Euclidean Algorithm

$\to$ Repetition / Iteration.

Calculate g.c.d (567, 315) and express

$$\text{g.c.d}(567, 315) = 567u + 315v.$$

By division algorithm

$$\frac{567}{315} = 1 + \frac{252}{315}$$

$$\frac{315}{252} = 1 + \frac{63}{252}$$

$$\frac{252}{63} = 4 + 0$$

$$567 = 315 \times 1 + 252 \quad — \text{I}$$

$$315 = 252 \times 1 + \boxed{63} \quad — \text{II}$$

$$252 = 63 \times 4 + \underline{\underline{0}} \quad — \text{III}$$

63 is the last non-zero remainder.

$$\text{g.c.d of } (567, 315) = 63.$$

$$xu + yv$$

g.c.d of (,)

$xu + yv$

From Step – II,

$63 = 315 - 252 \times 1$.

$= 315 - (567 - 315)$.

$= (-1)\,567 + (2)\,315$ $u = -1$

$v = 2$

\# Find two integers u and v satisfying

$63u + 55v = 1$.

$(63, 55)$

→ $63, 55$ → co-prime to each other.

$g.c.d\,(63, 55) = 63u + 55v$.

or, $63u + 55v = 1$.

$u = 7$, $v = -8$

L.C.M (Least Common Multiple).

$-2, -6, 10$ → what is L.C.M ?

$-2 \times 5 = -10$

$-6 \times 5 = -30$

$10 \times 5 = 50$

multiples.

$10 \times 5 = 50$

ut of multiple

$2 \times 15 = 30$ $\quad$ $10 \times 3 = 30$ $\quad$ 10, 20

$6 \times 5 = 30$

Prime Numbers.

An integer $p > 1$ is said to be a prime no. if only positive divisors are only 1 and p.

even prime $\longrightarrow$ 2.

Thm: If p be a prime number and $1 \leq a \leq p$, then p is prime to a.

$p = 13$ $\quad$ 5, 6

$1 \leq \underline{?} < 13$

$1 \leq \_\_ < 5$ $\quad$ $1 \; \_\_ ? \; 567$

2, 3, 4,

Thm:— If p be a prime and a is an integer $> p$ such that p is not a divisor of a then p is prime to a.

integer, p ... of a, then p is prime to a.

$\hookrightarrow p \nmid a$

$p = 17$.
$a = 19$.

$17 \nmid 19$

{17 is prime to 19}

$p = 19$.
$a = 21$ → co-prime.

$p \nmid 21$

<u>Thm</u>: If p be a prime number and a is an integer $> p$ such that p is a divisor of a then $g.c.d\,(a, p) = p$.

<u>Thm</u>; If p be a prime number and $p \mid ab$. then either $p \mid a$ or $p \mid b$.

<u>Proof</u>: If $p \mid a$, then the thm is done

If $p \nmid a$. then $g.c.d\,(p, a) = 1$.

Since, $g.c.d$ of $(a, p) = 1$, $\exists$ u and v such that $au + pv = 1$.

$$\Rightarrow b(au + pv) = b.$$

$\Rightarrow abu + pbv = b.$

$\Rightarrow \underbrace{(ab)u + (pb)v} = b.$

Now, $p \mid ab$ and $p \mid pb$ $\longrightarrow$ p divides b.

$\Rightarrow p \mid \underline{(ab)u + (pb)v}.$

$\hookrightarrow p \mid b$ **PROVED !**

<u>Corollary</u>: If p be a prime and $\underline{p \mid a_1 a_2 \dots a_n}$ then $p \mid a_k$ for some k where $1 \le k \le n$.

<u>Examples :-</u>

1. P.T for $n > 3$, the integer $n, n+2, n+4$ cannot be all primes.

$\Rightarrow$ $4, 4+2, 4+4 = 4, 6, 8$

$5, 5+2, 5+4 = 5, 7, 9$ $\longrightarrow$ non-prime

Any positive integer n is one of the forms $3k, 3k+1, 3k+2$ $k \in \mathbb{Z}^+$

of the forms $\underbrace{3k, 3k+1, 3k+2}$, $k \in \mathbb{Z}^+$

If $n = 3k$, n is not prime.

$n = 3k+1$

$\Rightarrow n+2 = 3k+1+2$

$= 3k+3 = 3(k+1) \neq$ prime.

$\Rightarrow n+4 = 3k+2+4$

$= 3k+6 = 3(k+2) \neq$ prime.

not primes.

Proved!

H/W p is a positive integer and p, $2p+1$, $4p+1$ are primes. Find p.

$3k$, $3k+1$, $3k+2$

$p = 3k+2$.

$\Rightarrow 2p+1 = 2(3k+2)+1$

$= 6k+4+1 = 6k+5$

So prime.

Check!

Check!