Last Monday

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

$\exists\, q, r$ s.t.

$$a = bq + r$$

$$0 \le r < b$$

(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 s

s.t. $s \mid a$

$s \mid b$

The greatest common divisor r

$\gcd(a, b)$

is the greatest one.

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

then $s' < r$.

(in fact $s' \mid r$)

<u>Def</u> $a, b \in \mathbb{Z}$

A common multiple of a & b is a positive integer s s.t. $a \mid s$, $b \mid s$.

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

$$\gcd(a, b) = \gcd(-a, b)$$
$$= \gcd(a, -b)$$
$$= \gcd(-a, -b)$$

Euclid's algorithm

is based on

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

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

$0 \leq r < b$

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

Theorem 7 (Bezout'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.

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

Prove $a \gcd(b, c)$

$= \gcd(ab, ac)$

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

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

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

$\gcd(ab, ac) = \gcd(64, 96)$

$= 32$

<u>Pf</u> Firstly, we'll prove

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

By definition, ← "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 ↑ 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 $\circledast$ & $\circledast\circledast$,

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

This means that

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

Secondly, we will prove

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

By definition,

$$\gcd(ab, ac) \mid ab \quad \cdots \quad (1)$$

$$\gcd(ab, ac) \mid ac \quad \cdots \quad (2)$$

By Bezout's identity (Theorem 7),

$\exists\, r, s$ s.t.

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

Multiplying this by a, we get

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

$\cdots \quad (3)$

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

divides the LHS of (mmm)

It therefore follows that

$\gcd(ab, ac)$ divides the RHS

$$= a \gcd(b, c)$$

i.e. $\gcd(ab, ac) \le a \gcd(b, c)$.

$\square$

Def A prime number

is a positive integer s.t.

its only <u>positive</u> <u>integer</u> divisors

are 1 and itself.

$\Longleftrightarrow$

P is a prime number

if the following holds:

if $p \mid ab$ then either $p \mid a$

or

$p \mid b$.

Theorem 8 (Fundamental Theorem of Algebra)

Every integer can be expressed as the product

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

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

$r_p \geq 0$ integer

Mon 2-4

Wed 10

Example

$$12 = 2^2 \cdot 3$$

$$-12 = (-1) \cdot 2^2 \cdot 3 .$$