

# Last Monday

Prop 1  $a, b \in \mathbb{Z}$   $b > 0$

$\exists q, r$  s.t.

$$a = bq + r$$

$$0 \leq r < b$$

$(q, r)$  is unique.

Def  $a$  divides  $b$

if  $\exists c$  s.t.  $b = ac$

0 is the only integer dividing 0

Def  $a, b \in \mathbb{Z}$

A common divisor is  
a non-negative integer  $d$

$$\text{s.t. } d \mid a \\ d \mid b$$

The greatest common divisor  $r$   
 $\text{gcd}(a, b)$   
is the greatest one,

if  $s'$  is a common divisor  
of  $a$  &  $b$ ,

then  $s' < r$ .

(in fact  $s' | r$ )

Def  $a, b \in \mathbb{Z}$

A common multiple of  $a$  &  $b$   
is a positive integer  $s'$

s.t.  $a | s'$   
 $b | s'$ .

PK 0 can NOT be

a common multiple.

because

$$a \mid 0$$

$$b \mid 0$$

hence 0 is always

a common multiple!

The least common multiple  
of  $a$  &  $b$

is the smallest common multiple

$r = \text{lcm}(a, b)$  of  $a$  &  $b$ , i.e.

if  $s$  is a common multiple  
of  $a$  &  $b$ ,

then  $r < s$ .

In fact  $r \mid s$ !

By definition,  $a, b \in \mathbb{Z}$

$$\begin{aligned} \gcd(a, b) &= \gcd(-a, b) \\ &= \gcd(a, -b) \\ &= \gcd(-a, -b) \end{aligned}$$

# Euclid's algorithm

is based on

Prop 6  $a, b \in \mathbb{Z}$

$$b > 0 \quad \& \quad a = bq + r$$

$$0 \leq r < b$$

$$\gcd(a, b) = \gcd(b, r).$$

Theorem 7 (Bezant's identity)

$$a, b \in \mathbb{Z}$$

$$\exists r, s \in \mathbb{Z}$$

$$ar + bs = \gcd(a, b)$$

In practice, given concrete  $a$  &  $b$ ,  
one can use Euclid's algorithm to  
compute  $r$  &  $s$ .

$$\text{Ex } a, b, c \in \mathbb{Z}$$

$$\text{Prove } a \gcd(b, c)$$

$$= \gcd(ab, ac)$$

$$a=4 \quad b=16 \quad c=24$$

$$\gcd(b, c) = \gcd(16, 24) = 8$$

$$\underline{a \gcd(b, c) = 4 \cdot 8 = 32}$$

$$\underline{\gcd(ab, ac) = \gcd(64, 96)}$$
$$= 32$$

pf

Firstly, we'll prove

$$a \gcd(b, c) \leq \gcd(ab, ac).$$

By definition,  $\gcd(b, c)$  "divides"

$$\gcd(b, c) \mid b$$

$$\gcd(b, c) \mid c$$



$$\Rightarrow a \gcd(b, c) \mid ab \quad (*)$$

[ Because  $\gcd(b, c) \mid b$ ,  
I know by definition that

$$\exists d \in \mathbb{Z} \quad b = \gcd(b, c) \cdot d$$

Multiplying this  $\uparrow$  by  $a$

$$ab = a \gcd(b, c) \cdot d$$

This means that

$a \gcd(b, c)$  divides  $ab$ . ]

$$a \gcd(b, c) \mid ac \quad (**)$$

By  $\textcircled{*}$  &  $\textcircled{**}$ ,

A  $\text{gcd}(b, c)$  is a common  
divisor of  $ab$   
&  $ac$ .

This means that

$$a \text{gcd}(b, c) \leq \text{gcd}(ab, ac)$$

Secondly, we will prove

$$a \text{gcd}(b, c) \geq \text{gcd}(ab, ac)$$

By definition,

$$\gcd(ab, ac) \mid ab \quad \dots \textcircled{1}$$

$$\gcd(ab, ac) \mid ac \quad \dots \textcircled{2}$$

By Bezant's identity (Theorem 7),

$$\exists r, s \text{ s.t.}$$

$$br + cs = \gcd(b, c)$$

Multiplying this by  $a$ , we get

$$abr + acs = a \gcd(b, c)$$

$$\dots \textcircled{3}$$

By  $(n)$   $(m)$ ,  $\gcd(ab, ac)$

divides the LHS of  $(m)$

It therefore follows that

$$\begin{aligned} \gcd(ab, ac) & \text{ divides the RHS} \\ & = a \gcd(b, c) \end{aligned}$$

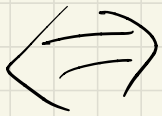
i.e.

$$|\gcd(ab, ac)| \leq a \gcd(b, c).$$

□

Def A prime number

is a positive integer s.t.  
its only positive integer divisors  
are 1 and itself.



$p$  is a prime number  
if the following holds:

if  $p \mid ab$  then either  $p \mid a$   
or  $p \mid b$ .

# Theorems (Fundamental Theorem of Algebra)

Every integer can be expressed

as the product

$$(-1)^r \prod_p p^{r_p}$$

$$r \in \{\pm 1\}$$

$$r_p \geq 0 \quad \text{integers}$$

Mon 2-4  
Wed 10

Example  $12 = 2^{\textcircled{2}} \cdot 3$

$$-12 = (-1) \cdot 2^{\textcircled{2}} \cdot 3$$