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

Def 1: We say $d \in \mathbb{Z}$ is a GREATEST COMMON DIVISOR for a and b

GCD

If: 1) $d \mid a$ and $d \mid b$

2) if $d_1 \in \mathbb{Z}$ s.t. $d_1 \mid a$ and $d_2 \mid b \Rightarrow$

$\Rightarrow d_1 \mid d$

Def 2: We say $l \in \mathbb{Z}$ is a LEAST COMMON MULTIPLE for a and b

If: 1) $a \mid l$ and $b \mid l$

2) if $l_1 \in \mathbb{Z}$ s.t. $a \mid l_1$ and $b \mid l_1 \Rightarrow l \mid l_1$

Rmk: • If d and d' are GCD for a and b

$\Rightarrow d \mid d'$ and $d' \mid d \ (\Leftrightarrow d' = \pm d$

•• If ℓ and ℓ' are LCM for a and b

$\Rightarrow \ell \mid \ell'$ and $\ell' \mid \ell \ (\Leftrightarrow \ell' = \pm \ell$

Convention: We prefer to denote the

• $\Rightarrow$ positive value as $\gcd(a,b)$

•• $\Rightarrow$ positive value as $\mathrm{lcm}(a,b)$

Fact: $\gcd(a,b) \cdot \mathrm{lcm}(a,b) = \pm a \cdot b$

Theorem (Extended Euclid Algorithm)

For any $a, b \in \mathbb{Z}$, $\gcd(a,b)$ exists

Lemma: $\gcd(a,b) = \gcd(a, b - s \cdot a)\ \forall s \in \mathbb{Z}$

Proof: E.T.S.

$$\left\{ \begin{array}{c} \text{the common} \\ \text{divisors of} \\ a \text{ and } b \end{array} \right\} = \left\{ \begin{array}{c} \text{the common} \\ \text{divisors of} \\ a \text{ and } b - s \cdot a \end{array} \right\}$$

"$\subseteq$" If $k \mid a$ and $k \mid b \Rightarrow \begin{cases} k \mid a \\ k \mid 1 \cdot b - s\,a \end{cases}$

"$\supseteq$" If $t \mid a$ and $t \mid b - sa \Rightarrow$

$$\begin{cases} t \mid s \cdot a + 1 \cdot (b - sa) = b \\ t \mid a \end{cases} \quad \otimes$$

Prof: In fact $\exists\, u, v \in \mathbb{Z}$ s.t.

$u \cdot a + v \cdot b = \gcd(a, b)$

E. Algorithm: Input: $a, b \in \mathbb{Z}$

Output: $\gcd(a, b)$ and $u, v \in \mathbb{Z}$ s.t. $ua + vb = \gcd(a, b)$

- If $b = 0$: $\gcd(a, b) = 0$

- Assume $b \neq 0$: Divide with reminder

$a = b \cdot q_1 + r_1 \qquad 0 \leq r_1 < |b|$

- if $r_1 = 0 \Rightarrow \gcd = b$

- if $r_1 \neq 0$, $b = r_1 \cdot q_2 + r_2$; $0 \leq r_2 < |r_1| = r_1$

- if $r_2 = 0 \Rightarrow \gcd = r_1$

- if $r_2 \neq 0 \Rightarrow r_1 = r_2 \cdot q_3 + r_3$;

$0 \leq r_3 < r_2$

$$r_t = r_{t+1} \cdot q_{t+2} + r_{t+2} \leftarrow \text{the last reminder} \neq 0$$

$$r_{t+1} = r_{t+2} \cdot q_{t+3} + 0$$

Claim: The last nonzero reminder is $\gcd(a,b)$

- The algorithm ends because

  $|b| > r_1 > r_2$

  So there are $\leq |b|$ divisors $\Rightarrow$ it stops

- Corectnes:

  $$\gcd(a,b) = \gcd(b, \underbrace{a - b \cdot q_1}_{r_1}) =$$

  $$= \gcd(r_1, r_2) = \gcd(r_2, r_3) = \dots$$

  $$\dots = \gcd(r_{t+1}, r_{t+2}) = r_{t+2}$$

  $$r_{t+2} \mid r_{t+2}$$

Fact: If $r_i \neq 0$

$$r_{i+2} < \frac{1}{2} \cdot r_i \quad \forall\, i \text{ with } r_i \neq 0$$

Idea: To get u and v: follow the direction backwards

$$a = r_{k+2} = 1 \cdot r_k - q_{k+2} \cdot r_{k+1} = \dots a + \dots b$$

Rmk: u and v s.t. $u \cdot a + v \cdot b = \gcd(a,b)$ are NOT unique

Rmk: The output is < 0

when: ($b = 0$ & $a < 0$)

AND: ($b \neq 0$ & $a < 0$ & $a \mid b$)

i.e. $r_1 = 0$

Defn: $a, b \in \mathbb{Z}$ are called **coprime** integers if $\gcd(a,b) = 1$

Properties of gcd

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

$\gcd(a,b) = 1 \iff \exists\, u, v \in \mathbb{Z}$ $ua + vb = 1$

Pf: "$\Rightarrow$" ✓

"$\Leftarrow$" Assume $ua + vb = 1$

Let $d \mid a$, $d \mid b$ $\Rightarrow d \mid ua + vb = 1 \Rightarrow d = \pm 1$

± 1 the only common divisors $\Rightarrow \gcd(a,b) = 1$

2) Let $d = \gcd(a,b)$

Then $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$

Pf $\exists u, v \in \mathbb{Z} \quad d = u \cdot a + v \cdot b$

$d \mid a \;\&\; d \mid b \quad 1 = u \cdot \frac{a}{d} + v \cdot \frac{b}{a} \Rightarrow$

1) $\Rightarrow \gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$

3) Assume $a, b \neq 0$

$\min \{ ua + vb \mid u, v \in \mathbb{Z}, ua + vb \geq 0 \} = \gcd(a, b)$

Pf: Denote $A = \{ \quad \subseteq \mathbb{N} \} \Rightarrow$

- $A \neq \phi \quad 0 = 0 \cdot a + 0 \cdot b \in A$

$\Rightarrow$ Let $d := \min A$

By Euclid's Alg. $\Rightarrow \gcd(a, b) \in A \Rightarrow$

$\Rightarrow d \leq \gcd(a, b)$

$\gcd(a, b) \mid ua + vb \quad \forall u, v \in \mathbb{Z} \Rightarrow$

$\Rightarrow \gcd(a,b) \mid d$ } $\Rightarrow d = \gcd(a,b)$

Positive terms }

4) $c \neq 0$

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

Pf: Use 3

$$\gcd(a \cdot c, bc) = \min\{u \cdot a \cdot c + v \cdot b \cdot c \mid u, v \in \mathbb{Z}, \; uac + vbc \geq 0\}$$

$$= c \cdot \min\{ua + vb \mid u, v \in \mathbb{Z} \;\; ua + vb \geq 0\}$$

3)

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

5) $a, b, c \in \mathbb{Z}$

$1 = \gcd(a,b) = \gcd(a,c) \Rightarrow \gcd(a, b\cdot c) = 1$

Pf: $1 = u\cdot a + v\cdot b$ for some $u, v \in \mathbb{Z}$

$\times \quad 1 = u'\cdot a + v'\cdot c$

$1 = (u\cdot u'\cdot a + u\cdot v'\cdot c + u'\cdot b)a + v\cdot v'\cdot bc \Rightarrow$

$\Rightarrow \gcd(a, bc) = 1$

6) If $a \mid b\cdot c$ and $\gcd(a,b) = 1 \Rightarrow a \mid c$

Pf: $1 = u\cdot a + v\cdot b$ for $u, v \in \mathbb{Z}$ $\quad 1\cdot c$

$c = u\cdot ac + v\cdot bc \Longrightarrow a \mid c$

$\downarrow$

$a \mid ac$

$\downarrow$

$a \mid bc$

7) If $c \neq 0$ and $ac \mid bc \Rightarrow a \mid b$

Pf: $\exists k \in \mathbb{Z}$ $k \cdot ac = b \cdot c \Rightarrow k a = b \Rightarrow a \mid b$

Prop: Assume $a, b \in \mathbb{N}^*$

Then $\gcd(a,b) \cdot \operatorname{lcm}(a,b) = a \cdot b$

Pf: $\frac{a \cdot b}{\gcd(a,b)}$ satisfy properties for LCM

Let $d = \gcd(a,b)$

$a = d \cdot a_1$

$b = d \cdot b_1$

where $a_1, b_1 \in \mathbb{Z}$, $1 = \gcd(a_1, b_1)$

Denote:

$l = \frac{ab}{d} = a_1 \cdot b = a \cdot b_1 \Rightarrow l$ is a common multiple for a & b

Let $m \in \mathbb{Z}$ be another common multiple

$a \mid m$ and $b \mid m$

$a \mid m \Rightarrow$ we note $m = a \cdot m_1, m_1 \in \mathbb{Z}$

$$b \mid a \cdot m_1$$

$$d \cdot b_1 \mid a \cdot m_1$$

$$b_1 \mid a_1 \cdot m_1 \xrightarrow{\gcd(a_1, b_1) = 1} b_1 \mid m_1 \mid \cdot a$$

$$l = a \cdot b_1 \mid m_1 \cdot a = m$$

So l is $LCM(a, b)$; $l = \gcd(a, b)$