 5) \equiv \ldots \equiv p(300k - 1, 5) \equiv 0 \pmod{5}.$$

For $m = 8$ and $j = 3$, $\mu(m,j) = \mu(8,3) = 7560$ and $\binom{m+1}{2} = \binom{9}{2} = 36$; hence,

$$p(7560k - 35, 8) \equiv p(7560k - 34, 8) \equiv \ldots \equiv p(7560k - 1, 8) \equiv 0 \pmod{3}.$$

Corollary 2. *For $k \geq 0$, $h \geq 0$, and $0 \leq s < \mu(m,j)$, if m is even one has*

$$p(\mu(m,j)k + s, m) \equiv -p\left(\mu(m,j)h + \mu(m,j) - \binom{m+1}{2} - s, m\right) \pmod{j}$$

and if m is odd one has

$$p(\mu(m,j)k + s, m) \equiv p\left(\mu(m,j)h + \mu(m,j) - \binom{m+1}{2} - s, m\right) \pmod{j}.$$

Proof. By Theorem 4, for m even, it follows that

$$p(s, m) \equiv -p\left(\mu(m,j) - \binom{m+1}{2} - s, m\right) \pmod{j}$$

when $0 \leq s \leq \mu(m,j) - \binom{m+1}{2}$. Note that $-p\left(\mu(m,j) - \binom{m+1}{2} - s, m\right) = 0$ when $s > \mu(m,j) - \binom{m+1}{2}$. By Corollary 1, for $\mu(m,j) - \binom{m+1}{2} < s < \mu(m,j)$ we have that $p(s,m) \equiv 0 \pmod{j}$. Thus, for $\mu(m,j) - \binom{m+1}{2} < s < \mu(m,j)$,

$$p(s, m) \equiv -p\left(\mu(m,j) - \binom{m+1}{2} - s, m\right) \pmod{j}.$$

This proves the case for m even by Remark 1. A similar argument holds for the case where m is odd. □

Using this corollary and taking Definition 4 into consideration, we can further prove interesting results.

Proposition 1. *If $m \equiv 0 \pmod 4$ and j is odd then*

$$p\left(\mu(m,j)k + \frac{\mu(m,j) - \binom{m+1}{2}}{2}, m\right) \equiv 0 \pmod j$$

and if j is even then

$$p\left(\mu(m,j)k + \frac{\mu(m,j) - \binom{m+1}{2}}{2}, m\right) \equiv 0 \pmod{j/2}. \tag{5}$$

Proof. Note that $\left(\mu(m,j) - \binom{m+1}{2}\right)/2$ is an integer when $m \equiv 0 \pmod 4$. By Corollary 2, we can say

$$\begin{aligned} p\left(\frac{\mu(m,j) - \binom{m+1}{2}}{2}, m\right) &\equiv -p\left(\mu(m,j) - \binom{m+1}{2} - \frac{\mu(m,j) - \binom{m+1}{2}}{2}, m\right) \\ &\equiv -p\left(\frac{\mu(m,j) - \binom{m+1}{2}}{2}, m\right) \pmod j \end{aligned}$$

and arrive at

$$2p\left(\frac{\mu(m,j) - \binom{m+1}{2}}{2}, m\right) \equiv 0 \pmod j.$$

If j is odd then the $gcd(2,j) = 1$, hence

$$p\left(\frac{\mu(m,j) - \binom{m+1}{2}}{2}, m\right) \equiv 0 \pmod j.$$

If j is even then the $gcd(2,j) = 2$, and hence

$$p\left(\frac{\mu(m,j) - \binom{m+1}{2}}{2}, m\right) \equiv 0 \pmod{j/2}.$$

Thus the proposition follows. □

Here are some examples of Proposition 3.4

Example 3. For $k \geq 0$ one has $p(60k+25,4) \equiv 0 \pmod 5$, $p(7560k+3762,8) \equiv 0 \pmod 3$ and $p(48k+19,4) \equiv 0 \pmod 2$.

3.2. Congruences in an Arithmetic Progession for a Small Family of Number of Parts

The following theorem deals with variability across the second variable, m, rather than the first one. It is a similar to a theorem proved by Kronholm [6].

Theorem 5. *For $k \geq 0$ and $2 \leq t \leq m$ and $1 \leq c < \binom{t+1}{2}$*

$$p(\mu(m,j)k - c, t) \equiv 0 \pmod{j}.$$

We require the following lemma.

Lemma 1. *For $1 \leq t \leq m$ and x is a natural number, we have that $\mu(m,j) = x\mu(t,j)$.*

Proof. The cases $t = 1$ and $t = m$ are trivial. When $t = 1$ then $\mu(1,j) = 1$ so $x = \mu(m,j)$. When $t = m$ then $\mu(t,j) = \mu(m,j)$ so $x = 1$.

We consider $2 \leq t < m$. Let $j = p_1^{e_1} p_2^{e_2} ... p_s^{e_s}$ be the prime factorization of j as in Theorem 3 so that for t, m and j we have

$$\mu(t,j) = lcm\{\mu(t,p_1^{e_1}), \mu(t,p_2^{e_2}), ..., \mu(t,p_s^{e_s})\} \tag{6}$$

and

$$\mu(m,j) = lcm\{\mu(m,p_1^{e_1}), \mu(m,p_2^{e_2}), ..., \mu(m,p_s^{e_s})\}. \tag{7}$$

From Theorem 2, we have for any natural number a,

$$\mu(a,p_i^{e_i}) = p_i^{e_i+b_{a,i}-1} L_{a,p_i} \tag{8}$$

where $b_{a,i}$ is the least integer such that $p_i^{b_{a,i}} \geq \sum_{\delta \geq 0} \phi(p_i^\delta) \left\lfloor \frac{a}{p_i^\delta} \right\rfloor$ and L_{a,p_i} is the p_i-free part of $lcm(a)$.

With $2 \leq t < m$ and Definition 1, it is clear that $lcm(t) \big| lcm(m)$. Moreover, from the definition of L from Theorem 3 and (8) that for every $p_i \big| j$, if p_i^g is the largest power of p_i dividing $lcm(m)$, then $lcm(t)$ cannot have a larger power of p_i dividing it. It then follows that for every $p_i \big| j$,

$$L_{t,p_i} \big| L_{m,p_i}. \tag{9}$$

Furthermore, with $2 \leq t < m$ and the definition of b from Theorem 3 and (8) it is clear that $b_{t,i} \leq b_{m,i}$. Hence for every $p_i \big| j$,

$$p_i^{b_{t,i}} \big| p_i^{b_{m,i}}. \tag{10}$$

Now, lines (9) and (10) together with (6) and (7) imply that $\mu(t,j) \big| \mu(m,j)$. Thus, $\mu(m,j) = x\mu(t,j)$ for some natural number x. $\square$

We now prove Theorem 5.

Proof. By Lemma 1, for $2 \leq t \leq m$, there exists an integer x such that $\mu(m,j) = x\mu(t,j)$. Also, by Corollary 2, for $1 \leq c < \binom{t+1}{2}$

$$p(\mu(t,j)k - c, t) \equiv 0 \pmod{j}.$$

By Remarks 1 we can say that $p((x-1)\mu(t,j)k + \mu(t,j)k - c, t) \equiv 0 \pmod{j}$, $p(x\mu(t,j)k - c, t) \equiv 0 \pmod{j}$, and $p(\mu(m,j)k - c, t) \equiv 0 \pmod{j}$. ☐

Example 4 serves to highlight the nature of Theorem 5; that these divisibilty results are not confinded to a fixed number of parts m. In Theorem 5 set $m = 6$ and $j = 10$ so that $\mu(m,j) = \mu(6,10) = 1200$ and $1 \leq c < \binom{6+1}{2}$. For the family of numbers of parts t with $2 \leq t \leq 6$ we have the following list of congruences in (11).

Example 4.

$$\begin{array}{lll}
p(1200k-1,t) \equiv 0 & \pmod{10} & 2 \leq t \leq 6\\
p(1200k-2,t) \equiv 0 & \pmod{10} & 2 \leq t \leq 6\\
p(1200k-3,t) \equiv 0 & \pmod{10} & 3 \leq t \leq 6\\
p(1200k-4,t) \equiv 0 & \pmod{10} & 3 \leq t \leq 6\\
p(1200k-5,t) \equiv 0 & \pmod{10} & 3 \leq t \leq 6\\
p(1200k-6,t) \equiv 0 & \pmod{10} & 4 \leq t \leq 6\\
p(1200k-7,t) \equiv 0 & \pmod{10} & 4 \leq t \leq 6\\
p(1200k-8,t) \equiv 0 & \pmod{10} & 4 \leq t \leq 6\\
p(1200k-9,t) \equiv 0 & \pmod{10} & 4 \leq t \leq 6\\
p(1200k-10,t) \equiv 0 & \pmod{10} & 5 \leq t \leq 6\\
p(1200k-11,t) \equiv 0 & \pmod{10} & 5 \leq t \leq 6\\
p(1200k-12,t) \equiv 0 & \pmod{10} & 5 \leq t \leq 6\\
p(1200k-13,t) \equiv 0 & \pmod{10} & 5 \leq t \leq 6\\
p(1200k-14,t) \equiv 0 & \pmod{10} & 5 \leq t \leq 6\\
p(1200k-15,t) \equiv 0 & \pmod{10} & t = 6\\
p(1200k-16,t) \equiv 0 & \pmod{10} & t = 6\\
p(1200k-17,t) \equiv 0 & \pmod{10} & t = 6\\
p(1200k-18,t) \equiv 0 & \pmod{10} & t = 6\\
p(1200k-19,t) \equiv 0 & \pmod{10} & t = 6\\
p(1200k-20,t) \equiv 0 & \pmod{10} & t = 6.
\end{array} \tag{11}$$

Acknowledgements This research was conducted through the SUNY Potsdam-Clarkson University REU with funding from the National Science Foundation under Grant No. DMA-1262737. The authors would like to thank Dr. Joel Foisy of the State University of New York Potsdam and and Dr. Tino Tamon of Clarkson University for organising the 2016 summer REU in Potsdam, New York. The authors are grateful to the referee for such thoughtful comments towards improving this paper.

References

[1] S. Ahlgren, *The partition function modulo composite integers M*, Math. Ann. **318** (2000), 795-803.

[2] G. E. Andrews. *The Theory of Partitions*, Cambridge University Press, New York, 1998.

[3] Danahy, Anne. *Undergraduate creates concrete proof from complex mathematical theory*, Intercom Online - Penn State's faculty/staff newspaper, **29**, 34, May 18, 2000.

[4] Gupta, H., E. E. Gwyther and J. C. P. Miller, *Tables of Partitions*, Royal Soc. Math. Tables, Vol. 4, Cambridge University Press, Cambridge, 1958.

[5] Kronholm, Brandt. *On congruence croperties of p(n,m)*, Proc. Amer. Math. Soc. **133** (2005), 2891-2895.

[6] Kronholm, Brandt. *On congruence properties of consecutive values of p(n,m)*, INTEGERS **7** (2007), A16.

[7] Kronholm, Brandt. *Generalized congruence properties of the restricted partition function* $p(n,m)$, Ramanujan J. **30(3)** (2012), 425-436.

[8] Kronholm, Brandt, and Acadia Larsen, *Symmetry and prime divisibility properties of partitions of n into exactly m parts*, Ann. Comb. **19** (2015), 735-747.

[9] Kwong, Y.H.H. *Minimum periods of partition functions modulo M*, Util. Math. **35** (1989), 3-8.

[10] A. Nijenhuis and H.S. Wilf, *Periodicities of partition functions and Stirling numbers modulo P*, J. Number Theory **25** (1987), 308-312.

[11] K. Ono, *Distribution of the partition function modulo m*, Ann. of Math. (2) **151** (2000), 293-307

[12] Ramanujan, S. *Collected Papers*, Cambridge University Press, London, 1927; reprinted: AMS, Chelsea, 2000 with new preface and extensive commentary by B. Berndt.

[13] Yifan Yang, *Modular forms of half-integral weights on $SL(2, Z)$*, Nagoya J. Math. **215**, (2014), 1-66.