CONGRUENCES AND DIVISIBILITY

Contents

1 Lecture Notes

1.1 Introduction

Our main object of study is the **partition function** $p(n)$. The definition of $p(n)$ is purely combinatorial.

Definition 1. *Let n be a positive integer. The partition function $p(n)$ is defined as*

$$p(n) = \#\{(a_1, \cdots, a_k) : k \geq 1, 1 \leq a_1 \leq a_2 \leq \cdots \leq a_k, a_1 + \cdots + a_k = n, a_i \in \mathbb{Z}^+\},$$

the number of all possible partitions of n, where permutations of a partition are counted as the same.

For example, all possible partitions of the first five integers are

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

So the sequence $p(n)$ starts as(by convention $p(0) = 1$)

$$1, 1, 2, 3, 5, 7, 11, 15, 22, \cdots .$$

There's a plethora of result about $p(n)$. We will focus the congruence pattern of $p(n)$. For example, the Fibonacci numbers

$$1, 1, 2, 3, 5, 8, 13, 21, 34, \cdots$$

has a clear parity pattern

$$1, 1, 0, 1, 1, 0, 1, 1, 0, \cdots .$$

Let's examine the parity pattern of $p(n)$, which is given by

$$1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, \cdots$$

Seems strange? Let's try mod 3

$$1, 1, 1, 2, 0, 2, 1, 2, 0, 2, 0, \cdots$$

However, Ramanujan looked further, and discovered a remarkable pattern.

Theorem 2. *For any positive integer n, we have*

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

$$p(7n+5) \equiv 0(\text{mod}7),$$

$$p(11n+6) \equiv 0(\text{mod}11).$$

1.2 Proof of Ramanujan Congruence mod 5

We will prove the Ramanujan Congruences via generating functions, following Hirschhorn in *A short and simple proof of Ramanujan's mod11 partition congruence.* We look at the generating function in q

$$\sum_{n=0}^{\infty} p(n)q^n.$$

Then we can show that

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

The denominator is usually denoted by $(q:q)_\infty$. We now note several important formulas, dating back to Euler and Jacobi.

Theorem 3.

$$(q:q)_\infty = \sum_{n\in\mathbb{Z}} (-1)^n q^{(3n^2+n)/2}.$$

$$(q:q)_\infty^3 = \sum_{n=0}^{\infty} (-1)^n (2n+1) q^{(n^2+n)/2}.$$

Now write

$$\sum_{n=0}^{\infty} p(n)q^n = \frac{(q:q)_\infty (q:q)_\infty^3}{(q:q)_\infty^5}.$$

And modulo 5 on both sides.

1.3 The Jacobi Triple Product Identity

It remains to show Theorem 3. It is a special case of the following result.

Theorem 4 (Jacobi Triple Product)**.** *The following holds as formal series*

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

1.4 Ramanujan's Original Proof

Finally, we briefly describe how Ramanujan showed these congruences in the first place. For more details, see *Ramanujan's Unpublished Manuscript on the Partition and Tau Functions with Proofs and Commentary* by Berndt and Ono.

In fact we will show something stronger.

Theorem 5.

$$p(25n-1) \equiv 0 (\text{mod} 25)$$

Proof. Define

$$P = 1 - 24 \sum_{n=1}^{\infty} \sigma_1(n) q^n,$$

$$Q = 1 + 240 \sum_{n=1}^{\infty} \sigma_3(n) q^n,$$

$$R = 1 - 504 \sum_{n=1}^{\infty} \sigma_5(n) q^n.$$

These are called Eisenstein series. Ramanujan noted the following identities[1].

$$Q^3 - R^2 = 1728 q (q:q)_{\infty}^{24},$$

$$Q^2 - PR = 1008 \sum_{n=1}^{\infty} n \sigma_5(n) q^n$$

$$Q - P^2 = 288 \sum_{n=1}^{\infty} n \sigma_1(n) q^n.$$

Can you now finish the proof for Ramanujan? □

1.5 Further works

Atkin: Ramanujan congruence for all powers of $5, 7, 11$, and Ramanujan congruence modulo 13:

$$p(11^3 \cdot 13n + C) \equiv 0 (\text{mod} 13).$$

Ono: Ramanujan congruence for all primes $m \geq 13$. But not explicit.

Radu(Subbarao's Conjecture): Ramanujan congruence **does not exist** modulo $2, 3$.

[1] These identities are not that surprising once you learned the basics of modular forms

2 Exercises

1. The Ramanujan τ function is defined as the coefficient of the series

$$\sum_{n=1}^{\infty} \tau(n) q^n = q(q:q)_\infty^{24}.$$

Ramanujan studied $\tau(n)$ alongside $p(n)$, and obtained a fountain of results. Here you can prove some of them.

- Show that $\tau(n) \equiv n\sigma_1(n) (\mathrm{mod} 2)$.
- Show that $\tau(n) \equiv n\sigma_1(n) (\mathrm{mod} 3)$.
- Show that $\tau(n) \equiv n\sigma_1(n) (\mathrm{mod} 5)$.

2. Let $n_1, n_2, \ldots, n_s$ be distinct integers such that

$$(n_1 + k)(n_2 + k) \cdots (n_s + k)$$

is an integral multiple of $n_1 n_2 \cdots n_s$ for every integer k. For each of the following assertions, give a proof or a counterexample:

- $|n_i| = 1$ for some i.
- If further all n_i are positive, then

$$\{n_1, n_2, \ldots, n_s\} = \{1, 2, \ldots, s\}.$$

3. How many coefficients of the polynomial

$$P_n(x_1, \ldots, x_n) = \prod_{1 \le i < j \le n} (x_i + x_j)$$

are odd?

4. If p is a prime number greater than 3 and $k = \lfloor 2p/3 \rfloor$, prove that the sum

$$\binom{p}{1} + \binom{p}{2} + \cdots + \binom{p}{k}$$

of binomial coefficients is divisible by p^2.

5. Do there exist positive integers a and b with $b - a > 1$ such for every $a < k < b$, either $\gcd(a, k) > 1$ or $\gcd(b, k) > 1$?

6. Suppose that $f(x)$ and $g(x)$ are polynomials (with $f(x)$ not identically 0) taking integers to integers such that for all $n \in \mathbb{Z}$, either $f(n) = 0$ or $f(n)|g(n)$. Show that $f(x)|g(x)$, i.e., there is a polynomial $h(x)$ with rational coefficients such that $g(x) = f(x)h(x)$.

7. Let q be an odd positive integer, and let N_q denote the number of integers a such that $0 < a < q/4$ and $\gcd(a, q) = 1$. Show that N_q is odd if and only if q is of the form p^k with k a positive integer and p a prime congruent to 5 or 7 modulo 8.

8. Let p be in the set $\{3, 5, 7, 11, \dots\}$ of odd primes, and let

$$F(n) = 1 + 2n + 3n^2 + \cdots + (p-1)n^{p-2}.$$

Prove that if a and b are distinct integers in $\{0, 1, 2, \dots, p-1\}$ then $F(a)$ and $F(b)$ are not congruent modulo p, that is, $F(a) - F(b)$ is not exactly divisible by p.

9. Do there exist 1,000,000 consecutive integers each of which contains a repeated prime factor?

10. A positive integer n is *powerful* if for every prime p dividing n, we have that p^2 divides n. Show that for any $k \geq 1$ there exist k consecutive integers, none of which is powerful.

11. Show that for any $k \geq 1$ there exist k consecutive positive integers, none of which is a sum of two squares. (You may use the fact that a positive integer n is a sum of two squares if and only if for every prime $p \equiv 3 \pmod 4$, the largest power of p dividing n is an even power of p.)

12. Prove that every positive integer has a multiple whose decimal representation involves all ten digits.

13. Prove that among any ten consecutive integers at least one is relatively prime to each of the others.

14. Find the length of the longest sequence of equal nonzero digits in which an integral square can terminate (in base 10), and find the smallest square which terminates in such a sequence.

15. Show that if n is an integer greater than 1, then n does not divide $2^n - 1$.

16. Show that if n is an odd integer greater than 1, then n does not divide $2^n + 2$.

17. * For positive integer a, we define the series

$$f_a(q) = \sum_{k \geq 0, ak+1 \text{ is a square}} q^k.$$

Find all positive integer triples (a, b, c) such that

$$f_a(q) \equiv f_b(q) f_c(q) \mod 2$$

which means that the corresponding coefficients match modulo 2. (**Hint**: Use a computer to find a few triple, then look for patterns.)

18. Define a sequence $\{a_i\}$ by $a_1 = 3$ and $a_{i+1} = 3^{a_i}$ for $i \geq 1$. Which integers between 00 and 99 inclusive occur as the last two digits in the decimal expansion of infinitely many a_i?

19. What is the units (i.e., rightmost) digit of

$$\left[\frac{10^{20000}}{10^{100} + 3} \right]?$$

Here $[x]$ is the greatest integer $\leq x$.

20. Suppose p is an odd prime. Prove that

$$\sum_{j=0}^{p} \binom{p}{j} \binom{p+j}{j} \equiv 2^p + 1 \pmod{p^2}.$$

21. Prove that for $n \geq 2$,

$$\overbrace{2^{2^{\cdots^{2}}}}^{n \text{ terms}} \equiv \overbrace{2^{2^{\cdots^{2}}}}^{n-1 \text{ terms}} \pmod{n}.$$

22. The sequence $(a_n)_{n\geq 1}$ is defined by $a_1 = 1$, $a_2 = 2$, $a_3 = 24$, and, for $n \geq 4$,

$$a_n = \frac{6a_{n-1}^2 a_{n-3} - 8a_{n-1}a_{n-2}^2}{a_{n-2}a_{n-3}}.$$

Show that, for all n, a_n is an integer multiple of n.

23. Prove that the expression

$$\frac{\gcd(m,n)}{n}\binom{n}{m}$$

is an integer for all pairs of integers $n \geq m \geq 1$.

24. Show that for each positive integer n,

$$n! = \prod_{i=1}^{n} \operatorname{lcm}\{1, 2, \ldots, \lfloor n/i \rfloor\}.$$

(Here lcm denotes the least common multiple, and $\lfloor x \rfloor$ denotes the greatest integer $\leq x$.)

25. Define a sequence $\{u_n\}_{n=0}^{\infty}$ by $u_0 = u_1 = u_2 = 1$, and thereafter by the condition that

$$\det \begin{pmatrix} u_n & u_{n+1} \\ u_{n+2} & u_{n+3} \end{pmatrix} = n!$$

for all $n \geq 0$. Show that u_n is an integer for all n. (By convention, $0! = 1$.)

26. Let p be a prime number. Let $h(x)$ be a polynomial with integer coefficients such that $h(0), h(1), \ldots, h(p^2-1)$ are distinct modulo p^2. Show that $h(0), h(1), \ldots, h(p^3-1)$ are distinct modulo p^3.

27. * Define $a_0 = a_1 = 1$ and

$$a_n = \frac{1}{n-1}\sum_{i=0}^{n-1} a_i^2, \quad n > 1.$$

Is a_n an integer for all $n \geq 0$?

28. Let $f(x) = a_0 + a_1 x + \cdots$ be a power series with integer coefficients, with $a_0 \neq 0$. Suppose that the power series expansion of $f'(x)/f(x)$ at $x = 0$ also has integer coefficients. Prove or disprove that $a_0 | a_n$ for all $n \geq 0$.

29. For each positive integer n, let S_n denote the set of positive integers $(a_1, \cdots, a_n)$ such that

(1) $a_1 \leq a_2 \leq \cdots \leq a_n$.

(2)

$$\frac{1}{a_1} + \cdots + \frac{1}{a_n} + \frac{1}{a_1 \cdots a_n}$$

is an integer.

Prove that S_n is a finite set, and $|S_n| \geq \frac{n^2}{10}$.

30. Let S be a set of rational numbers such that

   (a) $0 \in S$;

   (b) If $x \in S$ then $x+1 \in S$ and $x-1 \in S$; and

   (c) If $x \in S$ and $x \notin \{0,1\}$, then $1/(x(x-1)) \in S$.

   Must S contain all rational numbers?

31. Prove that for each positive integer n, the number $10^{10^{10^n}} + 10^{10^n} + 10^n - 1$ is not prime.

32. Let p be an odd prime. Show that for at least $(p+1)/2$ values of n in $\{0,1,2,\ldots,p-1\}$, $\sum_{k=0}^{p-1} k!n^k$ is not divisible by p.

33. Let a and b be distinct rational numbers such that $a^n - b^n$ is an integer for all positive integers n. Prove or disprove that a and b must themselves be integers.

34. Find the smallest integer $n \geq 2$ for which there exists an integer m with the following property: for each $i \in \{1,\ldots,n\}$, there exists $j \in \{1,\ldots,n\}$ different from i such that $\gcd(m+i, m+j) > 1$.

35. Let p be an odd prime number such that $p \equiv 2 \pmod 3$. Define a permutation π of the residue classes modulo p by $\pi(x) \equiv x^3 \pmod p$. Show that π is an even permutation if and only if $p \equiv 3 \pmod 4$.

36. Suppose that a positive integer N can be expressed as the sum of k consecutive positive integers

$$N = a + (a+1) + (a+2) + \cdots + (a+k-1)$$

   for $k = 2017$ but for no other values of $k > 1$. Considering all positive integers N with this property, what is the smallest positive integer a that occurs in any of these expressions?

37. Let n be a positive integers. Prove that

$$\sum_{k=1}^{n} (-1)^{\lfloor k(\sqrt{2}-1) \rfloor} \geq 0.$$