Number theory

Number theory is the part of mathematics that seeks to investigate the properties of integers, more specifically the properties of positive integers. In this chapter we will discuss some of the basic properties of integers of divisibility & congruence relation with their applications.

9840291613

9952946426

Divisibility Theory :-

Let $a \neq b$ are two integers with $a \neq 0$, we say that a divides b or b is divisible by a or a is a divisor or factor of b or b is a multiple of a if $b = aq$ for some $q \in Z$. The statement "a divides b" is written $a \mid b$ and its negation $a \nmid b$.

$a \mid b$

Example :- $11 \mid 66$

(i) 66 is divisible by 11 since $66 = 11 \times 6$

(ii) 16 is a divisor of 128, since $128 = 16 \times 8$

Neha 9791194790 9840291613

(iii) -7 divides 42 because $42 = (-7) \times$

(iv) 0 is divisible by every integer because $0 = b \times 0$ for every value of

Note :- If a divides b then $-a$ is also divides b because $b = aq$ implies $b = (-a)(-q)$. It is therefore enough if we consider +ve divisors of an integer only.

Theorem :- Let $a, b, c \in Z$ the set of integers then $a < b$.

(i) If $a|b$ & $a|c$ then $a|b+c$

(ii) If $a|b$ & $b|c$ then $a|c$

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

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

* The relation "a divides b" is a reflexive & transitive in the set of positive integers but not symmetric.

Proof :-

Since $a|b$ & $a|c$ it follows from the definition of divisibility that

$b = ma$ & $c = na$ where m & n are integers.

$3|15$, $3|9$ $\rightarrow 3|24$

$\therefore \quad b+c = (m+n)a$

This means that $a|(b+c)$ or a divides $b+c$

(ii) Since $a|b$ & $b|c$ we have

$b = ma$ & $c = nb$ where m & n are integers.

$\therefore \quad c = nb$

$= n(ma) = (nm)a$ $3|b$ $b|18$ $3|18$

This means that a divides c or $a|c$

(iii) Since $a|b$ we have $b = na$

$\therefore \quad mb = m(na)$

$= (mn)a$ where m & n are integers

This means that a divides mb or $a|mb$

(iv) Since $a|b$ we have $a|mb$ by (iii)

Since $a|c$ we have $a|nc$ by (iii)

Now since $a|mb$ & $a|nc$ we have

$a|mb+nc$ by (i).

Proof :-

Since $a|b$ & $a|c$ it follows from the definition of divisibility that

$b = ma$ & $c = na$ where m & n are integers.

$3|15 \rightarrow 3|24$
$3|9$

$\therefore b+c = (m+n)a$

This means that $a|(b+c)$ or a divides $b+c$

(ii) Since $a|b$ & $b|c$ we have

$b = ma$ & $c = nb$ where m & n are integers.

$3|b \quad b|18$
$3|18$

$\therefore c = nb$
$= n(ma) = (nm)a$

This means that a divides c or $a|c$

(iii) Since $a|b$ we have $b = na$

$\therefore mb = m(na)$
$= (mn)a$ where m & n are integers

This means that a divides mb or $a|mb$

(iv) Since $a|b$ we have $a|mb$ by (iii)

Since $a|c$ we have $a|nc$ by (iii)

Now since $a|mb$ & $a|nc$ we have

$a|mb+nc$ by (i).

20, 36, 38, 43, 44, 55, 56, 62, 64, 67, 68

Prime numbers :- 79,

A positive integer $p > 1$ is called prime, if the only positive factors of p are 1 & p.

divisor

A positive integer > 1 and is not prime is called composite.

Note :-

1. The positive integer 1 is neither prime nor composite.
2. The positive integer n is composite, if there exists positive integers a & b such that $n = ab$ where $1 < a, b < n$
3. A number that is not a prime is divisible by prime.

Fundamental Theorem of arithmetic :-

Every positive integer $n > 1$ can be written uniquely as a product of prime numbers, where the prime factors are written in order of increasing size.

Proof :-

we shall prove the theorem by mathematical induction.

Jeba Kn.

Padm

Number theory

Prime number :-

A positive integer $p > 1$ is called prime, if the only positive factors of p are 1 & p.

A positive integer > 1, and is not prime is called composite.

Note :-

1. The positive integer 1 is neither prime nor composite.
2. The positive integer n is composite, if there exists positive integer a & b such that $n = ab$ where $1 < a, b < n$.
3. A number that is not a prime is divisible by prime.

Fundamental theorem of arithmetic :-

Every positive integer $n > 1$ can be written either prime or can be expressed uniquely on a product of primes apart from the order in which the prime factors occur.

proof :-
We shall prove the theorem by Mathematical induction.

Initial step :-

Let $n = 2, 3$ since 2, 3 is a prime. $n = 2, 3$ is a product of primes
∴ a product may consist of a single factor.

for $n = 4 = 2 \times 2$ product of prime.

Induction hypothesis :-

Assume the result is true for all integers $\leq k$. (An integer which is either a prime or it is a product of prime)

Let us prove the result for $n = k+1$

Suppose $n = k+1$ is prime then nothing to prove

$(k+1)$ is not a prime. ie composite.

Then $k+1 = ab$ for some integers

Now by induction hypothesis, $a \leq k$, $b \leq k$.

$a = p_1 p_2 \cdots p_r$

$b = q_1 q_2 \cdots q_s$

Padm

theory of mathematics

$\therefore (K+1) = (p_1 \cdots k)(q_1 q_2 \cdots q_s)$

$\therefore$ The result is true for all integers.

$240 = 2^4 \times 3 \times 5$ → canonical form

2	240
2	120
2	60
2	30
3	15
	5

Theorem :- If $n > 1$ is a composite integer & p is a prime factor of n, then $p \leq \sqrt{n}$.

(OR)

Prove that a positive integer n is a prime number if no prime p less than or equal to $\sqrt{n}$ divides n.

proof :- Let n is composite

$\Rightarrow n = ab$ for some integer $a \neq b$ such that $1 < a, b < n$.

Without loss of generality, Suppose that $a \leq b$.

Let $a > \sqrt{n}$, then $b \geq a > \sqrt{n}$.

However ; if

$b \geq a > \sqrt{n}$ is true then

$n = ab > \sqrt{n}\sqrt{n} > n.$

which is a contradiction both the factors a, b are greater than $\sqrt{n}$ then their product would be greater than n.

So one of the factors say a must not be greater than $\sqrt{n}$,

ie $a \leq \sqrt{n}$.

Because both a & b are divisors of n, we see that n has a positive divisor $(= a)$ not exceeding $\sqrt{n}$, ie $a >$, This divisor is either prime or by the fundamental theorem of arithmetic has a prime factor less than itself. In either case, n has a prime divisor less than or equal to $\sqrt{n}$.

Jeba Kr

Padm

theo

Note :- To test if a given integer n is prime, it is enough to see that it is not divisible by any prime less than or equal to $\sqrt{n}$.

Eg :- To test the primability of 83, we check whether it is divisible by the prime numbers less than or equal to $\sqrt{83}$. namely 2, 3, 5 & 7, Since 83 is not divisible by any of these prime numbers. 83 is prime number.

$\sqrt{99} = 9.94$
$n = 99$
2, 3, 5, 7
2 ∤ 99
3 ∤ 99
∴ 99 is not prime

Theorem :- The number of prime numbers is infinite.

proof Assume there are finitely many prime numbers say N prime numbers

$N \in Z^+$ $\{p_1, p_2 \cdots p_N\}$ $p_i > 1 \ \forall i$

Let $q = (p_1 p_2 \cdots p_N) + 1$

$q > p_1$, $q > p_2$ $\cdots$ $q > p_N$

$\therefore q > p_i \quad \forall i$.

$\therefore$ q is greater than the biggest (largest) prime number.

$\Rightarrow q$ is not prime (composite)

$\Rightarrow q$ can be written as a product of prime number.

$\Rightarrow q$ is divisible by atleast one prime number.

Without loss of generality, q is divisible by p_1.

$\therefore \frac{q}{p_1} \in Z$.

$$\frac{q}{p_1} = \frac{(p_1 p_2 \cdots p_N) + 1}{p_1}$$

$$= \underbrace{p_2 \cdots p_N}_{\in Z} + \underbrace{\frac{1}{p_1}}_{\notin Z} \quad \because p_1 > 1$$

$\notin Z$

which is a contradiction.

$\therefore$ there are infinitely many primes.

$30 = (2 \times 3 \times 5) + 1$

$= 31$

$2 \mid 30 \quad 3 \mid 30 \quad 5 \mid 30 \quad 31$

$5 \mid 85$

5×17

$2 = 2 \times 1$

Let $n = 2$, since 2 is a prime, $n = 2$ is a product of primes.

∴ a product may consist of a single factor.

Let $n > 2$.

If n is prime, it is a product of primes. ie a single factor product.

If n is not prime (composite), Let us assume that the theorem holds good for positive integers less than n & one integer (one divisor $\neq 1$ or n) there is atleast that $n = ab$. Since $a, b < n$ each of a & b can be expressed as the product of primes. (by the assumption)

ie $a = p_1 \cdot p_2 \cdots p_k$ $\quad b = q_1 q_2 \cdots q_r$

$\therefore n = ab$ is also a product of primes $n = p_1 p_2 \cdots p_k \cdot q_1 \cdots q_r$

$240 = 2^4 \times 3 \times 5$

$81 = 3 \times 3 \times 3 \times 3$

$100 = 2^2 \times 5^2$ canonical form

3	81
3	27
3	9
3	3

2	240
2	120
2	60
2	30
3	15

Theorem :- If $n > 1$ is a composite integer & p is a prime factor of n, then $p \leq \sqrt{n}$.

$\therefore$ 99 is not prime.

5 & 101 arranging 2, 3, 5, 7

$a|n$ & $b|n$

Proof :- n is composite $\Rightarrow n = a \cdot b$ for some integer a & b such that $1 \leq a, b <$

If n is composite, by the definition of a composite integer, we know that it has a factor a with $1 < a < n$. Hence by the definition of a factor of a +ve integer, we have $n = ab$, where b is a positive integer greater than 1. We will show that $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.

If $a > \sqrt{n}$ & $b > \sqrt{n}$ then $ab > n$ which is a contradiction. Consequently, $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$. Because both a & b are divisors of n, we see that n has a positive divisor $(= a)$ not exceeding

Without loss of generality suppose that $a \leq b$.

Let $a > \sqrt{n}$.

Then $b \geq a > \sqrt{n}$

However if $b \geq a > \sqrt{n}$ is true then

$n = ab > \sqrt{n}\sqrt{n}$

$> n$.

which is a contradiction both the factors a, b are greater than $\sqrt{n}$ then their product would be greater than n.

So one of the factors say a must not be greater than $\sqrt{n}$ ie $a \leq \sqrt{n}$

Padm

@ $a > 1$

$\sqrt{n}$. This divisor is either prime or by the fundamental theorem of arithmetic has a prime factor divisor less than itself. In either case, n has a prime divisor less than or equal to $\sqrt{n}$.

Note :- To test if a given integer n is prime, it is enough to see that it is not divisible by any prime less than or equal to $\sqrt{n}$.

Eg: To test the primability of 83. we check whether it is divisible by the prime numbers less than or equal to $\sqrt{83}$ namely 2, 3, 5 & 7. Since 83 is not divisible by any of these prime numbers 83 is prime number.

P.T a positive integer n is a prime number, if no prime p less than or equal to $\sqrt{n}$ divides n.

$n = 101$ $\sqrt{n} = 10.04$

2, 3, 5, 7

$2 \nmid 101$

$3 \nmid 101$

$5 \nmid 101$

$7 \nmid 101$

101 is not divisible by 2, 3, 5, 7

99 $\sqrt{99} = 9.94$ 2, 3, 5, 7

$2 \nmid 99$ $3 \mid 99$

$\therefore$ 99 is not prime.

101 is prime

Example :- Find the prime factorization 7007.

Soln perform division of 7007 by successive primes starting with 2

2, 3, 5 do not divide 7007.

7 divides 7007. $\frac{7007}{7} = 1001$

$\frac{1001}{7} = 143$.

7 does not divide 143. Next prime is 11. $\frac{143}{11} = 13$ primes

$\therefore 7007 = 7^2 \times 11 \times 13$

Division Algorithm :-

Theorem :-

When a & b are any two integers, $b>0$, there exist unique integers q & r such that $a = bq + r$ where $0 \le r < b$

dividend, divisor, quotient, Remainder

Solution :- Existence of integer q & r :-

Let us consider the sequence of multiple of b namely

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

case (i) :- a is a multiple of b

If a non negative integer q such that

$a = qb$ i.e. $a = qb + 0$.

$$\boxed{a = qb + r \quad \text{where } r = 0} \quad (1)$$

case (ii) a is not a multiple of b

& a will fall between some multiples of qb & $(q+1)b$.

we can say that

$$qb < a < (q+1)b.$$

$49 = 5 \times 9 + 4$

$a = q \times b + r$

Take $r = a - qb$.

$qb < a$

$qb - qb < a - qb$

$0 < a - qb \Rightarrow a - qb > 0$

$r > 0$.

$a < (q+1)b$.

$a - qb < qb + b - qb$

$a - qb < b$ $\quad \therefore 0 < r < b$

$r < b$

$$\boxed{a = qb + r \quad 0 < r < b} \quad \text{---} \quad (2)$$

$\therefore$ from (1) & (2) we get

$$\boxed{a = qb + r \quad 0 \leq r < b}$$

uniqueness of q & r :-

We show the uniqueness of q & r Suppose that the integer q & r are not unique.

$a = bq + r$ & $a = bq' + r'$ $\quad 0 \leq r' < b$

where $0 \leq r < b$

$r = a - bq$ $\quad r' = a - bq'$

$r' - r = bq - bq' = b(q - q')$

$b \mid a$ $\quad a = bq + r$

Taking absolute value on both sides

$$|r' - r| = |b(q - q')|$$

$$= |b|\,|(q - q')| \quad \text{— (A)}$$

$\because$ absolute value of product is equal to the product of the absolute value.

$0 \le r < b$ & $0 \le r' < b$ *

↳ (A)

multiply equ (A) by -1.

$-b < -r \le 0$ & $0 \le r' < b$ *

Adding the above equation.

$-b < r' - r < b$ *

i.e. $|r' - r| < b$.

i.e. $|b|\,|q - q'| < b$.

i.e. $b\,|q - q'| < b$

i.e. $|q - q'| < 1$

↳ absolute value It is always ≥ 0.

$\Rightarrow$ $0 \le |q - q'| < 1$

$\Rightarrow$ $q - q' = 0$.

$\Rightarrow$ $\boxed{q = q'}$.

$\because r = r'$

Hence q & r are unique.

$0 \le 2 < 3$.

$0 \le -2 < -3$

$-3 \le -2 \le 0$

common divisor

Positive divisors of 12

Example :- what are the quotient & remainder when -11 is divided by 3 ?

$-11 = (-4)\,3 + 1$

quotient $q = -4$ $\quad r = 1$

$13 \mid 46$.

$46 = 13 \times 3 + 7$

$a \quad b$

Note that $-11 = 3(-3) - 2$.

$b \quad q \quad r$

This is not the correct representation as $r = -2$ But $0 \le r < b$.

$0 \le -2 < 3$

-3

$3 \mid -11$

$\frac{-11}{-3}$

$\frac{-11}{3}$

$a = bq + r$

$-2 < -3$

n...n on both sides

Let a & d be any two integers. We say that d is a divisor of a (↓ factor) written as $d|a$ if $a = qd$ for some integer q.

Ex :- $3|21$ $\quad$ $3|15$ $\quad$ 3 is a common divisor of 21 & 15

$21 = 7 \cdot 3$ $\quad$ $15 = 5 \cdot 3$

Let a & b be any two integers. Then an integer d is called a common divisor of a & b if $d|a$ & $d|b$.

Greatest common division :-

(or) GCD :-

Let a, b are non zero integers. Then an integer $d \geq 1$ is called a greatest common divisor of a & b, if the following properties hold.

(1) $d|a$ & $d|b$

(2) For any integer n, if $n|a$ & $n|b$ then $n|d$. $(n \leq d)$

d is multiple of every common divisor

Positive divisors of 192, 288

192 — 1, 2, 3, 4, 6, 8, 12, 16, 24, 32, 48, 64, 96

288 — 1, 2, 3, 4, 6, 8, 9, 12, 16, 18, 24, 32, 36, 48, 72, 96, 144

common positive divisors of 192 & 288

1, 2, 3, 4, 6, 8, 12, 16, 24, 32, 48, 96.

96 is the greatest common divisor of 192 & 288.

One way to find the greatest common divisor of two integers is to find all the common divisors of both integers & then take the largest divisor.

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

Note :- If gcd (a, b) = 1, then a, b are said to be relatively prime or coprime.

If gcd $(a_i, a_j) = 1$ $i \neq j$

$1 \leq i < j \leq n$, then $a_1, a_2 \ldots a_n$ are said to be pairwise relatively prime.

Example :-

3, 7, 11 are pairwise relatively prime.

gcd(3,7) = 1, gcd(7,11) = 1
gcd(3,11) = 1.

2, 9, 10 are not pairwise prime

as 2, 10 are not coprime.

∴ gcd(2,9) = 1, ~~gcd~~ but gcd(2,10) = 2 ≠ 1

gcd(9,10) = 1

$10 = \frac{1 \times 2}{1 \times 2 \times 5} \times 10$

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

Statement :- Let a, b be 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 & so on & if $r_{k+1} = 0$, then the last non-zero remainder r_k is the gcd(a, b).

$a > b$

$a = bq + r_1$

$b = r_1 q + r_2$

$r_1 = r_2 q + r_3$

Finding gcd(a,b) by prime factorization or prime decomposition.

If the prime factorisations of a & b are

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

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 factorisations, with zero exponent if necessary, Then

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

where $\min(x,y)$ → the minimum of no two numbers x & y.

Example :-

Find the gcd(120, 500) by prime factorization & Euclid's algorithm.

Solution :-

(i) **prime factorization :-**

$120 = 2^3 \times 3 \times 5$

2	120
2	60
2	30
3	15
	5

$500 = 2^2 \times 3^0 \times 5^3$

2	500
2	250
5	125
5	25
	5

$\gcd(120, 500) = 2^{\min(3,2)} \cdot 3^{\min(1,0)} \cdot 5^{\min(3,1)}$

$= 2^2 \cdot 3^0 \cdot 5^1 = 4 \times 5$

$= 20.$

120×3
360

120×4
480

Euclid's algorithm :-

$500 = 4 \times 120 + 20$

$120 = 6 \times 20 + 0$

$\therefore \gcd(120, 500) = 20$ [last non zero remainder = 20]

Find $\gcd(1575, 231)$ by using Euclid's algorithm.

231×6
1386

231×7
1617

$1575 = 6 \times 231 + 189$

$231 = 1 \times 189 + 42$

$189 = 4 \times 42 + 21$

$42 = 2 \times 21 + 0.$

$\therefore \gcd(1575, 231) = 21.$

(2)

Theorem :-
gcd(a,b) can be expressed as an integral linear combination of a, b. ie there are integers m, n s.t gcd(a,b) = ma + nb.

Example : Express gcd(252,198) = 18 as a linear combination of 252 & 198.

Soln To find the gcd(252,198) by using Euclid's algorithm

$252 = 1 \times 198 + 54$

$198 = 3 \times 54 + 36$

$54 = 1 \times 36 + 18$

$36 = 2 \times 18 + 0$.

$18 = 54 - 36$

$18 = 54 - (198 - 3 \times 54)$

$18 = 4 \cdot 54 - 198$

$18 = 4(252 - 198) - 198$

$= 4 \cdot 252 - 5 \cdot 198$

$= 4 \cdot 252 + (-5) 198$.

$(4 \times 252) - (5 \times 198)$

$= 202 \cdot 252 - 257 \cdot 198$

Thus the expression of gcd(a,b) in the form ma+nb is not unique.

↳ It is not necessarily the greatest common divisor.

2|500
250

Properties of GCD :-

1. If a, b, c are positive integers such that $\gcd(a,b) = 1$ & $a \mid bc$ then $a \mid c$.

Proof :- Let a & b be relatively prime integers.

Given $\gcd(a,b) = 1$

$\therefore$ There are integers m, n such that

$$ma + nb = 1 \quad . \quad m, n \in \mathbb{Z}$$

Multiplying both sides by c, we have

$$mac + ncb = c$$

ie $$mac + nka = c$$

$$(mc + nk)a = c$$

$$ra = c \Rightarrow a \mid c$$

$a \mid bc \Rightarrow bc = ka \quad k \in \mathbb{Z}$

2. If $\gcd(a,b) = 1$, $\gcd(a,c) = 1$, then $\gcd(a, bc) = 1$

(or)

Let $a, b, \& c$ be integers. Suppose that a & b are relatively prime & that a & c are relatively prime. Then a & bc are relatively prime.

Solution

a & b are relatively prime (m) then it can be expressed as a linear combination of a, b.

ie $\gcd(a,b) = 1$

ie $ma + nb = 1 \quad m, n \in Z$ —— (1)

a & c are relatively prime

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

ie $ra + sc = 1$ —— (2) $r, s \in Z$.

we have to prove that a & bc are relatively prime. ie $\gcd(a, bc) = 1$

ie $ja + kbc = 1 \quad j, k \in Z$

Multiplying eq (1) by c & s

$cma + cnb = c$

$scma + snbc = sc$

$smac + snbc = 1 - ra$ from (2).

$smac + snbc + ra = 1$

$(smc + r)a + sn(bc) = 1$

$ja + k(bc) = 1$

Thus a & bc are relatively prime.

gcd (192, 288)

$96 | 192 = 96$

$96 | 288$

If a, b are any integers, which are not simultaneously zero & k is a positive integer, then

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

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

Then there are integers m, n such that $ma + nb = d$. ——— (1)

Multiply eq (1) by k.

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

i.e. $\gcd(ka, kb) = kd$

$= k \cdot \gcd(a, b)$.

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

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

Proof :- Given $\gcd(a, b) = d$.

Then there exists integers m, n $m, n \in Z$.

such that $ma + nb = d$

i.e. $m\left(\frac{a}{d}\right) + n\left(\frac{b}{d}\right) = 1$ ——— (1)

Since $d|a$ & $d|b$, $\frac{a}{d}$ & $\frac{b}{d}$ are integers

$\therefore$ (1) means

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

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

proof :- $\gcd(a,b) = 1$

$\therefore$ If m_1, n_1 are integers s.t

$$m_1 a + n_1 b = 1 \quad \text{---} (1)$$

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

$\therefore$ $m_2(ac) + n_2 b = d$ for some integers m_2, n_2.

$$\text{---} (2)$$

from (1) & (2), we have.

$$(m_1 a + n_1 b)(m_2 ac + n_2 b) = d$$

$$m_1 m_2 a^2 c + m_1 n_2 ab + m_2 n_1 ac b + n_1 n_2 b^2 = d$$

$$m_1 m_2 a^2 c + (m_1 n_2 a + n_1 m_2 ac + n_1 n_2 b) b = d$$

$m_1 m_2 a^2 \in \mathbb{Z}$; $(m_1 n_2 a + n_1 m_2 ac + n_1 n_2 b) \in \mathbb{Z}$.

$\therefore$ $m_3 c + n_3 b = d$ for some integers m_3, n_3 which implies $\gcd(c, b) = d$.

$\therefore$ $gcd(ac, b) = gcd(c, b)$.

(b) If each of $a_1, a_2 \cdots a_n$ is coprime to b, ie $gcd(a_i, b) = 1$ $i = 1, 2 \cdots n$ then the product $a_1 \cdot a_2 \cdots a_n$ is also coprime to b ie $gcd(a_1 a_2 \cdots a_n, b) = 1$.

Proof :- $gcd(a_1, b) = 1$

By result 5, $gcd(a_1 a_2, b) = gcd(a_2, b)$
$= 1$

III^{ly} $gcd(a_1 a_2 a_3, b) = gcd(a_3, b) = 1$

$\vdots$

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

(7) If p is a prime & $p \mid a_1 a_2 \cdots a_n$ where each a_i is an integer, $i = 1, 2 \cdots n$ then $p \mid a_i$ for some i.

Proof :- By fundamental theorem of arithmetic, each a_i is a product of primes. As p is a prime, p must be one of the prime factors of a_i. $i = 1, 2 \cdots n$. Thus $p \mid a_i$ for some i

Least common multiple :-

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

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

Ex :- $lcm(4,14) = lcm(-4,14)$

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

$4 = 2 \times 2$
$14 = 7 \times 2$
$= 7 \times 2 \times 2$

$-4 = -2 \times 2$
$14 = 7 \times 2$
$= 7 \times 2 \times 2$

Alternative definition of $lcm(a,b)$:-

If the prime factorisation of a & b are $a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$

& $b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}$ with the conditions stated in the alternative definition of $gcd(a,b)$ then

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

* Let a & b be any two integers not both zero. Then an integer $m \geq 1$ is called a least common multiple of a & b if the following properties hold : (i) $a|m$ & $b|m$
(ii) for any integer n, if $a|n$ & $b|n$ then $m|n$.

$m =$

For ex :-

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

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

Then $\text{Lcm}(24,30) = 2^{\max(3,1)}\ 3^{\max(1,1)}\ 5^{\max(0,1)}$

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

Theorem :

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

Proof :- Let the prime factorization of a & b be

$$a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$$

$$b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}$$

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

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

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, $i = 1, 2, \ldots, n$.

Hence $\gcd(a,b) \times \text{Lcm}(a,b)$

$$= p_1^{\min(a_1,b_1)+\max(a_1,b_1)} \; p_2^{\min(a_2,b_2)+\max(a_2,\ldots)} \; \ldots\ldots \; p_n^{\min(a_n,b_n)+\max(a_n,b_n)}$$

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

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

$$= ab.$$

Example :- use the Euclidean algorithm to find $\gcd(1819, 3587)$

2) $\gcd(12345, 54321)$. In each case express the gcd as a linear combination of the given numbers.

Soln By division algorithm

$$3587 = 1 \times 1819 + 1768$$

~~54321~~

$$1819 = 1 \times 1768 + 51$$

$1768 = 34 \times 51 + 34$

$51 = 1 \times 34 + 17.$

$34 = 2 \times 17 + 0.$

Since the last non-zero remainder is 17. $\therefore \gcd(1819, 3587) = 17.$

$17 = 51 - 1 \times 34.$

$17 = 51 - (1768 - 34 \times 51)$

$= 35 \times 51 - 1768.$

$= 35(1819 - 1768) - 1768$

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

$= 35 \cdot 1819 - 36(3587 - 1819)$

$= 71 \cdot 1819 - 36 \cdot 3587.$

Example :- using prime factorisation find the gcd & lcm of (i) (231, 1575)

(ii) (337500, 21600). Verify also that $\gcd(m,n) \cdot \text{lcm}(m,n) = mn.$

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

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

3	231
7	77
11	11
	1

5	1575
5	315
3	63
3	21
7	7
	1

gcd (231, 1575)

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

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

$= 21$

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

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

$= 9 \cdot 25 \cdot 7 \cdot 11 = 17325$

gcd (231, 1575) · lcm (231, 1575)

$= 21 \cdot 17325$

$= 363825$

$= 231 \times 1575$

Example :-

Find the integers m & n such that $512m + 320n = 64$.

$am+bn = gcd(a,b)$

$512 = 1 \times 320 + 192$ — (1)

$320 = 1 \times 192 + 128$ — (2)

$192 = 1 \times 128 + 64$ — (3)

$128 = 2 \times 64 + 0$.

$$\begin{array}{r|l} & 1 \\ 320 & 512 \\ & 320 \\ \hline & 192 \end{array}$$

from equation (3), we have.

$64 = 192 - 1 \times 128$

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

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

$= 2 \times 192 - 320$

$= 2(512 - 320) - 320$

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

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

$\therefore m = 2, \quad \& \quad n = -3$.

~~41~~, ~~44~~, 56, ~~63~~, 63;

Prime number

(i) greater than 1

(ii) Factors are 1 & itself

2 = 1×2 ; 2×1

3 = 1×3, 3×1

composite number :

A composite number are those numbers which are not prime.

number, & the number is not prime.

Factorising a number :—

writing a number as a product of two or more numbers is called factorisation

12 = 2×2×3.

Fundamen

Every composite number can be uniquely expressed as a product of prime, except for the order in which these prime factor occurs.

105 = 5×21 = 5×3×7

105 = 3×35 = 3×7×5

105 = 7×15 = 7×5×3

Jeba Krisha → 8056256491

~~Padm~~