Announcements / Check in

- No labs next week
- HW1 due Tuesday 4:30pm (9/3)
  HW2 will be posted Thursday at the latest
- Lecture notes on website
- Any questions / issues?

Definition: Let a, b be integers with $a \neq 0$. We say that a divides b if there exists an integer q s.t. $b = q \cdot a$ or equivalently if $\frac{b}{a}$ is an integer

$\underline{a|b}$ iff $\exists q \in \mathbb{Z}$ s.t. $b = qa$

"a bar b" ↳ a divides b
↳ a is a factor / divisor of b
↳ b is a multiple of a
↳ b is divisible by a

$3|12$? Yes! $\exists k_1 = 4$ s.t. $12 = 4 \times 3$

$5|20$? Yes! $\exists k_2 = 4$ st $20 = 4 \times 5$

$3|7$? No! $\frac{7}{3} = 2.\overline{33} \notin \mathbb{Z}$

$3 \nmid 7 \qquad 2|4$

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

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

Statement:

$$\underbrace{a|b}_{\text{hypothesis}} \Rightarrow \underbrace{a|xb}_{\text{conclusion}} \quad \forall x \in \mathbb{Z}$$

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

$\Rightarrow xb = (xk_1)a$

Let $k_2 = xk_1$

$\Rightarrow xb = k_2 a$

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

Hence, $k_2 = xk_1 \in \mathbb{Z}$

$\Rightarrow \exists k_2 = xk_1 \in \mathbb{Z}$ s.t. $xb = k_2 a$

$\Rightarrow a|xb$

We know $a|b \Rightarrow a|xb$

What do we know about the converse?

$a|xb \Rightarrow a|b$?

Claim: $a|xb \Rightarrow a|b$ is FALSE.

Proof by counterexample:

$a = 3, x = 3, b = 2$

Hypothesis: $3|(2 \cdot 3) = 3|6$ ✓

Conclusion: $3|2$ ✗

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

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

Proof:

$a|b \Rightarrow \exists k_1 \in \mathbb{Z}$ s.t. $b = k_1 a$

$a|c \Rightarrow \exists k_2 \in \mathbb{Z}$ s.t. $c = k_2 a$

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

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

The integers are closed w/ respect to addition (adding 2 integers gets you an integer). We know $k_1, k_2 \in \mathbb{Z}$

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

Hence, $\exists k_3 \in \mathbb{Z}$ s.t. $(b+c) = k_3 a$

$\Rightarrow a|(b+c)$

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

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

$b - c = b + (-c)$

One option:

$\exists k_1 : b = k_1 a$

$\exists k_2 : c = k_2 a$

$b - c = k_1 a - k_2 a$

Another:

Recall that

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

and

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

From ①

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

Using ②

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

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

Recall

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

$a|b \Rightarrow a|sb \quad \forall s \in \mathbb{Z}$

$a|c \Rightarrow a|tc \quad \forall t \in \mathbb{Z}$

Recall:

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

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

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

$\boxed{a|b \Leftrightarrow \boxed{a|(-b)} \Leftrightarrow (-a)|b}$

$\forall a, b, c, d \in \mathbb{Z} \quad a \neq 0$

① $a|b \Rightarrow a|(-b)$

Recall

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

$-1 \in \mathbb{Z}$

$a|b \Rightarrow a|(-1)b$

$\Rightarrow a|(-b)$

② $a|(-b) \Rightarrow a|b$

Using ①

$a|(-b)$

$\Rightarrow a|(-1)(-b)$

$\Rightarrow a|b$

③ $a|(-b) \Rightarrow (-a)|b$

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

$-b = k_1 a$

$\Rightarrow b = k_1(-a)$

$\Rightarrow (-a)|b$

④ $(-a)|b \Rightarrow a|(-b)$

$(-a)|b \Rightarrow \exists k_2 \in \mathbb{Z}$ such that

$b = k_2(-a)$

$\Rightarrow -b = k_2(a)$

$\Rightarrow a|(-b)$