

## Solutions to two of the October 4 Homework Problems.

This problems have to do with ***congruence modulo  $n$*** . We recall the definition. If  $a$  and  $b$  are integers and  $n$  is a positive integer, then  $a \equiv b \pmod{n}$  if  $n \mid (b - a)$ . Therefore when ask to prove something about congruences, often the first step will be to write out the definition.

**1.** Let  $n$  be a positive integer and  $a$  and  $b$  any integers. Prove the following:

- (a)  $a \equiv a \pmod{n}$ .
- (b) If  $a \equiv b \pmod{n}$ , then  $b \equiv a \pmod{n}$ .

*Solution to (a).* Every integer  $n$  divides 0. Thus  $n \mid (a - a) = 0$ . Therefore  $a \equiv a \pmod{n}$ .  $\square$

*Solution to (b).* We are given that  $a \equiv b \pmod{n}$ . By definition this means  $n \mid (b - a)$ . Therefore there is an integer  $k$  such that

$$(b - a) = kn$$

Multiply this by  $-1$  to get

$$(a - b) = (-1)(b - a) = (-k)n = \ell n \quad \text{where } \ell = k \text{ is an integer.}$$

Thus  $n \mid (a - b)$  and so  $b \equiv a \pmod{n}$  by the definition of congruence.  $\square$

**2.** Let  $n$  be a positive integer and  $a$ ,  $b$ , and  $c$  any integers. Prove the following:

- (a) If  $a \equiv b \pmod{n}$  and  $b \equiv c \pmod{n}$ , then  $a \equiv c \pmod{n}$ .
- (b) If  $a \equiv b \pmod{n}$ , then  $a + c \equiv b + c \pmod{n}$ .

*Solution to (a).* We are given that  $a \equiv b \pmod{n}$  and  $b \equiv c \pmod{n}$ . Thus, by definition,  $n \mid (b - a)$  and  $n \mid (c - b)$ . Therefore there are integers  $k$  and  $\ell$  such that

$$\begin{aligned} b - a &= kn \\ c - b &= \ell b. \end{aligned}$$

Add these two equations to get

$$c - a = (c - b) + (b - a) = kn + \ell n = (k + \ell)n = mn$$

where  $m = k + \ell$  is an integer. Therefore  $n \mid (c - a)$  and thus  $a \equiv c \pmod{n}$ .  $\square$

*Solution to (b).* We are given that  $a \equiv b \pmod{n}$ , which by definition implies that  $n \mid (b - a)$ . Therefore there is an integer  $k$  such that

$$b - a = kn.$$

Then

$$(b + c) - (a + c) = b - a = kn$$

and therefore  $n \mid (b + c) - (a + c)$ . So by definition  $a + c \equiv b + c \pmod{n}$ .  $\square$