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 $n_1 = q_1 m + r_1$ and $n_2 = q_2 m + r_2$, then $n_1 + n_2 = (q_1 + q_2)m + (r_1 + r_2)$;
- Similarly, $n_1 n_2 = (q_1 q_2 m + q_1 r_2 + q_2 r_1)m + (r_1 r_2)$.

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. Determine whether each of the following congruence statements is true or false.
(a) $5 \cdot 4 \equiv 7 \mod 11$
(b) $4 \cdot 6 \equiv 0 \mod 8$
(c) $12 + 22 \equiv 4 \mod 5$
(d) $4 \cdot 2 + 1 \equiv 5 \cdot 2 + 1 \mod 4$
(e) $1 + 2 + 3 \equiv 4 + 5 + 6 \mod 9$
(f) $4 \cdot 8 \equiv 3 \cdot 9 \mod 5$

2. Solve each of the following congruence equations by finding an integer value for x that makes the equation true.
(a) $2x \equiv 1 \mod 5$
(b) $4x \equiv 2 \mod 6$
(c) $x + 5 \equiv 3 \mod 7$
(d) $x + 5 \equiv 3x \mod 11$

3. (a) Use $10 \equiv -1 \mod 11$ to compute $100 \mod 11$; $100,000,000 \mod 11$. Can you derive the general formula for $10^n \mod 11$?
(b) Without doing long division, compute $1375400 \mod 11$. [Hint: $1375400 = 10^6+3{\cdot}10^5+7{\cdot}10^4 \dots$]

4. (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 following sequence of remainders mod m:
$a \mod m$, $a^2 \mod m$, ...
sooner or later starts repeating periodically (we will find the period later). [Hint: have you heard of pigeonhole principle?]
(c) Find the last digit of 7^{2021}

5. (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 $a \not\equiv 0 \mod m$

6. (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 $11 \mod 41$

7. (a) Find $\gcd(48, 39)$
(b) Solve $48x + 39y = 3$
(c) Find inverse of 39 mod 48.

8. For a positive number n, let $\tau(n)$ (this is Greek letter "tau") be the number of all divisors of n (including 1 and n itself).
Compute
$\tau(10)$
$\tau(77)$
$\tau(p^a)$, where p is prime (the answer, of course, depends on p, a)
$\tau(p^a q^b)$, where p, q are different primes
$\tau(10000)$
$\tau(p_1^{a_1} p_2^{a_2} \dots p_k^{a_k})$, where p_i are distinct primes.