MATH 8, NUMBER THEORY 8: FERMAT'S LITTLE THEOREM

2021/05/09

The following two results are frequently useful in doing number theory problems:

Theorem (Fermat's Little theorem)**.** *For any prime p and any number a not divisible by p, we have $a^{p-1}-1$ is divisible by p, i.e.*

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

This shows that remainders of $a^k \mod p$ will be repeating periodically with period $p-1$ (or smaller). Note that this only works for prime p.

As a corollary, we get that for any a (including those divisible by p) we have

$$a^p \equiv a \mod p$$

More generally, $a^{k(p-1)+1} \equiv a \mod p$.

Note that the condition that p be prime is important: notice, for example, that $3^{(8-1)} \mod 8$ is congruent to 3, not 1.

There are many proofs of Fermat's little theorem; one of them is given in problem 7 below.

1. Find all integer solutions to the following system of congruences:

$$x \equiv 1 \mod 7$$
$$x \equiv 3 \mod 9$$

2. Find 5^{2021} modulo 11.

3. Prove that $2019^{3000} - 1$ is divisible by 1001. [Hint: you can use Chinese remainder theorem and equality $1001 = 7 * 11 * 13$.]

4. Find the last two digits of 7^{1000}. [Hint: first find what it is mod 2^2 and mod 5^2.]

5. Show that for any integer a, the number $a^{11} - a$ is a multiple of 66

6. Show that the number $111\ldots1$ (16 ones) is divisible by 17. [Hint: can you prove the same about number $999\ldots9$?]

7. Alice decided to encrypt a text by first replacing every letter by a number a between 1–26, and then replacing each such number a by $b = a^7 \mod 31$.

Show that then Bob can decrypt the message as follows: after receiving a number b, he computes b^{13} and this gives him original number a.

8. Let p be a prime number.

(a) Show that for any k, $1 \le k \le p-1$, the binomial coefficient ${}_pC_k$ is divisible by p.

(b) Without using Fermat's little theorem, deduce from the previous part and the binomial theorem that for any a, b we have $(a+b)^p \equiv a^p + b^p \mod p$

(c) Prove that for any a, we have $a^p \equiv a \mod p$. [Hint: $a^p = (1 + 1 + \cdots + 1)^p$]