# EUCLID'S ALGORISM

Algorism ① the art of computing with Hindu-Arabic numerals
Origin from al-Khowarrismi name (and work) translated into LATIN

Algorism - ② preserved in mathematics as repeated calculating process
Algorismus of John of Halifax (1250)

## GREATEST COMMON DIVISOR

① Let $a, b \in \mathbb{Z}$. IF a number c divides a and b simultaneously THEN c is called a COMMON DIVISOR of a and b

DEFINITION

c is a COMMON DIVISOR of a and b iff $c \mid a$ and $c \mid b$ $\quad a, b, c \in \mathbb{Z}$

Let $\boxed{A = \{c : c|a \text{ and } c|b\}}$

be a set of ALL COMMON DIVISORS of

a and b.

Set A is finite, hence it must

have a $\boxed{\text{GREATEST ELEMENT}}$

i.e a poset $(A, \leq)$ has a greatest

element. This element is

called the GREATEST COMMON

DIVISOR of a and b, (g.c.d)

of a and b.

NOTATION : $\boxed{(a, b) = g.c.d\,(a, b)}$

FORMAL DEFINITION (book)

$$\boxed{gcd(a,b) = (a,b) = \max\{c : c|a \wedge c|b\}}$$

REMARK : $(A, \leq)$ is a FINITE linear poset

hence maximal element is

unique and is the GREATEST

element. and exists!

$\gcd(a,b) = (a,b) = \max\{c : c|a \wedge c|b\}$

Remark:

Every number has the ~~or~~ divisor 1, so $\gcd(a,b)$ is a POSITIVE NUMBER

$a, b$ are RELATIVELY PRIME iff $(a,b) = 1$

In this case $\pm 1$ are the only common divisors

Example

$(24, 56) = 8$

$(15, 22) = 1$ i.e 15, 22 are relatively PRIME

THEOREM

Any common divisor of two numbers divides their greatest common divisor.

Proof: by procedure known as EUCLID ALGORISM (algorithm)

Euclid algorism from the seventh book of Euclid's ELEMENTS (about 300 B.C.); however it is certainly of earlier orgin

Let $a, b$ be two integers whose g.c.d$(a,b) = (a,b)$ we wants to find.

We assume $a \geq b$

1. we divide $a$ by $b$ with respect to the least positive reminder

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

2. We divide $b$ by $r_1$

$$b = q_2 r_1 + r_2 \qquad 0 \leq r_2 < r_1$$

3. we divide $r_1$ by $r_2$

$$r_1 = q_3 r_2 + r_3 \qquad 0 \leq r_3 < r_2$$

CONTINUE;

Observe:

reminders $r_1, r_2, \dots r_k \dots$

form a DECREASING sequence of positive integers

$$\boxed{r_1 > r_2 > \dots > r_n \dots}$$

and one MUST arrive on division for which $r_{n+1} = 0$

Process:

Euclid's algorithm

$$a = q_1 b + r_1$$
$$b = q_2 r_1 + r_2$$
$$r_1 = q_3 r_2 + r_3$$
$$\dots\dots$$
$$r_{n-2} = q_n r_{n-1} + r_n$$
$$r_{n-1} = q_{n+1} r_n$$

TO PROVE: $\boxed{g.c.d(a,b) = (a,b) = r_n}$

# EXAMPLE

Find $\boxed{\gcd(76{,}084,\ 63{,}020)}$

$$76{,}084 = 63{,}020 \cdot \overset{q_1}{1} + \overset{r_1}{13{,}064}$$

$$63{,}020 = 13{,}064 \cdot 4^{q_2} + 10{,}764^{r_2}$$

$$13{,}064 = 10{,}764 \cdot 1 + 2{,}300^{r_3}$$

$$10{,}764 = 2{,}300 \cdot 4 + 1{,}564^{r_4}$$

$$2{,}300 = 1{,}564 \cdot 1 + 736^{r_5}$$

$$1{,}564 = 736 \cdot 2 + 92^{r_6}$$

$$736 = 92 \cdot 2$$

$$\boxed{\gcd(76{,}084,\ 63{,}020) = 92}$$

$$\boxed{(76{,}084,\ 63{,}020) = 92}$$

**Proof** that $\boxed{(a,b) = \gcd(a,b) = r_n}$

i.e g.c.d$(a,b)$ is the last non-vanishing remainder in the process.

~~Observe:~~

**FIRST STEP**: show that $r_n$ divides $a$ and $b$:

$$\boxed{r_n \mid a \ \wedge \ r_n \mid b}$$

1. $\boxed{r_{n-1} = q_{n+1} \cdot r_n}$ hence $r_n \mid r_{n-1}$

2. $\boxed{r_{n-2} = q_n r_{n-1} + r_n}$ ~~hence~~

$$= q_n (q_{n+1} r_n) + r_n$$

$$= r_n ( q_n q_{n+1} + 1)$$

hence $r_n \mid r_{n-2}$

3. $\boxed{r_{n-3} = q_{n-1} r_{n-2} + r_{n-1}}$

and $r_n \mid r_{n-1}$, $r_n \mid r_{n-2}$ from 1, 2

hence $\boxed{r_n \mid r_{n-3}}$

DOUBLE INDUCTION

BASE CASE is 1 and 2

ASSUME $\boxed{r_n \mid r_{k-1} \text{ and } r_n \mid r_{k-1}}$

We have

$$r_k = q_{k+2} r_{k-1} + r_{k-2}$$

so we get $\boxed{r_n \mid r_k}$.

We proved

$\boxed{r_n \mid r_k \text{ for all } k \geq 1}$

in particular $\boxed{r_n \mid r_1 \text{ and } r_n \mid r_2}$

$b = q_2 r_2 + r_n$

and $r_n | r_2$, $r_n | r_1$, hence $r_n | b$.

$a = q_1 b + r_1$ and $r_n | b$, $r_n | r_1$

hence $r_n | a$.

$\boxed{\text{STEP 2}}$

Show that $r_n$ is the greatest common divisor of a and b

~~Assume~~ Let $\boxed{A = \{c : c|a \wedge c|b\}}$

We show that ~~for~~ any $c \in A$

$$\boxed{c | r_n}$$

i.e $r_n$ is the greatest common divisor

We have

$a = q_1 b + r_1$ and $\boxed{r_1 = a - q_1 b}$

So any $c$, $c|a$ and $c|b$ we have $c|r_1$

$b = q_2 r_1 + r_2$ and $\boxed{r_2 = b - q_2 r_1}$, hence

$c | r_2$ ... so on and get $c | r_n$!

# $\boxed{\text{FASTER ALGORITHM}}$

$\boxed{\text{KRONECKER}}$ (1823-1891) proved that no Euclid algorism can be SHORTER than one obtained by LEAST ABSOLUTE REMAINDERS ($r_n$ can be negative)

Example

FIND (76,084, 63,020) by the least absolute remainders

$$76{,}084 = 63{,}020 \cdot 1 + 13{,}064$$
$$63{,}020 = 13{,}064 \cdot 5 - 2{,}300$$
$$13{,}064 = 2{,}300 \cdot 6 - 736$$
$$2{,}300 = 736 \cdot 2 + 92$$
$$736 = 92 \cdot 8$$

$$(76{,}084\ ,\ 63{,}020) = 92$$

in 5 steps ($r_4$) instead of 7 steps

Book chapters 3, 4 

$\boxed{\lfloor x \rfloor = \text{the greatest integer less or equal to } x \text{ (floor)}}$

$\boxed{\lceil x \rceil = \text{the least integer greater than or equal to } x \text{ (ceiling)}}$

Properties

$\lfloor x \rfloor = n$ iff $n \le x < n+1$

$\lfloor x \rfloor = n$ iff $x-1 < n \le x$

$\lceil x \rceil = n$ iff $n-1 < x \le n$

$\lceil x \rceil = n$ iff $x \le n < x+1$

$\boxed{\lfloor x + n \rfloor = \lfloor x \rfloor + n}$ $\quad n \in \mathbb{Z}$

$\lfloor nx \rfloor \neq n \lfloor x \rfloor$ $\quad n = 2,\ x = \frac{1}{2}$

$\boxed{\{x\} = x - \lfloor x \rfloor}$

$\{x\}$ FUNCTIONAL PART of $x$

$\lfloor x \rfloor$ integer part

MOD ; the binary operation

$x, y \in$ Positive integers OR $x, y \in R$

$$x = qy + r$$

reminder $r$

$$x = \left\lfloor \frac{x}{y} \right\rfloor \cdot y + x \bmod y$$

Quotient $q$

$$\boxed{x \bmod y = x - y \left\lfloor \frac{x}{y} \right\rfloor} \quad y \neq \phi$$

$$5 \bmod 3 = 5 - 3 \cdot \left\lfloor \frac{5}{3} \right\rfloor = 5 - 3 = 2$$

$$5 \bmod -3 = 5 - (-3) \left\lfloor \frac{5}{(-3)} \right\rfloor = 5 - (-3)(-1) = -1$$

$5 = 3 \cdot 1 + 2$ $\quad$ $r = 2$ $\quad$ $5 \bmod 3 = 2$

$5 = (-3)(-1) - 1$ $\quad$ $r = -1$ $\quad$ $5 \bmod (-3) = -1$

$$-5 \bmod 3 = -5 - 3 \left\lfloor -\frac{5}{3} \right\rfloor = -5 - 3(-1) = 1$$

$$-5 \bmod 3 = -5 - (-3) \left\lfloor \frac{5}{3} \right\rfloor = -5 + 3 = -2$$

# EUCLID'S ALGORITHM

Function

$gcd(m, n)$, for $\boxed{0 \le m < n}$

Defined recursively

$$\boxed{\begin{aligned} &gcd(0, n) = n \qquad m = 0 \\ &gcd(m, n) = gcd(n \bmod m, m) \\ &\qquad \text{for } m > 0 \end{aligned}}$$

EXAMPLE 1

$\boxed{gcd(12, 18)} = gcd(6, 12) = gcd(0, 6) = \boxed{6}$

Example 2

$\boxed{gcd(63{,}020, 76{,}084)} = gcd(13{,}064, 63{,}020)$
$= gcd(10{,}764, 13{,}064) = gcd(2{,}300, 10{,}764)$
$= gcd(1{,}564, 2{,}300) = gcd(736, 1{,}564)$
$= gcd(92, 736) = gcd(0, 92) = 92$

# DIVISION LEMMA

Theorem 1

when a product $\boxed{ac}$ is divisible by a number $\boxed{b}$ that is relatively prime to $\boxed{a}$, the factor $c$ must be divisible by $b$

Symbolically:

relatively PRIME

If $b \mid ac$ and $(b, a) = 1$

$\gcd(b, a) = 1$

then $b \mid c$.

Proof. Since $(a, b) = 1$ ( $a, b$ relatively prime) hence the last reminder $r_n$ in EA must be 1, so EA has a form

$$a = q_1 b + r_1$$
$$b = q_2 r_1 + r_2$$
$$\cdots\cdots$$
$$r_{n-2} = q_n r_{n-1} + 1$$

HENCE

$$ac = q_1 bc + r_1 c$$
$$\cdots\cdots\cdots$$
$$r_{n-2} \cdot c = q_n r_{n-1} \cdot c + c$$

(1) $ac = q_1 bc + r_1 c$

(2) $bc = q_2 r_1 c + r_2 c$

$\cdots\cdots\cdots\cdots\cdots$

$r_{n-2} \cdot c = q_n r_{n-1} \cdot c + c$ (n-2)

and $b \mid ac$, so $b \mid r_1 c$ from (1)

from (2) $b \mid r_2 c$

By induction: $b \mid r_i c$ all $i \in \mathbb{N}$

in particular $b \mid r_{n-2} c$ and from (n-2)

$\boxed{b \mid c}$

Theorem 2

When a number is relatively prime to each of several numbers, it is relatively prime to their product.

SYMBOLICALLY:

If $(a, b_i) = 1 \quad i = 1..k$,

then $(a, b_1 \cdot b_2 .. b_k) = 1$

Theorem 2

If $(a, b_i) = 1$ for $i = 1 \dots k$

then $(a, b_1 b_2 \cdots b_k) = 1$

Proof (by contradiction) $b_1 = b$, $b_2 = c$

Case $i = 2$ + induction

Assume $\boxed{(a, b) = 1}$ and $\boxed{(a, c) = 1}$

and $(a, bc) \neq 1$ i.e $a$ has a common divisor $d$ with $bc$ i.e

$d \mid a$ and $d \mid bc$

and $(a, b) = 1$, hence $\boxed{(d, b) = 1}$

we get

$d \mid bc$ and $(d, b) = 1$, so By THEOREM 1

$d \mid c$.

We Have ~~get~~ $\boxed{d \mid a}$ and $\boxed{(a, c) = 1}$

hence $\boxed{(d, c) = 1}$ contradiction with $d \mid c$.

# Theorem 3

$$\boxed{(ma, mb) = m(a, b)}$$

i.e $\gcd(ma, mb) = m \gcd(a, b)$

Proof

$(a, b) = r_n$ in EA

$a = q_1 b + r_1$

$b = q_2 r_1 + r_2$

$\vdots$

$r_{n-2} = q_n r_{n-1} + r_n$

$r_{n-1} = q_{n+1} r_n$

MULTIPLY each step by $m$

$am = q_1 bm + r_1 m$

$bm = q_2 r_1 m + r_2 m$

$\vdots$

$r_{n-2} m = q_n r_{n-1} m + r_n m$

$r_{n-1} m = q_{n+1} r_n m$

This is EA for $am$, $bm$

$r_n m = m(a, b)$

and $r_n m = (ma, mb)$

so $(ma, mb) = m(a, b)$

Theorem 4



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

$a = a_1 (a,b)$ , $b = b_1 (a,b)$

then $(a_1, b_1) = 1$

(i.e $a_1 b$ are relatively prime

Proof

Use $\boxed{(ma\ mb) = m(a,b)}$

Denote $(a,b) = d$, we have

$a = a_1 d$ and $b = b_1 d$ we get

$$(a,b) = (a_1 d, b_1 d) = d(a_1 b_1)$$

i.e

$$\boxed{(a,b) = (a,b)(a_1, b_1)}$$

and $(a_1, b_1) = 1$

Reduction of FRACTIONS

$a = a_1 d$
$b = b_1 d$

$$\frac{a}{b} = \frac{a_1 d}{b_1 d} = \frac{a_1}{b_1} \quad \text{for } \boxed{(a_1, b_1) = 1}$$

# $\boxed{\text{LEAST COMMON MULTIPLE}}$

COMMON MULTIPLE

$\boxed{m = \text{lcm}(a,b) \text{ iff } a|m \text{ and } b|m}$

m is a $\boxed{\text{COMMON MULTIPLE}}$ of $a, b$ iff is divisible by both of them

Example

$ab$ is a common multiple of $a, b$

We CONSIDER ONLY POSITIVE MULTIPLES and hence we always have the smallest one between them (set of COMMON MULTIPLES is finite)

$\boxed{\text{LEAST}}$ COMMON MULTIPLE $[a b] = \text{lcm}(a, b)$

$$\boxed{[a,b] = \text{lcm}(a,b) = \min\{m : a|m \wedge b|m\}}$$

(In a linearly ordered finite set minimal element is the smallest)

$$\boxed{[a,b] = \text{lcm}(a,b) = \text{smalest}\{m : a|m \wedge b|m\}}$$

Theorem

$\boxed{\text{Any common multiple of } a \text{ and } b \text{ is divisible by the } \operatorname{lcm}(a,b)}$

Proof

Let $\boxed{m = \text{cm}(a,b)}$.

We divide $m$ by $\operatorname{lcm}(a,b) = [a,b]$

$\boxed{m = q\,[a,b] + r}$ $\quad 0 \le r < [a,b]$

But $a \mid [a,b]$ , $b \mid [a,b]$

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

HENCE $a \mid r$ and $a \mid r$

and $\boxed{r \text{ is a common multiple}}$ of $a, b$

and $0 \le r < [a,b]$ and $[a,b]$ is the smallest c.m , so $r = 0$ . what proves that $m = q[a,b]$ i.e

$m$ is divisible by $[a,b]$

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

$$a = a_1 (a,b) \qquad b = b_1 (a,b)$$

Denote $d = (a,b)$ and write

$$a = a_1 d \qquad b = b_1 d \qquad b_1 = \frac{b}{d}$$

Consider a multiple of $a$:

$$\boxed{h a = h a_1 d}$$

Observe that if $ha$ is divisible by $b = b_1 d$, the factor $h a_1 d$ is divisible by $b_1 d$ and hence $h a_1$ is divisible by $b_1$.

By theorem 3 ( If $a = a_1 d$, $b = b_1 d$, then $(a_1, b_1) = 1$ ) $a_1, b_1$ are relatively prime, so if $h a_1$ is div by $b_1$ we get that $h$ is divisible by $b_1$ i.e

$$\boxed{h = k b_1}$$

So any common multiple of $a, b$ has a form $\boxed{m} = k b_1 a = k \frac{b}{d} a = \boxed{k \frac{ab}{d}}$

We proved a fact:

FACT



Any common multiple $m$ of $a$ and $b$ has a form

$$\boxed{m = k \cdot \frac{ab}{(a,b)}}$$

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

Take $k=1$ ; we get

Theorem 4

When $a,b$ are two numbers with the greatest common diviser $(a,b)$, the least common multiple $[a,b]=m$ is

$$[a,b] = \frac{ab}{(a,b)}$$

and

$$\boxed{[a,b](a,b) = ab}$$

or

$$\boxed{\mathrm{lcm}(a,b) \cdot \gcd(a,b) = a \cdot b}$$