

**MATH 8**  
**ASSIGNMENT 23: CONGRUENCES**

APRIL 7, 2019

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

$$a \equiv b \pmod{m}$$

(reads:  $a$  is *congruent* to  $b$  modulo  $m$ ) if  $a, b$  have the same remainder 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

$$\begin{aligned} a &\equiv a' \pmod{m} \\ b &\equiv b' \pmod{m} \end{aligned}$$

then

$$\begin{aligned} a + b &\equiv a' + b' \pmod{m} \\ ab &\equiv a'b' \pmod{m} \end{aligned}$$

Here are some examples:

$$2 \equiv 9 \equiv 23 \equiv -5 \equiv -12 \pmod{7}$$

$$10 \equiv 100 \equiv 28 \equiv -8 \equiv 1 \pmod{9}$$

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

Since  $23 \equiv 2 \pmod{7}$ , we have

$$23^3 \equiv 2^3 \equiv 8 \equiv 1 \pmod{7}$$

And because  $10 \equiv 1 \pmod{9}$ , we have

$$10^4 \equiv 1^4 \equiv 1 \pmod{9}$$

One important difference is that in general, one can not divide both sides of an equivalence by a number: for example,  $5a \equiv 0 \pmod{m}$  does not necessarily mean that  $a \equiv 0 \pmod{m}$  (see problem 5 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  $\gcd(58, 38)$   
 (b) Solve  $58x + 38y = 4$
2. (a) Prove that for any  $a, m$ , the following sequence of remainders mod  $m$ :  
 $a \bmod m, a^2 \bmod m, \dots$   
 starts repeating periodically (we will find the period later). [Hint: have you heard of pigeonhole principle?]  
 (b) Compute  $5^{1000} \bmod 12$
3. Find the last digit of  $7^{2012}$ ; of  $7^{7^7}$
4. For of the following equations, find at least one solution (if exists; if not, explain why)
 
$$5x \equiv 1 \pmod{19}$$

$$9x \equiv 1 \pmod{24}$$

$$9x \equiv 6 \pmod{24}$$
5. Give an example of  $a, m$  such that  $5a \equiv 0 \pmod{m}$  but  $a \not\equiv 0 \pmod{m}$
6. Show that the equation  $ax \equiv 1 \pmod{m}$  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!]
7. Find the following inverses  
 inverse of 2 mod 5  
 inverse of 5 mod 7  
 inverse of 7 mod 11  
 Inverse of 11 mod 41
8. If  $a \equiv 1 \pmod{mn}$ , must it be true that  $a \equiv 1 \pmod{m}$ ? Provide proof or counterexample.
9. Given integers  $m, n$ ,  
 (a) Prove that  $(m + 1)^n \equiv 1 \pmod{m}$   
 (b) Given some integer  $k$ , determine the value of  $(m + 1)^0 + (m + 1)^1 + (m + 1)^2 + \dots + (m + 1)^k \pmod{m}$   
 (c) Determine the value of  $1111 \pmod{9}$   
 (d) Given some integer  $a$  written in base 10, determine a method for finding the value of  $a \pmod{9}$ .
10. Given a prime  $p$ , let  $a_1, a_2, \dots, a_k$  be a set of positive integers each less than  $p$ . Prove that the product  $a_1 a_2 \dots a_k$  cannot be divisible by  $p$ .