6-2002

# Congruences of Restricted Partition Functions

Matthew Culek

Amanda Knecht

Advisors:
John Rickert



MSTR 02-04

# Congruences of Restricted Partition Functions

**Matt Culek and Amanda Knecht**

**Adviser: John Rickert**

## Mathematical Sciences Technical Report Series
## MSTR 02-04

**June 2002**

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

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

# Congruences of Restricted Partition Functions

Matt Culek
Amanda Knecht

Sponsored by NSF Grant # DMS-0097804

## Acknowledgements:

[1] **Dr. John Rickert**, for his guidance and support.

[2] **Dr. S. Allen Broughton**, for organizing and running the REU.

[3] All the other students at the REU. The rest of the Number Theory group; Chris and Naomi. The Tilings group; Niles, Yvonne, Matt, and Steve.

[4] The computer support staff, Nick and Charles.

"One of the symptoms of an approaching nervous breakdown is the belief that one's work is terribly important." *Bertrand Russell*


# Abstract:

In this paper we study restricted partition functions of the form $p_k(q^2m+b)$, for certain primes $q$, with $k = 3, 5, 7$. For each $k$ we analyze which primes $q$ satisfy $p_k(q^2m + b) \equiv 0 \bmod k$ for all natural numbers $m$. We then prove our results by applying a common method of proof to each case.


# Introduction:

The essence of Number Theory is finding simple relationships that encapsulate complex properties of the integers. Amazingly enough, one of the simplest ideas in mathematics, writing a number as a sum of other numbers, can help illuminate the underlying structure of the integers. This is called partition theory.

A partition of a nonnegative integer $n$ is a representation of $n$ as a sum of positive integers, called summands, the order of which are irrelevant.

**Definition 0.1** *The function $p(n)$ denotes the number of partitions of $n$.*

The generating function, $P(q)$, for the partition function is

$$P(q) = \sum_{n=0}^{\infty} p(n)q^n = \prod_{n=1}^{\infty} \frac{1}{(1-q^n)}.$$

This general partition function, $p(n)$, has been studied extensively, most notably by Ramanujan who discovered the following congruences [Ra]:

$$p(5n+4) \equiv 0 \bmod 5$$
$$p(7n+5) \equiv 0 \bmod 7$$
$$p(11n+6) \equiv 0 \bmod 11.$$

In order to discover similar congruences we can consider alterations to the partition function. Namely we can define a restricted partition function as follows:

**Definition 0.2** *The restricted partition function, $p_k(n)$, is the partition of an integer into summands none of which are divisible by $k$.*

The generating function of $p_k(n)$ is:

$$P_k(q) = \sum_{n=0}^{\infty} p_k(n)q^n = \prod_{n=1}^{\infty} \frac{\frac{1}{(1-q^n)}}{\frac{1}{(1-q^{kn})}} = \prod_{n=1}^{\infty} \frac{(1-q^{kn})}{(1-q^n)} = P(q) \prod_{n=1}^{\infty} 1-q^{kn}. \quad (0.1)$$

Now we have $P_k(q)$ in terms of $P(q)$. In order to make this more explicit for actual calculations we can make an important simplification by recalling Euler's Pentagonal Number Theorem [HW].

**Theorem 0.1** *Euler's Pentagonal Number Theorem*

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

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

Now we see that by substituting $q^k$ for $q$ we get

$$P_k(q) = P(q) \left[ 1 + \sum_{n=1}^{\infty} (-1)^n q^{kn(3n+1)/2} + \sum_{n=1}^{\infty} (-1)^n q^{kn(3n-1)/2} \right]. \quad (0.2)$$

Now we have a relation that can be used to find $p_k(n)$ through $p(n)$, which is easier to compute. This is achieved by matching coefficients of the appropriate terms in the expansion. For example let's compute $p_2(6)$. By substituting 2 for $k$ in equation (**??**) we find that

$$P_2(q) = (1+q+2q^2+3q^3+5q^4+7q^5+11q^6+\cdots)(1-q^2-q^4+q^{10}+q^{14}+\cdots).$$

We know that $p_2(6)$ is equal to the coefficient of the $q^6$ term.

$$p_2(6) = p(6) - p(4) - p(2) = 11 - 5 - 2 = 4.$$

This approach can be verified by explicity listing all the partitions of 6 containing no even summands.

$$\begin{gathered} 5+1 \\ 3+3 \\ 3+1+1+1 \\ 1+1+1+1+1+1. \end{gathered}$$

Using this method, we developed an algorithim in Maple for computing $p_k(n)$. Having $p_k(n)$, we looked for congruence relations of the form:

$$p_k(An+B) \equiv 0 \bmod M \quad \forall n \in N.$$

Our second Maple algorithim computes the greatest common divisor of $p_k(An+B)$ and $p_k(A(n+1)+B)$ for $1 \leq n \leq max$, where $max$ is limited by the size our precomputed data file for $p(n)$. By using this algorithim, we were able to make conjectures by extrapolating that the modular congruences hold for all $n$.

In this paper we will prove congruences for $p_3(n) \bmod 3$, $p_5(n) \bmod 5$, and $p_7(n) \bmod 7$. Specifically, we will focus on congruences where $n = q^2m+b$, with $q$ being a prime. Our analysis will consist in seeing which primes lead to nice congruence properties for each restricted partition function. We will apply the same general method of proof to each case in an attempt to find an integrated result. Lastly we will state some stronger results as conjectures to be pursued in further research.

## Congruences of $p_3(n)$:

In this chapter we will be considering congruences of $p_3(n)$ mod 3. This is motivated by the following derivation involving the generating function of $p_3(n)$. If we recall equation (**??**) and let $k = 3$ we see

$$P_3(q) = \sum_{n=0}^{\infty} p_3(n)q^n = \prod_{n=1}^{\infty} \frac{(1-q^{3n})}{(1-q^n)}.$$

We know that $1 - q^{3n} \equiv (1 - q^n)^3 \mod 3$. Therefore

$$\sum_{n=0}^{\infty} p_3(n)q^n \equiv \prod_{n=1}^{\infty} \frac{(1-q^n)^3}{(1-q^n)} \mod 3.$$

Which can be reduced to

$$\sum_{n=0}^{\infty} p_3(n)q^n \equiv \left(\prod_{n=1}^{\infty} 1-q^n\right)^2 \mod 3.$$

By applying Euler's Pentagonal Number Theorem (0.1) the above equation becomes

$$\sum_{n=0}^{\infty} p_3(n)q^n \equiv \left(\sum_{n=-\infty}^{\infty} (-1)^n q^{n(3n-1)/2}\right)^2 \mod 3.$$

Now we can write this as a double sum,

$$\sum_{n=0}^{\infty} p_3(n)q^n \equiv \sum_{k,\ell=-\infty}^{\infty} (-1)^{k+\ell} q^{\frac{k(3k-1)}{2}+\frac{\ell(3\ell-1)}{2}} \mod 3.$$

When $n = \frac{k(3k-1)}{2} + \frac{\ell(3\ell-1)}{2}$,

$$\sum_{n=0}^{\infty} p_3(n)q^n \equiv \sum_{n=0}^{\infty} q^n \sum_{k,\ell} (-1)^{k+\ell} \mod 3.$$

Now we can equate coefficients to find

$$p_3(n) \equiv \sum_{\frac{k(3k-1)}{2}+\frac{\ell(3\ell-1)}{2}=n} (-1)^{k+\ell} \mod 3. \tag{1.1}$$

This tells us that, when working modulo 3, finding $p_3(n)$ becomes a problem of how to write an integer as a sum of two pentagonal numbers. In analyzing this, we start by writing

$$n = \frac{k(3k-1)}{2} + \frac{\ell(3\ell-1)}{2}.$$

We then complete the square.

$$24n + 2 = (6k-1)^2 + (6\ell-1)^2.$$

The manipulation shows that writing $n$ as a sum of two pentagonals can be treated as a sum of squares problem. This is helpful because writing an integer as a sum of squares is a well studied area. For simplicity in the remainder of the chapter we will let $\kappa = (6k-1)$ and $\lambda = (6\ell-1)$.

$$24n + 2 = (6k-1)^2 + (6\ell-1)^2 = \kappa^2 + \lambda^2. \tag{1.2}$$

We want to consider $n$ of the form $n = q^2m + b$, where $q$ is a prime. If we exclude the prime 2, we know that every prime, $q$, is equivalent to one or three modulo four. First let's consider primes $q \equiv 3 \bmod 4$. Before we proceed we need to introduce a well known theorem concerning when an integer can be written as a sum of two squares [HW].

**Theorem 1.1** *A number $n$ can be written as the sum of two squares if and only if when $n$ is expressed as a product of prime-powers, every prime factor $q \equiv 3 \bmod 4$ occurs with even exponent.*

This theorem, along with some numerical data, naturally leads to the following theorem.

**Theorem 1.2** $p_3(q^2m + b) \equiv 0 \mod 3$*, for all natural numbers $m$, where $q$ is a prime greater than 3 for which $q \equiv 3 \mod 4$ with $b$ satisfying $q \parallel 24b + 2$.*

**Proof:** We know that $n = q^2m + b$, so recalling equation (**??**) we see

$$24n + 2 = 24q^2m + 24b + 2 = \kappa^2 + \lambda^2.$$

Since $q \parallel 24b + 2$, we know that we can factor out exactly one $q$ to get

$$q\left(24qm + \frac{24b+2}{q}\right) = \kappa^2 + \lambda^2 = (6k-1)^2 + (6\ell-1)^2. \tag{1.3}$$

But because $ord_q(n) = 1$ we can apply Theorem **??**. This tells us that there exists no $(\kappa, \lambda)$, and hence no $(k, \ell)$, that satisfy equation (**??**). So recalling equation (**??**)

$$p_3(n) \equiv \sum_{\frac{k(3k-1)}{2}+\frac{\ell(3\ell-1)}{2}=n} (-1)^{k+\ell} \mod 3,$$

we see the sum has no terms and is exactly zero, therefore

$$p_3(q^2m + b) \equiv 0 \mod 3 \quad \square$$

Now that we have characterized the congruences for primes congruent to three modulo four, we need to analyze primes congruent to one modulo four. This will be much harder because we cannot simply apply Theorem **??**. It turns out that we need to consider these primes modulo 12. For any prime $q \equiv 1 \bmod 4$ we know that $q \equiv 1, 5 \bmod 12$. When $q \equiv 1 \bmod 12$ we can simply look at numerical data and see that no congruence properties are apparent. So we want to analyze the case when $q \equiv 5 \bmod 12$. First we will prove a specific congruence and then generalize our method to all primes $q \equiv 5 \bmod 12$.

**Theorem 1.3** $p_3(5^2m + b) \equiv 0 \mod 3$, *for all natural numbers* $m$, *with* $b$ *satisfying* $5 \parallel 24b + 2$.

**Proof:** We have $n = 5^2m + b$. By (**??**), we see that $24n + 2 = 600m + 24b + 2 = 5(120m + \frac{24b+2}{5}) = \kappa^2 + \lambda^2$, where $\frac{24b+2}{5} \in \mathbb{Z}$ because $5 \parallel 24b + 2$.
This tells us that 5 divides $\kappa^2 + \lambda^2$. Unfortunately knowing that a number divides a sum is not very helpful, so we want to write $\kappa^2 + \lambda^2$ as a product. For this we consider the Gaussian Integers [Mi] and write $\kappa^2 + \lambda^2 = (\kappa + \imath\lambda)(\kappa - \imath\lambda)$. So $5 \mid (\kappa+\imath\lambda)(\kappa-\imath\lambda)$. We know however that $5 \nmid (\kappa+\imath\lambda)$ and $5 \nmid (\kappa-\imath\lambda)$ because if five divides one it divides the other since they are complex conjugates. This forces $5^2 \mid (\kappa + \imath\lambda)(\kappa - \imath\lambda)$, which contradicts our condition that $5 \parallel 24b + 2$. It is widely known that five can be written as a product of two primes in the Gaussians, namely $5 = (2 + \imath)(2 - \imath)$. Thus we see that $(2 + \imath)(2 - \imath) \mid (\kappa + \imath\lambda)(\kappa - \imath\lambda)$.
Now assume that $(2 + \imath) \mid (\kappa + \imath\lambda)$. So $(\kappa + \imath\lambda) = (2 + \imath)(\kappa' + \imath\lambda')$.
We can find a conjugate solution when $(2 - \imath) \mid (\kappa^* + \imath\lambda^*) = (2 - \imath)(\kappa' + \imath\lambda')$. To see how this relates to our original solution we multiply by $\frac{2-\imath}{2+\imath}$. We know that $\frac{2-\imath}{2+\imath} = \frac{3-4\imath}{5}$. The real denominator will not affect the conjugation so we get:

$$\begin{aligned}\kappa^* + \imath\lambda^* &= [(6k - 1) + \imath(6\ell - 1)][3 - 4\imath] \\ &= [18k + 24\ell - 7] + \imath[18\ell - 24k + 1] \\ &= [6(3k + 4\ell - 1) - 1] + \imath[6(-3\ell + 4k) - 1].\end{aligned}$$

So $k^* = 3k + 4\ell - 1$ and $\ell^* = -3\ell + 4k$. Therefore

$$(-1)^{k^*+\ell^*} = (-1)^{7k+\ell-1} = (-1)^{k+\ell-1} = -\left[(-1)^{k+\ell}\right].$$

Since

$$p_3(n) \equiv \sum_{\frac{k(3k-1)}{2}+\frac{\ell(3\ell-1)}{2}=n} (-1)^{k+\ell} \mod 3,$$

and we know that $(-1)^{k+\ell}$ cancels out with $(-1)^{k^*+\ell^*}$ for any solution $(k,\ell)$, we are left with

$$p_3(5^2m+b) \equiv 0 \mod 3. \quad \square$$

It now appears possible to generalize this method to other primes, $q \equiv 5 \bmod 12$, besides 5. This can be done, but first we need to establish a Lemma.

**Lemma 1.1** *Let $q$ be prime and $q \equiv 5 \mod 12$. If we write $q$ as $q = (x+\imath y)(x-\imath y) = x^2+y^2$, then $-(x^2-y^2) \pm 2xy \equiv \pm 1 \bmod 6$.*

**Proof:**
Since $q \equiv 5 \mod 12$, we know that $q \equiv 5 \mod 6$. We also know that $q = x^2+y^2$ so $x^2+y^2 \equiv 5 \mod 6$.
Therefore one of $x^2, y^2 \equiv 1 \mod 6$ and the other is congruent to $4 \mod 6$.
Assume without loss of generality that $x^2 \equiv 1 \mod 6$ and $y^2 \equiv 4 \mod 6$.
Then $x \equiv 1, 5 \mod 6$ and $y \equiv 2, 4 \mod 6$
Thus $(x^2-y^2) \equiv 3 \mod 6$ and $2xy \equiv 2, 4 \mod 6$.
Therefore $-(x^2-y^2) \pm 2xy \equiv \pm 1 \mod 6$.
Also if $-(x^2-y^2) - 2xy \equiv -1 \mod 6$, then $-(x^2-y^2) + 2xy \equiv 1 \mod 6$.
$\square$

Now we can state and prove our generalized theorem.

**Theorem 1.4** *$p_3(q^2m+b) \equiv 0 \mod 3$, for all natural numbers $m$, where $q$ is a prime for which $q \equiv 5 \mod 12$ with $b$ satisfying $q \parallel 24b+2$.*

**Proof:**
Let $n = q^2m+b$ where $q$ is a prime for which $q \equiv 5 \mod 12$. Let $q \parallel 24b+2$.

Then

$$\begin{aligned} 24n+2 &= 24q^2m + 24b + 2, \\ &= q\left(24qm + \frac{24b+2}{q}\right). \end{aligned}$$

We can factor out this $q$ because we know that $\frac{24b+2}{q}$ is an integer since $q \parallel 24b+2$. Thus

$$q\left(24qm + \frac{24b+2}{q}\right) = (\kappa+\imath\lambda)(\kappa-\imath\lambda).$$

So $q \mid (\kappa+\imath\lambda)(\kappa-\imath\lambda)$. But $q$ cannot divide fully into only one of them since they are complex conjugates. If $q \mid (\kappa+\imath\lambda)$ then $q \mid (\kappa-\imath\lambda)$, but this implies that we can factor out a $q^2$ on the left side. This contradicts our condition that $q \parallel 24b+2$. Therefore $q$ must factor, but since it is prime we need to use the Gaussian integers $\mathbb{Z}[\imath]$. Since $q$ is prime and $q \equiv 1 \mod 4$, we know that there exist integers $x, y$ such that $q = (x+\imath y)(x-\imath y) = x^2+y^2$. So

$$(x+\imath y)(x-\imath y) \mid (\kappa+\imath\lambda)(\kappa-\imath\lambda).$$

At this point we know either $(x+\imath y) \mid (\kappa+\imath\lambda)$ which implies $(x-\imath y) \mid (\kappa-\imath\lambda)$, or $(x+\imath y) \mid (\kappa-\imath\lambda)$ which implies $(x-\imath y) \mid (\kappa+\imath\lambda)$. The choice is arbitrary.

Suppose that $(x+\imath y) \mid (\kappa+\imath\lambda)$. Then $\kappa+\imath\lambda = (x+\imath y)(\kappa'+\imath\lambda')$. Since this choice was arbitrary we know there exists a conjugate solution $(\kappa^*, \lambda^*)$ for which $(x-\imath y) \mid (\kappa^*+\imath\lambda^*) = (x-\imath y)(\kappa'+\imath\lambda')$. Therefore we can multiply $\kappa+\imath\lambda = (x+\imath y)(\kappa'+\imath\lambda')$ by $\frac{x-\imath y}{x+\imath y}$ to see how the conjugate solution relates to the original.

$$(\kappa^*+\imath\lambda^*) = (\kappa+\imath\lambda)\left(\frac{x-\imath y}{x+\imath y}\right).$$

We also know that

$$\frac{x-\imath y}{x+\imath y} = \frac{x^2-y^2-2xy\imath}{x^2+y^2}.$$

Since the denominator is real it will not affect the conjugation. For simplicity let $a = x^2-y^2$ and $b = 2xy$. So

$$\begin{aligned}(\kappa^*+\imath\lambda^*) &= (\kappa+\imath\lambda)(a-b\imath)\\ &= [(6k-1)+\imath(6\ell-1)][a-b\imath]\\ &= [6(ka+\ell b)-a-b]+\imath[6(\ell a-kb)-a+b].\end{aligned}$$

If we recall Lemma **??** we know that $-a \pm b \equiv \pm 1 \mod 6$. Without losing generality, we can assume $-a-b \equiv -1 \mod 6$. This also implies that
$a \equiv 3 \mod 6$, $b \equiv 4 \mod 6$ and $-a+b \equiv 1 \mod 6$.
So $-a-b+1 \equiv 0 \mod 6$ and $-a+b-1 \equiv 0 \mod 6$. We can factor out a 6 and rewrite our equation as

$$\kappa^*+\imath\lambda^* = \left[6\left(ka+\ell b+\frac{-a-b+1}{6}\right)-1\right]+\imath\left[6\left(-\ell a+kb+\frac{a-b+1}{6}\right)-1\right].$$

Now we have our equation in the correct form to realize that since
$\kappa^* = (6k^*-1)$ and $\lambda^* = (6\ell^*-1)$, we know that

$$k^* = ka+\ell b+\frac{-a-b+1}{6}$$

$$\ell^* = -\ell a+kb+\frac{a-b+1}{6}.$$

If we recall equation (**??**) it becomes clear that we want to compare the parity of $k+\ell$ with $k^*+\ell^*$.

$$k^*+\ell^* = (a+b)k + (b-a)\ell + \frac{1-b}{3}$$

First we need to ensure that $\frac{1-b}{3}$ is an integer. Earlier we established that since $-a-b \equiv -1 \mod 6$ then $b \equiv 4 \mod 6$, so $1-b \equiv -3 \equiv 3 \mod 6$. Therefore $\frac{1-b}{3}$ is an integer.

Now we must consider $k^*+\ell^* \mod 2$. We recall that $b = 2xy$, so $b$ is even. Also recall $a = x^2-y^2$. Now since $q$ is odd we know $q = x^2+y^2 \equiv 1 \mod 2$, So $a = x^2-y^2 \equiv (x^2+y^2)-2y^2 \equiv 1-0 \equiv 1 \mod 2$, so $a$ is odd. Therefore $(a+b) \equiv (b-a) \equiv 1 \mod 2$. We also know $\frac{1-b}{3} \equiv (1-b) \mod 2$. But since $(1-b) \equiv 3 \mod 6$ we know $(1-b)$ is odd, so $(1-b) \equiv 1 \mod 2$. So reducing $k^*+\ell^* \mod 2$ we see that $k+\ell \equiv k^*+\ell^*+1 \mod 2$. Therefore

$$(-1)^{k+\ell} = -\left[(-1)^{k^*+\ell^*}\right].$$

For every solution $(k,\ell)$ there necessarily exists a conjugate solution $(k^*,\ell^*)$. Combining this with the result above we see that

$$p_3(q^2m+b) = \sum_{\frac{k(3k-1)}{2}+\frac{\ell(3\ell-1)}{2}=n} (-1)^{k+\ell} \equiv 0 \mod 3$$

when the conditions of our theorem are met. □

To conclude we can combine our two main theorems into a general result for the conditions on $q$ which allow it to satisfy congruence relations.

**Theorem 1.5** *$p_3(q^2m+b) \equiv 0 \mod 3$, for all natural numbers $m$, where $q$ is a prime for which $q \equiv 5,7,11 \mod 12$ with $b$ satisfying $q \parallel 24b+2$.*

This theorem provides us with an infinite number of congruence relations for the function $p_3(q^2m+b)$, for all $q \not\equiv 1 \bmod 12$. We can plug in a few explicit values for $q$ to find the following corollary.

**Corollary 1**

1. *$p_3(7^2m+b) \equiv 0 \mod 3$, for all natural numbers $m$, with $b$ satisfying $b \equiv 4 \mod 7$ for which $b \not\equiv 4 \mod 7^2$.*
2. *$p_3(11^2m+b) \equiv 0 \mod 3$, for all natural numbers $m$, with $b$ satisfying $b \equiv 10 \mod 11$ for which $b \not\equiv 10 \mod 11^2$.*
3. *$p_3(17^2m+b) \equiv 0 \mod 3$, for all natural numbers $m$, with $b$ satisfying $b \equiv 7 \mod 17$ for which $b \not\equiv 24 \mod 17^2$.*

## Congruences of $p_5(n)$:

This chapter will be devoted to the study of $p_5(n) \mod 5$. This is initially motivated by the following theorem, due to Thanigasalam[Th], which provides a link between congruences of restricted partition fucntions and the Ramanujan congruences.

**Theorem 2.1** *(Thanigasalam) Let $k \geq 2$, and $\ell$ be an integer satisfying $0 \leq \ell \leq k-1$. If $p(km+1) \equiv 0 \mod k$ for all natural numbers $m$, then $p_k(km+1) \equiv 0 \mod k$ for all natural numbers $m$.*

If we apply this theorem to the known Ramanujan congruence of

$$p(5n+4) \equiv 0 \mod 5,$$

we see that

$$p_5(5n+4) \equiv 0 \mod 5.$$

The application of this idea is very limited however. To find more congruences we will consider the form $p_5(q^2m+b)$. In this analysis we will find which primes $q$ satisfy congruence relations for the function $p_5$. In order to study congruences $p_5(q^2m+b) \mod 5$, we need to study the generating function of the restricted partition function as in the previous chapter. First we need to recall a theorem of Jacobi [HW].

**Theorem 2.2** *Jacobi's Triangular Number Theorem*

$$\prod_{n=1}^{\infty}(1-q^n)^3 = \sum_{k=0}^{\infty}(-1)^k(2k+1)q^{\frac{k^2+k}{2}}.$$

If we recall equation (**??**) and let $k=5$ we see

$$P_5(q) = \sum_{n=0}^{\infty} p_5(n)q^n = \prod_{n=1}^{\infty}\frac{(1-q^{5n})}{(1-q^n)}.$$

Knowing $1 - q^{5n} \equiv (1 - q^n)^5 \bmod 5$ tells us that

$$\sum_{n=0}^{\infty} p_5(n)q^n \equiv \prod_{n=1}^{\infty} \frac{(1-q^n)^5}{(1-q^n)} \mod 5.$$

We reduce this to find

$$\begin{aligned}\sum_{n=0}^{\infty} p_5(n)q^n &\equiv \left(\prod_{n=1}^{\infty} 1-q^n\right)^4 \mod 5,\\ &\equiv \left(\prod_{n=1}^{\infty} 1-q^n\right)\left(\prod_{n=1}^{\infty} 1-q^n\right)^3 \mod 5.\end{aligned}$$

By Theorems (0.1) and (2.2) we get,

$$\begin{aligned}\sum_{n=0}^{\infty} p_5(n)q^n &\equiv \sum_{k=-\infty}^{\infty} (-1)^k q^{\frac{k(3k+1)}{2}} \sum_{\ell=0}^{\infty} (-1)^\ell (2\ell+1) q^{\frac{\ell^2+\ell}{2}} \mod 5,\\ &\equiv \sum_{k,\ell} (-1)^{k+\ell}\ (2\ell+1)\ q^{\frac{k(3k+1)}{2}+\frac{\ell^2+\ell}{2}} \mod 5.\end{aligned}$$

Equating the coefficients, we find

$$p_5(n) \equiv \sum_{\frac{k(3k+1)}{2}+\frac{\ell^2+\ell}{2}=n} (-1)^{k+\ell}\ (2\ell+1) \mod 5. \tag{2.1}$$

This tells us that finding $p_5(n)$ modulo five is a problem of writing $n$ as a sum of a pentagonal and a triangular number. We can write

$$n = \frac{k(3k+1)}{2} + \frac{\ell^2+\ell}{2}.$$

We complete the square to get

$$72n + 12 = 3(6k+1)^2 + (6\ell+3)^2.$$

As in the previous chapter, we see that our expression of $n$ can be treated as a sum of squares problem. Letting $\kappa = (6k+1)$ and $\lambda = (6\ell+3)$

$$72n + 12 = 3\kappa^2 + \lambda^2. \tag{2.2}$$

This naturally leads to the introduction of the following theorem [Ja].

**Theorem 2.3** *Natural numbers of the form $a^2 + 3b^2$ are products of powers of 3; powers of primes congruent to 1 modulo 3; and even powers of primes congruent to 2 modulo 3.*

Numerical data and Theorem 2.3 suggest Theorem 2.4.

**Theorem 2.4** *$p_5(q^2m+b) \equiv 0 \mod 5$, for all natural numbers $m$, where $q$ is a prime for which $q \equiv 5 \mod 6$ with $b$ satisfying $q \parallel 24b+4$.*

**Proof:**
We start by substituting $q^2m+b$ for $n$ in equation (**??**).

$$72q^2m + 72b + 12 = 3\kappa^2 + \lambda^2.$$

Since $q \parallel 24b+4$, we can factor out exactly one $q$ on the left side of the equation to find

$$3q\left(24qm + \frac{24b+4}{q}\right) = 3\kappa^2 + \lambda^2 = 3(6k+1)^2 + (6\ell+3)^2.$$

Since $q \equiv 5 \bmod 6$ implies that $q \equiv 2 \bmod 3$ and $ord_q(n) = 1$, we can apply Theorem **??** to find that there are no solutions $(\kappa, \lambda)$ satisfying $72q^2m + 72b + 12 = 3\kappa^2 + \lambda^2$, and therefore no solutions $(k, \ell)$. So if we recall equation (**??**)

$$p_5(n) \equiv \sum_{\frac{k(3k+1)}{2} + \frac{\ell^2+\ell}{2} = n} (-1)^{k+\ell}\,(2\ell+1) \mod 5,$$

we see that the sum has no terms, so it is zero. Thus

$$p_5(q^2m+b) \equiv 0 \mod 5 \quad \square$$

In this chapter we proved that congruence relations hold for primes of the form $q \equiv 5 \bmod 6$. Numerical data shows that other primes do not provide such relations. Now we can substitue some values of $q$ to form a corollary demonstrating our results.

**Corollary 2**

1. *$p_5(5^2m+b) \equiv 0 \mod 5$, for all natural numbers $m$, with $b$ satisfying $b \equiv 4 \mod 5$ for which $b \not\equiv 4 \mod 5^2$.*
2. *$p_5(11^2m+b) \equiv 0 \mod 5$, for all natural numbers $m$, with $b$ satisfying $b \equiv 9 \mod 11$ for which $b \not\equiv 20 \mod 11^2$.*
3. *$p_5(17^2m+b) \equiv 0 \mod 5$, for all natural numbers $m$, with $b$ satisfying $b \equiv 14 \mod 17$ for which $b \not\equiv 48 \mod 17^2$.*

## Congruences of $p_7(n)$:

Here we make the natural extension of our approach to study congruences of $p_7(n)$ mod 7. If we recall Theorem 2.1, we again note that since

$$p(7n+5) \equiv 0 \bmod 7,$$

we see that

$$p_7(7n+5) \equiv 0 \bmod 7.$$

As in Chapter 1, we need to consider the form $p_7(q^2m+b)$ in order to find more congruence relations. We will see which primes satisfy congruence relations for $p_7(q^2m+b)$. To study these general congruences of $p_7(q^2m+b)$ mod 7 we need to perform a similar derivation to those of the previous chapters. If we recall equation (**??**) and let $k = 7$ we see

$$P_7(q) = \sum_{n=0}^{\infty} p_7(n)q^n = \prod_{n=1}^{\infty} \frac{(1-q^{7n})}{(1-q^n)}.$$

We know that $1 - q^{7n} \equiv (1-q^n)^7 \bmod 7$. So

$$\sum_{n=0}^{\infty} p_7(n)q^n \equiv \prod_{n=1}^{\infty} \frac{(1-q^n)^7}{(1-q^n)} \mod 7.$$

We reduce this to find

$$\sum_{n=0}^{\infty} p_7(n)q^n \equiv \left(\prod_{n=1}^{\infty} 1-q^n\right)^6 \mod 7.$$

Recalling Theorem (2.2),

$$\sum_{n=0}^{\infty} p_7(n)q^n \equiv \left(\sum_{k\geq 0} (-1)^k(2k+1)q^{\frac{k^2+k}{2}}\right)^2 \mod 7.$$

We can write this as a double sum

$$\sum_{n=0}^{\infty} p_7(n)q^n \equiv \sum_{k,\ell\geq 0} (-1)^{k+\ell}(2k+1)(2\ell+1)q^{\frac{k^2+k}{2}+\frac{\ell^2+\ell}{2}} \mod 7.$$

Equating coefficients we find

$$p_7(n) \equiv \sum_{\frac{k^2+k}{2}+\frac{\ell^2+\ell}{2}=n} (-1)^{k+\ell}(2k+1)(2\ell+1) \mod 7. \tag{3.1}$$

This tells us that we need to study the number of ways of writing an integer as the sum of two triangular numbers. Fortunately Ewell has proven the following theorem [Ew]:

**Theorem 3.1** *A positive integer $n$ can be written as a sum of two triangular numbers if and only if when $4n+1$ is expressed as a product of prime-powers, every prime factor $q \equiv 3 \mod 4$ occurs with even exponent.*

This result, along with numerical data, leads us to consider primes congruent to 3 modulo 4.

**Theorem 3.2** *$p_7(q^2m+b) \equiv 0 \mod 7$, for all natural numbers $m$, where $q$ is a prime for which $q \equiv 3 \mod 4$ with $b$ satisfying $q \parallel 4b+1$.*

**Proof:**
We know that $n = q^2m + b$ where $q \equiv 3 \bmod 4$. Now we will analyze $4n+1$.

$$4n+1 = 4(q^2m+b)+1 = 4q^2m+4b+1.$$

Since $q \parallel 4b+1$ we can factor out exactly one $q$, so

$$4n+1 = q\left(4qm + \frac{4b+1}{q}\right).$$

But because $q \equiv 3 \bmod 4$ and $ord_q(n) = 1$, we can now apply Theorem 3.1 to find that $n$ cannot be written as a sum of two triangular numbers. If we recall equation (**??**)

$$p_7(n) \equiv \sum_{\frac{k^2+k}{2}+\frac{\ell^2+\ell}{2}=n} (-1)^{k+\ell}(2k+1)(2\ell+1) \mod 7,$$

we see that this sum has no terms, thus it is equal to zero. Therefore

$$p_7(q^2m+b) \equiv 0 \mod 7 \quad \square$$

Numerical data shows that similar congruence relations do not exist for primes congruent to one modulo four. Theorem 3.2 provides an infinite number of congruences, a few of which we will make explicit as a corollary by assigning values to $q$.

**Corollary 3**

1. $p_7(3^2m + b) \equiv 0 \mod 7$, *for all natural numbers* $m$, *with* $b$ *satisfying* $b \equiv 2 \mod 3$ *for which* $b \not\equiv 2 \mod 3^2$.
2. $p_7(7^2m + b) \equiv 0 \mod 7$, *for all natural numbers* $m$, *with* $b$ *satisfying* $b \equiv 5 \mod 7$ *for which* $b \not\equiv 12 \mod 7^2$.
3. $p_7(11^2m + b) \equiv 0 \mod 7$, *for all natural numbers* $m$, *with* $b$ *satisfying* $b \equiv 8 \mod 11$ *for which* $b \not\equiv 30 \mod 11^2$.

## Conjectures:

We have proven theorems of the form $p_k(q^2m+b) \equiv 0 \bmod k$ for $k = 3, 5, 7$. But our numerical data suggests that even stronger congruences exist.

**Conjecture 4.1** $p_3(q^2m+b) \equiv 0 \mod 9$, *for all natural numbers* $m$, *where* $q$ *is a prime for which* $q \equiv 5 \mod 12$ *with* $b$ *satisfying* $q \parallel 24b+2$.

**Conjecture 4.2** $p_5(q^2m+b) \equiv 0 \mod 25$, *for all natural numbers* $m$, *where* $q$ *is a prime for which* $q \equiv 5 \mod 6$ *with* $b$ *satisfying* $q \parallel 24b+4$.

Obviously these stronger relations are much harder to prove. We attempted to prove the first conjecture by making a natural alteration to our method in Chapter 1. The sketch of this method is as follows [Mi].

We start with the generating function, as before.
Knowing $(1-q^3) = (1-q)^3 + 3q(1-q)$, we get

$$\sum_{n=0}^{\infty} p_3(n)q^n = \prod_{n=1}^{\infty} \frac{(1-q^n)^3 + 3q^n(1-q^n)}{(1-q^n)}.$$

Which reduces to

$$\sum_{n=0}^{\infty} p_3(n)q^n \equiv \left(\prod_{n=1}^{\infty} 1-q^n\right)^2 \left(1+3\sum_{n=1}^{\infty} \frac{q^n}{(1-q^n)^2}\right) \mod 9. \tag{4.1}$$

We want to analyze $\sum_{n=1}^{\infty} \frac{q^n}{(1-q^n)^2}$ in order to simplify equation (**??**).

$$\begin{aligned}
\sum_{n=1}^{\infty} \frac{q^n}{(1-q^n)^2} &= \sum_{n,j\geq 1} j(q^n)^j \qquad \text{(by The Binomial Theorem)} \\
&= \sum_{m\geq 1} \sum_{nj=m} jq^m \quad \text{(replacing } nj \text{ with } m\text{)} \\
&= \sum_{m\geq 1} q^m \sum_{j|m} j \qquad \text{(realizing } (nj=m) \Rightarrow \ell \mid m\text{)} \\
&= \sum_{m\geq 1} q^m \sigma(m) \qquad \text{(where } \sigma(m) \text{ is the sum of divisors function)}
\end{aligned}$$

We can also substitute for the first term in equation (**??**) using Theorem 0.1. For simplicity let's call this sum $S(n)$. Combining all these steps together we can rewrite equation (**??**), equate coefficients and get

$$p_3(n) \equiv S(n) + 3\sum_{m=1}^{\infty} S(n-m)\sigma(m) \mod 9. \tag{4.2}$$

Where

$$S(n) = \sum_{\frac{k(3k-1)}{2}+\frac{\ell(3\ell-1)}{2}=n} (-1)^{k+\ell}.$$

At this point our analysis from Chapter 1 will be sufficient to show $S(n)$ is zero for the appropriate $n$. The remaining portion of the proof would consist of showing the second sum in equation 4.2 is equivalent to zero modulo three. Proving modulo three is sufficient because the sum is multiplied by a three. But we have not yet been able to prove this congruence.

We believe that the proof for Conjecture 4.2 will be similar.

## References:


[Ew] J. Ewell (1992). *On Sums of Triangular Numbers and Sums of Squares*, American Mathematical Monthly 99, 752-757.

[HW] G.H. Hardy and E.M. Wright. *An Introduction to the Theory of Numbers*, (Clarendon, 1979).

[Ja] T. Jackson. *From Polynomials to Sums of Squares*, (IOP Publishing, 1995).

[Mi] C. Mihelich (2001). Private Conversation.

[Ra] S. Ramanujan (1919). *Some Properties of p(n), the Number of Partitions of n*, Proc. Cam. Phil. Soc., 207-210.

[Th] K. Thanigasalam (1974). *Congruence Properties of Certain Restricted Partition Functions*, Mathematics Magazine 47, 154-155.