MATH 8, ASSIGNMENT 25: FERMAT'S LITTLE THEOREM

MAY 5, 2019

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). Noet that this only works for prime p.

As a corollary, we get that for any a 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.

1. Remember that you may use the Chinese Remainder Theorem to help you solve these!
   (a) Find 5^{2021} modulo 11.
   (b) Prove that $2019^{3000}-1$ is divisible by 1001. [Hint: $1001 = 7*11*13$.]
   (c) Find the last two digits of 7^{1000}. [Hint: first find what it is mod 2^2 and mod 5^2.]

2. (a) Show that for any number a which is not divisible by 5 or 7, we have $a^{12} \equiv 1 \mod 35$. [Hint: use Chinese remainder theorem!]
   (b) Show that for any a, $a^{13} \equiv a^{25} \equiv a \mod 35$.

3. (a) Prove that for any integer x, we have $x^5 \equiv x \mod 30$
   (b) Prove that if integers x, y, z are such that $x+y+z$ is divisible by 30, then $x^5+y^5+z^5$ si also divisible by 30.

4. 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.