MATH 8
NUMBER THEORY 4: CONGRUENCES

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 a multiple of $\gcd(a, b)$.

For example, if $a = 18$ and $b = 33$, 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

An important way to deduce properties about numbers, and discover fascinating facts in their own right, is the concept of what happens to the pieces leftover after division by a specific integer. The first key fact to notice is that, given some integer m and some remainder $r < m$, all integers n which have remainder r upon division by m have something in common - they can all be expressed as r plus a multiple of m.

Notice next the following facts, given an integer m:

- If $n_1 = q_1m + r_1$ and $n_2 = q_2m + r_2$, then $n_1 + n_2 = (q_1 + q_2)m + (r_1 + r_2)$;
- Similarly, $n_1n_2 = (q_1q_2m + q_1r_2 + q_2r_1)m + (r_1r_2)$.

This motivates the following definition: 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), and then notice that these congruences can be added and multiplied in the same way as equalities: if

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

then

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

Here are some examples:

$$2 \equiv 9 \equiv 23 \equiv -5 \equiv -12 \mod 7$$

$$10 \equiv 100 \equiv 28 \equiv -8 \equiv 1 \mod 9$$

Note: we will occasionally write $a \mod m$ for remainder of a upon division by m.

Since $23 \equiv 2 \mod 7$, we have

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

And because $10 \equiv 1 \mod 9$, we have

$$10^4 \equiv 1^4 \equiv 1 \mod 9$$

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 5 below).

Problems

1. (a) Prove that for any a, m, thefollowing sequence of remainders mod m:
$a \mod m, a^2 \mod m, \ldots\ldots$
starts repeating periodically (we will find the period later). [Hint: have you heard of pigeonhole principle?]
(b) Compute $5^{1000} \mod 12$
(c) Find the last digit of 7^{2012}

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

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

(b) Give an example of a, m such that $5a \equiv 0 \mod m$ but $a \not\equiv 0 \mod m$
(c) If $a \equiv 1$ mod mn, must it be true that $a \equiv 1$ mod m? Provide proof or counterexample.

3. (a) 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. [Hint: Euclid's algorithm!]
(b) Find the following inverses
inverse of $2 \mod 5$
inverse of $5 \mod 7$
inverse of $7 \mod 11$
Inverse of $11 \mod 41$

4. Given integers m, n,
(a) Prove that $(m+1)^n \equiv 1 \mod m$
(b) Given some integer k, determine the value of $(m+1)^0 + (m+1)^1 + (m+1)^2 + ... + (m+1)^k$ mod m
(c) Determine the value of $1111 \mod 9$
(d) Given some integer a written in base 10, determine a method for finding the value of a mod 9.

***5.** Prove that no positive integer solutions exist for the following equations.
(a) $x^3 = x + 10^n$ [Hint: see if you can prove that $x^3 \equiv x$ mod 3]
(b) $x^3 + y^3 = x + y + 10^n$
(c) $x^2 + y^2 = 10^n - 1$ [Hint: can $x^2 \equiv 2$ mod 4?]
(d) $x^{a+1}y^{b+1} = 10^n - 2$