09/05/2023
KVB
(1)

CS2312 Tuesday Lecture

MOTIVATION:

It is (one of) the most basic concept(s) to enter into Number Theory

- ↳ study of integers
- ↳ One of the oldest of sciences
- ↳ Has gotten more & more applications, recently
  - ↳ Ex: Cryptography
    - Study and science of "hiding" numbers

Applications:

1. SSNs, passcodes
2. Personal data,
3. Banking & Finance

09/05/2023 KVB

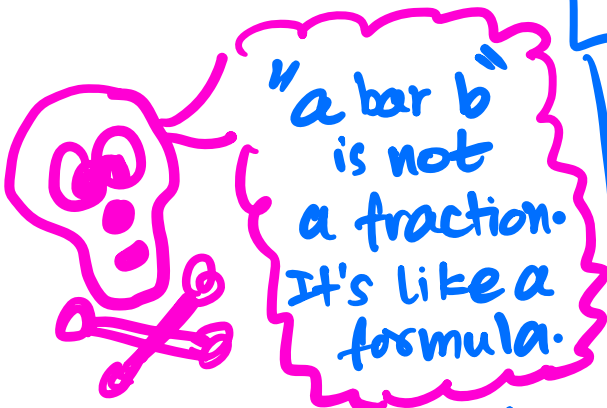
2

Def

$a|b$ iff $\exists k \in \mathbb{Z}$ such that $b = ka$

$a|b$ → a divides b

- a is a factor or divisor of b
- b is a multiple of a
- b is divisible by a



We talk about:

$\forall a, b, c, d \in \mathbb{Z}$, $a \neq 0$ and $k \in \mathbb{Z}^+$ unless specified

09|05|2023
KVB

(3)

(*) Integer division:

Ex: $3 \mid 12$

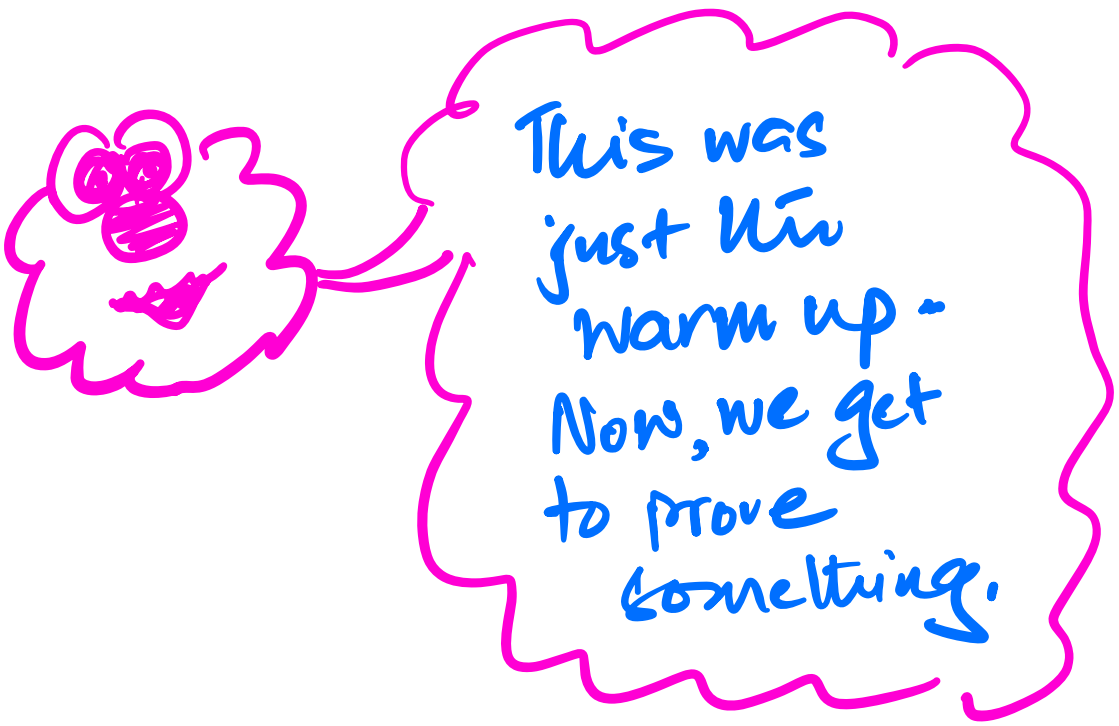
$\Rightarrow \exists\, k_1 = 4 \in \mathbb{Z}$ such that

$12 = 4 \times 3$

Ex: $5 \mid 20$

$\Rightarrow \exists\, k_2 = 4 \in \mathbb{Z}$ such that

$20 = 4 \times 5$



09/05/2023
KVB

(4)

If $a|b$ & x is any integer, then $a|xb$

Statement:

$$a|b \Rightarrow a|xb \quad \forall\, x \in \mathbb{Z}$$

hypothesis → conclusion

Proof:

$a|b \Rightarrow \exists\, k_1 \in \mathbb{Z}$ such that

$$b = k_1 a$$

$$\Rightarrow xb = (xk_1)a \quad \forall\, k_1 \in \mathbb{Z} \;\because x \in \mathbb{Z}$$

The integers are closed w.r.t multiplication and $k_1, x \in \mathbb{Z}$

Hence, $xk_1 \in \mathbb{Z} \quad \forall\, x \in \mathbb{Z}$

Hence,

$$\exists\, k_2 = xk_1 \in \mathbb{Z} \text{ such that}$$

$$xb = k_2 a$$

$\Rightarrow a \mid xb \quad \forall x \in \mathbb{Z}$

09/05/2023 KVB

(5)

□

[or ✓ QED]

Let's extend this discussion to converse.... meant a CONVERSE

We know $a \mid b \Rightarrow a \mid 7b$ is TRUE

NOW the CONVERSE. WHAT about it?

Statement

$a \mid 7b \Rightarrow a \mid b$ Claim: Statement is FALSE

OR

$a \mid 7b \not\Rightarrow a \mid b$ is TRUE

Proof by counter example:

Let $a = 7$ and $b = 2$

Hypothesis: $7 \mid 7 \cdot 2$ ✓

Conclusion: $7 \mid 2$ ×

Hence, the statement is FALSE □

09/05/2023
KVB

(6)

If $a|b$ and $a|c$, then $a|(b+c)$

Statement:

$a|b$ and $a|c \Rightarrow a|(b+c)$

$a|b \wedge a|c \Rightarrow a|(b+c)$

hypothesis — conclusion

Proof:

$a|b \Rightarrow \exists k_1 \in \mathbb{Z}$ such that $b = k_1 a$ → (1)

$a|c \Rightarrow \exists k_2 \in \mathbb{Z}$ such that $c = k_2 a$ → (2)

using (1) & (2)

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

The integers are closed with respect to addition and $k_1, k_2 \in \mathbb{Z}$

Hence, $k_3 = (k_1 + k_2) \in \mathbb{Z}$

Hence, $\exists k_3 \in \mathbb{Z}$ such that

$(b+c) = k_3 a$

Hence, $a|(b+c)$ □

09/05/2023
KVB

7

If $a|b$ and $a|c$, then $a|(b-c)$

Statement:

$(a|b) \wedge (a|c) \Rightarrow a|(b-c)$

Recall statements

$a|b \Rightarrow a|xb \quad \forall x \in \mathbb{Z} \rightarrow (1)$

and

$(a|b) \wedge (a|c) \Rightarrow a|(b+c) \rightarrow (2)$

From (1)

$a|c \Rightarrow a|(-1)c \quad \because -1 \in \mathbb{Z}$

Using (2)

$a|b \wedge a|(-c) \Rightarrow a|(b-c)$

□

If $a|b$ and $a|c$, then $a|(sb+tc)\ \forall\ s,t \in \mathbb{Z}$

09/05/2023
KVB
(8)

Statement:

$$a|b \wedge a|c \Rightarrow a|(sb+tc)\ \forall\ s,t \in \mathbb{Z}$$

Recall,

$$a|b \Rightarrow a|xb\ \forall\ x \in \mathbb{Z} \quad \hookrightarrow (1)$$

Using (1),

$$a|b \Rightarrow a|sb\ \forall\ s \in \mathbb{Z} \rightarrow (2)$$

and

$$a|c \Rightarrow a|tc\ \forall\ t \in \mathbb{Z} \rightarrow (3)$$

Recall

$$a|b \wedge a|c \Rightarrow a|(b+c) \rightarrow (4)$$

09/05/2023
KVB

9

Using ④ on ① & ②, we have

$a|b \wedge a|c \Rightarrow a|(sb+tc)$

$\forall\ s,t \in \mathbb{Z}$

□