

Name:

**Problem 1:** *Let  $a, b, c$  and  $m$  be integers, with  $m > 0$ .*

*Show that if  $a \equiv b \pmod{m}$  and  $b \equiv c \pmod{m}$ , then  $a \equiv c \pmod{m}$ .*

**Solution:** By Theorem 1 of Section 4 in the book, because  $a \equiv b \pmod{m}$  and  $b \equiv c \pmod{m}$ , this means that there are integers  $k_1$  and  $k_2$  such that  $a = b + k_1m$  and  $b = c + k_2m$ .

Substituting, we get

$$a = (c + k_2m) + k_1m = c + (k_1 + k_2)m,$$

where here we used associativity and distributivity.

Since  $k_1 + k_2$  is also an integer, Theorem 1 allows us to conclude that  $a \equiv c \pmod{m}$ .