MATH 8
HANDOUT 24: CONGRUENCES CONTINUED

Reminder: Euclid's algorithm

Recall that as a corollary of Euclid's algorithm we have the following result:

Theorem. *An integer m can be written in the form*

$$m = ax + by$$

if and only if m is the multiple of $\gcd(a, b)$.

Moreover, Euclid's algorithm gives us an explicit way to find x, y. Thus, it also gives us a way of solving congruences

$$ax \equiv m \mod b$$

As a corollary we get this:

Theorem. *Equation*

$$ax \equiv 1 \mod b$$

has a solution if and only if a, b are relatively prime, i.e. if $\gcd(a, b) = 1$.

Problems

1. Find the last two digits of $(2016)^{2019}$.

2. Recall that $n! = 1 \cdot 2 \cdots n$.
  (a) How many times 2 appears in the prime factorization of 25! ?
  (b) In how many zeroes does the number 25! end?

3. (a) Find $10^n \mod 11$ (the answer depends on n)
  (b) Find remainder upon division of 11 of the number 457289 (without doing the long division!).
  (c) Can you suggest a test to check if a number is divisible by 11, of the same sort as the familiar test for divisibility by 3.

4. Prove that for any integer n, $n^9 - n$ is a multiple of 5. [Hint: can you prove it if you know $n \equiv 1 \mod 5$? or if $n \equiv 2 \mod 5$? or …]

5. (a) Find the inverses of the following numbers modulo 14 (if they exist): 3; 9; 19; 21
  (b) Of all the numbers 1–14, how many are invertible modulo 14?

6. (a) Find inverse of 3 modulo 28.
  (b) Solve $3x \equiv 7 \mod 28$ [Hint: multiply both sides by inverse of 3...]

7. Find **all** solutions of the following equations
  (a) $5x \equiv 4 \mod 7$
  (b) $7x \equiv 12 \mod 30$

***8.** (a) Let p be an odd prime. Consider the remainders of numbers $2, 4, 6, \dots, 2(p-1)$ modulo p. Prove that they are all different and that every possible remainder from 1 to $p-1$ appears in this list exactly once. [Hint: if $2x \equiv 2y$, then $2(x-y) \equiv 0$.] Check it by writing this collection of remainders for $p = 7$.
  (b) Use the previous part to show that

$$1 \cdot 2 \cdots (p-1) \equiv 2 \cdot 4 \cdots 2(p-1) \mod p$$

  Deduce from it

$$2^{p-1} \equiv 1 \mod p$$

  (c) Show that for any a which is not a multiple of p, we have

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