NUMBER THEORY

Number theory is the part of mathematics, that deals with integers, more specifically positive integers and their properties. In this chapter we will discuss the notations of divisibility, greatest common divisors and prime numbers and a few applications. The theory of numbers finds its applications in computer arithmetic that includes transmission, coding and manipulation of numerical data and also in cryptology - the study of secret messages.

DIVISIBILITY :-

Defn:-

when a and b are any two integers $a \neq 0$, a is said to divide b, if there is an integer c such that $b = ac$ and it is denoted by the notation $a | b$.

Ex:- $4 | 8$ $\Rightarrow$ $8 = 4 \times 2$ 8 is divisible by 4.
(or)
4 divides 8
(or)
divisors

Prime numbers :-

Defn :-

A positive integer $P > 1$ is called prime number If the possible division are 1 and P.

Composite number - not a prime number.

Note :-

1) The positive integer 1 is neither prime nor Composite.
2) The positive integer n is composite, if there exists positive integer a and b such that $n = ab$, where $1 < a, b < n$.

Theorem :-

Let $a, b, c \in Z$ the set of integers. then

(i) If $a|b$ and $b|c$ then $a|c$.

(ii) If $a|b$ and $a|c$ then $a|(b+c)$

(iii) If $a|b$ then $a|mb$, for any integer m.

(iv) If $a|b$ and $a|c$ then $a|(mb+nc)$ for any integers m and n.

Fundamental theorem of Arithmetic :-

Defn :- Every integer $n>1$ can be written uniquely as a product of prime numbers.

Ex :- The prime factorisations of the integers

100,

$$100 = 2\times2\times5\times5 = 2^2 \cdot 5^2$$

$$5096 = 2^3 \times 7^2 \times 13$$

$$10! = 1\times2\times3\times4\times5\times6\times7\times8\times9\times10$$

$$= 2\times3\times2\times2\times5\times3\times2\times7\times2\times2\times2\times3\times3\times5\times2$$

$$10! = 2^8\times3^4\times5^2\times7$$

$$\begin{array}{r|l} 2 & 100 \\ 2 & 50 \\ 5 & 25 \\ & 5 \end{array}$$

$$\begin{array}{r|l} 2 & 5096 \\ 2 & 2548 \\ 2 & 1274 \\ 7 & 637 \\ 7 & 91 \\ & 13 \end{array}$$

(i) 6647

(ii) 45500

Theorem :- If $n>1$ is a Composite integer and p is a prime factor of n, then $p \le \sqrt{n}$.

Proof :-

Since $n>1$ is a Composite integer, n can be expressed as $n=ab$, where $1<a\le b<n$. Then $a \le \sqrt{n}$, since, if it is not true

$ab > \sqrt{n}\cdot\sqrt{n} = n$ which is a contradiction.

Thus n has a positive divisior $(=a)$ not exceeding $\sqrt{n}$.

now $a>1$, is either ~~case~~ Prime or by the fundamental theorem of Arithmetic, has a prime factor, In either case n has a prime factor $\le \sqrt{n}$.

Theorem :-

The number of prime numbers is infinite.

Division Theorem :-

Statement :-

Let a and b are any two integers, $b>0$, there exist unique integers q and r such that $a=bq+r$, where $0\leq r<b$.

Proof :-

Let us consider the infinite sequences of multiples of b.

$$\ldots\ldots -2b, -b, 0, b, 2b \ldots qb \ldots$$

clearly $a=qb$ or $qb<a<(q+1)b$ for some q.

Combining the two, we get

$$qb\leq a<(q+1)b \longrightarrow (1)$$

If we put $r=a-qb$ from (1) we get,

$$qb\leq a<qb+b$$

$$\cancel{qb}-\cancel{qb}\leq a-qb<\cancel{qb}+b-\cancel{qb}$$

$$0\leq r\leq b$$

$$\therefore \boxed{a=qb+r}$$

→ q → quotient r → remainder

To prove uniqueness of q and r, let us assume that a can be expressed in the given form in two ways.

Let $a=q_1b+r_1 \longrightarrow (2) \quad 0\leq r_1<b$ or $-b\leq r\leq 0$

$a=q_2b+r_2 \longrightarrow (3) \quad 0\leq r_2<b$

② and ③ gives $(q_1-q_2)b = r_2-r_1 \longrightarrow ④$

eqn ④ means that r_2-r_1 is an integral multiple of b.

but since $0 \leq r_2 < b$ and $-b < -r_1 \leq 0$

by ② & ③ we have $-b < r_2-r_1 < b$

Hence the only possibility is that r_2-r_1 is the zero multiple of b.

$\therefore$ $r_1 = r_2$ and also $q_1 = q_2$

Hence q and r are Unique.

Greatest Common Division :- (GCD)

When a and b are (non-zero) integers, then an integer $d (\neq 0)$ is said to be the common divisor of a and b, if $d|a$ and $d|b$. (If d divides both a and b)

If d is the largest of all common divisors then d is called the greatest common divisor of a and b and denoted as $\gcd(a,b)$.

The greatest common divisor is also called the highest common factor for which the abbreviation is. hcf (a,b).

If $\gcd(a,b) = 1$ then a and b are said to be relatively prime or coprime or each is said to be prime to the other.

If $\gcd(a_i, a_j) = 1$ for $1 \leq i < j \leq n$, then the integers $a_1, a_2 \ldots a_n$ are said to be pairwise relatively prime.

Alternative Definition of GCD :-

If the prime factorizations of a and b are $a = p_1^{a_1} \cdot p_2^{a_2} \cdot p_3^{a_3} \cdot \ldots \cdot p_n^{a_n}$ and $b = p_1^{b_1} \cdot p_2^{b_2} \cdot p_3^{b_3} \cdot \ldots \cdot p_n^{b_n}$.
where each exponent is a non-negative integer and where all primes occuring in the prime factorisation of either a or b are included in both factorizations, with zero exponent if necessary, then

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

Ex: To find GCD (24, 30).

Soln:-

$$\begin{array}{r|l} 2 & 24 \\ \hline 2 & 12 \\ \hline 2 & 6 \\ \hline & 3 \end{array} \qquad \begin{array}{r|l} 2 & 30 \\ \hline 3 & 15 \\ \hline & 5 \end{array}$$

$$24 = 2^3 \cdot 3^1 \cdot 5^0$$

$$30 = 2^1 \cdot 3^1 \cdot 5^1$$

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

$$= 2^1 \cdot 3^1 \cdot 5^0 = \underline{6}$$

Some properties of GCD :-

1) If $c \mid ab$ and a and c are coprime, then $c \mid b$

2) If a and b coprime and a and c are coprime, then a and bc are coprime.

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

4) If $\gcd(a,b) = d$, then $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$

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

6) If each of $a_1, a_2 \ldots a_n$ is coprime to b, then the product $(a_1 a_2 a_3 \ldots a_n)$ is coprime to b.

Least common multiple :- (LCM)

Defn:-

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

Alternative Definition of $\operatorname{lcm}(a,b)$:-

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

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

Ex:- To find LCM (24, 30).

$24 = 2^3 \cdot 3^1 \cdot 5^0$

$30 = 2^1 \cdot 3^1 \cdot 5^1$

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

$= 2^3 \cdot 3^1 \cdot 5^1 = 8 \times 3 \times 5 = \underline{\underline{120}}$

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 $a = p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \, p_n^{a_n}$ & $b = p_1^{b_1} \cdot p_2^{b_2} \cdot p_3^{b_3} \cdot \ldots \, p_n^{b_n}$.

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

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

$\gcd(a,b) \times \operatorname{lcm}(a,b) = p_1^{(\min(a_1,b_1)+\max(a_1,b_1))} \cdot p_2^{(\min(a_2,b_2)+\max(a_2,b_2))} \cdot \ldots \cdot p_n^{(\min(a_n,b_n)+\max(a_n,b_n))}$

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

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

$= \underline{ab}$ Hence Proved.

Problems :-

1) Find LCM & GCD of (625, 1000) using prime factorization.

Soln :- The prime factorizations are,

$625 = 5^4 \cdot 2^0$

$1000 = 2^3 \cdot 5^3$

5	625
5	125
5	25
	5

2	1000
2	500
2	250
5	125
5	25
	5

$LCM(625, 1000) = 2^{max(0,3)} \cdot 5^{max(4,3)}$

$= 2^3 \cdot 5^4 = 8 \times 625 = \underline{5000}$

HCF (or) $GCD(625, 1000) = 2^{min(0,3)} \cdot 5^{min(4,3)}$

$= 2^0 \cdot 5^3 = 1 \times 125 = \underline{125}$

$\therefore LCM(625, 1000) = 5000$ & $GCD(625, 1000) = 125$.

2) Find LCM & GCD of (231, 1575) using prime factorization. verify $gcd(m,n) \times lcm(m,n) = m \cdot n$.

Soln :-

The prime factorizations are,

$231 = 3^1 \cdot 5^0 \cdot 7^1 \cdot 11^1$

$1575 = 3^2 \cdot 5^2 \cdot 7^1 \cdot 11^0$

3	231
7	77
	11

5	1575
5	315
3	63
3	21
	7

now,

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

$= 3^2 \cdot 5^2 \cdot 7^1 \cdot 11^1$

$LCM(231, 1575) = 9 \times 25 \times 7 \times 11 = \underline{17325}$

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

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

$gcd(231, 1575) \cdot lcm(231, 1575) = 21 \times 17325$

$= 363825$

$= 231 \times 1575.$

$gcd(m,n) \cdot lcm(m,n) = m \cdot n$.

Hence verified.

3) Using prime factorization, find the gcd and lcm of $(337500, 21600)$. Verify also that $\gcd(m,n) \cdot \text{lcm}(m,n) = mn$

Soln:- The prime factorizations are

$$\begin{array}{r|l} 5 & 337500 \\ \hline 5 & 67500 \\ \hline 5 & 13500 \\ \hline 5 & 2700 \\ \hline 5 & 540 \\ \hline 2 & 108 \\ \hline 2 & 54 \\ \hline 3 & 27 \\ \hline 3 & 9 \\ \hline & 3 \end{array} \qquad \begin{array}{r|l} 5 & 21600 \\ \hline 5 & 4320 \\ \hline 2 & 864 \\ \hline 2 & 432 \\ \hline 2 & 216 \\ \hline 2 & 108 \\ \hline 2 & 54 \\ \hline 3 & 27 \\ \hline 3 & 9 \\ \hline & 3 \end{array}$$

$337500 = 2^2 \cdot 3^3 \cdot 5^5$

$21600 = 2^5 \cdot 3^3 \cdot 5^2$

now,

$$\text{GCD of } (337500, 21600) = 2^{\min(2,5)} \cdot 3^{\min(3,3)} \cdot 5^{\min(5,2)}$$

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

$$= 4 \times 27 \times 25 = \underline{\underline{2700}}$$

$$\text{LCM of } (337500, 21600) = 2^{\max(2,5)} \cdot 3^{\max(3,3)} \cdot 5^{\max(5,2)}$$

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

$$\text{LCM of } (337500, 21600) = 32 \cdot 27 \cdot 3125 = 2700000.$$

now

$$\gcd(337500, 21600) \cdot \text{lcm}(337500, 21600) = 2700 \times 2700000$$

$$= 7290000000 \rightarrow (1)$$

and $337500 \times 21600 = 7290000000 \longrightarrow (2)$

from (1) & (2) $\gcd(m,n) \times \text{lcm}(m,n) = mn$

Hence verified.

Ex:-

(i) let us consider the integers 9, 13, 25.

since $\gcd(9,13)=1$; $\gcd(9,25)=1$ and $\gcd(13,25)=1$

The integers 9, 13, 25 are pairwise relatively prime.

(ii) let us now consider the integers 10, 17, 25.

$\gcd(10,17)=1$; $\gcd(17,25)=1$, we see that $\gcd(10,25)=5$

Hence the integers 10, 17, 25 are not pairwise relatively prime.

Euclid's Algorithm for finding gcd (a,b):

Statement:-

When a and b are any two integers $(a>b)$ if r_1 is the remainder when a is divided by b, r_2 is the remainder when b is divided by r_1, r_3 is the remainder when r_1 is divided by r_2 and so on, and if $r_{k+1}=0$ then the last non-zero remainder r_k is the $\gcd(a,b)$.

Theorem:-

$\gcd(a,b)$ can be expressed as an integral linear combination of a and b.

(ie) $\gcd(a,b)=ma+nb$. where m and n are integers.

Proof:-

From the Euclid's algorithm, we have

$$r_{k-2}=q_k r_{k-1}+r_k \quad \text{where } r_k=\gcd(a,b)$$

$$r_k = r_{k-2}+(-q_k)r_{k-1}$$

$$= r_{k-2}+(-q_k)\{r_{k-3}+(-q_{k-1})r_{k-2}\}$$

$$= r_{k-3}(-q_k)+(1+q_{k-1}q_k)r_{k-2}$$

now we substitute $r_{k-4}+(-q_{k-2})r_{k-3}$ for r_{k-2} and continue the process. Finally we will have $r_k=\gcd(a,b)=ma+nb$. where m & n are integers.

Problems :-

1) Apply Euclidean algorithm, to find gcd(1819, 3587) and also express the gcd as a linear combination of the given number.

Soln :- given $a = 3587$ & $b = 1819$

by division algorithm, $a = qb + r$

$$3587 = (1 \times 1819) + 1768 \longrightarrow ①$$

$$1819 = (1 \times 1768) + 51 \longrightarrow ②$$

$$1768 = (34 \times 51) + 34 \longrightarrow ③$$

$$51 = (1 \times 34) + \underset{GCD}{17} \longrightarrow ④$$

$$34 = (2 \times \underline{17}) + \boxed{0}$$

Since the last non-zero remainder is 17,

GCD(1819, 3587) = 17.

linear Combination :-

now,
$$17 = 51 - (1 \times 34) \quad \text{by } ④$$
$$= 51 - (1 \times (1768 - (34 \times 51))) \quad \text{by } ③$$
$$= (35 \times 51) - (1 \times 1768)$$
$$= (35 \times (1819 - (1 \times 1768))) - (1 \times 1768) \quad \text{by } ②$$
$$= (35 \times 1819) - (36 \times 1768)$$
$$= (35 \times 1819) - (36 \times (3587 - (1 \times 1819))) \quad \text{by } ①$$

$$17 = (71 \times 1819) - (36 \times 3587)$$

linear combination is $GCD(a,b) = ma + nb$

$\therefore \quad m = -36 \quad \& \quad n = 71.$

2) Use the Eulidean algorithm to find (12345, 54321) and express the gcd as a linear combination m, n of the given numbers and also find m & n?

Soln :- given $a = 54321$; $b = 12345$

using Euclid's Algorithm,

by division algorithm, $a = qb + r$

$$54321 = (4 \times 12345) + 4941 \longrightarrow (1)$$
$$12345 = (2 \times 4941) + 2463 \longrightarrow (2)$$
$$4941 = (2 \times 2463) + 15 \longrightarrow (3)$$
$$2463 = (164 \times 15) + 3 \longrightarrow (4)$$
$$15 = (5 \times \underline{3}) + \boxed{0}.$$

Since the last non-zero remainder is 3.

$$\gcd(12345, 54321) = 3$$

linear combination:-

now,
$$3 = 2463 - (164 \times 15) \quad \text{by (4)}$$
$$= 2463 - (164 \times (4941 - (2 \times 2463))) \quad \text{by (3)}$$
$$= (329 \times 2463) - (164 \times 4941)$$
$$= (329 \times (12345 - (2 \times 4941))) - (164 \times 4941) \quad \text{by (2)}$$
$$= (329 \times 12345) - (658 \times 4941) - (164 \times 4941)$$
$$= (329 \times 12345) - (822 \times 4941)$$
$$= (329 \times 12345) - (822 \times (54321 - (4 \times 12345))) \quad \text{by (1)}$$
$$= (329 \times 12345) - (822 \times 54321) + (3288 \times 12345)$$
$$3 = (3617 \times 12345) - (822 \times 54321)$$

The linear combination is $GCD(a, b) = ma + nb$

$\therefore m = -822$ & $n = 3617$

3) Using Euclid's Algorithm, Find integers m and n such that $512m + 320n = 64$.

Soln:- From the given eqn. is $512m + 320n = 64$ we infer that 64 is the gcd (512, 320)

Using Euclid's algorithm, to find m and n.

by division algorithm $a = qb + r$

given $a = 512$, $b = 320$

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

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

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

$128 = (2 \times 64) + 0$

$GCD(512, 320) = 64$

linear combination:-

now $64 = 192 - (1 \times 128)$ from (3)

$= 192 - (1 \times (320 - (1 \times 192)))$ by (2)

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

$64 = (2 \times 192) - (1 \times 320)$

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

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

$64 = (2 \times 512) - (3 \times 320)$

The linear combination is $GCD(a, b) = ma + nb$

$\therefore m = 2$ & $n = -3$

4) Using Euclid's algorithm, Find integers m and n such that $28844m + 15712n = 4$

Soln :-

From the given eqn. is $28844m+15712n=4$.

we infer that 4 is the gcd (28844, 15712)

given $a=28844$; $b=15712$.

Using Euclid's algorithm to find m and n.

$$28844 = (1\times15712)+13132 \longrightarrow (1)$$
$$15712 = (1\times13132)+2580 \longrightarrow (2)$$
$$13132 = (5\times2580)+232 \longrightarrow (3)$$
$$2580 = (11\times232)+28 \longrightarrow (4)$$
$$232 = (8\times28)+8 \longrightarrow (5)$$
$$28 = (3\times8)+4 - \text{GCD} \longrightarrow (6)$$
$$8 = (2\times4)+0$$

linear combination :-

now,

from (6) $\Rightarrow$ $4 = 28-(3\times8)$

$= 28-(3\times(232-(8\times28)))$. by (5)

$= 28-(3\times232)+(24\times28)$

$= (25\times28)-(3\times232)$

$=(25\times(2580-(11\times232)))-(3\times232)$ by (4)

$= (25\times2580)-(275\times232)-(3\times232)$

$=(25\times2580)-(278\times232)$

$=(25\times2580)-(278\times(13132-(5\times2580)))$ by (3)

$=(25\times2580)-(278\times13132)+(1390\times2580)$

$=(1415\times2580)-(278\times13132)$

$=(1415\times((15712)-(1\times13132)))-(278\times13132)$ by (2)

$=(1415\times15712)-(1415\times13132)-(278\times13132)$

$=(1415\times15712)-(1693\times13132)$ by (1)

$=(1415\times15712)-(1693\times(28844-(1\times15712)))$

$=(1415\times15712)-(1693\times28844)+(1693\times15712)$

$4 = (3108\times15712)-(1693\times28844)$

The linear combination is $\text{GCD}(a,b) = ma+nb$

$\therefore$ $m=-1693$ & $n=3108$.