

**Exercise 6:** Suppose  $a$  and  $b$  are integers that divide the integer  $c$ . If  $a$  and  $b$  are relatively prime, show that  $ab$  divides  $c$ . Show, by example, that if  $a$  and  $b$  are not relatively prime, then  $ab$  need not divide  $c$ .

By the fundamental theorem of algebra we can create a prime factorization for  $a, b$ , and  $c$ . Note that  $a|c$  and  $b|c$  implies that  $c$  contains the primes of  $a$  and  $b$ . Since  $a$  and  $b$  are relatively prime we know that they share no common prime. Thus their multiple contains all of the primes of  $a$  and those of  $b$  to the power of the original in either  $a$  or  $b$ . Thus the primes in  $c$  are in  $ab$  and so  $ab|c$ .

Consider  $a = 4$  and  $b = 6$  and  $c = 12$ . Note that  $a$  and  $b$  divide  $c$  however  $ab = 24 > c$  and thus  $ab$  does not divide  $c$ .

**Exercise 7:** If  $a$  and  $b$  are integers and  $n$  is a positive integer, prove that  $a \bmod n = b \bmod n$  if and only if  $n$  divides  $a - b$ .

Suppose  $a \bmod n = b \bmod n$ . Note that there exists integer  $i$ , such that,  $a = in + (a \bmod n)$ , also there exists integer  $j$  such that  $b = jn + (b \bmod n)$ . Note that  $a - b = in + (a \bmod n) - jn - (b \bmod n) = in - jn = (i - j)n$  thus  $n$  divides  $a - b$ .

Suppose  $n$  divides  $a - b$ . Note that there exists integer  $i$ , such that,  $a = in + (a \bmod n)$ , also there exists integer  $j$  such that  $b = jn + (b \bmod n)$ . Note that  $a - b = in + (a \bmod n) - jn - (b \bmod n) = in - jn + (a \bmod n) - (b \bmod n) = (i - j)n + (a \bmod n) - (b \bmod n)$ . Note that  $(i - j)n + (a \bmod n) - (b \bmod n) = kn$  for some  $k$ . Thus we know that  $(a \bmod n) - (b \bmod n) = vn$  for some integer  $v$ . However we also know  $-n < (a \bmod n) - (b \bmod n) < n$ , thus  $(a \bmod n) - (b \bmod n) = 0$  or  $(a \bmod n) = (b \bmod n)$ .

**Exercise 9:** Let  $n$  be a fixed positive integer greater than 1. If  $a \bmod n = a'$  and  $b \bmod n = b'$ , prove that  $(a - b) \bmod n = (a' - b') \bmod n$  and  $(ab) \bmod n = (a'b') \bmod n$ . (This exercise is referred to in Chapters 6, 8, 10, and 15.)

Note there exists  $j$  and  $k$  such that  $a = jn + a'$  and  $b = kn + b'$ . Note  $(a - b) \bmod n = (jn + a' - kn - b') \bmod n = (a' - b') \bmod n$ . Note that  $(ab) \bmod n = (jn + a')(kn + b') \bmod n = (jnkn + kna' + jnb' + a'b') \bmod n = (a'b') \bmod n$ .

**Exercise 11:** Let  $n$  and  $a$  be positive integers and let  $d = \gcd(a, n)$ . Show that the equation  $ax \bmod n = 1$  has a solution if and only if  $d = 1$ . (This exercise is referred to in Chapter 2.)

Suppose there exists a  $x$  such that  $ax \bmod n = 1$ . Note that there exists some  $j$  such that  $ax = jn + ax \bmod n$ . Note that  $ax - jn = 1$  thus  $\gcd(a, n) = 1 = d$ .

**Exercise 12:** Show that  $5n + 3$  and  $7n + 4$  are relatively prime for all  $n$ .

Note that  $7(5n + 3) - 5(7n + 4) = 7 \cdot 5n + 21 - 5 \cdot 7n - 20 = 1$  thus  $5n + 3$  and  $7n + 4$  are relatively prime.

**Exercise 13:** Suppose that  $m$  and  $n$  are relatively prime and  $r$  is any integer. Show that there are integers  $x$  and  $y$  such that  $mx + ny = r$ .

Since  $m$  and  $n$  are relatively prime there exists integers  $j$  and  $k$  such that  $jm + kn = 1$ . Let

$x = rj$  and  $y = rk$ . Note that  $mx + ny = mrj + nrk = r(jm + kn) = r$ .