Congruence Properties of Partitions: Part 1

Introduction

We know that *any positive integer greater than* 1 *can be expressed as a product of prime numbers in a unique fashion ignoring the order of factors*. This is one of the most basic results in number theory and is aptly called *the fundamental theorem of arithmetic*. This result also shows that prime numbers are the building blocks for all integers and this justifies the importance given to prime numbers in number theory.

Let's now ponder what happens when we think from an *additive* point of view. Suppose we wish to express a positive integer as a sum of other positive integers. For example we can write:

$$3 = 1 + 1 + 1 = 1 + 2$$
$$4 = 1 + 1 + 1 + 1 = 1 + 1 + 2 = 1 + 3 = 2 + 2$$
$$5 = 1 + 1 + 1 + 1 + 1 = 1 + 1 + 1 + 2 = 1 + 1 + 3 = 1 + 4 = 1 + 2 + 2 = 2 + 3$$

therefore 3 can be expressed as sum of other positive integers in 3 different ways, 4 can be expressed so in 5 different ways and 5 can be expressed so in 7 different ways. Here the order of summands is not taken into consideration. We say that each of the unordered tuples $(3), (1, 1, 1)$ and $(1, 2)$ is a *partition* of the number 3. Each individual element of the tuple is called a part of the partition. In general a tuple $(a_1, a_2, \ldots, a_k)$ of positive integers a_i is called a ***partition of a positive integer*** n if

$$a_1 \leq a_2 \leq \cdots \leq a_k$$

and

$$a_1 + a_2 + \cdots + a_k = n$$

In this case we say that the partition has k parts $a_1, a_2, \ldots, a_k$. From the definition and examples above we can see that the parts of a partition can be repeated. Given a positive integer n, the *number of all possible partitions of* n is denoted by $p(n)$. This function $p(n)$ is one of most important arithmetical functions in advanced number theory. It is easy to calculate the values of $p(n)$ for small n by direct enumeration of all partitions of n. From the examples given above it follows that $p(3) = 3, p(4) = 5, p(5) = 7$.

As the value of n increases it is difficult to enumerate all the partitions of a given number (there is always a chance of missing out some partition, as the reader may figure out by trying to enumerate partitions of 10) and hence there is some difficulty in finding the value of $p(n)$ as n increases. To tackle this problem we will find out the generating function of $p(n)$.

The Generating Function for $p(n)$

Suppose first that the problem is simplified. We will limit the partitions by limiting the highest part. So let's denote by $p_k(n)$ the number of partitions of n with highest part equal to k. First

we start with partitions with parts not greater than 1 and then it is easy to see that each number will have only one partition consisting of all 1's i.e. we can write $n = n \cdot 1$. Now we note that we have

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

It therefore follows that

$$\frac{1}{1-x} = 1 + \sum_{n=1}^{\infty} p_1(n)x^n$$

If we now allow partitions with parts upto 2 then we need to express n in the form $n = n_1 \cdot 1 + n_2 \cdot 2$. Since

$$\frac{1}{1-x} = 1 + x + x^2 + \cdots = \sum_{n=0}^{\infty} x^{n\cdot 1}$$
$$\frac{1}{1-x^2} = 1 + x^2 + x^4 + \cdots = \sum_{n=0}^{\infty} x^{n\cdot 2}$$

it follows that

$$\frac{1}{(1-x)(1-x^2)} = 1 + \sum_{n_1\cdot 1 + n_2\cdot 2 = n} x^n = 1 + \sum_{n=1}^{\infty} p_2(n)x^n$$

Proceeding in the same fashion we can see that

$$\frac{1}{(1-x)(1-x^2)\cdots(1-x^k)} = 1 + \sum_{n=1}^{\infty} p_k(n)x^n$$

and therefore if we let $k \to \infty$ so that $p_k(n)$ becomes $p(n)$ it follows that

$$\frac{1}{(1-x)(1-x^2)(1-x^3)(1-x^4)\cdots} = 1 + \sum_{n=1}^{\infty} p(n)x^n$$

Setting $p(0) = 1$ (as a convenient convention) we have

$$\sum_{n=0}^{\infty} p(n)x^n = \frac{1}{(1-x)(1-x^2)(1-x^3)(1-x^4)\cdots}$$

Following the standard practice we switch to the variable q and then we can write the generating function of $p(n)$ as:

$$\sum_{n=0}^{\infty} p(n)q^n = \frac{1}{(1-q)(1-q^2)(1-q^3)(1-q^4)\cdots} = \frac{1}{\prod_{n=1}^{\infty}(1-q^n)} \tag{1}$$

Recursion for $p(n)$ via Euler's Pentagonal Theorem

Using *Euler's Pentagonal Theorem* (established in a previous post) we have

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

and from equation (1) above we deduce

$$\left(\sum_{n=0}^{\infty}p(n)q^n\right)\left(\sum_{n=-\infty}^{\infty}(-1)^n q^{(3n^2+n)/2}\right)=1$$

$$\Rightarrow \left(1+\sum_{n=1}^{\infty}p(n)q^n\right)\left(1+\sum_{n=1}^{\infty}(-1)^n\{q^{(3n^2-n)/2}+q^{(3n^2+n)/2}\}\right)=1$$

Equating coefficients of q^n for $n\geq 1$ we see that

$$p(n)-p(n-1)-p(n-2)+p(n-5)+p(n-7)-p(n-12)-p(n-15)+\cdots=0$$

Hence we arrive at

$$p(n)=\sum_{k=1}^{\infty}(-1)^{n+1}\left\{p\left(n-\frac{3k^2-k}{2}\right)+p\left(n-\frac{3k^2+k}{2}\right)\right\} \tag{2}$$

where the sum on right is actually a finite sum with the convention that $p(0)=1$ and $p(n)=0$ if n is negative.

Thus we have

$$\begin{aligned}
p(6)&=p(5)+p(4)-p(1)=7+5-1=11\\
p(7)&=p(6)+p(5)-p(2)-p(0)=11+7-2-1=15\\
p(8)&=p(7)+p(6)-p(3)-p(1)=15+11-3-1=22\\
p(9)&=p(8)+p(7)-p(4)-p(2)=22+15-5-2=30\\
p(10)&=p(9)+p(8)-p(5)-p(3)=30+22-7-3=42\\
p(11)&=p(10)+p(9)-p(6)-p(4)=42+30-11-5=56\\
p(12)&=p(11)+p(10)-p(7)-p(5)+p(0)=56+42-15-7+1=77
\end{aligned}$$

British mathematician P. A. MacMahon calculated the values of $p(n)$ for $n=1$ to $n=200$ using the above method. We reproduce a part of the table below:

n	$p(n)$	n	$p(n)$	n	$p(n)$
1	1	16	231	31	6842
2	2	17	297	32	8349
3	3	18	385	33	10143
4	5	19	490	34	12310
5	7	20	627	35	14883
6	11	21	792	36	17977
7	15	22	1002	37	21637
8	22	23	1255	38	26015
9	30	24	1575	39	31185
10	42	25	1958	40	37338
11	56	26	2436	41	44583
12	77	27	3010	42	53174
13	101	28	3718	43	63261
14	135	29	4565	44	75175
15	176	30	5604	45	89134

Ramanujan studied the table prepared by MacMahon and found various congruence properties of the partitions and then proved them using a variety of techniques. This we study next.

Congruence Properties of $p(n)$

Just by looking at the table of partitions above Ramanujan was able to spot patterns which revealed certain congruences. Simplest and notable among these are the following three:

$$p(5n+4) \equiv 0 \pmod{5} \tag{3}$$
$$p(7n+5) \equiv 0 \pmod{7} \tag{4}$$
$$p(11n+6) \equiv 0 \pmod{11} \tag{5}$$

Ramanujan provided three proofs for $(3), (4)$ and one proof for (5). We will provide two proofs each of $(3), (4)$ and one proof of (5). All of these proofs provided by Ramanujan are highly economical involving simplest machinery and manipulation. None of the other proofs which I have found in literature are simpler than that provided by Ramanujan and besides the modern proofs are full of unnecessary symbolism.

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

Before presenting the proof of this congruence we need a q-series identity which can be established using Jacobi's theta functions. Using series expansion of $\theta_1(z, q)$ from this post and its product expansion from this post we have

$$\begin{aligned}\theta_1(z,q) &= 2q^{1/4}\sum_{n=0}^{\infty}(-1)^n q^{n(n+1)}\sin(2n+1)z\\ &= 2q^{1/4}\sin z\prod_{n=1}^{\infty}(1-q^{2n})(1-2q^{2n}\cos 2z+q^{4n})\end{aligned}$$

Dividing the above equation by $2q^{1/4}z$ and then taking limits as $z \to 0$ we get

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

Replacing q^2 by q we get

$$\prod_{n=1}^{\infty}(1-q^{n})^3 = \sum_{n=0}^{\infty}(-1)^n(2n+1)q^{n(n+1)/2} \tag{6}$$

First Proof: Ramanujan starts with the expression $q\{(1-q)(1-q^2)(1-q^3)\cdots\}^4$ and simplifies it using Euler's Pentagonal theorem and equation (6) above

$$\begin{aligned}q\{(1-q)(1-q^2)(1-q^3)\cdots\}^4 &= q(1-3q+5q^3-\cdots)(1-q-q^2+q^5+q^7-\cdots)\\ &= q\sum_{m=0}^{\infty}(-1)^m(2m+1)q^{m(m+1)/2}\sum_{n=-\infty}^{\infty}(-1)^n q^{(3n^2+n)/2}\\ &= \sum_{m=0}^{\infty}\sum_{n=-\infty}^{\infty}(-1)^{m+n}(2m+1)q^{m(m+1)/2+(3n^2+n)/2+1}\end{aligned}$$

In this expansion Ramanujan analyzes the powers of q which are multiples of 5. Clearly we have

$$\begin{aligned}
&\frac{m(m+1)}{2}+\frac{n(3n+1)}{2}+1\equiv 0 \pmod 5\\
\Leftrightarrow\ &8+4m(m+1)+4n(3n+1)\equiv 0 \pmod 5\\
\Leftrightarrow\ &3+4m(m+1)+4n(3n+1)\equiv 0 \pmod 5\\
\Leftrightarrow\ &(2m+1)^2+2+12n^2+4n\equiv 0 \pmod 5\\
\Leftrightarrow\ &(2m+1)^2+2n^2+4n+2\equiv 0 \pmod 5\\
\Leftrightarrow\ &(2m+1)^2+2(n+1)^2\equiv 0 \pmod 5
\end{aligned}$$

Clearly $(2m+1)^2$ can take the values $0,1,4$ modulo 5 and $2(n+1)^2$ can take values $0,2,3$ modulo 5 and therefore the only way the above condition can be satisfied is when both $(2m+1)^2$ and $2(n+1)^2$ take value 0 modulo 5. This means that we must have $(2m+1)\equiv 0 \pmod 5$.

Thus it is established that the coefficient of q^{5n} in the expansion of

$$q\{(1-q)(1-q^2)(1-q^3)\cdots\}^4$$

is a multiple of 5. Now Ramanujan uses a formal technique which is very helpful here. Following Ramanujan we write

$$\sum a_nq^n\equiv\sum b_nq^n \pmod c$$

if

$$a_n\equiv b_n \pmod c$$

for all values of n.

It is easy to see that under the above conditions we can multiply both sides of congruence by any power series and the congruence would remain valid. Also if the first coefficient (i.e. constant term) of each series is 1 then we can take reciprocals and new series will also have integer coefficients and the congruence would remain valid after taking reciprocals.

Now it is quite obvious that

$$\begin{aligned}
&(1-q)^5\equiv 1-q^5 \pmod 5\\
\Rightarrow\ &\frac{1}{(1-q)^5}\equiv\frac{1}{1-q^5} \pmod 5\\
\Rightarrow\ &\frac{1-q^5}{(1-q)^5}\equiv 1 \pmod 5
\end{aligned}$$

Using the above identity repeatedly replacing q by $q^2,q^3,\ldots$ and multiplying these together we get

$$\frac{(1-q^5)(1-q^{10})(1-q^{15})\cdots}{\{(1-q)(1-q^2)(1-q^3)\cdots\}^5}\equiv 1 \pmod 5$$

We can now easily see that the coefficient of q^{5n} in the expression

$$\frac{q(1-q^5)(1-q^{10})(1-q^{15})\cdots}{(1-q)(1-q^2)(1-q^3)\cdots}$$
$$= q\{(1-q)(1-q^2)(1-q^3)\cdots\}^4\frac{(1-q^5)(1-q^{10})(1-q^{15})\cdots}{\{(1-q)(1-q^2)(1-q^3)\cdots\}^5}$$

is a multiple of 5. Since the expression $(1-q^5)(1-q^{10})(1-q^{15})\cdots$ consists of terms of the form q^{5n} with coefficients ± 1, it follows that the coefficient of q^{5n} in the expression

$$\frac{q}{\{(1-q)(1-q^2)(1-q^3)\cdots\}} = \sum_{n=0}^{\infty} p(n)q^{n+1}$$

is divisible by 5. We therefore have $p(5n+4) \equiv 0 \pmod 5$ for all $n \geq 0$.

Second Proof: Ramanujan uses his functions P, Q, R to provide another proof of the congruence identity modulo 5. Again he introduces a new formal technique by using symbol J to represent any power series with integral coefficients. Thus sums and products of J can also be written as J and that helps a lot in simplifications needed in the proof.

We begin by definitions of P, Q, R:

$$P(q) = 1 - 24\sum_{n=1}^{\infty}\frac{nq^n}{1-q^n}$$
$$Q(q) = 1 + 240\sum_{n=1}^{\infty}\frac{n^3q^n}{1-q^n}$$
$$R(q) = 1 - 504\sum_{n=1}^{\infty}\frac{n^5q^n}{1-q^n}$$

Various properties of P, Q, R are proved in these posts and the reader should visit them if needed.

We have from the definitions:

$$Q = 1 + 5J$$

and since $n^5 - n \equiv 0 \pmod 5$ it follows that

$$R = P + 5J$$

and therefore

$$Q^3 - R^2 = Q(1+5J)^2 - (P+5J)^2 = Q - P^2 + 5J = -12q\frac{dP}{dq} + 5J \quad (7)$$

Now let $f(q) = (1-q)(1-q^2)(1-q^3)\cdots$ so that

$$\sum_{n=0}^{\infty} p(n)q^n = \frac{1}{f(q)}$$

and we can now rewrite (7) as

$$1728q\{f(q)\}^{24} = -12q\frac{dP}{dq} + 5J \tag{8}$$

Again it is easy to observe that

$$\begin{aligned}(1-q)^5 &= 1 - q^5 + 5J\\ \Rightarrow (1-q)^{25} &= (1-q^5+5J)^5 = (1-q^5)^5 + 5J = 1 - q^{25} + 5J\end{aligned}$$

Now replacing q by $q^2, q^3, \ldots$ and then on multiplying the resulting equations we get

$$\begin{aligned}\{f(q)\}^{25} &= f(q^{25}) + 5J\\ \Rightarrow \{f(q)\}^{24} &= \frac{f(q^{25})}{f(q)} + 5J\end{aligned}$$

and from equation (8) we now obtain

$$\begin{aligned}1728q\frac{f(q^{25})}{f(q)} &= -12q\frac{dP}{dq} + 5J\\ \Rightarrow 1728q\left(\sum_{n=0}^{\infty}p(n)q^n\right) &= -12q\frac{dP}{dq}\left(\sum_{n=0}^{\infty}p(n)q^{25n}\right) + 5J\end{aligned}$$

Since P has integer coefficients it follows that the coefficient of q^{5n} in qdP/dq is divisible by 5 and therefore the coefficient of q^{5n} in the RHS of the last equation is divisible by 5. It follows that $p(5n-1) \equiv 0 \pmod 5$ or equivalently $p(5n+4) \equiv 0 \pmod 5$.

If we compare the two proofs above we find that the first proof is really elementary and does not require anything beyond the Euler's Pentagonal theorem whereas the second proof depends upon the theory of P, Q, R which lies somewhat deeper in the theory of elliptic functions. At the same time one can not help wondering at Ramanujan's use of the highly economical tool of congruence of power series based on the congruence of their coefficients (the J technique expresses this same congruence of power series in even simpler notation). In the next post we will deal with the partition congruences related to modulo 7 and 11.

By Paramanand Singh
Thursday, June 20, 2013

Labels: Lambert Series , Mathematical Analysis , Number Theory