CSE 16 7-17-24

Theorem

Let S be a set. Then no function $f : S \to \mathbb{P}(S)$ is surjective.

Proof (contradiction).

Assume $f : S \to \mathbb{P}(S)$ is surjective.

Define $A \subseteq S$ by

$$A = \{x \in S \mid x \notin f(x)\}$$

Since f is surjective, we have $A \in \text{range}(f)$, i.e. there exists $y \in S$ such that

$$f(y) = A \, .$$

But either $y \in A$ or $y \notin A$.

- $y \in A \Rightarrow y \in f(y) \Rightarrow y \notin A$ -X.

and

- $y \notin A \Rightarrow y \notin f(y) \Rightarrow y \in A$ -X.

This contradiction shows our assumption was false, so f is not surjective.

$\blacksquare$

observe, since $f : S \to \mathbb{P}(S)$ is not surjective, it is not bijective, so $|S| \neq |\mathbb{P}(S)|$

so have many infinities!

$$\mathbb{N} < \mathbb{P}(\mathbb{N}) < \mathbb{P}(\mathbb{P}(\mathbb{N})) < \ldots\ldots$$

not actually defined

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__: $a | b$

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.__ $3 | 24$ 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) $a|b \wedge a|c \rightarrow a|(b+c)$

(2) $a|b \rightarrow a|bd$ for any $d \in \mathbb{Z}$.

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

Proof of (1)

$$\left.\begin{array}{l} a|b \rightarrow b = ak_1 \\ a|c \rightarrow c = ak_2 \end{array}\right\} \rightarrow \begin{array}{l} b+c = ak_1 + ak_2 \\ \quad = a(k_1+k_2) \end{array}$$

defn.

$\therefore\ a \mid (b+c)$

$\blacksquare$

<u>Proof of (2)</u>

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

$$a \mid b \rightarrow b = ak \rightarrow bd = a(kd)$$

$$\therefore a \mid bd.$$

$\blacksquare$

<u>Exercise</u>: Prove (3).

<u>Note</u>

- $1 \mid a$ for all $a \in \mathbb{Z}$ $(k = a)$
- $a \mid a$ for all $a \in \mathbb{Z} - \{0\}$ $(k = 1)$
- $a \mid 0$ for all $a \in \mathbb{Z} - \{0\}$ $(k = 0)$

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) $\blacksquare$

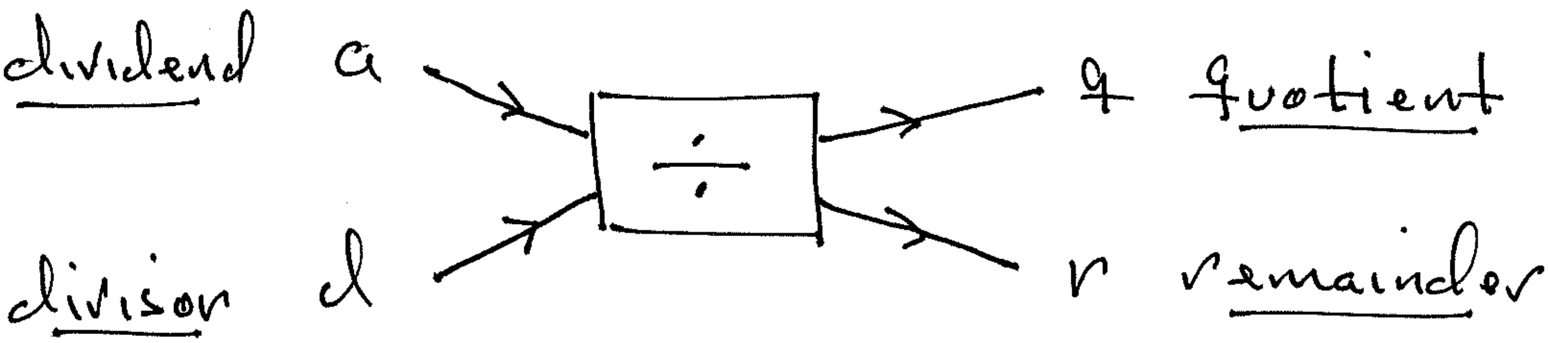
Proof 2

$$\left.\begin{array}{l} a \mid b \rightarrow b = ak_1 \rightarrow mb = a(mk_1) \\ a \mid c \rightarrow c = ak_2 \rightarrow nc = a(nk_2) \end{array}\right\} \rightarrow$$

$$mb + nc = a(mk_1 + nk_2)$$

$\therefore\ a \mid (mb + nc)$. $\blacksquare$

Integer Division is an operation with 2 inputs and 2 outputs.



Theorem (Division algorithm)
Let $a \in \mathbb{Z}$ and $d \in \mathbb{Z}^+$. Then there exist unique $q, r \in \mathbb{Z}$ such that

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

Proof of existence

Define

$$q = \max\{ j \in \mathbb{Z} \mid d \cdot j \le a \}$$

and

$$r = a - dq$$

Then $a = dq + r$. Also

$$dq \le a < d(q+1)$$

follows from defn. of q.

$$\therefore\ dq \le a < dq + d$$

$$\therefore\ 0 \le a - dq < d$$

$$\therefore\ 0 \le r < d.$$

$\blacksquare$

Exercise

Prove uniqueness, i.e. show that if also

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

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

Ex. $123 = 12 \cdot 10 + 3, \quad 0 \leq 3 < 12$

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

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

Defn

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

<u>a is congruent to b modulo m</u>

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

<u>notation</u>:

- $a \equiv b \pmod{m}$

- $a \equiv_m b$

<u>Ex.</u> $8 \equiv 22 \pmod{7}$ since $7 \mid (8-22) = -14$

$51 \equiv 18 \pmod{11}$ " $11 \mid (51-18) = 33$

$13 \equiv -7 \pmod{10}$ " $10 \mid (13-(-7)) = 20$

Theorem

$a \equiv b \pmod{m}$ $\underset{\longleftarrow}{\overset{\longrightarrow}{\text{iff}}}$ $a = b + km$ for some $k \in \mathbb{Z}$.

Proof

$$a \equiv_m b$$

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

$$\Longleftrightarrow \quad a-b = km \text{ for some } k \in \mathbb{Z}$$

$$\Longleftrightarrow \quad a = b + km \quad " \quad \ldots \quad "$$

$\blacksquare$

<u>Theorem</u>

$a \equiv b \pmod{m}$ $\underset{\Longleftarrow}{\overset{\Longrightarrow}{\text{iff}}}$ a and b have the same remainder upon division by m.

<u>Proof</u>

($\Longrightarrow$) let $a \equiv_m b$. Then $a-b=km$ for some $k \in \mathbb{Z}$. By the division algorithm

$$a = q_1 m + r_1 \text{ and } 0 \le r_1 < m$$

and

$$b = q_2 m + r_2 \text{ and } 0 \le r_2 < m$$

We must show $r_1 = r_2$.

Thus

$$km = a - b$$

$$= (q_1 m + r_1) - (q_2 m + r_2)$$

$$= (q_1 - q_2)m + (r_1 - r_2)$$

$$\therefore\ r_1 - r_2 = -(q_1 - q_2 - k)m$$

$$\therefore\ m \mid (r_1 - r_2)$$

Similarly, $m \mid (r_2 - r_1)$, At least one of $(r_1 - r_2)$ and $(r_2 - r_1)$ is non-negative, say $r_1 - r_2$ is non-negative. Then

$$0 \leq r_1 - r_2 < m$$

It follows that $r_1 - r_2 = 0$,

hence $r_1 = r_2$. $\square$

($\Leftarrow$) suppose a and b have the same remainder upon division by m. Then

$$a = q_1 \cdot m + r$$
$$b = q_2 \cdot m + r$$

we must show $a \equiv b \pmod{m}$.

$\therefore \quad a - b = (q_1 - q_2)m + (r - r)$

$\therefore \quad a - b = (q_1 - q_2)m$

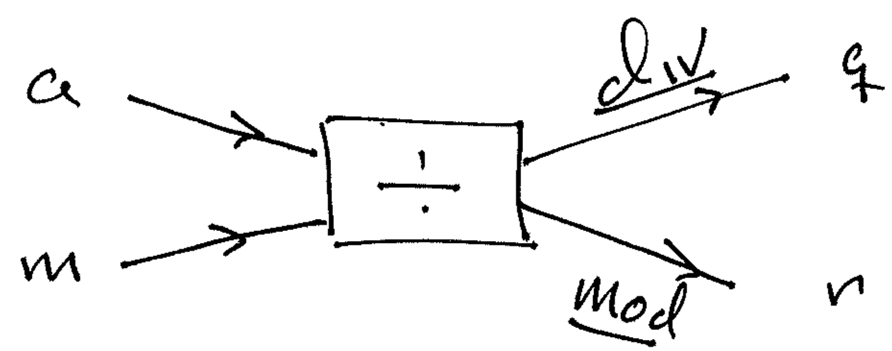
$\therefore \quad m \mid (a - b)$

$\therefore \quad a \equiv b \pmod{m}$. $\square$

Defn

We define operations <u>mod</u> and <u>div</u> as

- $a \ \underline{\text{mod}}\ m$ = rem. of a on division by m
- $a \ \underline{\text{div}}\ m$ = quotient of a on division by m



Thus

$$a = (a \ \underline{\text{div}}\ m)\cdot m + (a \ \underline{\text{mod}}\ m)$$

Preceding Theorem

$$a \equiv b \pmod m \ \text{ iff } \ a \ \underline{\text{mod}}\ m = b \ \underline{\text{mod}}\ m$$

<u>warning</u>

don't confuse 'mod' and boldface '**mod**'.

<u>Theorem</u>

Let $a, b, c \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$.

(1) <u>reflexive</u>: $a \equiv_m a$

(2) <u>symmetric</u>: $a \equiv_m b \to b \equiv_m a$

(3) <u>transitive</u>:

$$a \equiv_m b \wedge b \equiv_m c \to a \equiv_m c$$

<u>Proof of (3)</u>

$$\left.\begin{aligned} a \equiv_m b &\rightarrow m \mid (a-b) \\ b \equiv_m c &\rightarrow m \mid (b-c) \end{aligned}\right\} \longrightarrow$$

$$m \mid \left((a-\cancel{b}) + (\cancel{b}-c) \right)$$

$$\therefore \quad m \mid (a-c)$$

$$\therefore \quad a \equiv_m c \quad . \qquad \blacksquare$$

<u>Exercise</u>:

Prove (1) and (2).

Theorem

Let $a,b,c,d \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$.

Suppose $a \equiv_m b$, $c \equiv_m d$. Then

(1) $a+c \equiv_m b+d$

(2) $a-c \equiv_m b-d$

(3) $ac \equiv_m bd$