MATH 8
ASSIGNMENT 8: CONGRUENCES

NOV 12, 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 $\gcd(a, b)$.

For example, if $a = 18, b = 33$, then the numbers that can be written in the form $18x + 33y$ are exactly the multiples of 3.

To find the values of x, y, one can use Euclid's algorithm; for small a, b, one can just use guess-and-check.

Congruences

We will write

$$a \equiv b \mod m$$

(reads: a is congruent to b modulo m) if a, b have the same reminder upon division by m, or, equivalently, if $a - b$ is a multiple of m. For example

$$9 \equiv 2 \equiv 23 \equiv -5 \mod 7$$

We will occasionally write $a \mod m$ for remainder of a upon division by m.

Congruences can be added and multiplied in the same way as equalities: if

$$a \equiv a' \mod m$$
$$b \equiv b' \mod m$$

then

$$a + b \equiv a' + b' \mod m$$
$$ab \equiv a'b' \mod m$$

For example, since $23 \equiv 2 \mod 7$, we have

$$23^3 \equiv 2^3 \equiv 8 \equiv 1 \mod 7$$

One important difference is that in general, one can not divide both sides of an equivalence by a number: for example, $5a \equiv 0 \mod m$ does not necessarily mean that $a \equiv 0 \mod m$ (see problem 6 below).

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. (a) Find $\gcd(48, 39)$
(b) Solve $48x + 39y = 3$

2. (a) Compute remainders modulo 12 of 5, 5^2, 5^3, ... Find the pattern and use it to compute $5^{1000} \mod 12$
(b) Prove that for any a, m, the sequence of remainders mod m: $a \mod m$, $a^2 \mod m$, ... starts repeating periodically (we will find the period later). [Hint: have you heard of pigeonhole principle?]

3. Find the last digit of 7^{2013}; of 7^{7^7}

4. For each of the following equations, find at least one solution (if exists; if not, explain why)

$$5x \equiv 1 \mod 19$$
$$9x \equiv 1 \mod 24$$
$$9x \equiv 6 \mod 24$$

5. Give an example of a, m such that $5a \equiv 0 \mod m$ but $a \not\equiv 0 \mod m$

6. Show that the equation $ax \equiv 1 \mod m$ has a solution if and only if $\gcd(a, m) = 1$. [Such an x is called the inverse of a modulo m]

7. Find the following inverses
inverse of 2 mod 5
inverse of 5 mod 7
inverse of 7 mod 11