Discrete Mathematics
Divisibility and Modular Arithmetic

Definition: If a and b are integers with $a \neq 0$, then ***a divides b*** if there exists an integer c such that $b = ac$.

- When a divides b we say that a is a ***factor*** or ***divisor*** of b and that b is a ***multiple*** of a.
- The notation $a \mid b$ denotes that a divides b.
- If a does not divide b, we write $a \nmid b$.
- If $a \mid b$, then b/a is an integer.

Example: Determine if

a. $5|9$

b. $4|12$

c. $3|-12$

d. $0|5$

Theorem: Let a, b, and c be integers, where $a \neq 0$.

i. If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$;
ii. If $a \mid b$, then $a \mid bc$ for all integers c;
iii. If $a \mid b$ and $b \mid c$, then $a \mid c$.

Proof:

i. *If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$.*

ii. If $a \mid b$, then $a \mid bc$ for all integers c.

iii. If $a \mid b$ and $b \mid c$, then $a \mid c$.

Corollary: If a, b, and c be integers, where $a \neq 0$, such that $a \mid b$ and $a \mid c$, then $a \mid mb + nc$ whenever m and n are integers.

Proof:

Theorem (The Division Algorithm): If a is an integer and d a positive integer, then there are unique integers q and r, with $0 \leq r < d$, such that $a = dq + r$.

- d is called the ***divisor***.
- a is called the ***dividend***.
- q is called the ***quotient***.
- r is called the ***remainder***.

Note: The remainder cannot be negative!

The notation is used to express the quotient and remainder:

$$q = a \ \boldsymbol{div} \ d \qquad\qquad r = a \ \boldsymbol{mod} \ d.$$

Example: Find the following:

a. $101 \ \boldsymbol{div} \ 11$

b. $101 \ \boldsymbol{mod} \ 11$

c. $-11 \ \boldsymbol{div} \ 3$

d. $-11 \ \boldsymbol{mod} \ 3$

e. $0 \ \boldsymbol{div} \ 19$

f. $0 \ \boldsymbol{mod} \ 19$

Modular Arithmetic

In some situations, we are only interested in the remainder of an integer when it is divided by some specified positive integer.

Example: What time does a 24-hour clock reads 100 hours after it reads 2:00?

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

- The notation $a \equiv b \ (mod\ m)$ says that a is congruent to b modulo m.
- Two integers are congruent $mod\ m$ if and only if they have the same remainder when divided by m.
- If a is not congruent to b modulo m, we write a $\not\equiv$ b (mod m).

Example: Decide whether each of these integers is congruent to 5 modulo 17.

a. 80

b. -29

Note: Do not confuse a $\equiv$ b (mod m) and a ***mod*** m!

Theorem: Let a and b be integers, and let m be a positive integer. Then $a \equiv b \ (mod\ m)$ if and only if a ***mod*** $m = b$ ***mod*** m.

Theorem: Let m be a positive integer. The integers a and b are congruent modulo m if and only if there is an integer k such that $a = b + km$.

Theorem (congruences of sums and products): Let m be a positive integer.

If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$,

then $a + c \equiv b + d \pmod{m}$ and $ac \equiv bd \pmod{m}$

Example: $9 \equiv 4 \pmod{5}$ and $11 \equiv 1 \pmod{5}$

Be careful when working with congruences!

- Multiplying both sides of a valid congruence by an integer preserves validity.
  If $a \equiv b \pmod{m}$ holds then $c \cdot a \equiv c \cdot b \pmod{m}$, where c is any integer.

- Adding an integer to both sides of a valid congruence preserves validity.
  If $a \equiv b \pmod{m}$ holds then $c + a \equiv c + b \pmod{m}$, where c is any integer.

- Dividing a congruence by an integer does NOT always produce a valid congruence.

Example: Start with $14 \equiv 8 \pmod{6}$, then divide both sides by 2.

Example: Find an integer a such that

a. $a \equiv 24 \pmod{31}$

b. $a \equiv 24 \pmod{31}$ and $-15 \leq a \leq 15$

c. $a \equiv -15 \pmod{27}$ and $-26 \leq a \leq 0$.

Example: Find the following value $(3^4 \ \boldsymbol{mod}\ 17)^2 \ \boldsymbol{mod}\ 11 =$