cse 16 5-2-24

4.1 Divisibility & Congruence

Defn

Let $a, b \in \mathbb{Z}$, $a \neq 0$. We say a divides b iff $b = ak$ for some $k \in \mathbb{Z}$. notation: $a \mid b$

Also say: a is a factor of b

a is a divisor of b

b is a multiple of a

b is divisible by a

Ex. $3 \mid 24$ since $24 = 3 \cdot 8$

Ex. $5 \nmid 21$ since $21 \neq 5k$ for any $k \in \mathbb{Z}$.

Theorem

Let $a, b, c \in \mathbb{Z}$. Then

(1) $a \mid b \wedge a \mid c \rightarrow a \mid (b+c)$

(2) $a \mid b \longrightarrow \forall d : a \mid bd$

(3) $a \mid b \wedge b \mid c \rightarrow a \mid c$

Proof of (1)

$a|b \rightarrow b = ak_1$ (some $k_1 \in \mathbb{Z}$)

$a|c \rightarrow c = ak_2$ (some $k_2 \in \mathbb{Z}$)

$\rightarrow b+c = ak_1 + ak_2$

$\therefore b+c = a(k_1+k_2)$

$\therefore a|(b+c)$ since $k_1+k_2 \in \mathbb{Z}$.

∎

Proof of (2)

Let $d \in \mathbb{Z}$. Then

$a \mid b \rightarrow b = ak$ (some $k \in \mathbb{Z}$)

$\rightarrow bd = (ak)d$

$\rightarrow bd = a(kd)$

$\therefore a \mid bd$ since $kd \in \mathbb{Z}$. ∎

Exercise Prove (3).

Note

- $1 \mid a$ for all $a \in \mathbb{Z}$.
- $a \mid a$ for all $a \in \mathbb{Z} - \{0\}$
- $a \mid 0$ for all $a \in \mathbb{Z} - \{0\}$

Corollary

Let $a, b, c, m, n \in \mathbb{Z}$. Then

$$a \mid b \wedge a \mid c \rightarrow a \mid (mb + nc)$$

Proof 1:

$$\left.\begin{array}{l} a \mid b \rightarrow a \mid mb \\ a \mid c \rightarrow a \mid nc \end{array}\right\} \rightarrow a \mid (mb+nc)$$

by (2) by (1) ∎

Proof 2

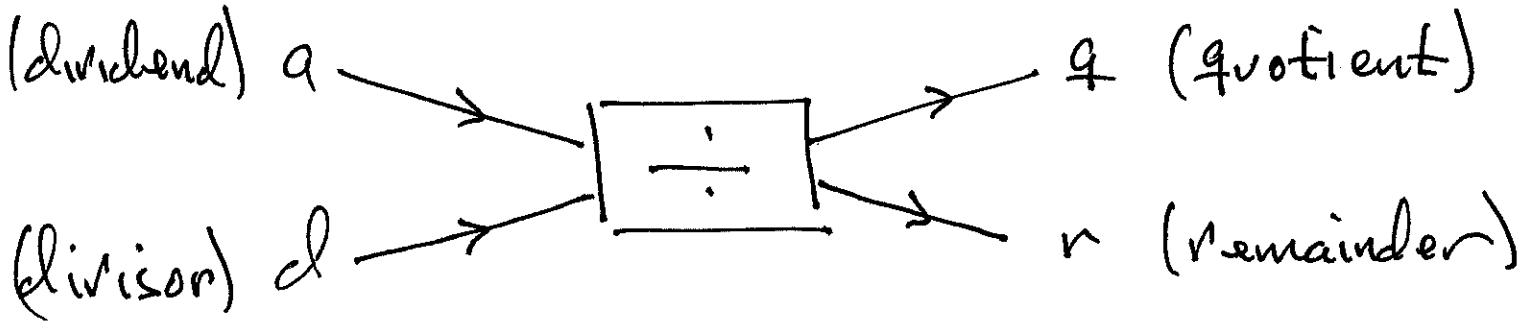
$$\left.\begin{array}{l} a \mid b \rightarrow b = a k_1 \rightarrow mb = a(mk_1) \\ a \mid c \rightarrow c = a k_2 \rightarrow nc = a(nk_2) \end{array}\right\}$$

$$mb+nc = a(mk_1)+a(nk_2) = a(\underbrace{mk_1+nk_2}_{\in \mathbb{Z}})$$

$\therefore a \mid (mb+nc)$. ∎

Integer Division

is an op. with 2 inputs & 2 outputs



Theorem (Division Algorithm)

Let $a \in \mathbb{Z}$, $d \in \mathbb{Z}^+$. Then there exist unique $q, r \in \mathbb{Z}$ such that

* $a = dq + r$ and $0 \leq r < d$

Proof of existence

Let $q = \left\lfloor \frac{a}{d} \right\rfloor$ and $r = a - dq$.

Then $\boxed{a = dq + r}$ ✓ and

$$q \leq \frac{a}{d} < q + 1$$

$$\therefore \quad dq \leq a < dq + d$$

$$\therefore \quad 0 \leq a - dq < d$$

$$\therefore \quad \boxed{0 \leq r < d}$$ ✓. ∎

Alternate defn of q:

$$q = \max\{ j \in \mathbb{Z} \mid dj \leq a \}$$

$$\therefore \quad dq \leq a < d(q+1) = dq + d$$

Exercise

Prove uniqueness, i.e. show that it also

$$a = dq' + r' \text{ and } 0 \le r' < d$$

then show $q' = q$ and $r' = r$.

Ex.

- $123 = 12 \cdot 10 + 3, \quad 0 \le 3 < 12$
  $a \quad d \quad q \quad r$

- $91 = 11 \cdot 8 + 3, \quad 0 \le 3 < 11$

- $-35 = 8(-5) + 5, \quad 0 \le 5 < 8$

Defn

Let $a, b \in \mathbb{Z}$, $m \in \mathbb{Z}^+$. We say

a is Congruent to b modulo m iff

$$m \mid (a-b)$$

notation. $a \equiv b \pmod{m}$

alternate notation! $a \equiv_m b$

Ex.

- $8 \equiv 22 \pmod 7$ since $7 \mid (8-22) = -14$
- $51 \equiv 18 \pmod{11}$ since $11 \mid (51-18) = 33$
- $13 \equiv -7 \pmod{10}$ since $10 \mid (13-(-7)) = 20$

Theorem

$a \equiv b \pmod m$ iff $a = b + km$, for some $k \in \mathbb{Z}$.

Proof

$$a \equiv_m b$$
$$\iff m \mid (a-b)$$
$$\iff a - b = km \quad \text{for some } k \in \mathbb{Z}$$
$$\iff a = b + km \quad " \quad " \quad "$$

∎

Theorem

$a \equiv b \pmod{m}$ $\overrightarrow{\text{iff}}$ $\overleftarrow{\text{iff}}$ a and b have same remainder upon division by m.