Q.1 Use Euclidean Algorithm to find gcd

i) $a = 143$ $\quad b = 227$.

→ By applying division Algorithm.

$$227 = 143 \times 1 + 84.$$
$$143 = 84 \times 1 + 59$$
$$84 = 59 \times 1 + 25$$
$$59 = 25 \times 2 + 9$$
$$25 = 9 \times 2 + 7$$
$$9 = 7 \times 1 + 2.$$
$$7 = 2 \times 3 + \boxed{1} \leftarrow \text{gcd.}$$
$$2 = 1 \times 2 + 0$$

$$\Rightarrow \gcd(143, 227) = 1.$$

ii) $a = 8316$ $\quad b = 10,920$.

→ By applying division algorithm.

$$10920 = 8316 \times 1 + 2604$$
$$8316 = 2604 \times 3 + 504.$$
$$2604 = 504 \times 5 + \underline{\underline{84}}$$
$$504 = 84 \times 6 + 0$$

$$\gcd(8316, 10920) = 84.$$

3) $a = 37$, $b = 249$

→ Apply division algorithm.

$249 = 37 \times 6 + 27$

$37 = 27 \times 1 + 10$

$27 = 10 \times 2 + 7$

$10 = 7 \times 1 + 3$

$7 = 3 \times 2 + \boxed{1}$

$3 = 1 \times 3 + 0.$

$\gcd(37, 249) = 1.$

Q2 Find integers x & y s.t.

i) $6x + 10y = 2.$

→ First find gcd of 6 & 10.

$10 = 6 \times 1 + 4$ —(i)

$6 = 4 \times 1 + \boxed{2}$ —(ii) $\therefore \gcd(6, 10) = 2$

$4 = 2 \times 2 + 0$ (—iii)

To find x & y s.t $6x + 10y = 2.$

From (ii)

$2 = 6 - 4 \times 1.$

$2 = 6 - (10 - 6 \times 1) \times 1$ from (i)

$2 = 6 - 10 \times 1 + 6 \times 1$

$2 = 6 \times 2 - 10 \times 1.$

$\Rightarrow \boxed{x = 2, \ y = -1}$

3) $128x + 58y = 2$

→ First find gcd of 128, 58

$128 = 58 \times 2 + 12$ —(i)

$58 = 12 \times 4 + 10$ —(ii)

$12 = 10 \times 1 + \boxed{2}$ —(iii) ← gcd.

$10 = 2 \times 5 + 0$ —(iv)

gcd (128, 58) = 2.

To find x & y

From step (iii)

$2 = 12 - 10 \times 1.$

$2 = 12 - (58 - 12 \times 4) \times 1$

$2 = 12 - 58 \times 1 + 12 \times 4$

$2 = 12 \times 5 - 58 \times 1.$

$2 = (128 - 58 \times 2) \times 5 - 58 \times 1$

$2 = 128 \times 5 - 58 \times 10 - 58 \times 1$

$2 = 128 \times 5 - 58 \times 11$

$\Rightarrow x = 5, \; y = -11$

Basic Properties of prime factors.

Property 1 If two integers a & b are relatively prime i.e. $\gcd(a,b)=1$ and a divides bc, then a divides c.

→ Since integers a & b are relatively prime, there exist integers x & y such that,

$$ax+by=1 \Rightarrow acx+bcy=c \quad \text{(Multiply by c)}$$

Given a divides bc ie $a|bc$

$\Rightarrow a|bcy$ also $a|acx$

$\Rightarrow a|c$ $\{$ as $c=acx+bcy\}$

(hence proved)

Note if a & b are not prime then this property may not hold.

Property 2 If p is prime integer & divides ab, where a & b are integers then either p divides a or p divides b.

→ Suppose p is not divisor of a.

then let, $\gcd(p,a)=s$.

$\Rightarrow s|p$ & $s|a$

Since p is prime integer the only positive divisor of p are 1 & p

$\Rightarrow$ either $s=1$ or $s=p$.

But s can not be equal to p as p is not divisor of a.

$\Rightarrow s=1$ $\therefore \gcd(p,a)=1$. ie p & a are relatively prime. by property 1 $p|ab \Rightarrow p|b$

Property 3 :- If p is prime number, divides the product $a_1 \cdot a_2 \cdot a_3 \cdots\cdots a_n$ of certain integers, then p must divide at least one of the integers $a_1, a_2, \cdots, a_n$.

→ given,

$$p \mid a_1 a_2 \cdots a_n$$

If $p \mid a_1$ then we need not to prove further.

But if $p \nmid a_1$ ie p is not divisor of a_1

then p is relatively prime to a_1.

$$\therefore \quad p \mid a_1 (a_2 a_3 \cdots a_n)$$

$$\Rightarrow \quad p \mid a_2 a_3 \cdots a_n$$

If $p \mid a_2$ then proof ends.

But if $p \nmid a_2$ ie p is not divisor of a_2.

then p & a_2 are relatively prime.

so $$p \mid a_2 (a_3 a_4 \cdots a_n)$$

$$\Rightarrow \quad p \mid a_3 a_4 \cdots a_n$$

Repeating this process till at least $p \mid a_n$ implying that p does not divide any of the integers $a_1, a_2 \cdots a_n$.

Least common Multiple :-

The least common multiple (or lcm) of two positive integers a, b is denoted by lcm (a, b) or [a, b] & is defined as to be a positive integer h such that,

i) $a|h$ & $b|h$ And,

ii) $a|c$ & $b|c \Rightarrow h|c$.

Note Lcm of a & b is unique if it exist.

Relation between Lcm & gcd.

If a & b are two positive integers then

- $\gcd(a, b) \times \operatorname{lcm}(a, b) = ab$.

V. Imp

Fundamental Thm. of Arithmetic or Unique factorisation.

Every positive integer $a > 1$ can be expressed as a product of a finite no. of primes not necessarily distinct and this expression is unique apart from the order of the factors.

Ex. $1200 = 2^4 \times 3^1 \times 5^2 = 2 \times 2 \times 2 \times 2 \times 3 \times 5 \times 5$

$= 5 \times 2 \times 5 \times 2 \times 3 \times 2 \times 2$

$= \cdots$

So thm states (or says) that, 1200 can be represented as a product of primes & no matter how this is done there will always be exactly four 2's One 3 & two 5's & no other primes in the product

Thm Let, $m = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ &

$n = p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}$ Then,

$$\gcd(m,n) = p_1^{\min(a_1 b_1)} p_2^{\min(a_2 b_2)} \cdots p_k^{\min(a_k b_k)}.$$

$$= \prod p_i^{\min(a_i b_i)}$$

where $\min(a,b)$ represents minimum of the two no.s a & b.

Thm Let, $m = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$

& $n = p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}$

then,

$$\mathrm{LCM}(m,n) = p_1^{\max(a_1, b_1)} p_2^{\max(a_2 b_2)} \cdots p_k^{\max(a_k b_k)}$$

$$= \prod p_i^{\max(a_i, b_i)}$$

Ex. Find LCM & gcd of 340 & 304.

→ $340 = 2^2 \times 5^1 \times 17^1$ ie $340 = 2^2 \times 5^1 \times 17^1 \times 19^0$

$304 = 2^4 \times 19$ ie $304 = 2^4 \times 5^0 \times 17^0 \times 19^1$

$$\therefore \gcd(340, 304) = 2^{\min(2,4)} 5^{\min(1,0)} 17^{\min(1,0)} 19^{\min(0,1)}$$

$$= 2^2 \times 5^0 \times 17^0 \times 19^0 = 4 \times 1 \times 1 \times 1$$

$$= \underline{4}$$

$$\mathrm{LCM}(340, 304) = 2^{\max(2,4)} 5^{\max(1,0)} 17^{\max(1,0)} 19^{\max(0,1)}$$

$$= 2^4 \times 5^1 \times 17^1 \times 19^1 = \underline{25840}$$