L24 - 01/11/2024

Euclidian 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

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

- <u>Key</u> : If $a \geq b$, then

$$GCD(a, b) = GCD(a-b, b)$$

<u>Consequences</u> (given in the elements)

<u>1</u> $\exists$ int. x_0, y_0 s.t $GCD(a, b) = ax_0 + by_0$

- <u>Key</u> : a_i & b_i are int. comb. of a, b

  By ind^n, all a_is & b_is are int. combs.

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

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

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

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

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

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

Pf - WLOG suppose $p \nmid a$

Then, $GCD(a, p) = 1$

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

$$\Rightarrow b = abx_0 + pby_0$$

$\because p \mid ab \Rightarrow p \mid abx_0 + pby_0$

$\therefore p \mid b$

$\square$

3. Fundamental Theorem of Arithmetic

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

- <u>Key</u>: If n is prime, then the hypothesis is true

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

$\because$ 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 ind^n.

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

Consider the smallest such no.

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

This implies $\{p_1, \ldots, p_k\}$ & $\{q_1, \ldots, q_r\}$ 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 contd^n

Pell's Eq^n

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

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

- Pythagoras $(N = 2)$

Suppose (x_n, y_n) is a sol^n.

i.e $x_n^2 - 2y_n^2 = 1$.

Then
$$x_{n+1} = (x_n + 2y_n)$$
$$y_{n+1} = (x_n + y_n)$$

$$x_{n+1}^2 - 2y_{n+1}^2 = (x_n + 2y_n)^2 - 2(x_n + y_n)^2$$
$$= 2y_n^2 - x_n^2 = -1$$

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

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

– Cattle problem of Archimedes

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

The smallest non-trivial sol^n has 206545 digits

(<u>See</u> : HW Lenstra Jr – Solving the Pell's Eq^n)

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