

UMASS AMHERST MATH 471 FALL 2006, F. HAJIR

HOMEWORK 6: CONGRUENCES II

1. True or False: (You don't have to justify)
  - (a)  $2x \equiv 5 \pmod{m}$  has a solution  $x \in \mathbb{Z}$  if and only if  $m$  is odd.
  - (b) For odd integers  $k$ ,  $2x \equiv k \pmod{m}$  has a solution  $x \in \mathbb{Z}$  if and only if  $m$  is odd.
  - (c) For integers  $a, b$ , the congruence  $ax \equiv b \pmod{m}$  has a solution  $x \in \mathbb{Z}$  if and only if  $\gcd(a, m) = 1$ .

2. Recall that we are using the notation  $\{a\}_m = \{a + km \mid k \in \mathbb{Z}\}$ , i.e.  $\{a\}_m \in \mathbb{Z}/m\mathbb{Z}$  is the congruence class of  $a$  modulo  $m$ . For integers  $a$  satisfying  $\gcd(a, m) = 1$ , define

$$\text{order}(\{a\}_m) = \min\{n \geq 1 \mid \{a\}_m^n = \{1\}_m\}.$$

In other words, the order of  $\{a\}_m$  is the smallest positive integer  $n$  such that  $a^n \equiv 1 \pmod{m}$ .

- (a) Why is  $\text{order}(\{a\}_m)$  only defined for  $a$  satisfying  $\gcd(a, m) = 1$ ?
- (b) Prove that when  $\gcd(a, m) = 1$ , the quantity  $\text{order}(\{a\}_m)$  is well-defined by showing that there exists a positive integer  $n$  such that  $\{a\}_m^n = \{1\}_m$ .

Hint: Consider the sequence  $\{a\}_m, \{a\}_m^2, \{a\}_m^3, \dots$ . Can this sequence have infinitely many *distinct* elements? Use your answer to the previous question to show that there exist integers  $1 \leq i < j$  such that  $\{a\}_m^j = \{a\}_m^i$ . Now use the miracle, proved in class, that  $\{a\}_m$  is invertible.

- (c) Again assuming that  $\gcd(a, m) = 1$ , prove that for  $k \geq 1$ ,  $\{a\}_m^k = \{1\}_m$  if and only if  $\text{order}(\{a\}_m) \mid k$ .

DEFINITION: Recall from HW 5 Problem 8 that if  $a \equiv b \pmod{m}$ , then  $\gcd(a, m) = \gcd(b, m)$ . Therefore the following set (called the set of “units modulo  $m$ ”, sometimes denoted  $(\mathbb{Z}/m\mathbb{Z})^\times$  and sometimes  $U(\mathbb{Z}/m\mathbb{Z})$ ) is well-defined:

$$U(\mathbb{Z}/m\mathbb{Z}) = (\mathbb{Z}/m\mathbb{Z})^\times = \{\{a\}_m \in \mathbb{Z}/m\mathbb{Z} \mid \gcd(a, m) = 1\}.$$

We can also write

$$U(\mathbb{Z}/m\mathbb{Z}) = (\mathbb{Z}/m\mathbb{Z})^\times = \{\{a\}_m \mid 1 \leq a \leq m \text{ and } \gcd(a, m) = 1\}.$$

3. For each integer  $m \geq 1$ , define “The Euler  $\varphi$  function” by

$$\varphi(m) = |\{1 \leq a \leq m \mid \gcd(a, m) = 1\}|.$$

- (a) Prove that  $m$  is a prime number if and only if  $\varphi(m) = m - 1$ .
- (b) Compute  $\varphi(m)$  for  $1 \leq m \leq 25$ .
- (c) Find integers  $m, n$  such that  $\varphi(mn) \neq \varphi(m)\varphi(n)$ .
- (d) Use your table to make a guess as to whether the following is true or false:

$$\text{If } \gcd(m, n) = 1, \text{ then } \varphi(mn) = \varphi(m)\varphi(n).$$

4. Suppose  $a, b, c, m, n \in \mathbb{Z}$  and  $\gcd(m, n) = 1$ .

(a) Prove that  $mn|c$  if and only if  $m|c$  and  $n|c$ .

Hint: I have three words for you: Bézout, Bézout, Bézout!

(b) Use (a) to prove that  $a \equiv b \pmod{mn}$  if and only if  $a \equiv b \pmod{m}$  and  $a \equiv b \pmod{n}$ .

5. We continue to assume that  $m, n \in \mathbb{Z}$  and  $\gcd(m, n) = 1$ . Consider the map  $f : \mathbb{Z}/mn\mathbb{Z} \rightarrow (\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z})$  defined by  $f(\{a\}_{mn}) = (\{a\}_m, \{a\}_n)$ . [Recall that if  $X$  and  $Y$  are sets, then the Cartesian product  $X \times Y$  is defined to be the set  $X \times Y = \{(x, y) \mid x \in X, y \in Y\}$ .

(a) Show that  $f$  is well-defined, i.e. show that if  $a, a' \in \mathbb{Z}$  and  $a \equiv a' \pmod{mn}$ , then  $(\{a\}_m, \{a\}_n) = (\{a'\}_m, \{a'\}_n)$ .

(b) Given integers  $r, s \in \mathbb{Z}$ , show that there exists  $x \in \mathbb{Z}$  that simultaneously solves both congruences

$$x \equiv r \pmod{m}, \quad x \equiv s \pmod{n}.$$

Hint: Use, what else?!, Bézout! Write  $mu + nv = 1$  with  $u, v \in \mathbb{Z}$ , then make the *unbelievably* clever choice  $x = mus + nvr$ . Check that this  $x$  works.

(c) Use (b) to show that  $f$  is surjective.

(d) Suppose  $X, Y$  are finite sets of the same size, i.e.  $|X| = |Y|$  and that  $F : X \rightarrow Y$  is a **surjective** map from  $X$  to  $Y$ . Show that  $F$  is injective also, i.e. show that if  $x_1, x_2 \in X$  and  $x_1 \neq x_2$ , then  $F(x_1) \neq F(x_2)$ .

(e) Use (c) and (d) to show that  $f$  is injective, hence bijective.

6. We continue to assume that  $m, n \in \mathbb{Z}$  and  $\gcd(m, n) = 1$ . Let  $f^*$  be the “restriction” of the map  $f$  from the previous problem to the classes which are co-prime to  $mn$ . In other words, consider the map  $f^* : (\mathbb{Z}/mn\mathbb{Z})^\times \rightarrow (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$  defined by  $f^*(\{a\}_{mn}) = (\{a\}_m, \{a\}_n)$ .

(a) Show that  $f^*$  is well-defined.

(b) Show that  $f^*$  is surjective and injective.

(c) Use (b) to show that  $\varphi(mn) = \varphi(m)\varphi(n)$ .

7. Solve the congruences

(a)  $7x \equiv 155 \pmod{181}$

(b)  $7y^3 \equiv 155 \pmod{181}$ .