3. Number theory

Po-Shen Loh

CMU Putnam Seminar, Fall 2015

1 Classical results

Warm-up. Let p be a prime. Expand $(x+y+z)^p$, reducing the coefficients modulo p.

Fermat. For any prime p and any integer a not divisible by p,

$$a^{p-1} \equiv 1 \pmod{p}.$$

Euler. For any positive integer n and any integer a relatively prime to n,

$$a^{\phi(n)} \equiv 1 \pmod{n},$$

where $\phi(n)$ is the number of integers in $\{1,\ldots,n\}$ that are relatively prime to n.

Wilson. For every prime p, we have $(p-1)! \equiv -1 \pmod{p}$.

Lucas. Let n and k be non-negative integers, with base-p expansions $n = (n_t n_{t-1} \ldots n_0)_{(p)}$ and $k = (k_t k_{t-1} \ldots k_0)_{(p)}$, respectively. Then

$$\binom{n}{k} \equiv \binom{n_t}{k_t} \times \binom{n_{t-1}}{k_{t-1}} \times \cdots \times \binom{n_0}{k_0} \pmod{p}.$$

2 Problems

1. Let p be an odd prime. Expand $(x-y)^{p-1}$, reducing the coefficients modulo p.

2. Does there exist an infinite sequence of positive integers $a_1, a_2, a_3, \ldots$ such that a_m and a_n are relatively prime if and only if $|m-n| = 1$?

3. The sets $\{a_1, a_2, \ldots, a_{999}\}$ and $\{b_1, b_2, \ldots, b_{999}\}$ together contain all the integers from 1 to 1998. For each i, $|a_i - b_i| \in \{1, 6\}$. For example, we might have $a_1 = 18$, $a_2 = 1$, $b_1 = 17$, $b_2 = 7$. Show that $\sum_1^{999} |a_i - b_i| \equiv 9 \pmod{10}$.

4. Let r and s be odd positive integers. The sequence a_n is defined as follows: $a_1 = r$, $a_2 = s$, and a_n is the greatest odd divisor of $a_{n-1} + a_{n-2}$. Show that, for sufficiently large n, a_n is constant and find this constant (in terms of r and s).

5. Let n be an arbitrary positive integer. Show that the following sequence is eventually constant modulo n:

$$2, \quad 2^2, \quad 2^{2^2}, \quad 2^{2^{2^2}}, \quad 2^{2^{2^{2^2}}}, \quad 2^{2^{2^{2^{2^2}}}}, \ldots$$

6. For a positive integer a, define a sequence of integers $x_1, x_2, \ldots$ by letting $x_1 = a$ and $x_{n+1} = 2x_n + 1$ for $n \geq 1$. Let $y_n = 2^{x_n} - 1$. Determine the largest possible k such that for some positive integer a, the numbers $y_1, \ldots, y_k$ are all prime.

7. Show that there exists a set A of positive integers with the following property: for any infinite set S of primes, there exist two positive integers m in A and n not in A, each of which is a product of k distinct elements of S for some $k \geq 2$.

3 Homework

Please write up solutions to two of the problems, to turn in at next week's meeting. One of them may be a problem that we discussed in class. You are encouraged to collaborate with each other. Even if you do not solve a problem, please spend two hours thinking, and submit a list of your ideas.