GCD

Greatest Common Divisor

Begin ~~lar~~

Def:- A positive integer 'a' is said to be the gcd (greatest common divisor) of two integers m and n if

(i) $a | m$, $a | n$ (a divides m & n)

and (ii) If $b | m$, $b | n$ then $b \leq a$.

we denote it by $\gcd(m,n) = a$ or simply $(m,n) = a$.

Euclidean Algorithm:-

To find $\gcd(m,n)$. Suppose $m > n$ then write

$m = q_1 n + r_1$ where $0 \leq r_1 < n$

$n = q_2 r_1 + r_2$ " $0 \leq r_2 < r_1$

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

Continue this way till the remainder become zero. Then the last nonzero remainder is the gcd

eg. (1) To find $\gcd(24, 18)$

$24 = 1 \cdot 18 + 6 \longrightarrow \gcd.$

$18 = 3 \cdot 6 + 0 \longrightarrow$ remainder zero

$\therefore \gcd(24,18) = 6$

(ii) To find gcd(83, 38)

$83 = 2 \cdot 38 + 7$

$38 = 5 \cdot 7 + 2$

$7 = 3 \cdot 2 + 1 \longrightarrow$ gcd

$2 = 2 \cdot 1 + 0$

$\therefore$ $\gcd(83, 38) = 1$.

(iii) To find gcd(126, 35)

$126 = 3 \cdot 35 + 21$

$35 = 1 \cdot 21 + 14$

$21 = 1 \cdot 14 + 7 \rightarrow$ gcd

$14 = 2 \cdot 7 + 0$

$\gcd(126, 35) = 7$

Prop:- If $d = \gcd(m, n)$ then there exist integers x & y s.t $d = mx + ny$.

For example, $\gcd(126, 35) = 7$

From above we see that

$$7 = 21 - 1 \cdot 14$$
$$= 21 - 1 \cdot (35 - 1 \cdot 21)$$
$$= 2 \cdot 21 - 1 \cdot 35$$
$$= 2(126 - 3 \cdot 35) - 1 \cdot 35$$
$$= 2 \cdot 126 - 7 \cdot 35$$

so $x = 2$, $y = -7$

Matrix representation of Euclidean Algorithm -

eg. To find gcd (126, 35) by matrix method.

Start with

$$x + 0.y = 126$$

$$0.x + y = 35$$

Then by elementary row operation try to make $mx + ny = d$ till the last digit of second row become zero.

Start with
$$\left[\begin{array}{cc:c} 1 & 0 & 126 \\ 0 & 1 & 35 \end{array}\right]$$

$$\sim \left[\begin{array}{cc:c} 1 & -3 & 21 \\ 0 & 1 & 35 \end{array}\right] \quad R_1 \to R_1 - 3.R_2$$

$$\sim \left[\begin{array}{cc:c} 1 & -3 & 21 \\ -1 & 4 & 14 \end{array}\right] \quad R_2 \to R_2 - R_1$$

$$\sim \left[\begin{array}{cc|c} 2 & -7 & 7 \\ -1 & 4 & 14 \end{array}\right] \quad R_1 \to R_1 - R_2$$

$$\sim \left[\begin{array}{cc:c} 2 & -7 & 7 \\ -5 & 18 & 0 \end{array}\right] \quad R_2 \to R_2 - 2R_1$$

So gcd (126, 35) = $\underline{\underline{7}}$

[N.B:- If you are reading these notes please confirm ~~to~~ me by sms, my no. is 9435109940]