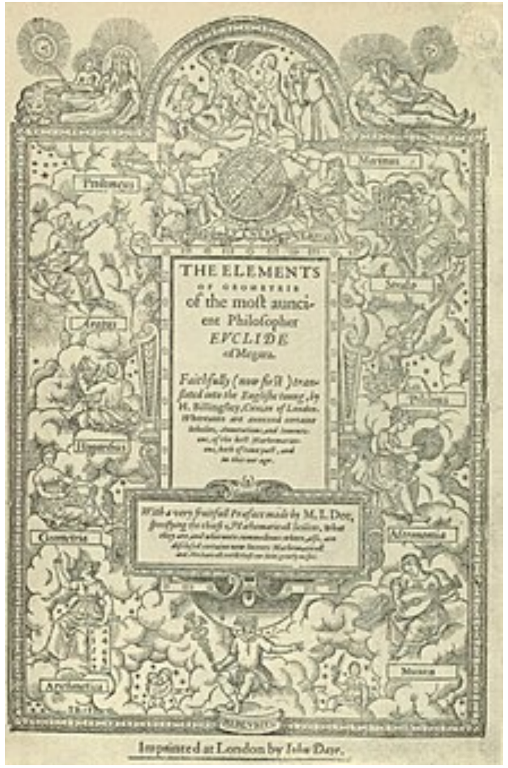
Euclidean Algorithms

In mathematics, the Euclidean algorithm or Euclid's algorithm, is an efficient method for computing the greatest common divisor (GCD) of two integers (numbers), the largest number that divides them both without a remainder.

- Euclid - Laws of nature are just the mathematical thoughts of God.
- Ancient Greek mathematician Euclid in Alexandria, Ptolemaic Egypt c. 300 BC.
- Father of Geometry



Algorithm:

Input: Two positive integers a,b

$$a = bq + r \qquad 0 \le r < b$$

$$b = rq_1 + r_1 \qquad 0 \le r_1 < r$$

$$r = r_1 q_2 + r_2 \qquad 0 \le r_2 < r_1$$

$$\vdots$$

(continue until remainder is zero)

$$r_{i-2} = r_{i-1} q_i + r_i \qquad 0 \le r_i < r_{i-1}$$

$$r_{i-1} = r_i q_{i+1} + 0$$

The last nonzero remainder is the gcd

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

https://www.youtube.com/watch?v=H_2_nqKAZ5w

Example:

Input: 34, 55

$$55 = 34(1) + 21$$

$$34 = 21(1) + 13$$

$$21 = 13(1) + 8$$

$$13 = 8(1) + 5$$

$$8 = 5(1) + 3$$

$$5 = 3(1) + 2$$

$$3 = 2(1) + 1$$

$$2 = 2(1) + 0$$

$$\gcd(55,34) = 1$$

Euclidean Algorithm

Algorithm:

Input: Two positive integers a,b

$a = bq + r \qquad 0 \le r < b$

$b = rq_1 + r_1 \qquad 0 \le r_1 < r$

$r = r_1q_2 + r_2 \qquad 0 \le r_2 < r_1$

.

.

.

(continue until remainder is zero)

$r_{i-2} = r_{i-1}q_i + r_i \quad 0 \le r_i < r_{i-1}$

$r_{i-1} = r_iq_{i+1} + 0$

$\gcd(a,b) = r_i$

Why it works:

Thm:

If $a = bq + r$, then $\gcd(a,b) = \gcd(b,r)$

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

$\gcd(b,r) = \gcd(r, r_1)$

$\gcd(r,r_1) = \gcd(r_1,r_2)$

$\vdots$

$= \gcd(r_{i-1},r_i) = \gcd(r_i,0) = r_i$

Euclidean Algorithm

Algorithm:

Input: Two positive integers a,b

$a = bq + r \qquad 0 \le r < b$

$b = rq_1 + r_1 \qquad 0 \le r_1 < r$

$r = r_1q_2 + r_2 \qquad 0 \le r_2 < r_1$

.

.

.

(continue until remainder is zero)

$r_{i-2} = r_{i-1}q_i + r_i \quad 0 \le r_i < r_{i-1}$

$r_{i-1} = r_iq_{i+1} + 0$

$\gcd(a,b) = r_i$

Why it works:

Thm:

If $a = bq + r$, then $\gcd(a,b) = \gcd(b,r)$

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

$\gcd(b,r) = \gcd(r, r_1)$

$\gcd(r,r_1) = \gcd(r_1,r_2)$

$\vdots$

$= \gcd(r_{i-1},r_i) = \gcd(r_i,0) = r_i$

Proof of Thm:

Let d be any common divisor of a and b.

$d \mid a,\ d \mid b \longrightarrow d \mid (a - bq) \longrightarrow d \mid r$

Let e be any common divisor of b and r.

$e \mid b,\ e \mid r \longrightarrow e \mid bq + r \longrightarrow e \mid a$

$\longrightarrow$ d is a common divisor of a and b iff

d is a common divisor of b and r.

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

DIVISIBILITY.

$a \mid b$ iff $\exists c : ac = b$

divides

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

$c \in \mathbb{Z}^+$

$2 \mid 8$

$2c = 8$

$c = 4$

$4 \in \mathbb{Z}^+$ ✓

$5 \mid 13$

$5c = 13$

$c = 13/5 = 2.6 \in \mathbb{Z}^+?$

✗

$5 \nmid 13$

PROVE:

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

$3|15$
$3|9$ $\rightarrow 3|24$

$ak=b$

$aj=c$

$$\boxed{\begin{aligned} b+c &= ak+aj \\ &= a(k+j) \end{aligned}}$$

$m=(b+c)$ $n=(k+j)$

$m=an \longrightarrow a|m \rightarrow a|b+c$

If $\underline{a|b}$ and $\underline{b|c}$ then $a|c$.

$ak = b$

$bj = c$

$3|6 \quad 6|18$

$3|108$

$$c = bj$$
$$= (ak)j$$
$$= a(\underbrace{kj})$$

$a|c$

DIVISION ALGORITHM

Let $a \in \mathbb{Z}$, $d \in \mathbb{Z}^+$.
Then there are unique integers q and r such that

$$\boxed{a} = \boxed{dq} + \underline{r}$$

$$1999 = \underbrace{1 \cdot 1000} + \underbrace{999}$$

Ex.

$$53 = 3 \cdot \underline{17} + \underline{2}$$

$$0 \leq r < q$$

Euçlidian Algorithm

If $a = bq + r$

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