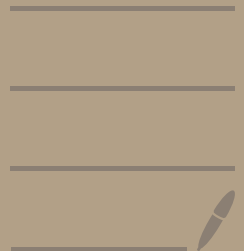


L24 - 01/11/2024



Euclidean Algorithm (Book VII)

- may be known earlier
credits to Euclid for its presentation
& applications to Number Theory

Recall, GCD of nat. nos m, n
is the largest nat. no. s.t it divides
both m & n .

- Input: A pair of non-(-ve) int. (a_0, b_0)

Set $i = 0$

If $a_i = 0$, output b_i and if $b_i = 0$,
output a_i

Else, set

$$a_{i+1} = \max(a_i, b_i) - \min(a_i, b_i)$$

$$b_{i+1} = \min(a_i, b_i)$$

- Key: If $a \geq b$, then
 $\text{GCD}(a, b) = \text{GCD}(a-b, b)$

Consequences (given in the elements)

1 \exists int. x_0, y_0 s.t. $\text{GCD}(a, b) = ax_0 + by_0$

- Key: a_i & b_i are int. comb. of a, b
By indⁿ, all a_i 's & b_i 's are
int. comb.

\therefore After finite steps, one of a_i, b_i
becomes GCD.

\therefore GCD is also an int. comb. of a & b .

Furthermore, if $\text{GCD}(a, b) \mid d$,

\exists int. x, y s.t. $d = ax + by$

where $x = \frac{dx_0}{\text{GCD}(a, b)}$, $y = \frac{dy_0}{\text{GCD}(a, b)}$

2. If a prime p divides ab , then
 $p|a$ or $p|b$.

Pf - wlog suppose $p \nmid a$
Then, $\text{GCD}(a, p) = 1$

$$\text{So, } \exists x_0, y_0 \in \mathbb{Z} \text{ s.t. } 1 = ax_0 + py_0$$

$$\Rightarrow b = abx_0 + pby_0$$

$$\therefore p|ab \Rightarrow p|abx_0 + pby_0$$

$$\therefore p|b$$

□

3. Fundamental Theorem of Arithmetic

Any (+ve) int. $n (\geq 2)$ can be expressed
as a product of primes $n = p_1 \dots p_k$
& the seq. (p_1, \dots, p_k) is unique upto
rearrangement.

- Key: If n is prime, then the hypothesis is true

Else, $\exists a, b \neq 1$ s.t. $n = a \cdot b$

$\therefore a$ & b can be written as a prod. of primes

$\therefore n$ can also be written as a prod. of primes

Hence, existence of prime factorization follows by indⁿ.

Suppose there are nos. ($n \geq 2$) having prime factorizations which are not rearrangements of each other.

Consider the smallest such no.

$$n = p_1 \cdots p_k = q_1 \cdots q_r$$

This implies $\{p_1, \dots, p_k\}$ & $\{q_1, \dots, q_r\}$ are disjoint.

But, $q_i \mid q_1 \cdots q_r \Rightarrow q_i \mid p_1 \cdots p_k$

$\therefore q_i = p_j$ for some $1 \leq j \leq k$
which is a contraⁿ

Pell's Eqⁿ

$$x^2 - Ny^2 = 1, \quad N - \text{non-perfect square}$$

Most well studied after $x^2 + y^2 = 1$

- Pythagoras ($N=2$)

Suppose (x_n, y_n) is a solⁿ.

$$\text{i.e. } x_n^2 - 2y_n^2 = 1.$$

$$\begin{aligned} \text{Then } x_{n+1} &= (x_n + 2y_n) \\ y_{n+1} &= (x_n + y_n) \end{aligned}$$

$$\begin{aligned} x_{n+1}^2 - 2y_{n+1}^2 &= (x_n + 2y_n)^2 - 2(x_n + y_n)^2 \\ &= 2y_n^2 - x_n^2 = -1 \end{aligned}$$

Hence, (x_{n+2}, y_{n+2}) will be a solⁿ.

$$(x_0, y_0) = (1, 0)$$

- Cattle problem of Archimedes

$$x^2 - 472424 y^2 = 1$$

The smallest non-trivial solⁿ has
206545 digits

(See : HW Lenstra Jr - Solving the Pell's Eqⁿ)

Comparison b/w Greek & Indian Math

Greek

Indian

Motivation

- Intrinsic

- Vedas, rituals,
astronomy, poetry

Proofs

- Heavy
emphasis

- Not much emphasis

Aim

- Explain
all of nature
with Math

- Specific applications