CSE 16 7-19-23

Recall

- Cantor diagonal argument
- shows $|\mathbb{R}| \neq |\mathbb{N}|$

Theorem

If $A_1, A_2, A_3, \ldots$ is a seq. of countable sets, then

$$S = \bigcup_{n=1}^{\infty} A_n$$

is also countable.

Exercise: Prove this (Hint: similar to proof of $|\mathbb{Z}^+ \times \mathbb{Z}^+| = |\mathbb{Z}^+|$)

note:

$$\{\text{Prog-ams}\} = \bigcup_{n=0}^{\infty} \{\text{Prog-ams of len. } n\}$$

∴ the set {Prog-ams} is countable.

Defn

A number $x \in \mathbb{R}$ is called computable iff there exists a Program that, given $n \in \mathbb{N}$, prints n decimal digits of x.

so, most $x \in \mathbb{R}$ are not computable!!

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, there exists $y \in S$ s.t. $f(y) = A$. But

$$y \in A \to y \in f(y) \to y \notin A \quad \dot{\times}$$

and $y \notin A \to y \notin f(y) \to y \in A \quad \dot{\times}$

This $\dot{\times}$ shows no such y exists.

$\therefore A \notin \text{range}(f) \therefore f$ is not surjective. ∎

In Particular:

$$|\mathbb{N}| < |\mathbb{P}(\mathbb{N})| < |\mathbb{P}(\mathbb{P}(\mathbb{N}))| < \cdots\cdots$$

↑

means no surjection $\mathbb{N} \to \mathbb{P}(\mathbb{N})$

4.1 Divisibility and 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 $24 = 3 \cdot 8$

$5 \nmid 21$ since $21 \neq 5k$ for all $k \in \mathbb{Z}$

Theorem

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

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

(2) $a|b \rightarrow \forall d : a|bd$

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

Proof of (1)

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

$$\rightarrow b + c = a(k_1 + k_2) \rightarrow a|(b+c)$$

∎

Proof of (2)

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

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

$\rightarrow bd = a(kd)$

$\therefore a \mid bd$. ∎

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

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

by (2) by (1)

■

Proof 2

$$\left.\begin{array}{l} a \mid b \rightarrow b = aK_1 \rightarrow mb = a(mK_1) \\ a \mid c \rightarrow c = aK_2 \rightarrow nc = a(nK_2) \end{array}\right\} \longrightarrow$$

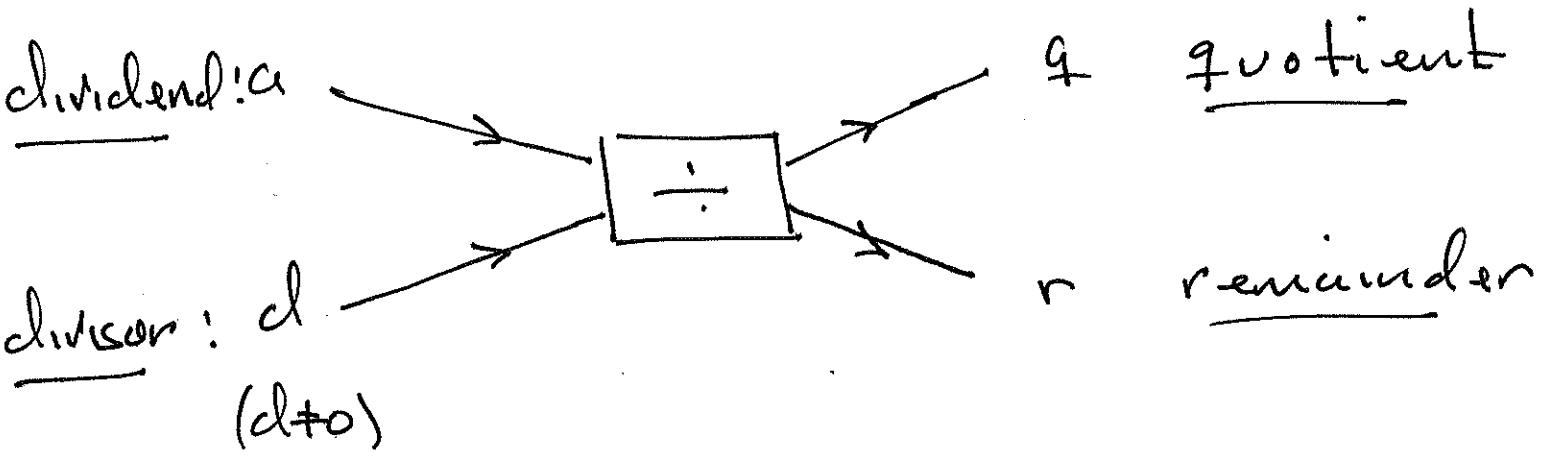
$$\longrightarrow mb + nc = a(mK_1) + a(nK_2) = a(mK_1 + nK_2)$$

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

■

Integer Division has 2 inputs and 2 outputs

$\mathbb{Z}$



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 $0 \leq r < d$

dividend, divisor, quotient, remainder

Proof of existence

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

Then $a = dq + r$ and

$$q \leq \frac{a}{d} < q+1 \quad (\text{defn of } \lfloor \cdot \rfloor)$$

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

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

$$\therefore \quad 0 \leq r < d.$$

Thus q, r exist satisfying $*$. ∎

Exercise Prove uniqueness, i.e. show that it also

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

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

Ex.

- $123 = 12 \cdot 10 + 3, \quad 0 \leq 3 < 12$
- $91 = 11 \cdot 8 + 3, \quad 0 \leq 3 < 11$
- $-35 = 8 \cdot (-5) + 5, \quad 0 \leq 5 < 8$

Def

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: $a \equiv_m b$

Ex.

- $8 \equiv 22 \pmod 7$ since $7 \mid (8-22) = -21$
- $51 \equiv 18 \pmod{11}$ 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 $a - b = km$, for some $k \in \mathbb{Z}$

iff $a = b + km$, " " " .

■

Theorem

$a \equiv b \pmod{m}$ $\overrightarrow{\text{iff}}$ $\overleftarrow{\text{iff}}$ a and b have the same remainder when divided by m.

Proof

($\Rightarrow$) Let $a \equiv_m b$. Then $a - b = km$ for some $k \in \mathbb{Z}$. By the Div. Alg.

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

also

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

Thus $km = a - b = (q_1 - q_2)m + (r_1 - r_2)$

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

Therefore $m \mid (r_1 - r_2)$, also $m \mid (r_2 - r_1)$.

At least one of $(r_1 - r_2)$ and $(r_2 - r_1)$ is non-negative, and less than m, say $r_1 - r_2$.

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

But then $m \mid (r_1 - r_2) \rightarrow r_1 - r_2 = 0$

$\square$

$\rightarrow r_1 = r_2$.

($\Longleftarrow$) suppose a and b have same remainder upon div. by m. Then

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

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

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

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

□

▨