Section 4.1 (continued)

Theorem 2: The Division Algorithm: Let a be an integer and d be a positive integer. Then there are unique integers q and r, with $0 \le r < d$, such that $a = dq + r$.

$\frac{5}{2}$ ← dividend, 2 ← divisor

$= 2\ r1$ ← remainder, quotient

Make sure remainder is not negative

EX: What are the quotient and remainder when 58 is divided by 17?

58 = dividend, a; 17 = divisor, d

$58 = 17q + r$

$58 = 17 \cdot 3 + 7$

$q = 3$

$r = 7$

$$17\overline{)58}\quad 3\ r7$$
$$-51$$
$$7$$

EX: What are the quotient and remainder when -11 is divided by 3?

Solution:

$a = dq + r$

$-11 = 3q + r$

~~$-3\ r-2$~~ ← This is wrong because r can't be negative.

$$3\overline{)-11}\quad -3$$
$$9$$
$$-2$$

Right Answer →

$$3\overline{)-11}\quad -4\ r1$$
$$12$$
$$1$$

When remainder is negative, make quotient 1 smaller (e.g. -3 becomes -4)

$-11 = 3 \cdot (-4) + 1$

$q = -4$

$r = 1$

Ex: What are the quotient and remainder when -21 is divided by 4?

Solution

$a = dq + r$ (a = -21, d = 4)

$-21 = 4q + r$

$4 \overline{)-21}$ → $q = -6$, r

-24

3

$-21 = 4(-6) + 3$

$q = -6$

$r = 3$

Modular Arithmetic

Definition 3: If a and b are integers and m is a positive integer, then a is congruent to b modulo m, if and only if $m \mid a - b$.

This also means

$a \bmod m = b \bmod m$ ← if that's the case, then a is congruent to b mod m.

$\equiv$ ← This is the symbol for congruency. If you see $a \equiv b \bmod m$, then that means $a \bmod m = b \bmod m$

$b \equiv a \bmod m$ ✓ yes

Ex: Determine whether 17 is congruent to 5 modulus 6.

Solution

m is 6

a is 17

b is 5

$m \mid a - b \rightarrow 6 \mid 17 - 5$

$6 \mid 12$, yes

17 is congruent to 5 mod 6

Other approach:

$17 \bmod 6 = 5 \bmod 6$

$5 = 5$

yes

Arithmetic modulo m

$a +_m b = (a+b) \bmod m$

$a \cdot_m b = (a \cdot b) \bmod m$

ex: What is $7 +_{11} 9$ and $7 \cdot_{11} 9$?

Solution:

$7 +_{11} 9 = (7+9) \bmod 11 = 16 \bmod 11 = \boxed{5}$

$7 \cdot_{11} 9 = (7 \cdot 9) \bmod 11 = 63 \bmod 11 = \boxed{8}$

Summary

congruent is important