UNIT-5

NUMBER THEORY

Properties of integers:

$Z = \{ \ldots, -3, -2, -1, 0, 1, 2, 3 \ldots \}$

i) $(N, +)$ – closure, Associative, Abelian

ii) $(N, *)$ – closure, Associative, identity, Abelian

iii) $(Z, +)$ – closure, Associative, identity, inverse, abelian

iv) $(Z, *)$ – closure, Associative, identity, abelian.

cancellation law:

Multiple cancellation law:

Suppose $a \neq 0$ then

$a \cdot b = a \cdot c$

$\Rightarrow b = c$ (Left cancellation law)

$b \cdot a = c \cdot a$

$\Rightarrow b = c$ (RCL)

Note: Additive cancellation

For a, b, c

$a + b = a + c \Rightarrow b = c$

$b + a = c + a \Rightarrow b = c$

⇒ show that cancellation law hold in a group.

Sol Suppose $a \neq 0 \in G$

$\Rightarrow \exists a^{-1} \in G \ni aa^{-1} = a^{-1}a = e$

let $ab = ac$

$a^{-1}(ab) = a^{-1}(ac)$

$(a^{-1}a)b = (a^{-1}a)c$

$eb = ec$

$b = c$

Def

Let $a>b$ be two integers. we say $a>b$ if $a-b$ is a +ve integer. we denote this by $b<a$ also

Ex: $3>2$ because $3-2=1>0$ +ve integer.

Well ordering principle:

Every non empty set of +ve integers has a least element.

i.e. let s be a non empty set then $\exists n \in z^+ \ni n \in m, \forall m \in s$

Theorem let a, b be two positive integers then there exist a positive integer n such that $a<n.b$

Example

$a=3, b=2$ then $n=2$

i.e $3<2.2 \Rightarrow 3<4$

Divisibility rule:

Let a and b be two positive integers with $a \neq 0$ if there exist a positive integer n such that $b = n \times a$ then we say 'a' divides 'b' (or) 'b' is divisible by 'a'. we denote it by $a|b$

Note:

i) $a|b \Leftrightarrow \exists n \in z \ni b = na$

ii) when $a|b$ we called 'a' as divisor (or) factor of b. and b is called multiple of a

iii) if a doesnot divides b ($a \nmid b$) we denote it by $a \nmid b$

Example $2|4, 3|9, 2 \nmid 5, 3 \nmid 7$

Note:

1. $1|a$ $(\because a = a \cdot 1)$
2. $a|a$ $(\because a = 1 \cdot a)$

Theorem

i. $a|b$ and $b \neq 0$ then $|a| \leq |b|$

ii. $a|b, b|c \Rightarrow a|c$

iii. $a|b, a|c \Rightarrow a|b \pm c$

iv. $a|b, m \in z, m \neq 0 \Rightarrow a|mb$

v. $a|b, b|a \Rightarrow a = \pm b$

vi. $a|b, a|b+c \Rightarrow a|c$

vii. $a|b, m \neq 0$ then $ma|mb$

viii. $a|b, a|c \Rightarrow a|mb+nc$

i. let $a|b, b \neq 0$

$\Rightarrow b = n.a, n \in z, n \neq 0$

$|n| \geq 1$

$|b| = |n.a|$

$|b| = |n| \cdot |a|$

$|b| \geq 1 \cdot |a|$

$|b| \geq |a|$

$\Rightarrow |a| \leq |b|$

ii. let $a|b, b|c$

$\Rightarrow b = n_1 \cdot a, \quad c = n_2 \cdot b \quad , n_1, n_2 \in z$

claim :- $a|c$

$c = n_2 \cdot b$

$c = n_2 \cdot n_1 \cdot a$

$c = n_1 \cdot n_2 \cdot a$

$c = na$

$\Rightarrow a|c$

iii, let $a|b$, $a|c$

$\Rightarrow b = m.a \quad c = n.a$

$b \pm c = m.a \pm n.a$

$b \pm c = a(m \pm n)$

$b \pm c = k.a$

$\Rightarrow a | b \pm c$

iv, $a|b$

$\Rightarrow b = n.a$

$mb = m.na$

$mb = mna$

$mb = ka$

$\Rightarrow a | mb$

v, $a|b$, $b|a$

$\Rightarrow b = m.a \quad a = n.b$

Claim:- $a = \pm b$

$a = n.b$

$a = n.(m.a)$

$a = mn.a$

$\Rightarrow mn = 1$

$\Rightarrow m = n = 1$

$\Rightarrow m = n = -1$

$a = n.b$

$a = 1.b$ and $a = -1.b$

$\Rightarrow a = \pm b$

vi) $a|b$, $a|b+c$

$\Rightarrow b = m \cdot a$ & $c = n \cdot a$

$b + c - b = n \cdot a - m \cdot a$

$c = (n-m)\, a$

$c = k \cdot a$

$\Rightarrow a|c$

vii) If $a|b$ then $ma|mb$

$a|b$

$\Rightarrow b = n \cdot a$

$mb = m(n \cdot a)$

$mb = m(na)$

$mb = (ma)\, n$

$\Rightarrow ma|mb$

viii) $a|b$ $a|c$

$\Rightarrow b = k_1 a$ $c = k_2 a$

$mb = mk_1 a$ $mc = mk_2 a$

$mb + mc = mk_1 a + mk_2 a$

$= a(mk_1 + mk_2)$

$= a \cdot (mk_1 + mk_2)$

$mb + mc = a \cdot k$

$\Rightarrow a|mb + mc$

Division Algorithm (or) Division Theorem:

Let a, b be any two integers, $b>0$ then there exist unique integers q and r such that $a = bq + r$, $0 \le r < b$

Proof:

Consider the infinite sequence of the multiples of b namely $\ldots -2\cdot b, -1\cdot b, 0, 1\cdot b, 2\cdot b, 3\cdot b \ldots$

clearly $a = bq$ (or) $bq < a < b(q+1)$

$\Rightarrow bq \le a < b(q+1)$

$\Rightarrow bq \le a < bq + b$

subtract bq on all sides

$\Rightarrow 0 \le a - bq < b$

let $r = a - bq \Rightarrow 0 \le r < b$

$a = bq + a - bq$

$a = bq + r$

Suppose $\exists\ q_1, q_2, r_1, r_2$

$\exists\ a = bq_1 + r_1,\ 0 \le r_1 < b$

$a = bq_2 + r_2,\ 0 \le r_2 < b$

$bq_1 + r_1 = bq_2 + r_2$ ——— (1)

$b(q_1 - q_2) = r_2 - r_1$ and $0 \le r_2 - r_1 < b$

$b \mid r_2 - r_1$ and $0 \le r_1 - r_2 < b$

$\Rightarrow r_2 - r_1 = 0$

$\Rightarrow \boxed{r_1 = r_2}$

from (1)

$bq_1 + r_1 = bq_2 + r_1$

$bq_1 = bq_2$

$\Rightarrow \boxed{q_1 = q_2}$

Ex: $b \to 2)\ 6 \mid 7\ (3 \le r$

$a = bq$, $bq < a < b(q+1)$

$6 \mid 6$

$0 \mid 1 \to r$

Greatest Common divisor (GCD):

A non-zero integer 'd' is said to be common divisor of integers a and b if d|a and d|b and d is said to be GCD of a and b if for any divisor 'c' of a, b is always divides d (c|d).

GCD of a and b is denoted by GCD(a, b)

Def: d' is said to be GCD of a, b if

ie GCD(a, b) = d if

1. d|a ; d|b
2. if c is any divisor of a, b then c|d

Example

Consider two integers 12 and 18.

common divisors → 2, 3, 6

Greatest common divisor is 6

because (2|6, 3|6, 6|6)

GCD(12, 18) = 6

Prime number:

A positive integer p > 1 is called prime if only divisor of p are one and itself. otherwise we call p as composite number

Example 2, 3, 5, 7, 11, 13 .... are prime numbers

4, 6, 8, 9, 10, ... are composite numbers.

Relative prime:

If GCD(a,b) = 1 then we say a and b are relatively prime

Example

2 and 3 are relatively prime but 2 and 8 are not relatively prime

Note:

$a_1, a_2, \ldots, a_n$ are said to be pair wise relatively prime. If $GCD(a_1, a_2, a_3, \ldots, a_n) = 1$. Also $GCD(a_i, a_j) = 1$

Example 2, 3, 15 are pair wise relatively prime.

Problem:

S.T GCD of any two integers is unique.

Proof: Let a,b be two integers

Suppose $GCD(a,b) = d_1$, $GCD(a,b) = d_2$

$\Rightarrow GCD(a,b) = d_1$ and take d_2 as a divisor of a,b

$\Rightarrow d_2 | d_1$ —— ①

Also, $GCD(a,b) = d_2$, and take d_1 as a divisor of a,b

$\Rightarrow d_1 | d_2$ —— ②

from ① and ②

$d_1 = d_2$

∴ The GCD of any two integers is unique.

Euclidean Algorithm for finding GCD:

Euclidean Theorem:

When a and b any two integers such that $a>b>0$ if r_1 is remainder when 'a' is divided by 'b', r_2 is remainder when 'b' is divided by r_1, r_3 is remainder when r_1 is divided by r_2 and so on and if $r_{n+1}=0$ then the last non-zero remainder r_n is the GCD of a, b

Proof:

First we prove the following lemma

lemma: If $a=bq+r$ where a, b, q, r are integers then $GCD(a,b)=GCD(b,r)$

Proof of lemma:

Let $GCD(a,b)=d_1$ and $GCD(b,r)=d_2$

$\Rightarrow d_1|a, d_1|b$ and $r=a-bq$

$\Rightarrow d_1|r, d_1|b$

$\Rightarrow d_1$ is common divisor of r, b and $GCD(b,r)=d_2$

$\Rightarrow d_1|d_2$ —①

$GCD(b,r)=d_2$

$\Rightarrow d_2|b, d_2|r$ and $a=bq+r$

$\Rightarrow d_2|a$ and $d_2|b$

$\Rightarrow d_2$ is common divisor of a, b and $GCD(a,b)=$

$d_2|d_1$ —②

from ① and ②

$d_1=d_2$.

$\Rightarrow GCD(a,b)=GCD(b,r)$

By division algorithm we have, ← (Proof of theorem)

$a=bq_1+r_1$, $0\le r_1<b$

if $r_1\neq 0$ $b=r_1q_2+r_2$, $0\le r_2<r_1$

if $r_2\neq 0$ $r_1=r_2q_3+r_3$, $0\le r_3<r_2$

if $r_{n-1} \neq 0$ $r_{n-2} = r_{n-1} q_n + (r_n \neq 0)$

if $r_n \neq 0$ $r_{n-1} = r_n q_{n+1} + (r_{n+1} = 0)$

By above lemma we have

$$GCD(a,b) = GCD(b,r_1) = GCD(r_2,r_1) = \cdots = GCD(r_{n+1}, r_n)$$
$$= r_n$$

$\therefore GCD(a,b) = r_n$

Theorem:

GCD(a,b) can be expressed as an integral linear combination of a and b $\quad gcd(a,b) = ua + vb,\ u,v \in Z$

Problems (on Euclidean theorem)

1. Find the GCD of 42823 and 6409

sol

$42823 > 6409$

$42823 = 6 \times 6409 + 4369$ — ①

$6409 = 1 \times 4369 + 2040$ — ②

$4369 = 2 \times 2040 + 289$ — ③

$2040 = 289 \times 7 + 17$ — ④

$289 = 17 \times 17 + 0$ $\quad r_{n+1}$

$GCD(42823, 6409) = 17$

from ④ $\quad 17 = 2040 - 7 \times 289$

from ② $\quad 2040 = 6409 - 1 \times 4369$

from ③ $\quad 289 = 4369 - 2 \times 2040$

from ① $\quad 4369 = 42823 - 6 \times 6409$

$17 = 6409 - 1 \times 4369 - 7(4369 - 2 \times 2040)$

$17 = 6409 - 8 \times 4369 + 14 \times 2040$

$17 = 6409 - 8(42823 - 6 \times 6409) + 14(6409 - 1 \times 4369)$

$17 = 63 \times 6409 - 8 \times 42823 - 14(42823 - 6 \times 6409 + 2 \times 2040)$

$17 = 147 \times 6409 - 22 \times 42823 \Rightarrow u = 147$ and $v = -22$

2. Find the GCD of 615 and 1080 and find integers u, v
GCD (615, 1080) = u·615 + v·1080.

Sol:

1080 > 615

$1080 = 1 \times 615 + 465$ — ①

$615 = 1 \times 465 + 150$ — ②

$465 = 3 \times 150 + 15 \rightarrow r_n$ — ③

$150 = 15 \times 10 + 0 \rightarrow r_{n+1}$

GCD (1080, 615) = 15

From ③

$15 = 465 - 3 \times 150$ — ④

From ① $465 = 1080 - 1 \times 615$ — ⑤

From ② $150 = 615 - 1 \times 465$ — ⑥

from ④, ⑤, ⑥

$15 = 1080 - 1 \times 615 - 3(615 - 1 \times 465)$

$15 = 1080 - 1 \times 615 - 3 \times 615 + 3 \times 465$

$15 = 1080 - 4 \times 615 + 3(1080 - 1 \times 465)$

$15 = 1080 - 4 \times 615 + 3 \times 1080 - 3 \times 465$

$15 = 4 \times 1080 - 7 \times 615$

$u = 4, \quad v = -7$

Note:

GCD(a, b) = 1 if and only if $au + bv = 1$

Theorem 1:

If $c|ab$ and gcd(a, c) = 1 then $c|b$

Proof Given gcd(a, c) = 1 and $c|ab$

$\Rightarrow au + cv = 1$ — ① and $c|ab$

claim :- $c|b$

multiply ① with b on both sides

$b = abu + bcv$

$\Rightarrow c|b$ ($\because c|ab$ and $c|bc$)

Theorem2:

GCD(a,b) = 1 and GCD(a,c) = 1 then GCD(a,bc) = 1

Proof

Given GCD(a,b) = 1 and GCD(a,c) = 1

$au_1 + bv_1 = 1$ — ① $au_2 + cv_2 = 1$ — ②

claim: GCD(a,bc) = 1

i.e., $au + bcv = 1$

Multiply ① and ②

$1 \times 1 = (au_1 + bv_1)(au_2 + cv_2)$

$1 = a^2u_1u_2 + acu_1v_2 + abu_2v_1 + bcv_1v_2$

$1 = a(au_1u_2 + cu_1v_2 + bu_2v_1) + bcv_1v_2$

$\boxed{1 = au + bcv}$

Theorem3:

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

Proof

let gcd(a,b) = d

$\Rightarrow au + bv = d$ — ① ; $u, v \in Z$

let k be any integer

Multiply ① with k on b.s

$(ak)u + (bk)v = dk$

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

Theorem-4:

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

proof

Given gcd(a,b) = d

$\Rightarrow au + bv = d$ — ① where $u, v \in Z$

Divide with d on b.s

$\left(\frac{a}{d}\right)u + \left(\frac{b}{d}\right)v = 1$, $u, v \in Z$

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

Theorem-5

If $\gcd(a,b)=1$ then $\gcd(ac,b)=\gcd(c,b)$

Proof

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

$\Rightarrow au_1+bv_1=1 \quad ; u_1,v_1 \in z \quad \text{①}$

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

$\Rightarrow acu_2+bv_2=d \quad \text{②} \quad u_2,v_2 \in z$

① × ②

$(au_1+bv_1)(acu_2+bv_2)=1\times d$

$a^2cu_1u_2+abu_1v_2+abcv_1u_2+b^2v_1v_2=d$

$ca(a^2u_1u_2+abv_1u_2)+b(au_1v_2+bv_1v_2)=d$

$cu+bv=\text{Gcd}(ac,b)$

$\text{Gcd}(c,b)=\text{Gcd}(ac,b)$

Theorem-6

If $a_1,a_2,a_3\ldots\ldots,a_n$ are relative prime to b then $a_1\cdot a_2\cdot a_3\cdot a_4\ldots\ldots a_n$ is relative prime to b

Proof Given $\gcd(a_1,b)=1$

By known theorem $\text{GCD}(a_1,a_2,b)=\text{GCD}(a,b)$

$\text{GCD}(a_1,a_2,b)=1$

Again by K.T $\gcd((a_1,a_2)a_3,b)=\text{GCD}(a_3,b)$

$\gcd(a_1,a_2a_3,b)=1$

Continue likewise

Finally we get $\gcd(a_1,a_2a_3\ldots\ldots a_n,b)=1$

Least common Multiple (LCM):

Let a, b be any two non zero integers then LCM(a,b) = m a non-zero integer if

i. a|m, b|m

ii. if c is any common multiple of a, b then m|c

Example.

LCM(12, 18) = 36

Note:

LCM(18, -8) = LCM(-18, 8) = LCM(8, 18) = 72

Theorem:

If a and b are two non zero integers then

gcd(a, b) · LCM(a, b) = |ab|

Proof:

Ex: gcd(9, 12) = 3

LCM(9, 12) = 36

3 × 36 = 9 × 12

∴ gcd(9, 12) · LCM(9, 12) = 3 × 36

Testing for prime numbers:

Prime testing is a common task for computers for deciding whether a number n is prime or composite.

primality testing have become important in application of cryptography

Result: Every integer $n \geq 2$ has a prime factor.

Example The prime factor for 24 are 2, 3 and every prime number is itself a prime factor

Theorem:

If $n > 1$ be a composite integer then there exist a prime P such that $p|n$ and $P \leq \sqrt{n}$

Proof

Suppose $n > 1$ is a composite number

$\exists u, v \in z \Rightarrow n = uv, \quad 1 < u \leq v < n$

By known result u has prime factor P

i.e $p|u$

∴ P is also has prime factor for n i.e $p|n$

$p|u \Rightarrow p < u$

To prove $P \leq \sqrt{n}$ we prove that $u \leq \sqrt{n}$

if possible suppose $u > \sqrt{n}$

$\Rightarrow \sqrt{n} < u \leq v$

$n = uv$

$> \sqrt{n}\sqrt{n}$

$\Rightarrow n > n$

which is contradition

∴ our assumption is wrong

∴ $u \leq \sqrt{n}$

$P \leq \sqrt{n}$

Algorithm for prime testing:

step 1: verify whether n is 2. If n is 2 then n is prime if not go to step 2.

step 2: verify whether 2 divides n. If 2 divides n, then n prime. If 2 does not devide n then go to step 3

step 3: Find all odd primes $p \leq \sqrt{n}$. If there is no such prime, then n is prime otherwise go to step 4.

Step 4: verify whether p divides n, where p is a prime obtained in step(3) If p divides n, then n is not a If p does not divide n for any prime p obtained in step(3), then n is prime.

Problem

1. Determine whether the integer 133 is prime or not.

sol step1: Note that $2 \nmid 133$

step2: Now we find all odd primes p such that $p^2 \leq n$

i.e $3^2, 5^2, 7^2, 11^2 \leq 133 < 13^2$

$P = 3, 5, 7, 11$ and $7 | 133$

$\therefore$ 133 is not a prime

2. Determine whether the integer 287 is prime or not

sol step 1: Note that $2 \nmid 287$

step2: Now we find all odd prime p such that $p^2 \leq n$

i.e $3^2, 5^2, 7^2, 11^2, 13^2 \leq 287 < 17^2$

$P = 3, 5, 7, 11, 13$ and $7 | 287$

$\therefore$ 287 is not a prime

1. Find all primes less than or equal to 100

Sol step 1: First we find all primes p

$\ni p^2 \leq 100$

$\rightarrow p = 2, 3, 5, 7$ $(2^2, 3^2, 5^2, 7^2)$

step 2: Now we find all primes less than or equal to 100 by finding those numbers that are not divisible by 2, 3, 5, 7. Those are 1, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97

Theorem:

Fundamental Theorem of Arthimatic:

statement:

Every integer $n > 1$ can be expressed uniquely as a product of primes upto the order of the factors.

More precisely, if $n = p_1 p_2 p_3 \ldots p_u$ and $n = \gamma_1 \gamma_2 \gamma_3 \ldots \gamma_v$ where p_i, γ_i are primes then $p_i = \gamma_j$ (in some order)

Proof:

Existance: we prove that every integer $n > 1$ is a product of prime numbers.

let $s(n)$: n is a product of primes

for $n = 2$, $2 = 2$

$\therefore s(2)$ is true

Now suppose that $s(k)$ is true

Therefore each of the integers $2, 3, 4, \ldots, k$ can be expressed as product of primes.

Now we prove that $s(k+1)$ is true

Case 1: if $k+1$ is prime then there is nothing to prove

Case 2: if $k+1$ is not prime then

$k+1 = uv$, where $1 < u \leq v < k+1$

Since $u, v < k+1$ we have by induction hypothesis u and v can be expressed as product of primes.

Therefore $n = u \cdot v$ can also be expressed as product of primes.

Uniqueness:

Now we Prove that if $n = p_1 \cdot p_2 \cdot p_3 \cdots p_i = q_1 \cdot q_2 \cdots q_j$ we can easily prove $p_i = q_j$ for some i and j and also we can prove $u = v$.

For example: $3526 = 2 \times 1763$

$= 2 \times 41 \times 43$

or $3526 = 41 \times 86$

$= 41 \times 2 \times 43$

or $3526 = 43 \times 41 \times 2$

Definition: The representation of n in the form called standard factorisation is as follows

$n = p_1^{r_1} \cdot p_2^{r_2} \cdots p_k^{r_k}$ where, $r_i > 0$ and p_i is prime integer and $p_i \neq p_j$ for $i \neq j$

Example

The standard factorisation of 972 is

$972 = 2^2 \times 3^5$

Problem

1. Find the prime factorisations of 81, 100, 289

sol

$81 = 3 \times 3 \times 3 \times 3 = 3^4$

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

$289 = 17 \times 17 = 17^2$

Theorem:

Let $m = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot p_3^{\alpha_3} \cdots p_u^{\alpha_u}$ and $n = p_1^{\beta_1} \cdot p_3^{\beta_2} \cdots p_v^{\beta_v}$ then

① $\gcd(m, n) = \pi p^{\min(\alpha, \beta)}$

where minimum (α, β) represents minimum of two numbers α and β.

② $\text{LCM}(m, n) = \pi p^{\max(\alpha, \beta)}$

Problems

1. Use prime factorisation to find GCD and LCM of the following i) 12, 18 ii) 16, 30 iii) 119, 544

Sol i) (12, 18)

$12 = 2^2 \times 3^1$

$18 = 2^1 \times 3^2$

$GCD(12, 18) = 2^{\min(2,1)} \cdot 3^{\min(1,2)}$

$= 2^1 \cdot 3^1$

$= 6$

$LCM(12, 18) = 2^{\max(2,1)} \cdot 3^{\max(1,2)}$

$= 2^2 \cdot 3^2$

$= 36$

ii) (16, 30)

$16 = 2^4$

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

$GCD(16, 30) = 2^{\min(4,1)} \cdot 3^{\min(0,1)} \cdot 5^{\min(0,1)}$

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

$= 2$

$LCM(16, 30) = 2^{\max(4,1)} \cdot 3^{\max(0,1)} \cdot 5^{\max(0,1)}$

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

$= 240$

iii) (119, 544)

$119 = 7^1 \times 17^1$

$544 = 2^5 \times 17^1$

$GCD(119, 544) = 2^{\min(0,5)} \cdot 7^{\min(0,1)} \cdot 17^{\min(1,1)}$

$= 2^0 \cdot 7^0 \cdot 17$

$= 17$

$LCM(119, 544) = 2^{\max(0,5)} \cdot 7^{\max(0,1)} \cdot 17^{\max(0,1)}$

$= 2^5 \cdot 7^1 \cdot 17$

$= 3808$

Modular Arthimatic:

Congurance Modulo m:

Let a, b any two integers and m is a positive integer then we say 'a' is congurient modulo m $(a \equiv b \pmod m)$. If $m \mid a-b$

Example

① $93 \equiv 13 \pmod 5$ $(\because 5 \mid 93-13)$

② $7 \equiv -5 \pmod 4$ $(\because 4 \mid 7-(-5))$

③ $20 \not\equiv 3 \pmod 5$ $(\because 5 \nmid 20-3)$

Properties of Congurence:

Theorem:

The congurence relation is an equivalence relation

Proof (i) Reflexive:

since $m \mid a-a$ we have $a \equiv a \pmod m$

(ii) Symmetric:

Let $a, b \in Z$ $\ni a \equiv b \pmod m$

$\Rightarrow m \mid a-b$

$\Rightarrow m \mid -(a-b)$

$\Rightarrow m \mid b-a$

$\Rightarrow b \equiv a \pmod m$

(iii) Transitive:

Let $a, b, c \in Z$ $\ni a \equiv b \pmod m$ and $b \equiv c \pmod m$

$\Rightarrow m \mid a-b$ and $m \mid b-c$

$\Rightarrow m \mid a-b+b-c$

$\Rightarrow m \mid a-c$

$\Rightarrow a \equiv c \pmod m$

Note 1:

1. Let $a \equiv b \pmod{m}$ and c be any integer then

(i) $a \pm c \equiv b \pm c \pmod{m}$

(ii) $a \cdot c \equiv b \cdot c \pmod{m}$

(iii) $a \equiv b \left(\mod \left(\frac{m}{\gcd(c,m)}\right)\right)$

(i) $a \pm c \equiv b \pm c \pmod{m}$

$a \equiv b \pmod{m}$

$\Rightarrow m \mid a-b$

$\Rightarrow m \mid a+c-b-c$

$\Rightarrow m \mid a+c-(b+c)$

$\Rightarrow a \pm c \equiv (b+c) \pmod{m}$

(ii) $a \cdot c \equiv b \cdot c \pmod{m}$

$a \equiv b \pmod{m}$

$\Rightarrow m \mid a-b$

$\Rightarrow m \mid c(a-b)$

$\Rightarrow m \mid ac-abc$

$\Rightarrow ac \equiv abc \pmod{m}$

(iii) $a \equiv b \left(\mod \left(\frac{m}{\gcd(c,m)}\right)\right)$

Note 2:

If $a, b, c, d \in z$ and m is a positive integer such that $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then

(i) $a+c \equiv b+d \pmod{m}$

(ii) $ac \equiv bd \pmod{m}$

(iii) $ax \equiv bx \pmod{m}$ for any x

** Fermets theorem:

If p is prime and a is integer such that $a \nmid p$ then $a^{p-1} \equiv 1 \pmod{p}$ (or) for every integer a,

$a^{p} \equiv a \pmod{p}$

Problems on Fermetts theorem:

1. Using Fermetts theorem prove that

i) 4^{13332} is congurent to $16 \pmod{13,331}$

ii) also show that fermetts theorem is true for a composite integer

sol i) Here $p = 13331$ and $a = 4 \nmid 13331$

$\therefore$ By Fermat's theorem

$a^{p-1} \equiv 1 \pmod{p}$

$4^{13331-1} \equiv 1 \pmod{13331}$

$4^{13330} \equiv 1 \pmod{13331}$

multiply 4^2 on b.s

$4^{13330} \cdot 4^2 \equiv 4^2 \cdot 1 \pmod{13331}$

$4^{13332} \equiv 16 \pmod{13331}$

ii) $p = 341$ a composite number

$= 11 \times 31$ and $2 \nmid 341$

Now $p = 31$ and $a = 2 \nmid 31$

$\therefore$ ~~By fermetts theorem~~

~~$a^{p-1} \equiv 1 \pmod{p}$~~

~~$2^{31-1} \equiv 1 \pmod{31}$~~

~~$2^{30} \equiv 1 \pmod{}$~~

$2^5 \equiv 1 \pmod{31}$

$(2^5)^{68} \equiv 1^{68} \pmod{31}$

$2^{340} \equiv 1 \pmod{31}$ —(1)

Take $p = 11$ and $a = 2 \nmid 11$

$2^{11-1} \equiv 1 \pmod{11}$

$2^{10} \equiv 1 \pmod{11}$

$(2^{10})^{34} \equiv 1^{34} \pmod{11}$

$2^{340} = 1 \pmod{11}$ — ②

From ① and ②

$2^{340} = 1 \times 1 \pmod{(31 \times 11)}$

$2^{340} = 1 \pmod{341}$

2. prove that $\log_3 7$ is irrational

Sol

If possible let $\log_3 7 = \frac{u}{v}$

$\Rightarrow 3^{u/v} = 7$

$\Rightarrow (3^{u/v})^v = 7^v$

$\Rightarrow 3^u = 7^v$

$\Rightarrow 3^u = 7^v = m$ (say)

which is a contradiction because, an integer $m > 1$ is expressed as product of prime numbers into two ways which contradicts FTA

Therefore, our assumption is wrong

Hence, $\log_3 7$ is an irrational number.

3. prove that $\sqrt{11}$ is irrational

Sol

If possible let $\sqrt{11} = \frac{u}{v}$ where u and v are relative primes to each other

$\Rightarrow 11 = \left(\frac{u}{v}\right)^2$

$\Rightarrow 11 = \frac{u^2}{v^2}$

$\Rightarrow u^2 = 11 v^2$ — ①

$\Rightarrow 11 | u^2$

$\Rightarrow 11 | u$

$\Rightarrow u = 11k$, where $k \in Z$

from ①

$(11k)^2 = 11v^2$

$\Rightarrow 11^2k^2 = 11 \cdot v^2$

$\Rightarrow 11k^2 = v^2$

$\Rightarrow 11 | v^2$

$\Rightarrow 11 | v$ $\quad \therefore$ u and v has common factor 11

11 divides u and v. which is contradiction

$\therefore$ Our assumption is wrong.

Hence $\sqrt{11}$ is an irrational number.

UNIT-6

Recurrence Relations:

Recurrence Relation:

If you can express an n^{th} term "a_n" in terms of some or all of its previous terms. we say this relation as recurrence relation.

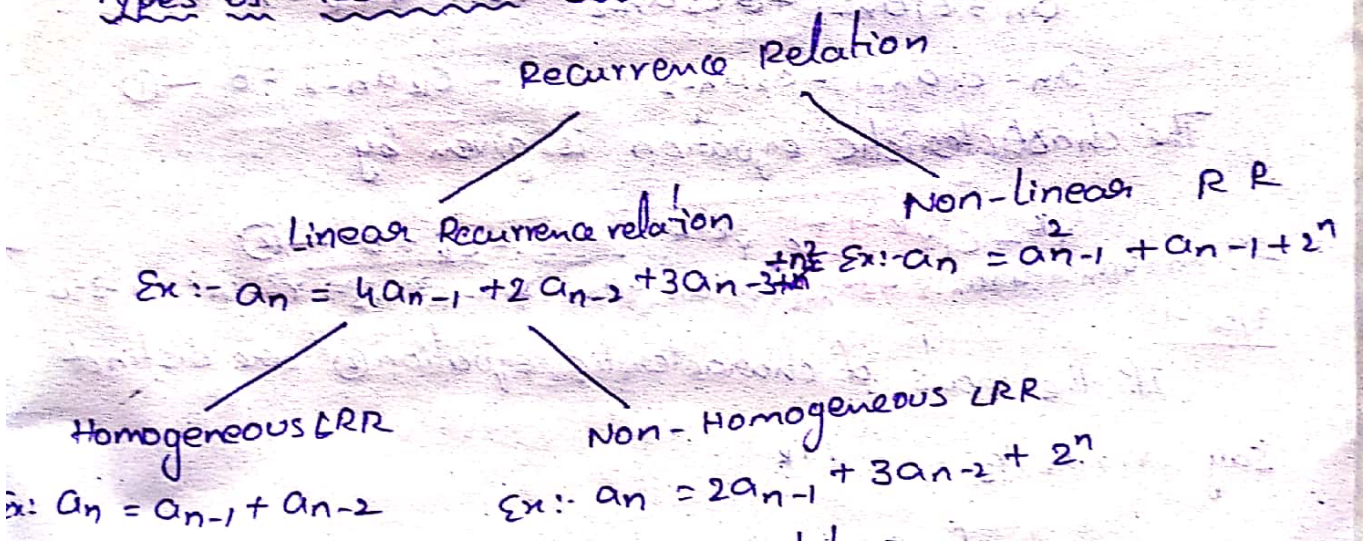
More precisely $a_n = c_1 a_1 + c_2 a_2^2 + \cdots + c_{n-1} a_{n-1} + f(n)$

Example $a_n = 2a_{n-1} - a_{n-2}$, $\forall\, n \geq 2 = n_0 \rightarrow$ Recurrence Relation

$a_0 = 0,\ a_1 = 3 \longrightarrow$ Initial conditions.

$a_n = 3n \rightarrow$ solution

Types of recurrence relation:



Linear Homogenous Recurrence Relation:

A linear homogeneous recurrence relation of degree 'k' with constant coefficients is a recurrence relation of the form $a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k};\ n \geq k$

and $c_k \neq 0$

This recurrence relation includes 'k' initial conditions.

Example

Determine the type of following recurrence relations.

i. $P_n = (1.11) P_{n-1} \rightarrow$ Linear homogeneous recurrence relation of degree '1'.

2. $a_n = a_{n-1} + a_{n-2}^2$ → Non linear Homogeneous of degree 2

3. $f_n = f_{n-1} + f_{n-2}$ → Linear homogeneous RR of degree 2

4. $H_n = 2 \cdot H_{n-1} + 1$ → linear nonhomogeneous Recurrence Relation.

5. $a_n = n a_{n-2}$ → linear Homogeneous RR with non constant coefficient.

Solving linear homogeneous Recurrence Relation:

Given recurrence relation

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k}$$

$$a_n - c_1 a_{n-1} - c_2 a_{n-2} - \cdots - c_k a_{n-k} = 0 \quad \text{—(1)}$$

The characteristic equation is given by

$$r^k - c_1 r^{k-1} - c_2 r^{k-2} - \cdots - c_k = 0 \quad \text{—(2)}$$

Ex: $a_n = 4a_{n-1} + 2a_{n-2} + 3a_{n-3} \Rightarrow a_n - 4a_{n-1} - 2a_{n-2} - 3a_{n-3} = 0 \Rightarrow r^3 - 4r^2 - 2r - 3 = 0$

Type-1

If the roots of characteristic equation (2) are distinct say $r_1, r_2, r_3 \cdots, r_k$

∴ The sol of (1) is given by

$$a_n = \alpha_1 r_1^n + \alpha_2 r_2^n + \cdots + \alpha_k r_k^n$$

Ex: If characteristic equation is $r^3 + r^2 - 4r - 4 = 0$

$$r = -1, -2, 2$$

$$a_n = \alpha_1 (-1)^n + \alpha_2 (-2)^n + \alpha_3 2^n$$

Problems for TYPE-1

1. solve the recurrance relation $a_n = 5a_{n-1} - 6a_{n-2}$, $\forall n \geq 2$

$a_0 = 1$, $a_1 = 0$

Sol Given recurrence relation is

$a_n = 5a_{n-1} - 6a_{n-2}$, $\forall n \geq 2$, $a_0 = 1, a_1 = 0$

$a_n - 5a_{n-1} + 6a_{n-2} = 0$ —— (1)

The characteristic eqn of (1) is given by

$r^2 - 5r + 6 = 0$ —(2)

$r^2 - 2r - 3r + 6 = 0$

$r(r-2) - 3(r-2) = 0$

$\Rightarrow r = 2, 3$

The sol is given by $a_n = \alpha_1 2^n + \alpha_2 3^n$ —(3)

$a_0 = 1 \Rightarrow a_0 = \alpha_1 2^0 + \alpha_2 3^0$

$1 = \alpha_1 + \alpha_2$ — (4)

$a_1 = 0 \Rightarrow a_1 = \alpha_1 2^1 + \alpha_2 3^1$

$0 = 2\alpha_1 + 3\alpha_2$ — (5)

$2 \times (4)$ $2\alpha_1 + 2\alpha_2 = 2$

$2\alpha_1 + 3\alpha_2 = 0$

$-\alpha_2 = 2$

$\alpha_2 = -2$

from (4) $\alpha_1 = 1 - \alpha_2$

$\alpha_1 = 1 - (-2)$

$\alpha_1 = 1 + 2 = 3$

The solution is given by $a_n = 3 \cdot 2^n - 2 \cdot 3^n$

2. Solve the R.R $a_n = 2a_{n-1} + a_{n-2} - 2a_{n-3}$, $a_0 = 3$, $a_1 = 6$, $a_2 = 0$

Sol Given R.R

$$a_n = 2a_{n-1} + a_{n-2} - 2a_{n-3}$$

$$a_n - 2a_{n-1} - a_{n-2} + 2a_{n-3} = 0 \quad -(1)$$

The characteristic eqn is

$$r^3 - 2r^2 - r + 2 = 0 \quad -(2)$$

put $r = 1$ in (2)

$$1 - 2 - 1 + 2 = 0$$

$$0 = 0$$

Therefore one root is $r = 1$

	1	-2	-1	2
1		1	-1	-2
	1	-1	-2	0

For other two roots $r^2 - r - 2 = 0$

$$r^2 + r - 2r - 2 = 0$$

$$r(r+1) - 2(r+1) = 0$$

$$r = 2, -1$$

The roots are $1, -1, 2$

The solution is given by $a_n = \alpha_1 (1)^n + \alpha_2 (-1)^n + \alpha_3 (2)^n$ —(3)

$a_0 = 3 \Rightarrow a_0 = \alpha_1 (1)^0 + \alpha_2 (-1)^0 + \alpha_3 (2)^0$

$$3 = \alpha_1 + \alpha_2 + \alpha_3 \quad -(4)$$

$a_1 = 6 \Rightarrow a_1 = \alpha_1 (1)^1 + \alpha_2 (-1)^1 + \alpha_3 (2)^1$

$$6 = \alpha_1 - \alpha_2 + 2\alpha_3 \quad -(5)$$

$a_2 = 0 \Rightarrow a_2 = \alpha_1 (1)^2 + \alpha_2 (-1)^2 + \alpha_3 (2)^2$

$$0 = \alpha_1 + \alpha_2 + 4\alpha_3 \quad -(6)$$

From (4) and (5)

$$\alpha_1 - \alpha_2 + 2\alpha_3 = 6$$
$$\alpha_1 + \alpha_2 + \alpha_3 = 3$$

$$2\alpha_1 + 3\alpha_3 = 9 \quad \text{— (7)}$$

From (5) and (6)

$$\alpha_1 - \alpha_2 + 2\alpha_3 = 6$$
$$\alpha_1 + \alpha_2 + 4\alpha_3 = 0$$

$$2\alpha_1 + 6\alpha_3 = 6 \quad \text{— (8)}$$

From (7) and (8)

$$2\alpha_1 + 3\alpha_3 = 9$$
$$2\alpha_1 + 6\alpha_3 = 6$$

$$-3\alpha_3 = 3$$
$$\alpha_3 = -1$$

from (7) $2\alpha_1 + 3\alpha_3 = 9 \Rightarrow 2\alpha_1 + 3(-1) = 9$

$$2\alpha_1 = 12$$
$$\alpha_1 = 6$$

from (5)

$$\alpha_1 - \alpha_2 + 2\alpha_3 = 6$$
$$6 - \alpha_2 + 2(-1) = 6$$
$$\alpha_2 = 6 - 6 - 2$$
$$\alpha_2 = -2$$

The solution is given by $a_n = 6 \cdot (1)^n - 2(-1)^n + 1(2)^n$

3. Find an explicit formula for the fibonacci series

Sol The recurrance relation for fibonacci sequence $\{F_n\}$ $\langle F_n \rangle$ is given by $F_n = F_{n-1} + F_{n-2}$, $\forall n \geq 2$,

$F_0 = 0$, $F_1 = 1$

$$F_n - F_{n-1} - F_{n-2} = 0 \quad \text{— (1)}$$

characteristic equation

$$r^2 - r - 1 = 0$$

$$r = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} = \frac{-(-1) \pm \sqrt{1 - 4(1)(-1)}}{2(1)} = \frac{1 \pm \sqrt{5}}{2}$$

$r = \frac{1+\sqrt{5}}{2}, \frac{1-\sqrt{5}}{2}$

The solution is given by $F_n = \alpha_1\left(\frac{1+\sqrt{5}}{2}\right)^n + \alpha_2\left(\frac{1-\sqrt{5}}{2}\right)^n$

$F_0 = 0 \Rightarrow F_0 = \alpha_1\left(\frac{1+\sqrt{5}}{2}\right)^0 + \alpha_2\left(\frac{1-\sqrt{5}}{2}\right)^0$

$0 = \alpha_1 + \alpha_2 \quad -(2)$

$F_1 = 1 \Rightarrow F_1 = \alpha_1\left(\frac{1+\sqrt{5}}{2}\right)^1 + \alpha_2\left(\frac{1-\sqrt{5}}{2}\right)^1$

from $1 = \alpha_1\left(\frac{1+\sqrt{5}}{2}\right) + \alpha_2\left(\frac{1-\sqrt{5}}{2}\right) \quad -(3)$

$\frac{2}{1+\sqrt{5}}\,1 = \alpha_1\left(\frac{1+\sqrt{5}}{2}\right) + \alpha_2\left(\frac{1-\sqrt{5}}{2}\right)$

$(2) \times \frac{1+\sqrt{5}}{2} \quad 0 = \alpha_1\left(\frac{1+\sqrt{5}}{2}\right) + \alpha_2\left(\frac{1+\sqrt{5}}{2}\right)$

$1 = \alpha_2\left(\frac{1-\sqrt{5}}{2} - \frac{1+\sqrt{5}}{2}\right)$

$1 = \alpha_2\left(\frac{1-\sqrt{5}-1-\sqrt{5}}{2}\right)$

$\alpha_2 = \frac{2\sqrt{5}}{2} = -1/\sqrt{5}$

from (2) $\alpha_1 + \alpha_2 = 0$

$\alpha_1 + \sqrt{5} = 0$

$\alpha_1 = +1/\sqrt{5}$

The solution is given $F_n = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n$

4. Solve the recurrance relation $a_n = 2a_{n-1} - 2a_{n-2}$, $a_0 = 1$, $a_1 = 2$

Sol $a_n = 2a_{n-1} - 2a_{n-2}$

$a_n - 2a_{n-1} + 2a_{n-2} = 0$

characteristic equation is

$r^2 - 2r + 2 = 0$

$r = \frac{2 \pm \sqrt{4-8}}{2(1)}$

$r = \frac{2 \pm 2i}{2} = 1 \pm i$

The solution is given by $a_n = \alpha_1(1+i)^n + \alpha_2(1-i)^n$

$a_0 = 1 \Rightarrow a_0 = \alpha_1(1+i)^0 + \alpha_2(1-i)^0$

$1 = \alpha_1 + \alpha_2 \quad -(1)$

$a_1 = 2 \Rightarrow a_1 = \alpha_1(1+i)^1 + \alpha_2(1-i)^1$

$2 = \alpha_1(1+i) + \alpha_2(1-i) \quad -(2)$

$(1) \times (1+i) \quad (1+i) = \alpha_1(1+i) + \alpha_2(1+i)$

$-(2) \quad 2 = \alpha_1(1+i) + \alpha_2(1-i)$

$i-1 = \alpha_2(1+i-1+i)$

$i-1 = \alpha_2(2i)$

$\alpha_2 = \frac{i-1}{2i}$

$\alpha_2 = \frac{(i-1)(-2i)}{(2i)(-2i)}$

$\alpha_2 = \frac{2(1)+2i}{-4i^2} = \frac{2+2i}{4} = \frac{1+i}{2}$

from (1)

$1 = \alpha_1 + \alpha_2$

$1 = \alpha_1 + \frac{1+i}{2}$

$\alpha_1 = 1 - \frac{1+i}{2}$

$\alpha_1 = \frac{2-1-i}{2}$

$\alpha_1 = \frac{1-i}{2}$

Solution is given by $a_n = \left(\frac{1-i}{2}\right)(1+i)^n + \left(\frac{1+i}{2}\right)(1-i)^n$

Type-2

If the characteristic equation of recurrence relation is having repeated roots say $r = r_1, r_1$ then the solution is given by $a_n = (C_1 + C_2 n) r_1^n$ ← 2 times

$a_n = (C_1 + C_2 n + C_3 n^2) r_2^n$ ← 3 times

Problems

1. solve the RR $a_n = 8a_{n-1} - 16a_{n-2}$ for $n \geq 2$, $a_0 = 16$, $a_1 = 80$

Sol

Given RR $a_n = 8a_{n-1} - 16a_{n-2}$

$$a_n - 8a_{n-1} + 16a_{n-2} = 0 \quad \text{— (1)}$$

The characteristic eqn is given by

$$r^2 - 8r + 16 = 0$$

$$(r-4)^2 = 0$$

$$r = 4, 4$$

The solution is given by $a_n = (C_1 + C_2 n)(4)^n$ — (2)

$a_0 = 16 \Rightarrow a_0 = (C_1 + C_2(0)) 4^0$

$16 = C_1 (1)$

$C_1 = 16$

$a_1 = 80 \Rightarrow a_1 = (C_1 + C_2(1)) 4^1$

$80 = (C_1 + C_2) 4$

$C_1 + C_2 = 20$

$16 + C_2 = 20$

$C_2 = 4$

The solution is $a_n = (16 + 4n) 4^n$

2. solve the RR ① $a_n - 2a_{n-1} + a_{n-2} = 0$ with $a_0 = 25, a_1 = 16$

② $a_n = 4a_{n-1} - 4a_{n-2}$ with $a_0 = 1, a_1 = 2$

① $a_n - 2a_{n-1} + a_{n-2} = 0$

characteristic eqn is

$r^2 - 2r + 1 = 0$

$(r-1)^2 = 0$

$r = 1, 1$

The solution is given by $a_n = (c_1 + c_2)(1)^n$ — ②

$a_0 = 25$ $\quad a_0 = (c_1 + c_2(0))(1)^0$

$\boxed{25 = c_1}$

$a_1 = 16$ $\quad a_1 = (c_1 + c_2)(1)^1$

$16 = c_1 + c_2$

$16 = c_2 + 25$

$\boxed{c_2 = -9}$

$a_n = (25 - 9n)(1)^n$

②

$a_n = 4a_{n-1} - 4a_{n-2}$

$a_n - 4a_{n-1} + 4a_{n-2} = 0$

characteristic eqn is

$r^2 - 4r + 4 = 0$

$(r-2)^2 = 0$

$r = 2, 2$

The solution is given by $a_n = (c_1 + c_2 n)(2)^n$

$a_0 = 1 \Rightarrow a_0 = (c_1 + c_2(0))\, 2^0$

$\boxed{1 = c_1}$

$a_1 = 2 \Rightarrow a_1 = (c_1 + c_2)\, 2^1$

$2 = (1 + c_2)2$

~~$2 = 2 + 2c_2$~~

$\Rightarrow 1 = 1 + c_2$

$\boxed{c_2 = 0}$

The solution is given by $a_n = (1 + 0 \cdot n)\, 2^n$

$a_n = 2^n$

3. Solve $a_n + a_{n-1} - a_{n-2} - a_{n-3} = 0$ $a_0 = 1, a_1 = 2, a_2 = 3$

Sol

$$a_n + a_{n-1} - a_{n-2} - a_{n-3} = 0$$

Chara eqn is

$$r^3 + r^2 - r - 1 = 0 \quad -(1)$$

put 1 in eq (1)

$$1 + 1 - 1 - 1 = 0$$

$$0 = 0$$

$r = 1$

	1	1	−1	−1
	0	1	2	1
	1	2	1	0

$$r^2 + 2r + 1 = 0$$

$$(r+1)^2 = 0$$

$$r = -1, -1, 1$$

~~Characteristic eqn~~

solution is given by $a_n = (C_1 + C_2)(-1)^n + C_3(1)^n$

$a_0 = 1 \Rightarrow$ $a_0 = (C_1 + 0)(-1)^0 + C_3(1)^0$

$$1 = C_1 + C_3 \quad -(2)$$

$a_1 = 2 \Rightarrow$ $a_1 = (C_1 + C_2)(-1)^1 + C_3(1)^1$

$$2 = -C_1 - C_2 + C_3 \quad -(3)$$

$a_2 = 3 \Rightarrow$ $a_2 = (C_1 + 2C_2)(-1)^2 + C_3(1)^2$

$$3 = C_1 + 2C_2 + C_3 \quad -(4)$$

from (3) and (4)

$(3) \times 2$ $\quad 4 = -2C_1 - 2C_2 + 2C_3$

$+ 4$ $\quad 3 = C_1 + 2C_2 + C_3$

$$7 = -C_1 + 3C_3 \quad -(5)$$

from (2) and (5)

$$7 = -C_1 + 3C_3$$

$$1 = C_1 + C_3$$

$$8 = 4C_3$$

$C_3 = \frac{8}{5}$ 2

from ② $1 = C_1 + C_3$

$C_1 = 1 - \frac{8}{5} = \frac{-3}{5}$ $1 - 2 = -1$

from ③ $2 = -C_1 - C_2 + C_3$

$C_2 = -C_1 + C_3 - 2$ $C_2 = 1 + 2 - 2$

$C_2 = \frac{3}{5} + \frac{8}{5} - 2$ $C_2 = 1$

$C_2 = 1/5$ $(-1+n)(-1)^n + 2(1)^n$

solution is given by $a_n = \left(\frac{-3}{5} + \frac{1}{5}n\right)(-1)^n + \frac{8}{5}(1)^n$

Non - Homogeneous Linear Recurrance relations:

① solve $a_n = 3a_{n-1} + 2^n$ ① , $a_0 = 1$

i consider homogeneous equation for given recurrance relation

$a_n = 3a_{n-1}$

$a_n - 3a_{n-1} = 0$

charcteristic eqn

$r - 3 = 0$

$r = 3$

solution is given by $a_n^{(h)} = \alpha_1 (3)^n$

ii Here $F(n) = 2^n = s^n$

and the characteric eqn root is $r = 3 \neq s$

$a_n(P) = d\,2^n$

put in ①

$d2^n = 3d2^{n-1} + 2^n$

$d2^n - 3d2^{n-1} = 2^n$

$d2^n(1 - \frac{3}{2}) = 2^n$

$d(-1/2) = 1$

$d = -2$

$a_n(P) = -2 \cdot 2^n$

$a_n(P) = -2^{n+1}$

∴ The solution of given equation is

$$a_n = a_n(h) + a_n(p)$$

$$a_n = \alpha_1 3^n - 2^{n+1}$$

$a_0 = 1 \Rightarrow a_0 = \alpha_1 3^0 - 2^1$

$1 = \alpha_1 - 2$

$\alpha_1 = 3$

The solution is $a_n = 3 \cdot 3^n - 2^{n+1} = 3^{n+1} - 2^{n+1}$

2. Solve $a_n = 2a_{n-1} + 2^n$, $a_0 = 2$

Sol

Consider homogeneous equation for the given RR

$$a_n - 2a_{n-1} = 0$$

characteristic equation is

$$r - 2 = 0$$

$$r = 2$$

Solution is given by $a_n^{(h)} = \alpha_1 (2)^n$

Here $F(n) = 2^n = s^n$

and the root of ch. equation is $r = 2 = s$

$$a_n(p) = dn\,2^n$$

put in (1)

$$dn2^n = 2d(n-1)2^{n-1} + 2^n$$

$$d2^n\left(n + \frac{(n+1)n}{2}\right) = 2^n$$

$$d(n - n + 1) = 1$$

$$d\{1\} = 1$$

$$a_n(p) = (1)n\,2^n$$

The solution of given equation is

$$a_n = a_n(h) + a_n(p)$$

$$a_n = \alpha_1 2^n + n2^n$$

$a_0 = 2 \Rightarrow a_0 = \alpha_1 2^0 + 0 2^0$

$2 \neq 0$

$r_1 = 2$

The solution is $a_n = 2 \cdot 2^n + n2^n$

$2^{n+1} + n2^n \Rightarrow 2^n(n+2)$

Solve $a_n = 2a_{n-1} + c(n-2) = 2$ ① $a_{10} = 25$, $a_1 = 16$

Consider homogeneous equation for given RR

$a_n - 2a_{n-1} + a_{n-2} = 0$

characteristic equation is

$r^2 - 2r + 1 = 0$

$(r-1)^2 = 0$

$r = 1, 1$

solution is given by $a_n = (C_1 + C_2 n)(1)^n$

Here $F(n) = 2$ = constant.

and the root of ch. equation is $r = 1 = s$

$a_n(P) = d$

put in ①

$d - 2d + d = 2$

$0 = 2$

which is impossible.

Assume $a_n(P) = nd$

put in ①

$nd - 2((n-1)d) + (n-2)d = 2$

$d(n - 2n + 2 + n - 2) = 2$

$d(0) = 2$

$0 = 2$

which is also impossible.

Assume $a_n(P) = n^2 d$

put in ① $n^2 d - 2((n-1)^2 d + (n-2)^2 d = 2$

$(n^2 - 2n^2 - 2 + 4n + n^2 + 4 - 4n)d = 2$

$2d = 2$

$d = 1$

$a_n(P) = n^2(1)$

$a_n = a_n(h) + a_n(P) \Rightarrow (c_1 + c_2 n)(1)^n + n^2(1)$

$a_0 = 25 \rightarrow 25 = c_1 + 0^2 \Rightarrow c_1 = 25$

$a_1 = 16 \Rightarrow 16 = c_1 + c_2 + 1 \Rightarrow 16 = 25 + c_2 + 1 \Rightarrow c_2 = -10$

$a_n = (25 - 10n)(1)^n + n^2(1)$

4. Solve $a_k - 7a_{k-1} + 10a_{k-2} = 6 + 8k$; $a_0 = 1, a_1 = 2$

Sol consider the homogeneous equation for given RR.

$a_k - 7a_{k-1} + 10a_{k-2} = 0$

characteristic eqn is

$r^2 - 7r + 10 = 0$

$r^2 - 5r - 2r + 10 = 0$

$r(r-2) - 5(r-2) = 0$

$r = 5, 2$

The solution is given by $a_n = d_1(5)^n + d_2(2)^n$

Here $F(n) = 6 + 8k$

$a_n(P) = d_0 + d_1 k$

put in (1)

$d_0 + d_1 k - 7(d_0 + d_1(k-1)) + 10(d_0 + d_1(k-2)) = 6 + 8k$

$d_0(1 - 7 + 10) + d_1(k - 7k + 7 + 10k - 20) = 6 + 8k$

$4d_0 + d_1(4k - 13) = 6 + 8k$

$4d_0 + 4kd_1 - 13d_1 = 6 + 8k$

$4kd_1 + 4d_0 - 13d_1 = 6 + 8k$

$4d_0 - 13d_1 = 6$ ~~$+ 8k$~~ $\quad 4kd_1 = 8k \Rightarrow d_1 = 2$

~~$d_1 = 0$~~

$4d_0 - 13(2) = 6$ ~~$+ 8k$~~

$4d_0 - 26 = 6$

$4d_0 = 32$

$d_0 = 8$

$a_n(P) = 8 + 2k$

$a_k = a_n(h) + a_n(P)$

$a_k = d_1 5^k + d_2 2^k + 8 + 2k$

$a_0 = 1 \Rightarrow a_0 = \alpha_1 + \alpha_2 + 8 + 2 = 1 \rightarrow$

$a_1 = 2 \Rightarrow a_1 = 5\alpha_1 + 2\alpha_2 + 8 + 2 = 2 \rightarrow 5\alpha_1 + 2\alpha_2 = -8$

from the above equation

$2\alpha_1 + 2\alpha_2 = -14$

$5\alpha_1 + 2\alpha_2 = -8$

$-3\alpha_1 = -6$

$\alpha_1 = 2 \Rightarrow 2 + \alpha_2 = -7 \Rightarrow \alpha_2 = -9$

$a_k = 2(5^k) + (-9)(2)^k + 8 + 2k$

solve $a_n = 4a_{n-1} - 4a_{n-2} + (n+1)2^n$; $a_0 = 1, a_1 = 2$ ①

consider the homogeneous equation for given RR.

$a_n - 4a_{n-1} + 4a_{n-2} = 0$

characteristic eqn is given by

$r^2 - 4r + 4 = 0$

$(r-2)^2 = 0$

$r = 2, 2$

The solution is given by $a_n = (\alpha_1 + \alpha_2 n)(2)^n$

Here $f(n) = (n+1)2^n = s^n$

and the characteristic root $r = 2 \Rightarrow r = s$

let $a_n(p) = (d_0 + d_1 n)\, n^2 2^n$

from ①

$(d_0 + d_1 n)\, n^2 2^n - 4(d_0 + d_1(n-1))(n-1)^2 2^{n-1} + 4(d_0 + d_1(n-2))(n-2)^2 \cdot 2^{n-2} = (n+1)2^n$

Put $n = 0$

$-4(d_0 + d_1(-1))(-1)^2 2^{-1} + 4(d_0 + d_1(-2))(-2)^2 \cdot 2^{-2} = 2^0$

$-2d_0 + 2d_1 + 4d_0 - 8d_1 = 1$

$2d_0 - 6d_1 = 1$ — ②

$(d_0 + d_1 n)\, n^2 2^n - 4(d_0 + nd_1 - d_1)(n^2 + 1 - 2n)\, 2^{n-1} + 4(d_0 + nd_1 - 2d_1)(n^2 + 4 - 4n)2^{n-2} = (n+1)2^n$

Comparing $n \cdot 2^n$ on b.s

$\frac{-4d_0(-2) - 4d_1 + 4d_1(-2)}{2} + \frac{4d_0(-4) + 4d_1(4) - 8d_1(-4)}{4} = 1$

$+4d_0 - 4d_1 - 8d_1 - 4d_0 + 4d_1 + 8d_1 = 1$

$8d_1 = 1$

$d_1 = 1/8$

$2d_0 - 6\left(\frac{1}{8}\right) = 1 \Rightarrow 2d_0 - \frac{3}{4} = 1 \Rightarrow 2d_0 = \frac{7}{4} \Rightarrow d_0 = \frac{7}{8}$

$a_n = a_n(h) + a_n(p) \Rightarrow a_n = (\alpha_1 + \alpha_2 n)2^n + (1 + \frac{1}{6}\alpha_3 n)n^0 2^n$

$a_0 = 1 \Rightarrow 1 = (\alpha_1 + 0)1 + (1+0)0 \Rightarrow \alpha_1 = 1$

$a_1 = 2 \Rightarrow 2 = (\alpha_1 + \alpha_2)2 + (1+\frac{1}{6})2 \Rightarrow 2 = (1+\alpha_2)2 + \frac{7}{3} \Rightarrow 1 + \alpha_2 = -\frac{7}{6}$

$1 = \alpha_1 + \alpha_2 + \frac{7}{6}$

$0 = \alpha_2 + \frac{7}{6} \Rightarrow \alpha_2 = -7/6$

$a_n = (1 - \frac{7}{6}n)2^n + (1 + \frac{n}{6})n^2 2^n$

6. Solve $a_n = 4a_{n-1} - 4a_{n-2} + 3n + 2^n$, $a_0 = 1, a_1 = 1$

Sol Consider the homogeneous eqn for given RR

$a_n - 4a_{n-1} + 4a_{n-2} = 0$

characteristic equation is given by

$r^2 - 4r + 4 = 0$

$(r-2)^2 = 0$

$r = 2, 2$

The solution is given by $a_n = (C_1 + C_2 n)(2)^n$

Here $F(n) = 3n + 2^n$

$a_n(p) = d_0 + d_1 n + n^2 2^n$

from (1)

$d_0 + d_1 n + n^2 2^n - 4(d_0 + d_1(n-1) + (n-1)^2 2^{n-1}) + 4(d_0 + d_1(n-2) + (n-2)^2 2^{n-2}) = 3n + 2^n$

Put $n = 0$

$d_0 = 4(d_0 + d_1(-1) + 2C) + 4(d_0 + d_1(-2) + 4C) = 0$

$-3d_0 + 4d_1 - 2 + 4d_0 - 8d_1 + 4 = 0$

$d_0 - 4d_1 = -2 \quad \text{---} (2) \Rightarrow d_0 - 4d_1 + 2C = 0$

$d_1 - 4d_1 + 4d_1 = 3$

$d_1 = 3$

$d_0 - 4(3) = -1$

$d_0 = -1 + 12$

$d_0 = 12$

$d_0 + 2C = 12$

$Cn^2 + (n-1)$

$a_n = a_n(h) + a_n(p) = (C_1 + C_2 n)2^n + 12 + 3n + n^2 2^n$

$a_0 = 1 \Rightarrow 1 = (C_1 + 0)1 + 12 + 0$

$C_1 = -11$

$a_1 = 1 \Rightarrow 1 = (C_1 + C_2)2 + 12 + 2 + 2$

$1 = 2C_1 + 2C_2 + 17$

$-16 = 2(C_1 + C_2)$

$-8 = C_1 + C_2$

$-8 = -11 + C_2$

$C_2 = 3$

$a_n = (-11+3n)1^n + 12+3n+n^2 2^n$

particular solution for given F(n):

F(n)	Form of particular solution
i. A constant, c	i. A constant d
ii. A linear function c_0+c_1n	ii. A linear function d_0+d_1k
N	d_0+d_1K
iii. n^2	iii. $d_0+d_1k+d_2k^2$
iv. An mth degree polynomial $c_0+c_1n+c_2n^2+\dots+c_mn^m$	iv. An mth degree polynomial $d_0+d_1k+d_2k^2+\dots+d_mk^m$
v. $r^n, r\in R$	v. dr^n

Q solve the recurrance relation $a_k = 2a_{k-1}+k+10$

Sol Given RR $a_k = 2a_{k-1}+k+10$

Consider The homogeneous equation $a_k - 2a_{k-1} = 0$

The characteristic equation is

$r-2=0$

$r=2$

$a_n(h) = c_1 2^n$

here $F(n) = k+10$

$a_n(p) = d_0 + d_1k$

from ①

$d_0+d_1k - 2(d_0+d_1(k-1)) = k+10$

$d_0+d_1k-2d_0-2d_1(k-1) = k+10$

$d_0-2d_0+2d_1+10$ $\qquad d_1-2d_1=1$

$-d_0-2d_1+d_0 = 10$ $\qquad -d_1=1$

$-d_0+2(-1)+10 = 10$ $\qquad d_1=-1$

$-d_0+8=10$

$d_0 = -8+2$

$a_n = a_n(h) + a_n(p)$

$a_n = c_1 2^n + -12 + -1k$

$a_n = c_1 2^n - 12 - k$

8. solve $a_n = 4a_{n-1} - 3a_{n-2} + 2^n + n + 3$ $a_0 = 1, a_1 = 4$

Sol Given RR $a_n = 4a_{n-1} - 3a_{n-2} + 2^n + n + 3$ — (1)

Consider the homogeneous equation

$a_n - 4a_{n-1} + 3a_{n-2} = 0$

characteristic equation :

$r^2 - 4r + 3 = 0$

$r - 3r - r + 3 = 0$

$r(r-3) - 1(r-3) = 0$

$r = 1, 3$

$a_n(h) = c_1(1)^n + c_2 3^n$

ii) Here $F(n) = 2^n + (n+3)$

$a_n(p) = c 2^n$

Generation function:

A generating function can be used to solve many counting problems. Further a generating function is a powerful tool that can be used to solve a recurrance relation. The generating function of the sequence $a_0, a_1, \ldots a_n$ of real numbers is written as the series given below

$$G(z) = \sum_{n=0}^{\infty} a_n z^n = a_0 + a_1 z + \cdots + a_n z^n + \cdots$$

Example

The generating function of the sequence $1, 2, 3, 4, \ldots$ is $G(z) = 1 + 2z + 3z^2 + 4z^3 + \cdots + (n+1)z^n$

$$= \frac{1}{(1-z)^2} = (1-z)^{-2}$$

Solving Recurrance Relation using generating function:

1. Use the method of generating function to solve the recurrance relation $a_n = 4a_{n-1} - 4a_{n-2} + 4^n$, $\forall n \geq 2$ Given that $a_0 = 2$, $a_1 = 8$

Sol $a_n = 4a_{n-1} - 4a_{n-2} + 4^n$

$$a_n z^n = 4a_{n-1} z^n - 4a_{n-2} z^n + (4z)^n$$

$$a_n z^n = 4z a_{n-1} z^{n-1} - 4z^2 a_{n-2} z^{n-2} + (4z)^n$$

Taking Σ on b.s

$$\sum_{n=2}^{\infty} a_n z^n = 4z \sum_{n=2}^{\infty} a_{n-1} z^{n-1} - 4z^2 \sum_{n=2}^{\infty} a_{n-2} z^{n-2} + \sum_{n=2}^{\infty} (4z)^n$$

$$[G(z) - a_0 - a_1 z] = 4z \sum_{n=1}^{\infty} a_n z^n - 4z^2 \sum_{n=0}^{\infty} a_n z^n + \left[\frac{1}{1-4z} - (1+4z)\right]$$

$$[G(z) - 2 - 8z] = 4z(G(z) - 2) - 4z^2(G(z)) + \frac{1}{1-4z} - (1+8z)$$

$$G(z)(1-4z+4z^2) = \frac{1}{1-4z} - (1+4z) + 2+8z-8z$$

$$G(z)(1-2z)^2 = \frac{1}{1-4z} - 1 - 4z + 2$$

$$G(z)(1-2z)^2 = \frac{1}{1-4z} + (1-4z)$$

$$G(z)(1-2z)^2 = \frac{1+(1-4z)^2}{1-4z}$$

$$G(z) = \frac{1+(1-4z)^2}{(1-4z)(1-2z)^2}$$

~~G(z)~~ - To split this, we use the partial fraction technique

$$\text{let } \frac{1+(1-4z)^2}{(1-4z)(1-2z)^2} = \frac{A}{1-4z} + \frac{B}{(1-2z)} + \frac{C}{(1-2z)^2}$$

Equating the numerators on b.s we get

$$1+(1-4z)^2 = A(1-2z)^2 + B(1-4z)(1-2z) + C(1-4z)$$

substituting $z = 1/2, z = 1/4$ and $z = 0$

we get $C = -2, A = 4$ and $B = 0$

$$\therefore G(z) = \frac{4}{1-4z} + 0 - \frac{2}{(1-2z)^2}$$

$$= 4(1-4z)^{-1} - 2(1-2z)^{-2}$$

$$= 4\sum_{n=0}^{\infty}(4z)^n - 2\sum_{n=0}^{\infty}(n+1)(2z)^n$$

$$= 4\sum_{n=0}^{\infty}4^n z^n - 2\sum_{n=0}^{\infty}2^n(n+1)z^n$$

$$= \sum_{n=0}^{\infty}\left(4^{n+1} - (n+1)2^{n+1}\right)z^n$$

$$a_n = 4^{n+1} - (n+1)2^{n+1}$$

$a_n = 2a_{n-1} + 2^n$, $a_0 = 2$

Sol

$a_n = 2a_{n-1} + 2^n$

$a_n z^n = 2a_{n-1} z^n + 2^n z^n$

$a_n z^n = 2z\, a_{n-1} z^{n-1} + (2z)^n$

Taking Σ on b's

$\sum_{n=1}^{\infty} a_n z^n = 2z \sum_{n=1}^{\infty} a_{n-1} z^{n-1} + \sum_{n=1}^{\infty} (2z)^n$

$G(z) - a_0 = 2z \sum_{n=0}^{\infty} a_n z^n + \frac{1}{1-2z} - 1$

$G(z) - 2 = 2z\, G(z) + \frac{1 - 1 + 2z}{1-2z}$

$G(z)(1-2z) = 2 + \frac{2z}{1-2z}$

$G(z)(1-2z) = \frac{2 - 4z + 2z}{1-2z}$

$= \frac{2 - 2z}{1-2z}$

$G(z) = \frac{2-2z}{(1-2z)^2}$

To split this, we use the partial fraction

let $\frac{2-2z}{(1-2z)^2} = \frac{A}{1-2z} + \frac{B}{(1-2z)^2}$

$2 - 2z = A(1-2z) + B$

put $z = \frac{1}{2}$

$2 - 1 = A(0) + B$

$B = 1$

Compare constants on b's

$2 = A + B$

$2 = A + 1$

$A = 1$

$\therefore G(z) = \frac{1}{1-2z} + \frac{1}{(1-2z)^2}$

$= (1-2z)^{-1} + (1-2z)^{-2}$

$= \sum_{n=0}^{\infty} (2z)^n + \sum_{n=0}^{\infty} (n+1)(2z)^n$

$= \sum_{n=0}^{\infty} \left(2^n + (n+1)2^n\right) z^n$

$= 2^n + (n+1)2^n$

$= 2^n + n2^n + 2^n$ $\quad 2^n(1+n+1) = 2^n(n+2)$

3. $a_n - 2a_{n-1} + a_{n-2} = 2$, $a_0 = 25$, $a_1 = 16$

Sol

$$a_n - 2a_{n-1} + a_{n-2} = 2$$

$$a_n z^n - 2a_{n-1} z^n + a_{n-2} z^n = 2z^n$$

$$a_n z^n - 2z\, a_{n-1} z^{n-1} + z^2 a_{n-2} z^{n-2} = 2z^n$$

Taking Σ on b/s

$$\sum_{n=0}^{\infty} a_n z^n - 2z \sum_{n=2}^{\infty} a_{n-1} z^{n-1} + z^2 \sum_{n=2}^{\infty} a_{n-2} z^{n-2} = \sum_{n=2}^{\infty} 2z^n$$

$$[G(z) - a_0 - a_1 z] - 2z[G(z) - a_0] + z^2[G(z)] = 2\left[\frac{1}{1-z} - 1 - z\right]$$

$$G(z)(1 - 2z + z^2) = 2\left[\frac{1 - 1 + z^2}{1-z}\right] + 25 + 16z - 2z(25)$$

$$G(z)(1-z)^2 = \frac{2z^2}{1-z} - 34z + 25$$

$$= \frac{2z^2 - 34z + 34z^2 + 25 - 25z}{1-z}$$

$$= 36z^2$$

UNIT-4

Graph theory

Basic concepts of graph:

Graph:

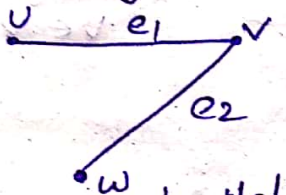
A graph g consists of a pair (V, E) where V is a non-empty finite set whose elements are called vertices (or) nodes and E is another set whose elements are called edges.

An edge $e \in E$ is associated with unordered (say $\{a, b\}$) or ordered (say (a, b)) of elements of V

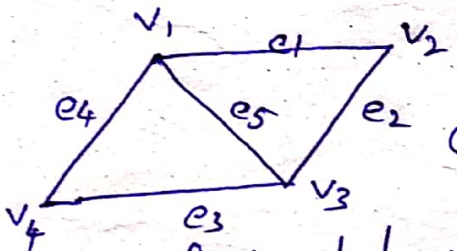
Note:

1. Any two vertices connected by an edge e in a graph are called adjacent vertices Ex: u —e— v
   - Otherwise the vertices are called as isolated
   Example w .
2. If two distinct edges e_1, e_2 are incident with a common vertex then they are called as incidence edges

Ex:

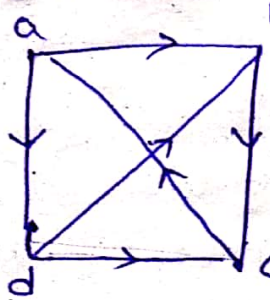


Example of undirected simple graph:



$G_1(V, E)$

Example of directed graph:



$G_2(V, E)$

Degree of a vertex in a graph G:

Let $v \in V$ be a vertex in a graph $G(V, E)$ then the degree of v is $\deg(v)$ = no. of edges incident with vertex v

Example

In $G1(V, E)$ $\deg(v_1) = 3$, $\deg(v_2) = 2$, $\deg(v_3) = 3$

$\deg(v_4) = 2$

Hand shaking theorm:

Let $G(V, E)$ be an undirected graph then $\sum_{v \in V} \deg(v) = 2 \times |E|$

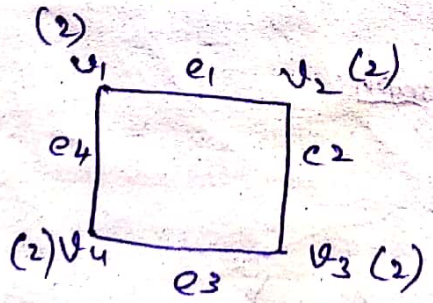
Proof:

Let $G(V, E)$ be an undirected graph.

since, every edge $e \in E$ in G, contributes 2 to the sum of degrees of all vertices in G $\left(\sum_{v \in V} \deg(v)\right)$

Therefore $\sum_{v \in V} \deg(v) = 2|E|$

Example



Theorem:

In a graph $G(V,E)$ the no. of odd degree vertices is even

Proof:

Let $G(V,E)$ be a graph

$$V = V_e \cup V_o$$

we know that By HST

$$\sum_{v \in V} deg(v) = 2|E| = \text{Even}$$

$$\sum_{v \in V_e} deg(v) + \sum_{v \in V_o} deg(v) = \text{Even}$$

$$\text{Even} + \sum_{v \in V_o} deg(v) = \text{Even} \quad \left(v \in V_e \Rightarrow deg(v) = \text{even} \Rightarrow \sum_{v \in V_e} deg(v) = \text{even} \right)$$

$$\sum_{v \in V_o} deg(v) = \text{Even} - \text{Even}$$

$$= \text{Even}$$

$\Rightarrow |V_o| = \text{even}$

$\therefore$ The number of odd degree vertices is even

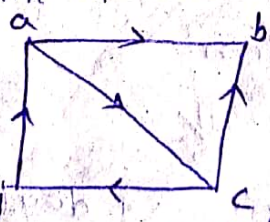
In-degree and out-degree:

Let $G(V,E)$ be a directed graph then the indegree and outdegree of a vertex v in G are defined as

$deg^-(v)$ = The no. of edges incident into v i.e v will be the end point of edge

$deg^+(v)$ = The no. of edges going out of v i.e v will be the starting point of the edge.

Example



$deg^-(a) = 1$, $deg^+(a) = 2$

$deg^-(b) = 2$, $deg^+(b) = 0$

$deg^-(c) = 1$, $deg^+(c) = 2$

$deg^-(d) = 1$, $deg^+(d) = 1$

$\sum deg^-(v) = 1+2+1+1 = 5$ $\quad \therefore \sum deg^-(v) = |E| = \sum deg^+(v)$

$\sum deg^+(v) = 2+0+2+1 = 5$

Theorm:
Show that in a graph $G(V, E)$, $\Sigma deg^-(v) = \Sigma deg^+(v) = |E|$

Proof

Let $G(V, E)$ be a graph and let $v \in V$.

since, each directed edge contributes one to sum of indegrees of all vertices and one to sum of outdegrees of all vertices.

Therefore we have

$$\Sigma deg^-(v) = \Sigma deg^+(v) = |E|$$

Problem

1. show that the degree of a vertex of a simple graph G on 'n' vertices can not be more than $n-1$

Proof:

Let $G(V, E)$ be a simple graph such that $|V| = n$ and let $v \in V$ be any vertex of G.

claim: $deg(v) \leq n-1$

Since, v can be adjacent to atmost all the remaining $n-1$ vertices of G

Hence: $0 \leq deg(v) \leq n-1$

2. show that the maximum number of edges in a simple graph with n vertices is $\frac{n(n-1)}{2}$

Sol

Let G be a simple graph with n vertices and e edges.

By handshaking theorm

$$\sum_{i=1}^{n} deg(v_i) = 2e$$

$$deg(v_1) + deg(v_2) + \cdots + deg(v_n) \geq 2e$$

$$(n-1) + (n-1) + \cdots + n(n-1) \geq 2e$$

$$n(n-1) \geq 2e$$

$$e \leq \frac{n(n-1)}{2}$$

Types of G

Let G be a simple graph with 7 vertices having degrees (1, 3, 3, 4, 5, 6, 6) then find the no. of edges of the graph

Sol we know that $\sum_{v \in V} \deg(v) = 2e$

$$1+3+3+4+5+6+6 = 2e$$
$$28 = 2e$$
$$e = 14$$

Types of Graphs:

1. NULL graph: A graph which contains only an isolated node is called null graph. That is the set of edges in a null graph is empty.

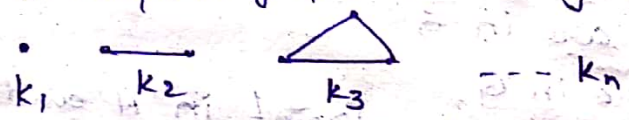
NULL graph with n vertices is denoted by N_n

Note:

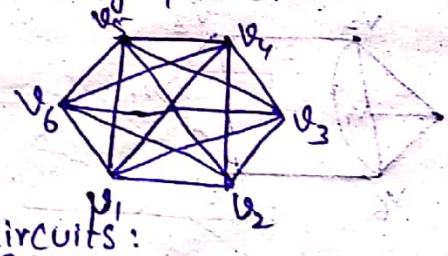
Each vertex of null graph is isolated

2. Complete graph: A simple graph G is said to be complete if every vertex in G is connected with every other vertex i.e., G must contain exactly one edge between any pair of vertices

A complete graph is usually defined by K_n

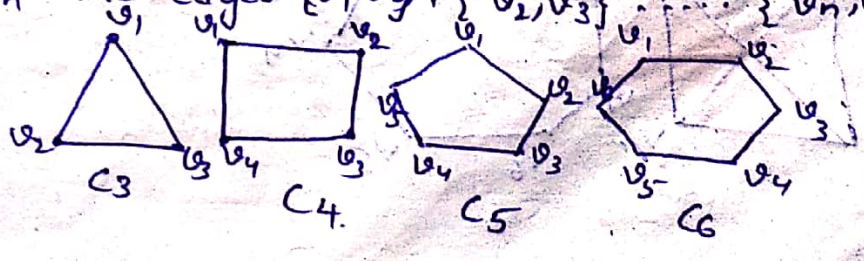
Ex:- 

3. Regular graph: A graph G is said to be a regular graph if all the vertices of graph G are having equal degree.

Ex: 

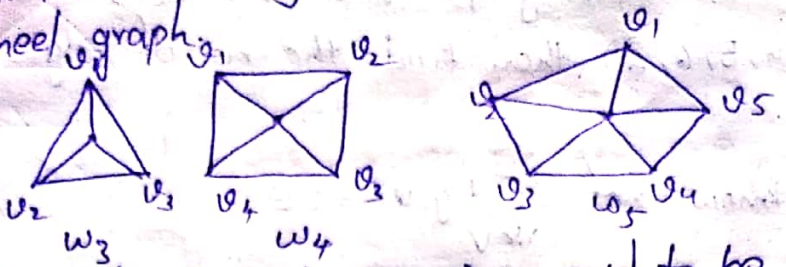
4. Cycles (or) circuits:

A cycle or circuit C_n, $n \geq 3$ consists of n vertices $v_1, v_2, \ldots, v_n$ and edges $\{v_1, v_2\}, \{v_2, v_3\}, \ldots, \{v_n, v_1\}$

Example 

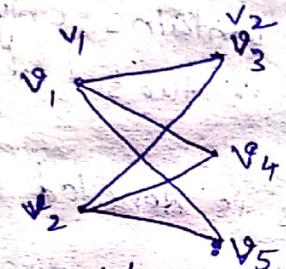
Wheel graph: If you add an additional vertex in a cycle and connect all the remaining vertices with edges we say the graph as an wheel graph.

Ex:

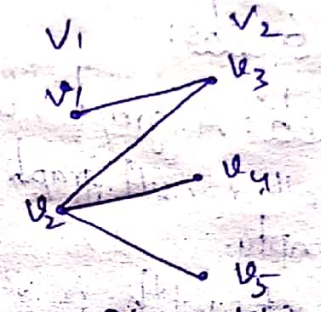


Bipartite graph: A graph $G(V,E)$ is said to be bipartite graph if the vertex of V can be partitioned into two disjoint sets V_1, V_2, so that no edge in G connects either two vertices in V_1 or two vertices in V_2

Ex:



Complete bipartite



Bi-partite

Subgraph: A graph $H=(V_1,E_1)$ is called a subgraph of $G=(V,E)$ if $V_1 \subseteq V$ and $E_1 \subseteq E$. A graph $H=(V_1,E_1)$ is called a proper subgraph of $G=(V,E)$ if $V_1 \subset V$ and $E_1 \subset E$.

H is called a sponing subgraph of G if $(V_1 = V)$

If H is subgraph of G then.

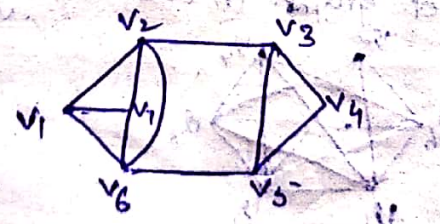
All the vectices of H are in G

All the edges of H are in G

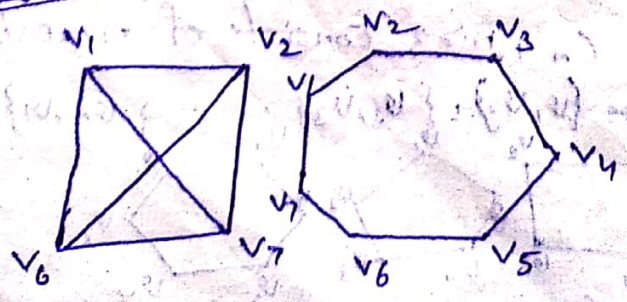
Each edge of H has the same endpoint in H and G

Example:

Graph =

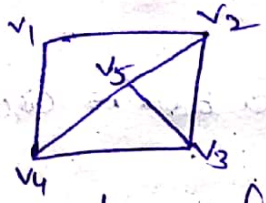


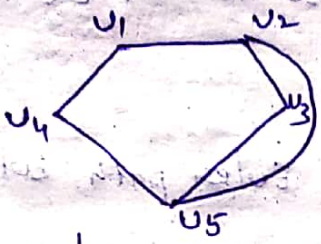
subgraph:



Isomorphism:

Two graphs $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ are said to be isomorphitic if there exists $v_1 \to v_2$ such that u, v are adjacent in G_1 if and only if $f(u), f(v)$ are adjacent in isomorphic to G_2, we write $G_1 \cong G_2$. The map f is called an isomorphism from G_1 to G_2.



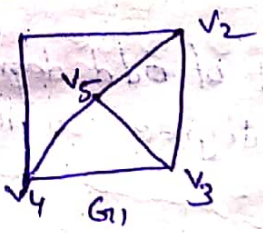


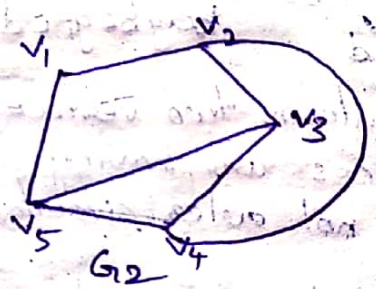
Isomorphism of two graphs:

Let $G_1(V, E)$ and $G_2(V_2, E_2)$ be two graphs then we say G_1 isomorphic to G_2 $(G_1 \cong G_2)$ if

1. no. of vertices in two graphs should be same.
2. no. of edges in two graphs should be same.
3. The no. of vertices having various degree in G_1 should be same as no. of vertices having various degrees.

Example





i. $|V_1| = 5$ $|V_2| = 5$

ii. $|E_1| = 7$ $|E_2| = 7$

iii. $\deg(v_1) = 2$ $\deg(v_1') = 2$

$(v_2) = 3$ $\deg(v_2') = 3$

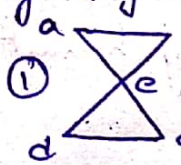
$(v_3) = 3$ $v_3' = 3$

$(v_4) = 3$ $v_4' = 3$

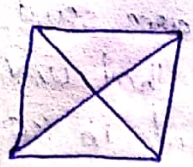
$(v_5) = 3$ $v_5' = 3$

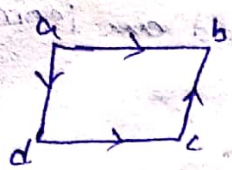
Euler circuit:

Let $G(V, E)$ be a graph. An euler circuit in a graph 'G' is a simple circuit containing every edge of 'G'. An Euler path in 'G' is a simple path in 'G' containing every edge of 'G'.

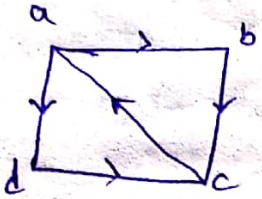
Ex: ① 

It is a euler circuit but not a Euler path

②  It is neither Euler circuit nor Euler path

③ 

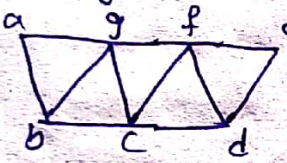
It is also neither E·C nor E·P

④ 

it is a Euler path but not a Euler circuit.

Theorm: A connected multigraph has an euler circuit if and only if each of its vertices has even degree.

Theorem: A connected multigraph has an euler path but not a circuit. If and only if it has exactly two vertices of odd degree exactly.

Ex: 

deg(v_1) = 2

bagbcgfcdfed

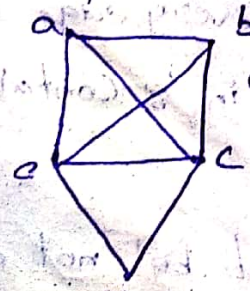
This graph contains two vertices b, d of odd degree and the remaining vertices are having even degree. so it contains Euler path but not euler circuit

Hamiltonian path (or) circuit:

Let G(V, E) be a graph assume $V = \{x_0, x_1, x_2, \ldots x_n\}, |V| = n$

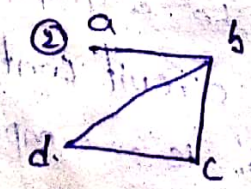
A path $x_0, x_1, x_2 \ldots x_{n-1}, x_n$ in G is called a hamiltonian path if $x_i \neq x_j$ for any i, j.

A circuit $x_0, x_1, x_2 \ldots, x_{n-1}, x_n, x_0$ in G with $n > 1$ in G is called hamiltonian circuit if $x_0, x_1, x_2 \ldots x_{n-1}, x_n$ is a hamiltonian path

Ex: ① 

abcde

It is having hamiltonian path and hamiltonian circuit

② 

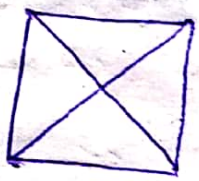
abcd

It is having hamiltonian path and not having hamiltonian circuit.

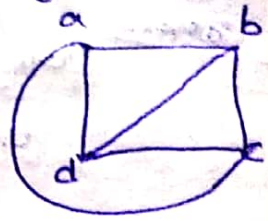
planar graph:

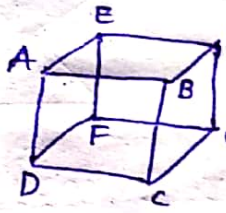
A simple graph which is said to be a planar graph if we can draw that graph without any edge crossing

Example

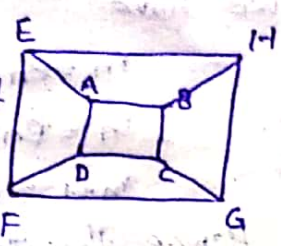
① 

It is a planar graph
Because we can represent it without having edge crossing.



② 

It is a planar graph
Because we can represent it as



*** Euler's ~~theor~~ Formula:

Let G be a connected planar simple graph with e edges and 'v' vertices. Let r be the numbers of regions in a planar representation of G. Then $r = e - v + 2$

Proof

~~Let G~~

First we specify a planar representation of G, we will prove the theorem by constructing a sequence of subgraph $G_1, G_2, G_3 \ldots G_e = G$ successively by adding an edge at each stage.

Let r_n, e_n, v_n represents the no. of regions, edges, vertices of the planar representation of G_n and we prove the theorem by mathematical induction.

For $n=1$, i.e., for G_1: $v_1 \quad R_1 \quad v_1$

$v_1 = 1, v_1 = 2, e_1 = 1$

∴ LHS $r_1 = 1$

RHS $e_1 - v_1 + 2 = 1 - 2 + 2 = 1$

∴ LHS = RHS

∴ $r_1 = e_1 - v_1 + 2$

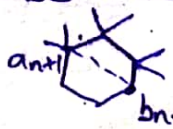
∴ The theorem is true for $n=1$

Now assume that the theorem is true for G_n

i.e., $r_n = e_n - v_n + 2$ ——①

Let $\{a_{n+1}, b_{n+1}\}$ be the edge i.e added to G_n to obtain G_{n+1}. There are 2 possibilities to consider.

Case-1 In this case already a_{n+1}, b_{n+1} are already in G_n



$v_{n+1} = v_n$

$e_{n+1} = e_n + 1$

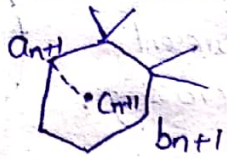
$r_{n+1} = r_n + 1$

we have $r_n = e_n - v_n + 2$

$r_n + 1 = e_n + 1 - v_n + 2$

$r_{n+1} = e_{n+1} - v_{n+1} + 2$

Case-2 Here we add another edge by adding with edge new vertex



$v_{n+1} = v_n + 1$

$e_{n+1} = e_n + 1$

$r_{n+1} = r_n$

we have

$r_n = e_n - v_n + 2$

$r_n = (e_{n+1}) - (v_n + 1) + 2$

$r_{n+1} = e_{n+1} - v_{n+1} + 2$

Hence the theorem is proved for $n = n+1$

$\therefore r = e - v + 2$

Problems

1. Suppose that a connected planar simple graph has 20 vertices, each of degree 3. Into how many regions does a representation of this planar graph split the plane

Sol Given $v = 20$ $\deg(v) = 3, \forall v \in V$

By Hand shaking theorem $2e = \Sigma \deg v \Rightarrow 2e = 60$

$e = 30$

From eulers formula $r = e - v + 2$

$r = 30 - 20 + 2$

No. of regions $r = 12$

***

Theorem : If G is connected planar simple graph with e edges and v vertices where $v \geq 3$ then $e \leq 3v - 6$

Proof :

Let G be a connected planar simple graph with e edges and v vertices where $v \geq 3$

we know that $2e = \sum_{\text{all regions } R} \deg(R)$ ——①

Because, each region has degree ≥ 3 ($\because v \geq 3$)

Therefore. $\Sigma \deg(R) = \deg(R_1) + \deg(R_2) + \cdots + \deg(R_r)$

$\Sigma \deg(R) \geq 3 + 3 + 3 + \cdots + 3$ (r times)

$\Sigma \deg(R) \geq 3r$

$2e = \Sigma \deg(R) \geq 3r$

$\frac{2}{3} e \geq r$ ——②

Euler's formula $r = e - v + 2$

$e - v + 2 = r \leq 2/3\, e$ (from ②)

$3e - 3v + 6 \leq 2e$

$\boxed{e \leq 3v - 6}$

Theorem: If a connected planar simple graph has e edges and v vertices with $v \geq 3$ and no circuit of length 3 then $e \leq 2v - 4$

Proof: Let G be a connected planar simple graph with e edges and v vertices where $v \geq 3$ and it has no circuit of length '3'

Therefore $\deg(R) \geq 4 \ \forall R$ in G

we know that $2e = \sum_{\text{all region } R} \deg(R)$ — ①

Because, each region has degree ≥ 4

Therefore, $\sum \deg(R) = \deg(R_1) + \deg(R_2) + \ldots + \deg(R_r)$

$\sum \deg(R) \geq 4 + 4 + 4 + \ldots + 4$

$\sum \deg(R) \geq 4r$

$2e = \sum \deg(R) \geq 4r$

$\frac{2}{4} e \geq r$

$\frac{1}{2} e \geq r$ — ②

Eulers formula $r = e - v + 2$

$e - v + 2 = r \leq \frac{1}{2} e$

$2e - 2v + 4 \leq e$

$\boxed{e \leq 2v - 4}$

* show that K_5 is non planar

Sol The graph K_5 has 5 vertices and 10 edges ($5C_2$)

K_5 is planar if and only if $e \leq 3v - 6$ — ①

LHS $e = 10$

RHS $3v - 6 = 3(5) - 6$

$= 9$

$LHS \neq RHS$

$\therefore K_5$ not satisfies ev ①

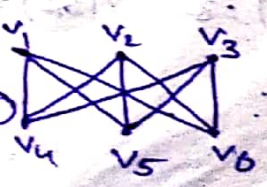
$\therefore K_5$ is non planar

* show that $K_{3,3}$ is non planar

Sol $v = 6$

$e = 9$

$K_{3,3}$ is planar $\Leftrightarrow e \leq 2v - 4$ - ①



LHS $= 9$

RHS $= 2 \times 6 - 4$

$= 8$

$\therefore K_{3,3}$ not satisfies ev ①

$\therefore K_{3,3}$ is non planar

Theorem: If G is connected planar simple graph then G has a vertex of degree not exceeding 5

Proof If G has 1 (or) 2 vertices the result is true.

If G has atleast 3 vertices then by known result

$$e \leq 3v - 6$$

$$2e \leq 6v - 12 \quad \text{—— (1)}$$

claim There is a vertex v_i in G such that $\deg(v_i) \leq 5$

if possible suppose, all the vertices of in G ≥ 6 (deg of)

$$2e \geq \sum \deg v_i$$

$$2e \geq 6 + 6 + 6 + \ldots + 6 \text{ (} v \text{ times)}$$

$$2e \geq 6v$$

$$2e > 6v - 12 \quad \text{—— (2)}$$

Therefore (1) and (2) are contradicting each other

Hence our assumption is wrong.

Therefore there is a vertex v in G such that

$\deg(v_i) \leq 5$

Graph colouring:

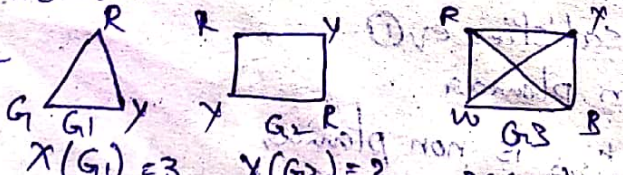
Definition: A colouring of a simple graph is the assignment of a colour to each vertex of the graph so that no two adjacent vertices are assigned the same colour.

chromatic Number:

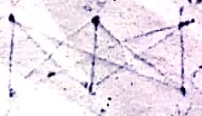
chromatic number of a graph is the least number of colours needed for a colouring of this graph.

The chromatic number of G is denoted by $\chi(G)$

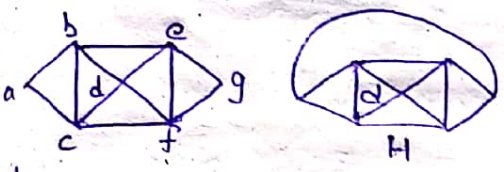
Example



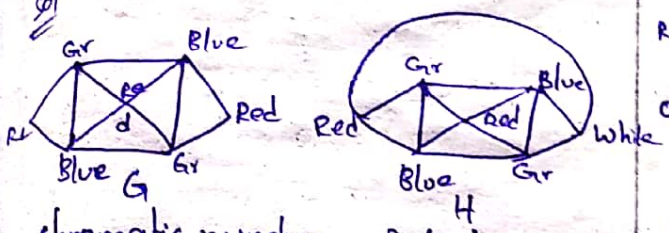
$\chi(G_1) = 3$ $\chi(G_2) = 2$ $\chi(G_3) = 4$



1. Find the chromatic number of the following graph G and H



Sol

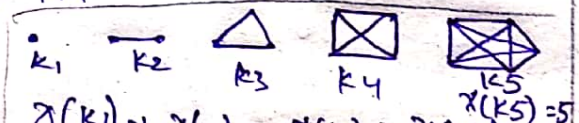


chromatic number $\chi(H) = 4$

$\chi(G) = 3$

2. what is chromatic number of k_n

Sol

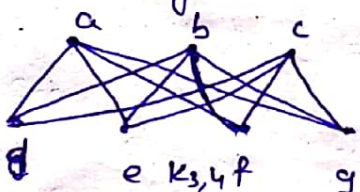


$\chi(k_1) = 1, \chi(k_2) = 2, \chi(k_3) = 3, \chi(k_4) = 4, \chi(k_5) = 5$

A colouring of k_n: A complete graph with n vertices that is there is an edge between every pair of vertices so we cannot colour a complete graph by assigning same colour. so, all the vertices will have different colours.

Therefore $\chi(k_n) = n$

3. what is chromatic number of the complete bipartite graph $k_{m,n}$ where m and n are positive integers.



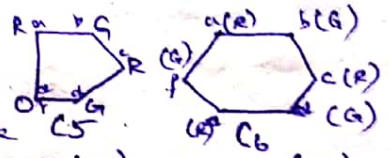
$k_{3,4}$

$\chi(k_{3,4}) = 2$

Sol Since $k_{m,n}$ is a complete bipartite graph so, the chromatic number will not be dependent on m and n. and also only 2 colours are needed to colour any complete bipartite graph as shown in figure $\chi(k_{m,n}) = 2$

4. what is chromatic number of the graph C_n where $n \geq 3$

Sol we first consider the individual cases. i.e first we find $\chi(C_5)$, $\chi(C_6)$



$\chi(C_5) = 3$ $\chi(C_6) = 2$

Now, we can observe that

$\chi(C_5) = 3$ and $\chi(C_6) = 2$

From this we can conclude that

$$\chi(C_n) = \begin{cases} 2, & \text{when } n \text{ is even} \\ 3, & \text{when } n \text{ is odd} \end{cases}$$