7-20-2002

A Restricted Partition Function Modulo 3

Naomi Utgof

Advisors:
John Rickert

MSTR 02-01

A Restricted Partition Function Modulo 3

Naomi Utgoff

Adviser: John Rickert

Mathematical Sciences Technical Report Series
MSTR 02-01

July 20, 2001

Department of Mathematics
Rose-Hulman Institute of Technology
http://www.rose-hulman.edu/math

Fax (812)-877-8333 **Phone (812)-877-8193**

A RESTRICTED PARTITION FUNCTION MODULO 3

NAOMI UTGOFF *

Abstract. The ordinary partition function $p(n)$ counts the number of representations of a positive integer n as the sum of positive integers. We denote by $p_3(n)$ the number of partitions of n with no parts divisible by 3. We demonstrate congruence relations for arithmetic sequences $qn + (2q^2 - 2)/24$ where q is a prime other than 3 congruent to 3 (mod 4). We also prove a result when $q = 5$ and make a conjecture about a generalization.

Date: 20 July 2001.
* Sponsored by NSF grant DMS-0097804.

1. Introduction and Statement of Results

The partition function $p(n)$ counts the number of representations of n as the sum of positive integers. The function $p(n)$ has attracted much attention for its divisibility patterns. Ramanujan conjectured the following identities for $p(n)$:

$$\begin{aligned} p(5n+4) &\equiv 0 \pmod 5 \\ p(7n+5) &\equiv 0 \pmod 7 \\ p(11n+6) &\equiv 0 \pmod{11}. \end{aligned}$$

Ramanujan proved the former two of these. He also observed that there do not seem to be any similar relationships for primes other than 5, 7, and 11. Numerical observation supports Ramanujan's statement. Since then, other congruences have been discovered for primes larger than 11, but congruences modulo 3 remain elusive. Examination of n such that $p(n) \equiv 0 \pmod 3$ reveals no obvious pattern. We will examine congruences modulo 3 for the restricted partition function $p_3(n)$. Our main result provides a congruence relation for all primes greater than 3 and congruent to 3 (mod 4).

Theorem: Let q be a prime greater than 3 such that $q \equiv 3 \pmod 4$. Then $p_3(qn + \frac{2q^2-2}{24}) - p_3(\frac{n}{q}) \equiv 0 \pmod 3$ for all $n \in \mathbb{N}$.

We note that this equivalence is not quite as neat as Ramanujan's congruences. However, it is a nice result because it shows that there are infinitely many congruence relations such that $p_3(qn + r) \equiv 0 \pmod 3$.

We will also demonstrate that when $q = 5$, $p_3(5n + 2) + p_3(n/5) \equiv 0 \pmod 3$. Numerical evidence supports the idea that there is and appropriate sequence $qn+r$ for all primes q congruent both to 1 (mod 4) and 5 (mod 6) and we conjecture what values of r are appropriate.

2. Preliminaries

We will first give the appropriate background material and then we will prove the congruences.

Definition 1. *A partition of a positive integer n is a representation of n as the sum of positive integers. We call the summands of any partition parts.*

We take as an example the case $n = 5$. It is a simple matter to list all of the partitions of 5 as follows:

$$\begin{aligned} &5 \\ &4+1 \\ &3+2 \\ &3+1+1 \\ &2+2+1 \\ &2+1+1+1 \\ &1+1+1+1+1. \end{aligned}$$

We do not care about the order in which the summands are written and thus $3+2$ and $2+3$ are considered the same partition. We therefore list only one of the permutations. The parts of this partition are 3 and 2. By $p(n)$ we denote the number of partitions of n. We define $p(0) = 1$ and $p(n) = 0$ for all other n that are not non-negative integers. In the example, it is easy to see that $p(5) = 7$. It is natural to examine how the partition function changes when we alter its modify

it. We will modify it by restricting the set of integers from which we can draw the parts of a partition. By $p_k(n)$ we denote the number of partitions of n into parts not divisible by k. Since the paper focuses on $p_3(n)$ we will let $k = 3$. With $n = 5$ as in our last example, we enumerate the restricted partitions of n :

$$5$$
$$4+1$$
$$2+2+1$$
$$2+1+1+1$$
$$1+1+1+1+1.$$

Note the omission of $3+2$ and $3+1+1$ since three divides three.

While for small n it is a simple matter to list the partitions of n and count them to evaluate $p(n)$ or $p_k(n)$, this procedure becomes difficult and time consuming as n becomes large. It is only natural to seek a more efficient way of studying the partition functions. It is convenient to use generating functions and study the coefficients rather than attacking $p_k(n)$ directly.

Definition 2. *The generating function for a sequence* $\{a_i\}$ *is the formal power series* $f(q) = \sum_1^\infty a_n q^n$.

This definition does not immediately facilitate study of the partition function. The technique is only useful when we find another way of expressing the generating function for $p(n)$. Fortunately, this is easily done. For S a set of positive integers, we denote by $p(S, n)$ the number of partitions of n with all parts in S.

Theorem 1. *The generating function for* $p(S, n)$ *is* $f(q) = \prod_{n \in H} (1 - q^n)^{-1}$.

Proof. We give no proof here. The interested reader may refer to Andrews's book on partitions [**?**]. □

We note that for the ordinary partition function the generating function is

$$\prod_{n=1}^{\infty} \frac{1}{1-q^n}.$$

For the restricted partition function $p_k(n)$ the generating function is

$$\prod_{n=1}^{\infty} \frac{1-q^{kn}}{1-q^n}.$$

In conjunction with the generating function, we find Euler's pentagonal number theorem useful.

Definition 3. *A pentagonal number is a number of the form* $\frac{3k^2+k}{2}$ *where* k *is an integer.*

We now state Euler's pentagonal number theorem.

Theorem 2. *(Euler's Pentagonal Number Theorem)* [**?**]

$$\prod_{n=1}^{\infty} (1-q^n) = \sum_{-\infty}^{\infty} (-1)^m q^{(3m^2+m)/2}. \tag{1}$$

We note immediately that (**??**) is simply the reciprocal of the generating function for $p(n)$.

3. Congruences modulo 3 for $p_3(n)$

We now state and prove our main result. The problem will reduce to determining the representations of integers as the sum of two squares. So first we need a theorem about these representations

Theorem 3. *A positive integer n can be represented as the sum of two integer squares if and only if every divisor of n of the form $4t+3$ has an even exponent in the prime factorization of n.* [**?**]

We now can prove our main result.

Theorem 4. *Let q be a prime greater than 3 such that $q \equiv 3 \pmod 4$. Then $p_3(qn + \frac{2q^2-2}{24}) - p_3(\frac{n}{q}) \equiv 0 \pmod 3$ for all $n \in \mathbb{N}$.*

Proof. We begin with a lemma.

Lemma 1. *For all $n \in \mathbb{N}$,*

$$p_3(n) \equiv \sum_{\substack{k,l \\ \frac{3k^2+k+3l^2+l}{2}=n}} (-1)^{k+l} \pmod 3.$$

Proof. We recall that the generating function for $p_3(n)$ is $\prod_{n=1}^{\infty} \frac{1-q^{3n}}{1-q^n}$. By the binomial theorem, we see that

$$\begin{aligned} \prod_{n=1}^{\infty} \frac{1-q^{3n}}{1-q^n} &\equiv \prod_{n=1}^{\infty} \frac{(1-q^n)^3}{1-q^n} \pmod 3 \\ &\equiv \prod_{n=1}^{\infty} (1-q^n)^2 \pmod 3. \end{aligned}$$

By Euler's Pentagonal Number Theorem, we have

$$\begin{aligned} \prod_{n=1}^{\infty} (1-q^n)^2 &\equiv \left(\sum_{-\infty}^{\infty} (-1)^{\frac{3k^2+k}{2}} \right)^2 \pmod 3 \\ &\equiv \sum_{\frac{3k^2+k+3l^2+l}{2}=n} (-1)^{k+l} \pmod 3. \end{aligned}$$

□

Thus it is enough to show that for all natural numbers n and all primes q greater than 3 and $q \equiv 3 \pmod 4$, we have

$$\sum_{\frac{3k^2+k+3l^2+l}{2}=qn+\frac{2q^2-2}{24}} (-1)^{k+l} - \sum_{\frac{3k^2+k+3l^2+l}{2}=\frac{n}{q}} (-1)^{k+l} \equiv 0 \pmod 3.$$

We now demonstrate this for natural numbers n such that q does not divide n. Clearly, the second sum will be zero since n/q is not integral. So we need to show that

$$\sum_{\frac{3k^2+k+3l2+l}{2}=qn+\frac{2q^2-2}{24}} (-1)^{k+l} \equiv 0 \pmod 3.$$

We show this by proving that there are no integers k and l that satisfy

$$\frac{3k^2+k+3l^2+l}{2} = qn + \frac{2q^2-2}{24}.$$

We complete the squares [**?**] and observe that

$$(6k+1)^2 + (6l+1)^2 = 24qn + 2q^2. \tag{2}$$

Since q divides the right side of (**??**) only once and $q \equiv 3 \pmod 4$ there are no integers k and l such that (**??**) is true. Since there are no solutions, the sum is zero and hence congruent to $0 \pmod 3$.

We now consider the case when q divides n. We want to show that

$$\sum_{\frac{3k^2+k+3l^2+l}{2} = qn + \frac{2q^2-2}{24}} (-1)^{k+l} - \sum_{\frac{3k^2+k+3l^2+l}{2} = \frac{n}{q}} (-1)^{k+l} \equiv 0 \pmod 3. \tag{3}$$

We complete the squares of the second sum and make a change of variable from n to qn' to obtain

$$(6k+1)^2 + (6l+1)^2 = 24n' + 2. \tag{4}$$

We now prove a lemma that will help show that every solution (k,l) of (**??**) corresponds to exactly one solution (k',l') of (**??**) where $k+l$ and $k'+l'$ are of the same parity.

Lemma 2. *Let n be a natural number and let q be a prime congruent to $3 \pmod 4$. We denote by $r_2(n)$ the number of ordered integer pairs (x,y) such that $x^2+y^2 = n$. Then $r_2(n) = r_2(q^2n)$.*

Proof. Let $D(n) = \{d_1, d_2, \cdots, d_m\}$ denote the set of odd divisors of n. We denote by $qD(n)$ the set $\{qd_1, qd_2, \cdots, qd_m\}$. Clearly, $D(q^2n) = D(n) \bigcup qD(n) \bigcup q^2D(n)$. For all i, if $qd_i \equiv 1 \pmod 4$ then $q^2d_i \equiv 3 \pmod 4$. Also, if $qd_i \equiv 3 \pmod 4$ then $q^2d_i \equiv 1 \pmod 4$. The formula for $r_2(n)$ is [**?**]

$$4\left(\sum_{\substack{d \mid n \\ d \equiv 1 \pmod 4}} 1 - \sum_{\substack{d \mid n \\ d \equiv 3 \pmod 4}} 1 \right). \tag{5}$$

So for every i, qd_i and q^2d_i cancel each other out in (**??**). So $r_2(n) = r_2(q^2n)$. □

We now let (k',l') be a solution to (**??**) and exhibit a corresponding solution to (**??**). Multiplying (**??**) by q^2 we obtain

$$q^2(6k'-1)^2 + q^2(6l'-1)^2 = 24nq + 2q^2. \tag{6}$$

We now rewrite the left side of (**??**) as

$$[6(qk' + (q-1)/6) + 1]^2 + [6(ql' + (q-1)/6) + 1]^2 \text{ if } q \equiv 1 \pmod 6 \tag{7}$$

This expression has the same form as the left side of (**??**) where $k = qk' + (q-1)/6$ and $l = ql' + (q-1)/6$. We know that $(q-1)/6$ is integral because $q \equiv 1 \pmod 6$. Since q is odd, $k'+l'$ and $k+l$ have the same parity.

The proof in the case $q \equiv 5 \pmod 6$ is exactly the same, except that we rewrite the left side of (**??**) as

$$[6(-qk' - (-q-1)/6) + 1]^2 + [6(-ql' - (-q-1)/6) + 1]^2. \tag{8}$$

In both (**??**) and (**??**) Lemma **??** forces the correspondence between solutions to be a bijection. So the difference in (**??**) is 0 and hence congruent to 0 (mod 3). □

We give as a corollary the case $q = 7$.

Corollary 1. *For all* $n \in \mathbb{N}$, $p_3(7n+4) - p_3(\frac{n}{7}) \equiv 0 \pmod 3$.

Recall that for n not divisible by 7, $p_3(\frac{n}{7}) = 0$. So the corollary tells us that $p_3(7n+4) \equiv 0 \pmod 3$ when n is not divisible by 7. Only when n is divisible by 7 must we subtract $p_3(\frac{n}{7})$.

Theorem 5. *For all* $n \in \mathbb{N}$, $p_3(5n+2) + p_3(\frac{n}{5}) \equiv 0 \pmod 3$.

Proof. By Lemma **??** from the last theorem, we know that it is enough to show that

$$\sum_{\frac{3k^2+k+3l^2+l}{2}=5n+2} (-1)^{k+l} + \sum_{\frac{3k^2+k+3l^2+l}{2}=\frac{n}{5}} (-1)^{k+l} \equiv 0 \pmod 3.$$

We first exhibit this for $n \not\equiv 0 \pmod 5$. Since $n/5$ is not integral, we need only concern ourselves with the first sum. We again complete the square so that

$$(6k+1)^2 + (6l+1)^2 = 120n + 50. \tag{9}$$

We wish to exhibit a correspondence between solutions such that $k+l$ is even and solutions such that $k+l$ is odd. We let $\kappa = 6k+1$ and $\lambda = 6l+1$. We then factor $\kappa^2 + \lambda^2$ in the Gaussian integers [**?**]. We can write

$$120n + 50 = (\kappa + i\lambda)(\kappa - i\lambda).$$

Clearly, 5 divides this expression but 25 does not. So we may conclude that 5 divides neither κ nor λ. This implies that either $(2+i)$ divides $(\kappa + i\lambda)$ or that $(2-i)$ divides $(\kappa + i\lambda)$. We may assume the former without loss of generality and write

$$(2+i)(\kappa' + i\lambda')(2-i)(\kappa' - i\lambda')$$

with $(2+i)(\kappa'+i\lambda') = \kappa+i\lambda$. There exists a corresponding solution $(2-i)(\kappa'+i\lambda') = (\kappa + i\lambda)\frac{2-i}{2+i}$. We manipulate as follows [**?**]:

$$\begin{aligned} \frac{(\kappa+i\lambda)(2-i)}{2+i} &= \frac{(\kappa+i\lambda)(3-4i)}{5} \\ &= \frac{18k+24l+7+18li-24ki-i}{5} \\ &= \frac{[6(3k+4l+1)+1] - i[6(4k-3l+1)+1]}{5}. \end{aligned}$$

We let $k' = 3k+4l+1$ and $l' = 4k-3l+1$. So $k'+l' = \frac{7k+l+1}{5}$ which has different parity from $k+l$. So there is a one-to-one correspondence between solutions such that $k+l$ is even and $k+l$ is odd.

We now consider the case when n is divisible by 5. We want to show that

$$\sum_{\frac{3k^2+k+3l^2+l}{2}=5n+2} (-1)^{k+l} + \sum_{\frac{3k^2+k+3l^2+l}{2}=\frac{n}{5}} (-1)^{k+l} \equiv 0 \pmod 3.$$

Completing the squares in the second sum and factoring in the Gaussian integers, we see that

$$(2+i)(2-i)(\kappa' + i\lambda')(2+i)(2-i)(\kappa' - i\lambda') = 120n + 50.$$

As in the case when n is not divisible by 5, there is a bijection between solutions given by

$$(2+i)^2(\kappa' + i\lambda')$$
$$(2-i)^2(\kappa' - i\lambda')$$

and

$$(2+i)^2(\kappa' - i\lambda')$$
$$(2-i)^2(\kappa' + i\lambda')$$

However, we have one factorization $(5\kappa' + 5i\lambda')(5\kappa' - i\lambda')$ which corresponds to some solution (k', l') of (**??**). We may perform a similar change of variable as in the proof of Theorem 1 and the proof follows in the same way. □

Theorems **??** and **??** suggest that there should be a similar generalization for $q \equiv 1 \pmod 4$. Numerical evidence indicates that there is no similar relationship when both $q \equiv 1 \pmod 4$ and $q \equiv 1 \pmod 6$. The following conjecture remains an open question with some numerical support:

Conjecture 1. *Let q be a prime such that $q \equiv 1 \pmod 4$ and $q \equiv 5 \pmod 6$. Then for all $n \in \mathbb{N}$, $p_3(qn + (2q^2 - 2)/24) + p_3(n/q) \equiv 0 \pmod 3$.*

Although we only listed the case $q = 7$, Theorem **??** provides a congruence relation for every prime q congruent to 3 (mod 4). Proving conjecture **??** would provide a parallel result for primes congruent to 1 (mod 4). Examining the cases when both $q \equiv 1 \pmod 4$ and $q \equiv 1 \pmod 6$ would be an interesting area for further study.

I would like to thank the following people and entity for their generous and kind support:

- The National Science Foundation, for the money that makes the REU possible
- Professor John Rickert, my advisor
- Professor S. Allen Broughton, the tilings advisor and REU coordinator
- My number theory colleagues: Amanda Knecht, Christopher Mihelich, and Matthew Culek
- The tilings group: Matthew Ong, Niles Johnson, Stephen Young, and Yvonne Lai
- The computer staff, Charles Clancy and Nik Reiman. Especially Charles, who patiently fixed many of my mistakes

References

[An] Andrews, George E. *The Theory of Partitions.* Addison Wesley Publishing Company, Reading, MA, 1976.

[C-K] Culek, Matthew and Amanda Knecht. Personal Communication and REU paper.

[H-W] Hardy, G.H. and E.M. Wright. *An Introduction to the Theory of Numbers.* Clarendon Press, Oxford, 1979.

[Mi] Mihelich, Christopher. Personal communication.

[Na] Nathanson, Melvyn B. *Elementary Methods in Number Theory.* Springer–Verlag, New York, 2000.

Department of Mathematics, Rose-Hulman Institute of Technology, 5500 Wabash Avenue Terre Haute, IN 47803

E-mail address: utgoff@brandeis.edu

URL: http://www.brandeis.edu/~utgoff/Math