MATH 8
ASSIGNMENT 9: CONGRUENCES CONTINUED

NOV. 19, 2017

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

When doing this homework, be careful that you only used the material we had proved or discussed so far — in particular, please do not use the prime factorization. And I ask that you only use integer numbers — no fractions or real numbers.

1. Find the last two digits of $(2016)^{2012}$.

2. 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 ...]

3. (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?

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

5. (a) Prove that if a, b are relatively prime, and $ax \equiv 0 \mod b$ for some x, then $x \equiv 0$.
(b) Prove that if ax is divisible by a prime number p, then one of a, x must be divisible by p (you probably have known this fact for a long time, but without a proof...)

6. Use the previous problem to prove the following: if a, b are relatively prime, and m divisible by a and also divisible by b, then m is divisible by ab. [Hint: $m = ax = by$, so $ax \equiv 0 \mod b$.] Deduce from this that the least common multiple of a, b is ab.

Is it true without the assumption that a, b are relatively prime?

7. Find **all** solutions of the following equations
(a) $5x \equiv 4 \mod 7$
(b) $7x \equiv 12 \mod 30$
(c) In a calendar of some ancient race, all months were exactly 30 days long; however, they used same weeks as we do. If in that calendar, first day of a certain month is Friday, how many weeks will pass before Friday will fall on the 13th day of a month? [Hint: this can be rewritten as some congruence of the form $7x \equiv \dots$, where x is the number of weeks.]

***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

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