Alternative definition of GCD(a,b) :-

If the prime factorisations of a and b are $a = p_1^{a_1} \cdot p_2^{a_2} \cdot p_3^{a_3} \cdots\cdots p_n^{a_n}$ and

$b = p_1^{b_1} \cdot p_2^{b_2} \cdot p_3^{b_3} \cdots\cdots p_n^{b_n}$ where each exponent is a non-negative integer and where all primes occuring in the prime factorization of either a (or) b are included in both factorizations with zero exponent if necessary then

$$\gcd(a,b) = p_1^{\min(a_1,b_1)} \cdot p_2^{\min(a_2,b_2)} \cdots\cdots p_n^{\min(a_n,b_n)}$$

where $\min(x,y)$ means the minimum of the two numbers x and y.

---

for eg:-

$24 = 2^3 \times 3^1 \times 5^0$ and $30 = 2^1 \times 3^1 \times 5^1$

$$\therefore \gcd(24,30) = 2^{\min(3,1)} \cdot 3^{\min(1,1)} \cdot 5^{\min(0,1)}$$

$$= 2^1 \cdot 3^1 \cdot 5^0$$

$$= 2 \cdot 3 = 6$$

Some properties of GCD

1\. If $c|ab$ and a and c are Co-prime then $c|b$.

Proof!. a and c are co-prime.

$\gcd(a,c)=1.$

$\therefore$ By the previous theorem, there exists integers 'm' and 'n' suchthat,

$$ma+nc = \gcd(a,c)=1 \longrightarrow (1)$$

multiplying the eqn (1) by b we get

$$mab+ncb=b. \longrightarrow (2).$$

Now $c|mab$ $\{\because c|ab\}$.

Also $c|nbc$

$\therefore$ $c|(mab+nbc)$ by an earlier theorem,

ie., $c|b$.

2\. If 'a' and 'b' are Co-prime and a and c are Co-prime then a and bc are Co-prime.

Proof!. 'a' and 'b' are co-prime,

$\gcd(a,b)=1$

$\therefore$ there exists integers 'm' and 'n' suchthat, $ma+nb=1.$

Similarly, $pa+qc=1$ for some integers, p and q. → ②

from ① & ②.

$(ma+nb)\cdot(pa+qc)=1$

ie., $mpa^2+mqca+nbpa+nbqc=1.$

ie., $(mpa+mqc+nbq)\cdot a+nbqc=1$

ie., $(mpa+mqc+nbq)\cdot a+(nq)\cdot(bc)=1$

ie., this is of the form $ra+sbc=1$ where r and s are integers.

ie., $GCD(a,bc)=1$ (or) a and bc are relatively prime.

---

③ If a, b are any integers, which are not simultaneously zero and k is a positive integer then $\gcd(ka,kb)=k\gcd(a,b)$

Proof:- Let $d=\gcd(a,b)$ then

$ma+nb=d$ where m and n are integers.

$\therefore m(ka)+n(kb)=kd.$

$\gcd(ka,kb)=kd=k(\gcd(a,b))$

If k is any integer, then result becomes $\gcd(ka,kb)=k\gcd(a,b).$

4. If $\gcd(a,b)=d$ then $\gcd(a/d, b/d)=1$.

<u>Proof</u>:- Since $\gcd(a,b)=d$ there exists integer m and n suchthat $ma+nb=d$

$$\therefore m(a/d)+n(b/d)=1 \longrightarrow (1).$$

Since d/a and d/b, a/d and d/b are integers.

$\therefore$ eqn (1), $\gcd(a/d, b/d)=1$.

5. If $\gcd(a,b)=1$ then for any integers c $\gcd(ac,b)=\gcd(c,b)$.

<u>Proof</u>:- $\gcd(a,b)=1$. $\therefore m_1a+n_1b=1 \longrightarrow (1)$ for any integers m_1 and n_1.

Let $\gcd(ac,b)=d$

$m_2(ac)+n_2b=d$ for any integers m_2 and n_2. $\longrightarrow (2)$

<u>from (1) & (2)</u>

$$(m_1a+n_1b).(m_2ac+n_2b)=d$$

$$\Rightarrow m_1m_2a^2c+m_1n_2ab+n_1abc+n_1n_2b^2=d.$$

$$\Rightarrow m_1m_2a^2c+(m_1n_2a+n_1ac+n_1n_2b)b=d$$

$$\Rightarrow m_2c+n_3b=d \longrightarrow (3) \text{ (say)}$$

$$\boxed{\gcd(c,b)=d.}$$

(b). If each of $a_1, a_2 \ldots a_n$ is co-prime to b then the product $(a_1 a_2 \ldots a_n)$ is also co-prime to b.

a_1 is co-prime to b.

$\therefore \gcd(a_1, b) = 1$

By property 5

$\gcd(a_1 a_2, b) = \gcd(a_2, b)$

$= 1$ {$\because a_2$ and b are co-prime}.

Again by property 5,

$\gcd(a_1 a_2 a_3, b) = \gcd(a_3, b)$

$= 1$ {$\because a_3$ and b are co-prime}.

Proceeding like this we get,

$\gcd(a_1 a_2 a_3 \ldots a_n, b) = 1$

ie., $a_1 a_2 a_3 \ldots a_n$ and b are co-prime.

Least Common multiple:-

If 'a' and 'b' are positive integers, then the smallest positive integer that is divisible by both a and b is called least common multiple of a and b and is denoted by lcm(a, b).

Note:- Even if either (or) both of a and b are negative, lcm (a, b) is always positive.

eg:- $lcm(4, 14) = lcm(-4, 14) = lcm(-4, -14)$
$= 28.$

Alternative definition of lcm(a, b)

If the prime factorizations of 'a' and 'b' are $a = p_1^{a_1} \cdot p_2^{a_2} \cdots\cdots p_n^{a_n}$ and $b = p_1^{b_1} \cdot p_2^{b_2} \cdots p_n^{b_n}$ with the conditions stated in the alternative definition of gcd (a, b) then

$$lcm(a, b) = p_1^{max(a_1, b_1)} \cdot p_2^{max(a_2, b_2)} \cdots\cdots p_n^{max(a_n, b_n)}$$

eg:- $24 = 2^3 \cdot 3^1 \cdot 5^0$ and $30 = 2^1 \cdot 3^1 \cdot 5^1$

$\therefore lcm(24, 30) = 2^{max(3,1)} \cdot 3^{max(1,1)} \cdot 5^{max(0,1)}$

$= 2^3 \cdot 3^1 \cdot 5^1 = 120$

Theorem :-

If 'a' and 'b' are two positive integers then $\gcd(a,b) \cdot \operatorname{lcm}(a,b) = ab$.

Proof :- Let the prime factorization of 'a' and 'b' be

$$a = p_1^{a_1} \cdot p_2^{a_2} \cdots p_n^{a_n} \text{ and}$$
$$b = p_1^{b_1} \cdot p_2^{b_2} \cdots p_n^{b_n}$$

then $\gcd(a,b) = p_1^{\min(a_1,b_1)} \cdot p_2^{(a_2,b_2)} \cdots p_n^{\min(a_n,b_n)}$

and $\operatorname{LCM}(a,b) = p_1^{\max(a_1,b_1)} \cdot p_2^{\max(a_2,b_2)} \cdots p_n^{\max(a_n,b_n)}$

We observe that, if $\min(a_i,b_i)$ is $(a_i$ (or b_i) then $\max(a_i,b_i)$ is b_i (or a_i), $i = 1,2 \ldots$

Hence, $\gcd(a,b) \times \operatorname{lcm}(a,b)$

$$= p_1^{\min(a_1,b_1)+\max(a_1,b_1)} \cdot p_2^{[\min(a_2,b_2)+\max(a_2,b_2)]} \cdots p_n^{[\min(a_n,b_n)+\max(a_n,b_n)]}$$

$$= p_1^{(a_1+b_1)} \cdot p_2^{(a_2+b_2)} + \cdots p_n^{a_n+b_n}$$

$$= (p_1^{a_1} \cdot p_2^{a_2} \cdots p_n^{a_n}) \cdot (p_1^{b_1} \cdot p_2^{b_2} \cdots p_n^{b_n}) = ab.$$

eg:- Use the Euclidean Algorithm to find (i) gcd (1819, 3587)
(ii) gcd (12345, 54321). In each case express the gcd as a linear combination of the given numbers,

By division Algorithm,

$3587 = 1 \times 1819 + 1768$

$$\begin{array}{r|l} & \;\;1 \\ 1819 & 3587 \\ & 1819 \\ \hline & 1768 \end{array}$$

$1819 = 1 \times 1768 + 51$

$1768 = 34 \times 51 + 34$

$51 = 1 \times 34 + 17$

$34 = 2 \times 17 + 0.$

Since the last non-zero remainder is 17.

$\therefore$ gcd (1819, 3587) = 17.

$17 = 51 - 1 \times 34$

$= 51 - 1 \times (1768 - 34 \times 51)$

$= 1 \times 51 - 1 \times 1768 + 34 \times 51$

$= 35 \times 51 - 1 \times 1768$

$= 35 \times (1819 - 1 \times 1768) - 1 \times 1768$

$= 35 \times 1819 - 35 \times 1768 - 1 \times 1768$

$= 35 \times 1819 - 36 \times 1768$

$= 35 \times 1819 - 36(3587 - 1 \times 1819)$

$= 35 \times 1819 - 36 \times 3587 + 36 \times 1819$

$= 71 \times 1819 - 36 \times 3587$

H.W

(2) gcd(12345, 54321).

---

(3) Using prime factorization find the gcd and lcm of (i) (231, 1575) (ii) 337500, 21600) verify also that gcd (m,n). lcm(m,n) = mn.

$$\begin{array}{r|l} 3 & 231 \\ \hline 7 & 77 \\ \hline 11 & 11 \\ \hline & 1 \end{array} \qquad \begin{array}{r|l} 5 & 1575 \\ \hline 5 & 315 \\ \hline 3 & 63 \\ \hline 3 & 21 \\ \hline 7 & 7 \\ \hline & 1 \end{array}$$

$231 = 3^{0} \times 7^{0} \times 11^{0} \times 5^{0}$

$1575 = 3^{2} \times 7^{1} \times 5^{2} \times 11^{0}$

$\therefore gcd(231, 1575) = 3^{\min(1,2)} \cdot 7^{\min(1,1)} \cdot 11^{\min(0,1)} \cdot 5^{\min(0,2)}$

$= 3^{1} \times 7^{1} \times 11^{0} \times 5^{0} = 21.$

$lcm(231, 1575) = 3^{\max(1,2)} \cdot 7^{\max(1,1)} \cdot 11^{\max(0,1)} \cdot 5^{\max(0,2)}$

$= 3^{2} \cdot 7^{1} \cdot 11^{1} \cdot 5^{2} = 17325.$

$= gcd(231, 1575) \cdot lcm(231, 1575)$

$= 21 \times 17325$

$= 363825 = 23 \times 1575.$

(1) eg:- find the integers 'm' and 'n' such that

$512m + 320n = 64.$

$512 = 1 \times 320 + 192 \rightarrow (1)$

$$320 \overline{)\,512\,(1} \quad \begin{array}{r} 320 \\ \hline 192 \end{array}$$

$320 = 1 \times 192 + 128 \rightarrow (2)$

$192 = 1 \times 128 + 64 \rightarrow (3)$

$128 = 2 \times 64 + 0. \rightarrow (4).$

from the equation (3), we've,

$64 = 192 - 1 \times 128$

$= 192 - 1 \times (320 - 1 \times 192)$

$= 1 \times 192 - 1 \times 320 + 1 \times 192$

$= 2 \times 192 - 320$

$= 2 \times (512 - 1 \times 320) - 320$

$= 2 \times 512 - 2 \times 320 - 1 \times 320$

$= 2 \times 512 - 3 \times 320$

$= \underset{\downarrow\, m}{2} \times 512 - \underset{\downarrow\, n}{3} \times 320$

$\therefore \boxed{m = 2}$ and $\boxed{n = -3}$

---

(2) $28844m + 15712n = 4$ (Exercise) } exercise Problem.

$\boxed{\text{Ans: } m = -1693 \text{ and } n = 3108}$