ANALYTICAL NUMBER THEORY AND GRAPH THEORY (DM23)

(MSC MATHEMATICS)

ACHARYA NAGARJUNA UNIVERSITY

CENTRE FOR DISTANCE EDUCATION

NAGARJUNA NAGAR,

GUNTUR

ANDHRA PRADESH

LESSON 1

PRELIMINARIES IN NUMBER THEORY

Objectives

The Objectives of this lesson are to:

- learn the fundamental definitions of Number Theory
- understand the properties of numbers and to identify the prime numbers
- use factorization concept in proving the fundamental theorem of arithmetic
- know the notion of Arithmetical functions
- study the properties of Mobius function and Euler's Totient function.
- understand the relation between Mobius and Euler's Totient functions and to derive a product formula for Euler's Totient function.

Structure

1.0 INTRODUCTION

Historical record shows that as early as 5700 B.C. ancient Sumerians kept a calendar, so they must have developed some form of arithmetic. By 2500 B.C. the Sumerians had developed a number system using 60 as a base. This was passed on to the Babylonians, who became highly skilled calculators. Babylonian clay tablets containing elaborate mathematical tables have been found, dating back to 2000 B.C.

The first scientific approach to the study of integers, i.e. the true origin of the theory of numbers is generally attributed to the Greeks. Around 600 B.C. Pythagoras and his disciples made rather thorough study of integers. They were the first to classify integers in various ways. Such as, even numbers, odd numbers, prime numbers, composite numbers etc.

Around 300 B.C an important event occurred in the history of Mathematics. The appearance of Euclids Elements, a collection of 13 books, transformed Mathematics from numerology into a deductive science. Euclid was the first to present Mathematical facts along with rigorous proofs of these facts.

After Euclid in 300 B.C, no significant advances were made in number theory until about AD 250, when another Greek mathematician, Diophantus of Alexandria made systematic use of algebraic symbols. Many of his problems originated from number theory and it was natural for him to seek integer solutions of equations. Equations to be solved with integer values of the unknowns are now called Diophantine equations.

In the 17^{th} century, the subject was revived in Western Europe, largely through the efforts of a remarkable French Mathematician Pierre de Fermat (1601 - 1665), who is generally acknowledged to be the father of Modern Number Theory. He was the first to discover really deep properties of the integers.

Shortly after Fermat's time, the names of Euler (1707 -1783), Lagrange (1736 - 1833), Legendre (1752 - 1833), Gauss (1777 - 1855) and Dirichlet (1805 - 1859) became prominent in the further development of the subject. The first text book in number theory was published by Legendre in 1798. Three years later Gauss published Disquisitiones Arithmeticae, a book which transformed the subject into a systematic & beautiful science.

1.1 DIVISIBILITY

1.1.1 Definition: **The Principle of induction**: If Q is a set of integers such that

a) $1 \in Q$,

b) $n \in Q \Rightarrow n+1 \in Q$, then

c) all integers greater than or equal to 1 belong to Q.

1.1.2 Definition: **The Well Ordering Principle**: If A is a non-empty set of positive integers, then A contains a smallest member.

1.1.3 Definition: For two integers d and n, we say that d **divides** n (we write $d \mid n$) if $n = cd$ for some integer c. In this case, we also say that d is a **factor** of n, or n is a multiple of d, or d is a divisor of n. If d does not divide n, we write $d \nmid n$.

1.1.4 Note: Properties of Divisibility:

(i) $n \mid n$ (reflexive property)

(ii) $d \mid n$ and $n \mid m \Rightarrow d \mid m$ (transitive property)

(iii) $d \mid n$ and $d \mid m \Rightarrow d \mid (an + bm)$ for any two integers a and b (linearity)

(iv) $d \mid n \Rightarrow ad \mid an$ (multiplication property)

(v) $ad \mid an$ and $a \neq 0 \Rightarrow d \mid n$ (cancellation law)

(vi) $1 \mid n$ (1 divides every integer)

(vii) $n \mid 0$ (every integer divides zero)
(viii) $0 \mid n \Rightarrow n = 0$ (zero divides only zero)
(ix) $d \mid n$ and $n \neq 0 \Rightarrow |d| \leq |n|$ (comparison property)
(x) $d \mid n$ and $n \mid d \Rightarrow |d| = |n|$
(xi) $d \mid n$ and $d \neq 0 \Rightarrow (n/d) \mid n$.

1.1.5 Definition: (i) If $d \mid n$, then $\frac{n}{d}$ is called the **divisor conjugate** to d.

(ii) If d divides both a and b, then d is called a **common divisor** of a and b

1.1.6 Definition: We say that an integer $d \geq 0$ is the **greatest common divisor (g.c.d)** of two integers a and b if it satisfies:
(i) d is a divisor of a and b, and
(ii) $e|a,\ e|b \Rightarrow e|d$ for every integer e.

1.1.7 Note: Every pair of integers a and b have g.c.d. If d is the greatest common divisor of a and b, then $d = ax + by$ for some integers x and y. The g.c.d of a, b is denoted by (a, b) or by a D b. If (a, b) = 1, then a and b are said to be **relatively prime.**
Self Assessment Question 1: *Show that if (a,m) = 1, then (m-a ,m) = 1.*

1.1.8 Properties of g.c.d :
(i) (a, b) = (b, a) or aDb = bDa (commutative law)
(ii) (a, (b, c)) = ((a, b), c) (associative law)
(iii) (ac, bc) = |c|(a, b) (distributive law)
(iv) (a, 1) = (1, a) = 1 and (a, 0) = (0, a) = |a|.
Self Assessment Question 2: *Prove that any two Consecutive integers are relatively prime.*

1.1.9 Lemma:(Euclid's lemma) If $a \mid bc$ and if (a, b) = 1, then $a \mid c$.
Proof : Suppose (a,b) =1.
Then by Note 1.1.7 ,we get $1= ax+by$ for some integers x and y.
Now $c = acx + bcy$.
But we know that $a \mid acx$ and $a \mid bcy$. So we have $a \mid c$.

1.2 PRIME NUMBERS AND FUNDAMENTAL THEOREM OF ARITHMETIC

1.2.1 Definition: (i) An integer n is said to be **prime** if $n > 1$ and if the only positive divisors of n are 1 and n.
(ii). If $n > 1$ and n is not prime, then n is called **composite number**

1.2.2 Result: Every integer n>1 is either a prime number or a product of prime numbers
Proof. We use induction on n. The result is clearly true for $n = 2$
Induction Hypothesis: Assume that the result is true for every integer < n.
Suppose n is not prime. Then it has a positive devisor $d \neq 1, d \neq n$.
Therefore $n = cd$, where $c \neq n$.

But both c and d are less than n and greater than 1.
By induction hypothesis, c and d can be written as a product of prime numbers.
Hence n can be expressed as a product of primes.

1.2.3 Result: (Euclid) There are infinite number of prime numbers.
Proof: If possible suppose that, the number of primes is finite. Therefore there exists the greatest prime number say q.
Let n denote the product of primes 2,3,5,....,q. That is $n = 2\cdot 3\cdot\ldots\ldots\cdot q$.
Let $m = n + 1$. Clearly $m \neq 1$ (Since $m = n + 1 > 1$.)
Therefore m must have a prime factor say p. That is, $p \mid m$.
Now p is one of the primes 2,3,5,......,q.
Therefore $p \mid n$.(Since $n = 2\cdot 3\cdot\ldots\ldots\cdot q$).
Since $p \mid m$ and $p \mid n$, we have $p \mid m - n$. That is, $p \mid 1$.
This implies $p = 1$, a contradiction (Since 1 is not a prime number).
Therefore the number of primes is infinite.
This completes the proof.

1.2.4 Note:(i) If a prime p does not divide a, then $(p, a) = 1$.
(ii) If a prime p divides ab, then $p \mid a$ or $p \mid b$. More generally, if a prime p divides a product $a_1 . a_2 \ldots a_n$, then $p \mid a_i$ for at least one i.

1.2.5 Fundamental Theorem of Arithmetic: Every integer $n > 1$ can be written as a product of prime factors in only one way, apart from the order of the factors.
***Self Assessment Question 3:** Express 3000 as a product of prime powers.*
1.2.6 Note: (i) Let n be an integer. If the distinct prime factors of n are $p_1, p_2, \ldots p_r$ and if p_i occurs as a factor a_i times, then we write

$$n = p_1^{a_1} \times p_2^{a_2} \times \ldots \times p_r^{a_r} \text{ or } n = \prod_{i=1}^{r} p_i^{a_i}$$

and is called the **factorization** of n into prime powers.
(ii) We can express 1 in this form by taking each exponent a_i to be zero.

(iii) If $n = \prod_{i=1}^{r} p_i^{a_i}$, then the set of positive divisors of n is the set of numbers of the form $\prod_{i=1}^{r} p_i^{c_i}$, where $0 \leq c_i \leq a_i$ for $i = 1, 2, \ldots, r$.

(iv) If two positive integers a and b have the factorization $a = \prod_{i=1}^{\infty} p_i^{a_i}$, $b = \prod_{i=1}^{r} p_i^{b_i}$, then their g.c.d. has the factorization $(a, b) = \prod_{i=1}^{r} p_i^{c_i}$ where $c_i = \min\{a_i, b_i\}$

1.2.7 Note : (i) The infinite series $\sum_{n=1}^{\infty} \frac{1}{p_n}$ diverges where p_n's are primes.

(ii) **The Division Algorithm**: Given integers a and b with $b > 0$. If there exists a unique pair of integers q and r such that $a = bq + r$, with $0 \le r < b$, then we say that q is the quotient and r is the remainder when b is divided into a. Moreover, $r = 0 \Leftrightarrow b \mid a$.

1.3 EUCLIDEAN ALGORITHM

1.3.1 Euclidean Algorithm: Given positive integers a and b, where $b \dagger a$.
Let $r_0 = a$, $r_1 = b$ and apply the division algorithm repeatedly to obtain a set of remainders $r_2, r_3, \ldots, r_n, r_{n+1}$ defined successively by the relations

$r_0 = r_1q_1 + r_2$ $\quad 0 < r_2 < r_1$,
$r_1 = r_2q_2 + r_3$ $\quad 0 < r_3 < r_2$

......

$r_{n-2} = r_{n-1}q_{n-1} + r_n$ $\quad 0 < r_n < r_{n-1}$
$r_{n-1} = r_nq_n + r_{n+1}$ $\quad r_{n+1} = 0$

Then r_n, the last non zero remainder in this process, is the g.c.d. of a and b.

1.3.2 Definition : The greatest common divisor of three integers a, b, c is denoted by (a, b, c) and is defined as (a, b, c) = (a, (b, c)).

1.3.3 Note : By the properties of g.c.d , we have (a, (b, c)) = ((a, b), c). So the g.c.d. depends only on a, b, c and not on the order in which they are written.

1.3.4 Definition : The g.c.d. of n integers $a_1, a_2, \ldots, a_n$ is defined inductively by the relation $(a_1, a_2, \ldots, a_n) = (a_1, (a_2, \ldots, a_n))$. Again this number is independent of the order in which the a_i appear.

1.3.5 Note : If $d = (a_1, a_2, \ldots, a_n)$, then d is a linear combination of the a_i. That is, there exist integers $x_1, x_2, \ldots, x_n$ such that $(a_1, a_2, \ldots, a_n) = a_1x_1 + a_2x_2 + \ldots + a_nx_n$.
(i) If $d = 1$, then the numbers are said to be **relatively prime.**
(ii) If $(a_i, a_j) = 1$ whenever $i \neq j$, then the numbers $a_1, a_2, \ldots, a_n$ are said to be **relatively prime in pairs.**
(iv) If $a_1, a_2, \ldots, a_n$ are relatively prime in pairs, then $(a_1, a_2, \ldots, a_n) = 1$.
But the converse is not necessarily true since (2,3,10) =1 and $(2,10) \neq 1$.

1.4 ARITHMETICAL FUNCTIONS

1.4.1 Definition: A real or complex valued function defined on the positive integers is called an **arithmetical function** or **number theoretic function**.
If f is an Arithmetical function, then $f : N \to \mathcal{R}$ or $f : N \to C$.

1.4.2 Example: (i) The following are Arithmetical functions:

a) $f(n) = 2n$ for all $n \in N$.
b) $U(n) = \frac{1}{n}$ for all $n \in N$.
c) $N(n) = n + \frac{1}{n}$ for all $n \in N$.

1.4.3 Example: The number of divisors of a positive integer n is denoted by $d(n)$. It is an Arithmetical function and is represented as, $d(n) = \sum_{d|n} 1$.

Here is a table of values of $d(n)$.

Number (n)	Divisors	d(n)
10	1, 2, 5, 10	d(10) = 4
20	1, 2, 4, 5, 10, 20	d(2) = 6
6	1, 2, 3, 6	d(6) = 4

1.4.4 Note: If $n = p_1^{\alpha_1}.p_2^{\alpha_2} \dots p_k^{\alpha_k}$ is the prime factorization of $n > 1$, then the number of divisors of n is $d(n) = (1 + \alpha_1)(1 + \alpha_2) \dots (1 + \alpha_k)$, where $\alpha_i \geq 1$.

1.4.5 Example: The sum of the divisors of a positive integer n is denoted by $\sigma(n)$. That is, $\sigma(n) = \sum_{d|n} d$ and it is an Arithmetical function.

If $n = p_1^{\alpha_1}.p_2^{\alpha_2} \dots p_k^{\alpha_k}$ is the prime factorization of n, then

$$\sigma(n) = \sum_{d|n} d = \frac{p_1^{\alpha_1+1}-1}{p_1-1}.\frac{p_2^{\alpha_2+1}-1}{p_2-1} \dots \frac{p_k^{\alpha_k+1}-1}{p_k-1} \quad \dots (*)$$

For example, consider the positive integer 4. The divisors of 4 are 1, 2, 4.
Therefore $\sigma(4) = 1 + 2 + 4 = 7$.
For example, consider

$\sigma(100) = 1 + 2 + 4 + 5 + 10 + 20 + 25 + 50 + 100 = 217$ (by definition)

We can also write $100 = 2^2 \times 5^2 = p_1^{\alpha_1}.p_2^{\alpha_2}$.

So $\sigma(100) = \frac{p_1^{\alpha_1+1}-1}{p_1-1}.\frac{p_2^{\alpha_2+1}-1}{p_2-1} = \left(\frac{2^3-1}{2-1}\right)\left(\frac{5^3-1}{5-1}\right) = 7.\frac{124}{4} = 217$ (by (*))

1.4.6 Definition: The sum of the α^{th} powers of the divisors of n is denoted by $\sigma_\alpha(n)$. That is $\sigma_\alpha(n) = \sum_{d|n} d^\alpha$.

Since the function $\sigma_\alpha(n)$ is defined on positive integers, it is an Arithmetical function.
For example consider the following:

(i) $\sigma_2(6) = 1^2 + 2^2 + 3^2 + 6^2 = 1 + 4 + 9 + 36 = 50$.

(ii) $\sigma_3(10) = 1^3 + 2^3 + 5^3 + 10^3 = 1134$.

1.4.7 Example: $\sigma_0(n) = d(n)$ and $\sigma_1(n) = \sum_{d|n} d^1 = \sigma(n)$.

1.5 MOBIUS FUNCTION AND EULER TOTIENT FUNCTION

1.5.1 Definition: An integer n is said to be **square free** if it has no square factor. (Equivalently, $n = p_1^{\alpha_1}.p_2^{\alpha_2}\ldots p_k^{\alpha_k}$ is a **square free** if $\alpha_i = 1$ for $1 \le i \le k$.)

1.5.2 Example: 1, 2, 3, 5, 6, 7, 10, 11, 13, 14, 15, 17, 19 are square free numbers between 1 and 20. 4, 8, 9, 12, 16, 18 are not square free numbers.
(Because $4 = 2^2, 8 = 2^3, 9 = 3^2, 12 = 2^2 \times 3, 16 = 4^2, 18 = 3^2.2$)

1.5.3 Definition Mobius function μ(n):
The function $\mu : \mathcal{N} \to \mathcal{R}$ defined by $\mu(1) = 1$.
If $n > 1$ and $n = p_1^{a_1}.p_2^{a_2}\ldots p_k^{a_k}$ (the prime decomposition for n),
then $\mu(n) = (-1)^k$ if $a_1 = a_2 = \ldots = a_k = 1$ (that is, n is square free)
$= 0$ otherwise.

1.5.4 Example: Here is a table of values of μ(n).

n	1	2	3	4	5	6	7	8	9	10	30
μ(n)	1	-1	-1	0	-1	1	-1	0	0	1	-1

1.5.5 Notation: (i) For any real number x, [x] denote the integral part of x. That is [x] is the greatest integer less than or equal to x.

For example $\left[\frac{20}{3}\right] = 6, \left[\frac{-13}{3}\right] = -5.$

(ii) [x] is not an arithmetical function
(because its domain is not the set of all positive integers)

1.5.6 Definition: For any $n \ge 1$, define $I(n) = \left[\frac{1}{n}\right] = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n > 1 \end{cases}$.

Then I(n) is an arithmetical function.

1.5.7 Theorem: If $n \ge 1$ and μ(n) is the Mobius function, then $\sum_{d|n} \mu(d) = I(n)$, where the summation on left is over all positive divisors d of n.

1.5.8 Definition Euler totient function φ(n): If $n \ge 1$, then the Euler totient function φ(n) is defined to be the number of positive integers not exceeding n which are relatively prime to n.

That is, $\varphi(n) = \sum_{k=1}^{n} 1$, where $(k, n) = 1$ and the summation is taken over all the numbers k $(1 \le k \le n)$ which are relatively prime to n.

Self Assessment Question 4 : *If m> 2, then show that φ(m) is even.*

1.5.9 Note: (i) If p is a prime number, then $\varphi(p) = p - 1$.
(ii) Here is a Table of values of φ(n) for n = 1, 2, ...,11.

n	1	2	3	4	5	6	7	8	9	10	11
φ(n)	1	1	2	2	4	2	6	4	6	4	10

Self Assessment Question 5 : *Verify that* $\varphi(p^k) = p^k\left(1 - \frac{1}{p}\right)$, *where p is prime.*

1.5.10 Note: Consider positive integer n and write $S = \{1, 2, \ldots, n\}$.
Define ~ on S by $a \sim b \Leftrightarrow (a, n) = (b, n)$.
Then ~ is an equivalence relation.
For a divisor of n, $A(d) = \{k \,/\, (k, n) = d\}$ is an equivalence class. So $S = \bigcup_{d|n} A(d)$.

1.5.11 Example: Take n = 6. Follow the notation given in the Note 1.5.10.
$S = \{1, 2, \ldots, 6\}$. Then divisors of 6 are 1, 2, 3, 6.
Now $A(1) = \{1, 5\}$, $A(2) = \{2, 4\}$, $A(3) = \{3\}$, $A(6) = \{6\}$.
The union of A(1), A(2), A(3), A(6) is S.
Note that these sets A(1), A(2), A(3), A(6) are disjoint.

1.5.12 Theorem: If $n \geq 1$, then $\sum_{d|n} \varphi(d) = n$.

1.5.13 Note: If (k, n) = 1, then $I(k, n) = \left[\frac{1}{(k,n)}\right] = \left[\frac{1}{1}\right] = [1] = 1$.

If $(k, n) \neq 1$, then $(k, n) > 1 \Rightarrow \left[\frac{1}{(k,n)}\right] = 0 \Rightarrow I[(k, n)] = 0$.

1.5.14 Theorem: **A relation between the Euler totient function and the Mobius function:**

If $n \geq 1$, we have $\varphi(n) = \sum_{d|n} \mu(d) \cdot \frac{n}{d}$.

Proof: $\varphi(n) = \sum_{\substack{k=1 \\ (k,n)=1}}^{n} 1$ (by the definition of φ)

$= \sum_{k=1}^{n} \left[\frac{1}{(k,n)}\right]$ (by the above note)

$= \sum_{k=1}^{n} I(k,n)$

$= \sum_{k=1}^{n} \left(\sum_{d|(k,n)} \mu(d) \right)$ (by Theorem 1.5.7 , $I(n) = \sum_{d|n} \mu(d)$)

$= \sum_{k=1}^{n} \sum_{d|n \text{ and } d|k} \mu(d)$ ... (i)

For a fixed divisor d of n, we must sum over all those k in the range $1 \leq k \leq n$ which are multiples of d.

If we write $k = qd$, then $1 \le k \le n \Leftrightarrow 1 \le \frac{k}{d} \le \frac{n}{d} \Leftrightarrow 1 \le q \le \frac{n}{d}$.

Consider $\varphi(n) = \sum_{k=1}^{n} \sum_{d|n \text{ and } d|k} \mu(d)$ (by (i))

$$= \sum_{d|n} \sum_{q=1}^{(n/d)} \mu(d) = \sum_{d|n} \mu(d) \sum_{q=1}^{n/d} 1 = \sum_{d|n} \mu(d) \cdot \frac{n}{d}$$

[since $\sum_{q=1}^{n/d} 1 = 1 + 1 + \ldots + 1$ ($\frac{n}{d}$ times) $= \frac{n}{d}$]

This completes the proof.

1.5.15 Theorem A product formula for $\varphi(n)$: For $n \ge 1$ we have

$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$ where p runs over distinct prime factors of n.

Self Assessment Question 6: *Find the number of positive integers $\le$ 2500 and relatively prime to 2500.*

1.5.16 Theorem: Prove that

(i) $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$ for a prime number p and $\alpha \ge 1$.

(ii) $\varphi(mn) = \varphi(m).\ \varphi(n) \frac{d}{\varphi(d)}$ where $d = (m, n)$

(iii) $\varphi(mn) = \varphi(m).\ \varphi(n)$ if $(m, n) = 1$.

(iv) $a \mid b \Rightarrow \varphi(a) \mid \varphi(b)$.

(v) $\varphi(n)$ is even for $n \ge 3$.

Moreover if n has r distinct odd prime factors, then $2^r \mid \varphi(n)$

1.5.17 Problem: Find all integers n such that $\varphi(n) = \frac{n}{2}$.

Solution: Suppose n is an integer such that $\varphi(n) = \frac{n}{2}$

$$\Rightarrow \prod_{p|n} \left(1 - \frac{1}{p}\right) = \frac{1}{2}.$$

Observe that if $n = 2^\alpha$, then $\prod_{p|n} \left(1 - \frac{1}{p}\right) = \left(1 - \frac{1}{2}\right) = \frac{1}{2}$ ... (i)

(since 2 is only the prime number dividing 2^α)

If n has an odd prime factor, then $n = 2^\alpha.k$ for some odd number k.

Now for this n, we have $\prod_{p|n} \left(1 - \frac{1}{p}\right) = \prod_{p|2^\alpha.k} \left(1 - \frac{1}{p}\right) = \prod_{p|2^\alpha} \left(1 - \frac{1}{p}\right) \prod_{p|k} \left(1 - \frac{1}{p}\right)$

$$= \frac{1}{2} \cdot \prod_{p \mid k}\left(1 - \frac{1}{p}\right) < \frac{1}{2} \quad (\text{since } \prod_{p \mid 2^{\alpha}}\left(1 - \frac{1}{p}\right) = \frac{1}{2})$$

(observe that this part is < 1)

Therefore if an odd prime divides n, then $\varphi(n) < \frac{1}{2}$ ... (ii)

Now if $n = 2^{\alpha}$, then $\varphi(n) = n \prod_{p \mid n}\left(1 - \frac{1}{p}\right)$ (by Theorem 1.5.15)

$$= n(\frac{1}{2}) \text{ (by (i))} = \frac{n}{2}$$

If $n = 2^{\alpha}.k$ with k prime, then $\varphi(n) = n\left(\prod_{p \mid n}\left(1 - \frac{1}{p}\right)\right) < n.\frac{1}{2}$ (by (ii)

$\Rightarrow \varphi(n) < \frac{n}{2}$.

Hence, $n = 2^{\alpha} \Leftrightarrow \varphi(n) = \frac{n}{2}$.

1.5.18 Note: If $n = 2^{\alpha}$ and $\alpha \geq 2$, then $\varphi(n) = \frac{2^{\alpha}}{2} = 2^{\alpha - 1}$ is an even number.

1.5.19 Problem: If the same prime divides m and n, then $n.\ \varphi(m) = m.\ \varphi(n)$.

Solution: Suppose same primes divides both m and n

$$\Rightarrow \prod_{p \mid m}\left(1 - \frac{1}{p}\right) = \prod_{p \mid n}\left(1 - \frac{1}{p}\right) \quad \text{... (i)}$$

Consider $\varphi(m) = m. \prod_{p \mid m}\left(1 - \frac{1}{p}\right)$ and $\varphi(n) = n. \prod_{p \mid n}\left(1 - \frac{1}{p}\right)$

$$\Rightarrow \frac{\varphi(m)}{m} = \prod_{p \mid m}\left(1 - \frac{1}{p}\right) \text{ and } \frac{\varphi(n)}{n} = \prod_{p \mid n}\left(1 - \frac{1}{p}\right)$$

$$\Rightarrow \frac{\varphi(m)}{m} = \frac{\varphi(n)}{n} \text{ (by (i))} \Rightarrow n.\ \varphi(m) = m.\ \varphi(n).$$

1.5.20 Problem: Prove that $a \mid b \Rightarrow \varphi(a) \mid \varphi(b)$.

Solution: Consider $a \mid b \Rightarrow b = a.c$ for some integer c.

Now $\varphi(b) = \varphi(ac) = \varphi(a).\ \varphi(c). \frac{d}{\varphi(d)}$, where $(a, c) = d$

$$= d.\ \varphi(a). \frac{\varphi(c)}{\varphi(d)} \Rightarrow \frac{\varphi(b)}{\varphi(a)} = d.\ \frac{\varphi(c)}{\varphi(d)} \quad \text{... (i)}$$

Now we prove this by induction on b.
If $b = 1$, then $a = 1$ and so $\varphi(a) \mid \varphi(b)$.
Suppose this result is true for all numbers less than b.
Since $ac = b$ we have that $c < b$.
So by induction hypothesis, the result is true for c.

Now $d \mid c \Rightarrow \varphi(d) \mid \varphi(c) \Rightarrow \frac{\varphi(c)}{\varphi(d)}$ is an integer $\Rightarrow d.\frac{\varphi(c)}{\varphi(d)}$ is an integer

$\Rightarrow \frac{\varphi(b)}{\varphi(a)}$ is an integer (by (i)) $\Rightarrow \varphi(a) \mid \varphi(b)$. This completes the proof

1.6 SUMMARY

In this lesson some basic concepts of Number Theory have been introduced and some elementary results were obtained. Also the properties of divisibility, prime numbers were discussed. Representation of positive integer greater than 1, as the product of prime powers was identified. This lesson also provides an algorithm for computing the quotient 'q' and the remainder 'r' for the given integers 'a' and 'b' with $b > 0$. An uniqueness for these numbers also obtained. Finally, we discussed some important arithmetical functions like Mobius function and Euler totient function with examples.

1.7 TECHNICAL TERMS

Divisibility: For two integers d and n: "d divides n if $n = cd$ for some integer c".

Greatest Common Divisor: If d is a divisor of a and b and $e|a, e|b \Rightarrow e|d$ for every integer e, then d is called greatest common divisor.

Prime number: An integer greater than 1 and whose positive divisors are only 1 and itself.

Factorization: $n = p_1^{a_1} \times p_2^{a_2} \times \ldots \times p_r^{a_r}$ or $n = \prod_{i=1}^{r} p_i^{a_i}$, where $n \in Z^+$ and primes p_i occurs as a factor a_i, $1 \leq i \leq r$.

Arithmetical function: A real or complex valued function defined on the set positive Integers.

Mobius function: $\mu : \mathcal{N} \rightarrow \mathcal{R}$ defined by $\mu(1) = 1$.
If $n > 1$ and $n = p_1^{a_1} . p_2^{a_2} \ldots p_k^{a_k}$ (the prime decomposition for n).
then $\mu(n) = (-1)^k$ if $a_1 = a_2 = \ldots = a_k = 1$ (that is n is square free)
$= 0$ otherwise.

Euler totient function: $\phi(n)$: The number of positive integers not exceeding n ($n \geq 1$) which are relatively prime to n.

1.8 ANSWERS TO SELF ASSESSMENT QUESTIONS

1: Suppose (m-a ,m) = d

$\Rightarrow d \mid m-a$ and $d \mid m$ $\Rightarrow d \mid m-(m-a) = d \mid a$.

Now $d \mid m$ and $d \mid a$.

$\Rightarrow d \mid (a,m) \Rightarrow d \mid 1 \Rightarrow d = 1$

Therefore (m-a ,m) = 1.

2: Let n and n+1 be two consecutive integers and let (n, n+1) = d.

$\Rightarrow d \mid n$ and $d \mid n+1 \Rightarrow d \mid n+1-n \Rightarrow d \mid 1$

Therefore (n, n+1) = 1

Hence n and n+1 are relatively prime.

3: $3000 = 2 \times 2 \times 2 \times 5 \times 5 \times 5 \times 3 = 2^3.5^3.3^1$.

4: We know that if $\phi(m, n) = 1$, then $(m-n, n) = 1$ (by SAQ 1)

Therefore Integers relatively prime to m occur in pairs of type n, m-n.

Hence $\varphi(m)$ is even.

5: The integers from 1 to p^k which are not relatively prime to p^k are $p.1, p.2, p.3 \ldots p.p^{k-1}$.

Total no. of such integers which are not relatively prime to p^k is p^{k-1}.

Therefore $\phi(p^k)$ = number of integers relatively prime to p^k and less than p^k.

$$= p^k - p^{k-1} = p^k(1 - \frac{1}{p}).$$

6: Here $n = 2500 = 2^2 \times 5^4$

Therefore $\varphi(n) = \varphi(2500)$

$= \varphi(2^2 \times 5^4)$

$= 2500(1-\frac{1}{2})(1-\frac{1}{5}) = 1000.$

1.9 MODEL QUESTIONS

1. Define the terms: (i) Division Algorithm (ii) Euclidean Algorithm
2. State and Prove fundamental theorem of Arithmetic.
3. Define an Arithmetical function and give an example.
4 Define Euler totient function and Mobius function
5. Derive the relation between Euler totient function and Mobius function.
6. Derive a Product formula for φ (n).

1.10 REFERENCE BOOKS

1. Chandrasekharan, K. "Introduction to Analytic Number Theory", Springer Verlag .
2. Hardy, G.H. & Wright, E.M. "Introduction to the Theory of Numbers", Fourth Edition, Oxford Publications,
3. Levegue W.J. (1986) "Topics in Number Theory (2 volumes), Addition - Wesley Publ. Co.
4. Rademacher (1964) "Lectures on Elementary Number Theory", New York, Blaisdell Publ. Co.
5. Tom M. Apostol "Introduction to Analytic Number Theory", Springer International Student Edition, Narosa Publishing House, 1995.
6. Uspensky, J.V., and Heaslett, M.A. (1939) "Elementary Number Theory", New York, Mc. Graw - Hill Book. Co.
7. Vinogrador, "Elements of Number Theory", Dover Publications

Name of the Author of this Lesson: **Dr. Kuncham Syam Prasad**

LESSON – 2

ARITHMETICAL FUNCTIONS AND DIRICHLET MULTIPLICATION

Objectives

The objectives of this lesson are to:

- know the concept of Dirichlet multiplication of two arithmetical functions and to study the algebraic properties of Dirichlet multiplication
- identify the significance of Dirichlet product and related inversion formulae
- study Mongoldt function $\wedge(n)$, Liouville's function $\lambda(n)$, and divisor functions $\sigma_\alpha(n)$
- study the properties of multiplicative arithmetical functions using formal power series.
- prove the Selberg identity.

Structure

2.0 INTRODUCTION

Certain functions are found to be of special importance in connection with the study of the divisors of an integer. Particularly Arithmetical functions play an important role in the study of divisibility properties of integers and the distribution of primes. In this lesson, we introduce some functions like Mongoldt, Multiplicative function, Liouville's and Divisor functions $\lambda(n)$ and $\sigma_\alpha(n)$. We define the multiplicative functions whose significance is that, they are completely determined once their values at prime powers are known.

2.1 DIRICHLET PRODUCT OF ARITHMETICAL FUNCTIONS

2.1.1 Definition: Suppose f and g are two arithmetical functions, then we define their **product (Dirichlet product** or **Dirichlet convolution**, denoted by $f*g$) to be the arithmetical function defined by the equation $f*g = \sum_{d|n} f(d).g(\frac{n}{d})$ where the summation is over all positive divisors d of n.

It is clear that, $(f*g)(n) = \sum_{d.\delta = n} f(d).g(\delta)$. Here $\delta = \frac{n}{d}$ and the summation runs over all positive divisors d and δ such that $d.\delta = n$.

2.1.2 Example: (i) $(f*g)(4) = \sum_{d|4} f(d).g(\frac{4}{d}) = f(1)g(4) + f(2)g(2) + f(4)g(1)$.

(ii) $(f*g)(6) = f(1)g(6) + f(2)g(3) + f(3)g(2) + f(6)g(1)$.

(iii) If $n = p^m$ where p is the prime number, then

$$(f*g)(p^m) = \sum_{d|p^m} f(d).g\left(\frac{p^m}{d}\right)$$

$$= \sum_{k=0}^{m} f(p^k)g\left(\frac{p^m}{p^k}\right) = \sum_{k=0}^{m} f(p^k)g(p^{m-k}) = \sum_{k+l=m} f(p^k)f(p^l) \text{ where } 0 \le k, l \le m.$$

2.1.3 Notation: (i) The symbol N used for the arithmetical function for which $N(n) = n$ for all n.

(ii) By the Theorem 1.5.14 of Lesson 1, we have

$$\varphi(n) = \sum_{d|n} \mu(d).\frac{n}{d} = \sum_{d|n} \mu(d).N\left(\frac{n}{d}\right) = \mu * N.$$

(iii) The arithmetical function I defined by

$$I(n) = \left[\frac{1}{n}\right] = 1 \text{ if } n = 1$$

$$= 0 \text{ if } n > 1$$ is called the **identity function.**

2.1.4 Theorem: Dirichlet multiplication is commutative and associative.
That is., for any arithmetical functions f, g, k we have
(i) $f*g = g*f$ (commutative)
(ii) $f*(g*k) = (f*g)*k$ (associative)

2.1.5 Theorem: For all f, we have $I * f = f * I = f$.

2.1.6 Note: The function $I(n) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{otherwise} \end{cases}$ is the identity function with respect to Dirichlet product.

2.1.7 Theorem: The set A of all arithmetical functions f with $f(1) \neq 0$ forms an Abelian group with respect to Dirichlet product or Dirichlet convolution '*'.

Proof: Let $f, g \in A$.
By the definition of $f * g$ we have that $f * g$ is an arithmetical function.
Therefore $f, g \in A \Rightarrow f * g \in A$.
Commutative law:
Consider $(f * g)(n) = \sum_{d|n} f(d).g(\frac{n}{d}) = \sum_{d.\delta=n} f(d).g(\delta) = \sum_{\delta.d=n} g(\delta).f(d) = (g * f)(n)$

This is true for all n.
Therefore $f * g = g * f$.
Associative law: Let f, g, h are arithmetical functions and $H = g * h$ and consider

$$[f * (g * h)](n) = \sum_{d.\delta=n} f(d).(g * h)(\delta)$$

$$= \sum_{d.\delta=n} f(d). \sum_{a.b=.\delta} g(a)\, h(b) = \sum_{a.b.d=n} f(d).g(a).h(b)$$

Similarly $[(f * g) * h)](n) = \sum_{x.y.z=n} f(x).g(y).h(z)$

Therefore $f * (g * h) = (f * g) * h$.

Identity law: Consider the function I defined by $I(n) = \left[\frac{1}{n}\right] = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n > 1 \end{cases}$.

Consider $(f * I)(n) = \sum_{d\,|\,n} f(d).I(\frac{n}{d})$.

If $d = n$, then $\frac{n}{d} = \frac{n}{n} = 1$ and $I\left(\frac{n}{d}\right) = 1$.

Otherwise $I\left(\frac{n}{d}\right) = 0$.

Therefore $(f * I)(n) = \sum_{d\,|\,n} f(d).I(\frac{n}{d}) = f(n)$.

This is true for all n.

Similarly we can prove that $f = (I * f)$.
Hence $f * I = f = I * f$.
Therefore I is the identity element with respect to $*$.

Inverse law: Let f be an arithmetical function with $f(1) \neq 0$.
Suppose there exists an arithmetical function g such that $f * g = I$.

If $n = 1$ then $1 = I(1) = (f * g)(1) = f(1).g(1) \Rightarrow g(1) = \frac{1}{f(1)}$

Suppose $n > 1$, then $f * g = I$

$$\Leftrightarrow 0 = I(n) = (f * g)(n) = \sum f(d).g\left(\tfrac{n}{d}\right)$$

$$\Leftrightarrow 0 = f(1)g(n) + \sum_{\substack{d|n \\ d \neq 1}} f(d).g\left(\tfrac{n}{d}\right)$$

$$\Leftrightarrow f(1)g(n) = -\sum_{d|n,\, d \neq 1} f(d).g\left(\tfrac{n}{d}\right) \Leftrightarrow g(n) = \frac{-1}{f(1)} . \sum_{\substack{d|n \\ d \neq 1}} f(d).g\left(\tfrac{n}{d}\right).$$

We prove that if g is an arithmetical function such that $f * g = I$, then

$$g(n) = \frac{-1}{f(1)} . \sum_{\substack{d|n \\ d \neq 1}} f(d).g\left(\tfrac{n}{d}\right).$$

This shows that there exists inverse of f and it is also equals to the same expression. This means there exist unique inverse.
Hence A is an Abelian group with respect to Dirichlet product.

2.1.8 Note: The function f^{-1} defined by $f^{-1}(1) = \frac{1}{f(1)}$ and

$$f^{-1}(n) = \frac{-1}{f(1)} \sum_{\substack{d|n \\ d<n}} f^{-1}(d).f\left(\tfrac{n}{d}\right) \text{ (for } n > 1)$$ is called the Dirichlet inverse of f.

2.1.9 Definition: We define the **unit function** u to be the arithmetical function such that $u(n) = 1$ for all n.

2.1.10 Note: By Theorem 1.5.7 of lesson 1, we have $\sum_{d|n} \mu(d) = I(n)$.

Now $\mu * u = \sum_{d|n} \mu(d)\, u\left(\tfrac{n}{d}\right)$

$= \sum_{d|n} \mu(d).1$ (by definition of u)

$= \sum_{d|n} \mu(d) = I(n)$ (by Theorem 1.5.7 of lesson 1).

Hence $\mu * u = I$. Thus u and μ are Dirichlet inverses of each other.

That is., $u = \mu^{-1}$, $\mu = u^{-1}$.

2.1.11 Theorem: (Mobius inversion formula)

The equation $f(n) = \sum_{d|n} g(d) \Leftrightarrow g(n) = \sum_{d|n} f(d).\mu(\frac{n}{d})$. (Equivalently $f = g*u \Leftrightarrow g = f*\mu$).

Proof: Suppose $f(n) = \sum_{d|n} g(d)$ ... (i)

We know that $\sum_{d|n} \mu(d) = I(n)$ (by Theorem 1.5.7 of lesson 1) ... (ii)

We have unit function $u(n) = 1$ for all n (by Definition 2.1.9) ... (iii)

Consider $f(n) = \sum_{d|n} g(d)$ ((i) given)

$\Leftrightarrow f(n) = \sum_{d|n} g(d).u(\frac{n}{d})$ (by (iii))

$\Leftrightarrow f(n) = (g * u)(n)$ (since by the definition of Dirichlet multiplication)

$\Leftrightarrow f = g * u$

$\Leftrightarrow f * u^{-1} = (g * u) * u^{-1} = g * (u * u^{-1})$ (by associative law)

$\Leftrightarrow f * \mu = g$ (since $u^{-1} = \mu$ (by Note 2.1.10))

$\Leftrightarrow g(n) = (f * \mu)(n)$ for all n

$\Leftrightarrow g(n) = \sum_{d|n} f(d).\mu(\frac{n}{d})$

Hence $f(n) = \sum_{d|n} g(d) \Leftrightarrow g(n) = \sum_{d|n} f(d).\mu(\frac{n}{d})$.

2.2 MANGOLDT AND MULTIPLICATIVE FUNCTIONS

2.2.1 Definition: For every integer $n \geq 1$, we define

$$\wedge(n) = \begin{cases} \log p & \text{if } n = p^m \text{ for some prime } p \text{ and some } m \geq 1 \\ 0 & \text{otherwise} \end{cases}$$

The function $\wedge(n)$ is called **Mangoldt function.**

2.2.2 Example: For example consider the following table which shows the values of n and the corresponding values of $\wedge(n)$.

n	1	2	3	4	5	6	7	8	9	10
$\wedge(n)$	0	log 2	log 3	log 2	log 5	0	log 7	log 2	log 3	0

2.2.3 Theorem: If $n \geq 1$, we have $\log n = \sum_{d|n} \wedge(d)$.

Proof: If $n = 1$, then $\log 1 = 0 = \wedge(1) = \sum_{d|n} \wedge(d)$.

Assume that $n > 1$ and $n = \prod_{k=1}^{r} p_k^{a_k}$.

Now consider the sum $\sum_{d|n} \wedge(d)$.

In this sum (by the definition of $\wedge$) we have $\wedge(d) \neq 0 \Leftrightarrow d = p_k^m$ for some $1 \leq k \leq r$ and $1 \leq m \leq a_k$.

Hence $\sum_{d|n} \wedge(d) = \sum_{k=1}^{r} \sum_{m=1}^{a_k} \wedge(p_k^m)$

$$= \sum_{k=1}^{r} \sum_{m=1}^{a_k} \log p_k$$

$$= \sum_{m=1}^{a_1} \log p_1 + \sum_{m=1}^{a_2} \log p_2 + \ldots + \sum_{m=1}^{a_r} \log p_r$$

$$= a_1 \log p_1 + a_2 \log p_2 + \ldots + a_r \log p_r$$

$$= \sum_{k=1}^{r} a_k \log p_k$$

$$= \sum_{k=1}^{r} \log(p_k^{a_k}) = \log\left(\prod_{k=1}^{r} p_k^{a_k}\right) = \log n.$$

Therefore $\log n = \sum_{d|n} \wedge(d)$.

2.2.4 Theorem: If $n \geq 1$, we have $\wedge(n) = \sum_{d|n} \mu(d) \log\left(\frac{n}{d}\right) = -\sum_{d|n} \mu(d).(\log d)$.

Proof: By the Theorem 2.2.3, we have

$$\log n = \sum_{d|n} \wedge(d) \quad \text{for } n \geq 1 \quad \ldots (i)$$

By Mobius inversion formula (see Theorem 2.1.11)

$\left(f(n) = \sum_{d|n} g(d) \Leftrightarrow g = f * \mu.\right.$ That is., $\left.g(n) = \sum_{d|n} f(d).\mu\left(\frac{n}{d}\right)\right)$

we have $\wedge(n) = \sum_{d|n} \mu(d).\log\left(\frac{n}{d}\right)$ (since $f * \mu = \mu * f$)

$= \sum_{d|n} \mu(d)(\log n - \log d)$

$= \log n \sum_{d|n} \mu(d) - \sum_{d|n} \mu(d) \log d.$

$= \log n\ I(n) - \sum_{d|n} \mu(d) \log d$ (Since $\sum_{d|n} \mu(d) = I(n)$, by the Theorem 1.5.7 of lesson 1)

$= -\sum_{d|n} \mu(d) \log d$

(for $n = 1$ $\log n = 0$ and for $n > 1$, $I(n) = 0$ and so $\log n.\ I(n) = 0$ for all n)

Therefore $\wedge(n) = -\sum_{d|n} \mu(d) \log d$.

2.2.5 Definition: (i) An arithmetical function f is called **multiplicative** if f is not identically zero. That is., $f \neq 0$ and $f(mn) = f(m).f(n)$ whenever $(m, n) = 1$.

(ii) An arithmetic function f is called **completely multiplicative function** if f is not identically zero and $f(mn) = f(m).f(n)$ for all m, n.

2.2.6 Note: Every completely multiplicative function is multiplicative but the converse is not true.

Consider the example: The Mobius function μ is multiplicative but not completely multiplicative.
Suppose $(m, n) = 1$. Then m and n have no common prime factor.
Case-(i): If m, n are square free, then $m = p_1p_2 \ldots p_k$ and $n = q_1q_2 \ldots q_s$ for some distinct primes p_i's and q_j's
$\Rightarrow m.n = p_1p_2 \ldots p_k\, q_1q_2 \ldots q_s$ is also square free.
Now $\mu(m) = (-1)^k$, $\mu(n) = (-1)^s$, $\mu(m.n) = (-1)^{k+s}$.
Hence $\mu(m.n) = \mu(m).\mu(n)$.
Case-(ii): Suppose either m and n has a prime square factor.
Then m.n has a square factor.
Now m, n has a square factor $\Rightarrow \mu(m) = 0$ or $\mu(n) = 0 \Rightarrow \mu(m).\mu(n) = 0$.
Since mn has a square factor, we have $\mu(mn) = 0$. Hence $\mu(mn) = \mu(m).\mu(n)$.

Therefore μ is multiplicative.
To see that μ is not completely multiplicative, take $m = 2$, $n = 2$.
Then $\mu(mn) = \mu(2^2) = 0$ (since 2^2 is not square free)
$\mu(m).\mu(n) = \mu(2).\mu(2) = (-1)(-1) = 1$.
Therefore $\mu(mn) = \mu(4) \neq \mu(2)\mu(2) = \mu(m).\mu(n)$
This shows that μ is not completely multiplicative.

2.2.7 Example: Let $f_\alpha(n) = n^\alpha$, where α is a fixed real or complex number. This function is completely multiplicative. In particular, the unit function $u = f_0$ is completely multiplicative. We denote the function f_α by N^α and call it as the power function.

2.2.8 Example: The Euler totient function $\varphi(n)$ is multiplicative but not completely multiplicative.
(i) In theorem 1.5.16 of lesson 1, we proved that $\varphi(m.n) = \varphi(m).\ \varphi(n)$ is $(m, n) = 1$.
Therefore φ is multiplicative.

(ii) Take $m = 2, n = 2$ then $\varphi(mn) = \varphi(4) = \sum_{\substack{k=1 \\ (k,4)=1}}^{4} 1 = 2$.

$\varphi(m) = \varphi(2) = 1$, $\varphi(n) = \varphi(2) = 1$. Therefore $\varphi(mn) = 2 \neq 1 = \varphi(m).\ \varphi(n)$.

Hence φ is not completely multiplicative.

2.2.9 Theorem: If f is multiplicative, then $f(1) = 1$.

Proof: Let f be multiplicative. Then f is not identically zero.
(by definition of multiplicative function)

This implies that $f(n) \neq 0$ for some n.

Also $f(mn) = f(m).f(n)$ if $(m, n) = 1$.

Consider $f(n) = f(1.n) = f(1).f(n)$ (since $(1, n) = 1$).

$\Rightarrow f(1).f(n) - f(n) = 0$

$\Rightarrow (f(1) - 1)f(n) = 0$

$\Rightarrow f(1) - 1 = 0$ (since $f(n) \neq 0$) $\Rightarrow f(1) = 1$.

Therefore $f(1) = 1$.

2.2.10 Theorem: Given $f(1) = 1$. Then
(i) f is multiplicative
$\Rightarrow f(p_1^{\alpha_1}.p_2^{\alpha_2} \dots p_r^{\alpha_r}) = f(p_1^{\alpha_1}) \dots f(p_r^{\alpha_r})$ for all primes p_i and for all integers $\alpha_i \geq 1$. [In other words, if f is a multiplicative function, then f is completely determined by the values at prime powers]
(ii) converse of (i) is true.

(iii) Suppose f is multiplicative. Then f is completely multiplicative $\Rightarrow f(p^{\alpha}) = (f(p))^{\alpha}$ for all primes p and for all integers $\alpha \geq 1$. [In other words, if f is completely multiplicative, then f is completely determined by its values at prime numbers]

(iv) If f is multiplicative and $f(p^{\alpha}) = (f(p))^{\alpha}$ for all primes p and for all integers $\alpha \geq 1$, then f is completely multiplicative.

2.2.11 Theorem: If f and g are multiplicative, so is their Dirichlet product $f * g$. That is, $f * g$ is multiplicative.

2.2.12 Note: The Dirichlet product of two completely multiplicative functions need not be completely multiplicative.

2.2.13 Theorem: If both g and $f * g$ are multiplicative, then f is also multiplicative.

2.2.14 Note: The function I (defined by $I(n) = 1$ if $n = 1$ and $I(n) = 0$, otherwise) is completely multiplicative.

For this take n, m. If $n = 1, m = 1$, then $I(nm) = I(1) = 1 = 1.1 = I(n).I(m)$

Suppose one of m or n is > 1.

Then $mn > 1$ and $I(n) = 0$ or $I(m) = 0 \Rightarrow I(n).I(m) = 0$.

Now $mn > 1 \Rightarrow I(mn) = 0 = I(n).I(m)$. Hence I is completely multiplicative.

2.2.15 Theorem: If g is multiplicative, then its Dirichlet inverse g^{-1} is also multiplicative.

Proof: Given that g is multiplicative. By Note 2.2.14, $g^{-1} * g = I$ is multiplicative.

Now by Theorem 2.2.13, g^{-1} is multiplicative.

2.2.16 Theorem: Let f be multiplicative.

Then f is completely multiplicative $\Leftrightarrow f^{1}(n) = \mu(n).f(n)$ for all $n \geq 1$.

2.2.17 Example: The inverse of Euler's φ function.

Since $\varphi = \mu * N$ we have $\varphi^{-1} = \mu^{-1} * N^{-1}$.

But $N^{-1} = \mu N$ since N is completely multiplicative, so $\varphi^{-1} = \mu^{-1} * \mu N = u * \mu N$.

Thus $\varphi^{-1}(n) = \sum_{d \mid n} d\mu(d)$.

2.2.18 Problem: Show that $\varphi^{-1}(n) = \prod_{p \mid n}(1 - p)$, where φ is the Euler totient function. [Here $\varphi(n) = \sum_{k=1, (k,n)=1}^{n} 1$].

2.2.19 Theorem: If f is multiplicative, then $\sum_{d|n} \mu(d).f(d) = \prod_{p|n}(1-f(p))$.

2.3 LIOUVILLE'S AND DIVISOR FUNCTIONS

2.3.1 Definition: The **Liouville's function** λ is defined as

$$\lambda(n) = \begin{cases} 1 & \text{if } n = 1 \\ (-1)^{\alpha_1+\alpha_2+\ldots+\alpha_k} & \text{if } n = p_1^{\alpha_1}.p_2^{\alpha_2}\ldots p_k^{\alpha_k} \end{cases}$$

where $p_1, p_2, \ldots, p_k$ are distinct prime numbers and $\alpha_i \geq 1$ for all i.

2.3.2 Note: (i) Observe the table.

n	1	2	3	4	5	6	7	8	9	10
λ (n)	1	-1	-1	1	-1	1	-1	-1	1	1

(ii) The Liouville's function is completely multiplicative.

2. 3. 3 Note: We know that $\lambda(n)$ is completely multiplicative but

$g(n) = \sum_{d|n} \lambda(d) = g(n)$ is not completely multiplicative.

Verification: Let $n = p^\alpha$ for some integer α

In a contrary way, suppose g(n) is completely multiplicative.

Now $g(p) = \sum_{d|p} \lambda(d) = \lambda(1) + \lambda(p) = 1 + (-1) = 0$

$$(g(p))^\alpha = (0)^\alpha = 0 \quad \ldots \text{(i)}$$

Consider $g(p^\alpha) = \sum_{d\,|\,p^\alpha} \lambda(d)$

$$= \lambda(1) + \lambda(p) + \ldots + \lambda(p^\alpha)$$

$$= 1 + (-1) + (-1)^2 + \ldots + (-1)^\alpha$$

$$= \begin{cases} 1 & \text{if } \alpha \text{ is even} \\ 0 & \text{if } \alpha \text{ is odd} \end{cases} \quad \ldots \text{(ii)}$$

If α is even, then from (i) and (ii), we get $(g(p))^\alpha = 0 \neq 1 = g(p^\alpha)$

Hence g is not completely multiplicative.

2.3.4 Theorem: For every $n \geq 1$, we have $\sum_{d|n} \lambda(d) = \begin{cases} 1 & \text{if } n \text{ is a square} \\ 0 & \text{otherwise} \end{cases}$

Also $\lambda^{-1}(n) = |\mu(n)|$ for all n.

Proof: Write $g(n) = \sum_{d|n} \lambda(d)$. Now g is multiplicative.

So to determine $g(n)$, we need only to compute $g(p^\alpha)$ for prime power.

Consider $g(p^\alpha) = \sum_{d|p^\alpha} \lambda(d)$

$$= \lambda(1) + \lambda(p) + \ldots + \lambda(p^\alpha)$$

$$= 1 + (-1) + (-1)^2 + .. + (-1)^\alpha$$

$$= \begin{cases} 1 & \text{if } \alpha \text{ is even} \\ 0 & \text{if } \alpha \text{ is odd} \end{cases} \quad \ldots. \text{(i)}$$

Suppose $n = \prod_{i=1}^{k} p_i^{a_i}$. Then $g(n) = \prod_{i=1}^{k} g(p_i^{a_i})$ ... (ii)

Suppose at least one a_i is odd.

Then $g(p_i^{a_i}) = 0$ (by (i))

$\Rightarrow g(n) = 0$ (by (ii)).

Suppose the other case that all a_i's are even.

Then $g(p_i^{a_i}) = 1$ (by (i))

$\Rightarrow g(n) = \prod g(p_i^{a_i}) = \prod 1 = 1.$

[All a_i's are even $\Leftrightarrow$ $a_i = 2b_i$ for some b_i's

$\Leftrightarrow n = (p_1^{a_1} . p_2^{a_2} \ldots p_k^{a_k}) = (p_1^{b_1} . p_2^{b_2} \ldots p_k^{b_k})^2$ for some b_i's.

Therefore each a_i is even $\Leftrightarrow$ n is a square].

This shows that $g(n) = \begin{cases} 1 \text{ if all } a_i\text{'s are even; that is } n \text{ is a square.} \\ 0 \text{ otherwise.} \end{cases}$

2.3.5 Note: We know that $\lambda^{-1} = \mu\lambda$ (see Theorem 2.2.16)

So $\lambda^{-1}(n) = \mu(n).\lambda(n)$

$= \mu(n).\ \mu(n). = \mu^2(n) = |\mu(n)|$

$\Rightarrow \lambda^{-1}(n) = |\mu(n)|$ for all n.

[If n has a square $p_i^{\alpha_i}$, then $\mu(n) = 0$. If $\mu(n) \neq 0$, then n is square free.

$\mu(p_1.p_2. \dots .p_k) = (-1)^k \Rightarrow \lambda(p_1.p_2. \dots .p_k) = (-1)^k$. Therefore in this case, $\mu = \lambda$.].

2.3.6 Definition: For real or complex α and any integer $n \geq 1$, we define

$\sigma_\alpha(n) = \sum_{d|n} d^\alpha$. (The sum of the α^{th} powers of the divisors of n).

The functions σ_α defined above are called **divisor functions**.

2.3.7 Note: (i) Consider $(N^\alpha * u)(n) = \sum_{d|n} N^\alpha(d).u(\frac{n}{d})$

$$= \sum_{d|n} (N(d))^\alpha.1 = \sum_{d|n} d^\alpha = \sigma_\alpha(n).$$

Therefore $\sigma_\alpha = N^\alpha * u$.

(ii) The divisor functions are multiplicative because $\sigma_\alpha = u * N^\alpha$, the Dirichlet product of two multiplicative functions.

When $\alpha = 0$, $\sigma_0(n)$ is the number of divisors of n. This is often denoted by $d(n)$.

When $\alpha = 1$, $\sigma_1(n)$ is the sum of divisors of n. This is often denoted by $\sigma(n)$.

Since σ_α is multiplicative we have $\sigma_\alpha\left(p_1^{a_1} \dots p_k^{a_k}\right) = \sigma_\alpha\left(p_1^{a_1}\right) \dots \sigma_\alpha\left(p_k^{a_k}\right)$.

To compute $\sigma_\alpha(p^a)$ we note that the divisors of a prime power p^a are $1, p, p^2, \dots, p^a$.

Hence $\sigma_\alpha(p^a) = 1^\alpha + p^\alpha + p^{2\alpha} + \dots P^{a\alpha} = \begin{cases} \dfrac{p^{\alpha(a+1)} - 1}{p^\alpha - 1} & \text{if } \alpha \neq 0 \\ a+1 \text{ if } \alpha = 0 \end{cases}$

2.3.8 Theorem: For $n \geq 1$, we have $\sigma_\alpha^{-1}(n) = \sum_{d|n} d^\alpha.\mu(d).\mu(\frac{n}{d})$.

2.4 GENERALIZED CONVOLUTIONS AND FORMAL POWER SERIES

Throughout this section F denotes a real or complex valued function defined on $(0, +)$ such that $F(x) = 0$ for $0 < x < 1$

2.4.1 Definition: Let $F(x)$ be a real or complex valued function defined on $(0,)$ such that $F(x) = 0$, for $0 < x < 1$. For any arithmetic function $\alpha(n)$,
we define the generalized convolution of α and F as $(\alpha \circ F)(x) = \sum_{n \leq x} \alpha(n).F(\frac{x}{n})$ where

n is a natural number.

3)

2.4.2 Example: (i) $(\alpha \circ F)(3) = \sum_{n \le 3} \alpha(n).F(\frac{3}{n})$.

$$= \alpha(1)F(3) + \alpha(2)F(\tfrac{3}{2}) + \alpha(3)F(1)$$

(ii) $(\alpha \circ F)(4.7) = \sum_{n \le 4.7} \alpha(n).F(\frac{4.7}{3}) = \alpha(1)F(4.7) + \alpha(2)F(\frac{4.7}{2}) + \alpha(3)F(\frac{4.7}{3}) + \alpha(4)F(\frac{4.7}{4})$

2.4.3 Definition: Let f be an arithmetical function.

Suppose $F(x) = \begin{cases} 0 & \text{if } x \text{ is not an integer} \\ f(x) & \text{if } x \text{ is an integer} \end{cases}$

Then $(\alpha \circ F)(x) = \sum_{n \le x} \alpha(n).F(\frac{x}{n})$

$$= \begin{cases} \sum_{n \le x} \alpha(n).f(\frac{x}{n}) & \text{if } \frac{x}{n} \text{ is an integer} \\ 0 & \text{if } \frac{x}{n} \text{ is not an integer} \end{cases}$$

If $\frac{x}{n}$ is an integer (in this case x must be an integer)

Then $(\alpha \circ F)(x) = \sum_{n \le x} \alpha(n).f(\frac{x}{n}) = \sum_{n|x} \alpha(n).f(\frac{x}{n}) = (\alpha * f)(x)$

Therefore $(\alpha \circ F)(x) = (\alpha * f)(x)$

Hence the operation $\circ$ is generalized convolution of Dirichlet product convolution "*".

2.4.4 Theorem: Associative property relating $\circ$ and $*$.

For any two arithmetical functions g and h, we have $g \circ (h \circ F) = (g * h) \circ F$.

Self Assessment Question 1: *The identity function $I(n) = \left[\frac{1}{n}\right]$ for the Dirichlet product (Convolution) is also a left identity for the operation $\circ$.*

2.4.5 Theorem: Generalized Inversion Formula: If α has a Dirichlet inverse α^{-1}, then the equation $G(x) = \sum_{n \le x} \alpha(n).F(\frac{x}{n}) \Leftrightarrow F(x) = \sum_{n \le x} \alpha^{-1}(n).G(\frac{x}{n})$.

2.4.6 Corollary: Generalized Mobius Inversion Formula: Let α be the arithmetical and its Dirichlet inverse α^{-1} exists. If α is completely multiplicative, then prove that

$$G(x) = \sum_{n\le x}\alpha(n).F(\tfrac{x}{n}) \Leftrightarrow F(x) = \sum_{n\le x}\mu(n).\alpha(n).G(\tfrac{x}{n}).$$

2.4.7 Definition: An infinite series of the form $\sum_{n=0}^{\infty} a(n)x^n = a(0) + a(1)x + a(2)x^2 + \ldots + a(n)x^n + \ldots$ is called a **power series** in x. Both x and the coefficients a(n) are real or complex numbers.

2.4.8 Note: (i). To each power series there corresponds a radius of convergence $r \ge 0$ such that the series converges absolutely if $|x| < r$ and diverges if $|x| > r$. (The radius r can be +)

(ii). We consider power series from a different point of view. We call them **formal** power series to distinguish them from the ordinary power series.
The object of interest is the sequence of coefficients (a(0), a(1), ...,a(n),.......).

(iii). The symbol x^n is simply a device for locating the position of the n^{th} coefficient a(n). The coefficient a(0) is called the **constant coefficient** of the series.

2.4.9 Definition: If A(x) and B(x) are two formal power series, say $A(x) = \sum_{n=0}^{\infty} a(n)x^n$ and $B(x) = \sum_{n=0}^{\infty} b(n)x^n$, then we define

Equality : A(x) = B(x) means that a(n) = b(n) for all $n \ge 0$.

Sum : $A(x) + B(x) = \sum_{n=0}^{\infty}(a(n)+b(n))x^n$.

Product : $A(x)\cdot B(x) = \sum_{n=0}^{\infty} c(n)x^n$, where $c(n) = \sum_{k=0}^{n} a(k)b(n-k)$. (Cauchy product)

2.4.10 Definition: A formal power series is called a **formal polynomial** if all its coefficients are 0 from some point on.

2.4.11 Note: For each formal power series $A(x) = \sum_{n=0}^{\infty} a(n)x^n$ with constant coefficient $a(0) \ne 0$ there is a uniquely determined formal power series $B(x) = \sum_{n=0}^{\infty} b(n)x^n$ such that

$A(x)\cdot B(x) = 1$. Its coefficients can be determined by solving the infinite system of equations

$a(0)\, b(0) = 1$

$a(0)\, b(1) + a(1)\, b(0) = 0$

$a(0)\, b(2) + a(1)\, b(1) + a(2)\, b(0) = 0,$

....

....

in succession for b(0), b(1), b(2),......The series B(x) is called the **inverse** of A(x) and is denoted by $A(x)^{-1}$ or by 1/A(x).

2.4.12 Definition The series $A(x) = 1 + \sum_{n=1}^{\infty} a^n x^n$ is called **a geometric series.** Here a is an arbitrary real or complex number. Its inverse is the formal polynomial B(x) = 1 - ax. In other words, we have $\dfrac{1}{1-ax} = 1 + \sum_{n=1}^{\infty} a^n x^n$

2.5 BELL SERIES AND DERIVATIVES OF ARITHMETICAL FUNCTIONS

2.5.1 Definition : Let f be an arithmetical function and a p, prime. Then $f_p(x)$, the formal power series defined by $f_p(x) = \sum_{n=1}^{\infty} f(p^n)x^n$, is called the **Bell series of f modulo p.**

2.5.2 Example : Consider the Mobius function μ.

Since $\mu(p) = -1$ and $\mu(p^n) = 0$ for $n \ge 2$, we have $\mu_p(x) = 1 - x$.

2.5.3 Example : Consider the Euler totient function φ.

Since $\varphi(p^n) = p^n - p^{n-1}$ for $n \ge 1$ we have

$$\varphi_p(x) = 1 + \sum_{n=1}^{\infty}(p^n - p^{n-1})x^n = \sum_{n=0}^{\infty} p^n x^n - x\sum_{n=0}^{\infty} p^n x^n$$

$$= (1-x)\sum_{n=0}^{\infty} p^n x^n = \frac{1-x}{1-px}.$$

Self Assessment Question 2: *Let f and g be multiplicative functions. Then verify that* $f = g \Leftrightarrow f_p(x) = g_p(x)$ *for all primes p.*

2.5.4 Theorem : For any two arithmetical functions f and g let $h = f * g$. Then for every prime p we have $h_p(x) = f_p(x)g_p(x)$.

2.5.5 Example :Since $\mu^2(n) = \lambda^{-1}(n)$ the Bell series of μ^2 modulo p

is $\mu_p^{\,2}(x) = \dfrac{1}{\lambda_p(x)} = 1 + x$.

2.5.6 Example : Since $\sigma_\alpha = N^\alpha * u$ the Bell series of σ_α modulo p is

$$(\sigma_\alpha)_p(x) = N_p^{\ \alpha}(x)\, u_p(x) = \frac{1}{1-p^\alpha x}\cdot\frac{1}{1-x} = \frac{1}{1-\sigma_\alpha(p)x + p^\alpha x^2}.$$

2.5.7 Definition: For any arithmetical function f, we define its derivative f^1 to be an arithmetical function given by the equation $f^1(n) = f(n).\log n$ for $n \geq 1$.

2.5.8 Example: (i) Consider $I(n) = \begin{cases} 0 & \text{if } n > 1 \\ 1 & \text{if } n = 1 \end{cases}$

We know that $\log 1 = 0$.

Therefore $I(n).\log n = 0$ for all $n \geq 1$. By definition of derivative of arithmetical function we have $I^1(n) = I(n).\log n = 0$ for all $n \geq 1$.

(ii) Consider $u(n)$ the unitary function.

($u(n) = 1$ for all $n \geq 1$). Now $u^1(n) = u(n).\log n = \log n$.

Self Assessment Question 3: $\log n = (\wedge * u)(n)$ where $\wedge$ is Mangoldt function.

2.5.9 Theorem: If f and g are arithmetical functions, then

(i) $(f+g)^1 = f^1 + g^1$

(ii) $(f*g)^1 = f^1 * g + f * g^1$

(iii) $(f^{-1})^1 = -f^1 * (f*f)^{-1}$ provided $f(1) \neq 0$.

Proof: (i) By the definition, $f^1(n) = f(n).\log n$.

Let f and g are arithmetical functions. Consider

$(f+g)^1(n) = (f+g)(n)\log n$

$= (f(n) + g(n))\log n = f(n)\log n + g(n)\log n = f^1(n) + g^1(n)$.

Therefore $(f+g)^1(n) = f^1(n) + g^1(n)$.

(ii) Let d be the divisor of n.

Then $n = d(\frac{n}{d}) \Rightarrow \log n = \log d + \log \frac{n}{d}$ ... (i)

$$(f*g)^1 = \left(\sum_{d|n} f(d).g(\tfrac{n}{d})\right)^1$$

$$= \left(\sum_{d|n} f(d).g(\tfrac{n}{d})\right) \log n$$

$$= \left(\sum_{d|n} f(d).g(\tfrac{n}{d})\right)(\log d + \log(\tfrac{n}{d})) \quad \text{(form above)}$$

$$= \sum_{d|n}(f(d).\log d)g(\tfrac{n}{d}) + \sum_{d|n} f(d)(g(\tfrac{n}{d}).\log(\tfrac{n}{d}))$$

$$= \sum_{d|n} f^1(d).g(\tfrac{n}{d}) + \sum_{d|n} f(d).g^1(\tfrac{n}{d}) = (f^1*g)(n) + (f*g^1)(n)$$

Therefore $(f*g)^1(n) = (f^1*g)(n) + (f*g^1)(n)$

(iii) Let f be an arithmetical function and f^1 is its Dirichlet inverse.

Now $(f*f^1)(n) = I(n)$

$\Rightarrow (f*f^1)^1(n) = I^1(n) = \log n\, I(n) = 0$

$\Rightarrow (f*f^{-1})^1(n) = 0$

$\Rightarrow 0 = (f*f^1)^1(n) = (f^1*f^{-1})(n) + (f*(f^{-1})^1)(n)$ (by (ii))

$\Rightarrow (f*(f^{-1})^1)(n) = -(f^1*f^{-1})(n)$

$\Rightarrow f*(f^1)^1 = -(f^1*f^1)$.

By multiplying on both sides with f^1 (with respect to $*$), we get

$(f^1)^1 = f^1*(-f^1*f^{-1})$

$= -(f^1*f^1)*f^{-1}$

$= -(f^1*f^1)*f^{-1} = -(f^1*(f^{-1}*f^{-1})) = -f^1*(f*f)^{-1}$.

2.6 THE SELLBERG IDENTITY

Till 1950 people believed that the prime number theorem could not be proved without the help of the properties of the zeta function and without recourse to complex function theory. In 1949, the Norwegian Mathematician Atle Selberg discovered a purely Arithmetical proof which was a great surprise. His paper "An elementary proof of the prime number theorem" did not use the *methods of modern analysis, indeed its content is exceedingly difficult. Selberg was awarded a fields medal which is considered as a Nobel prize in Mathematics, at the 1950 International congress of Mathematicians for his work in this area.*

2.6.1 Theorem: (The Selberg Identity) For $n \geq 1$,

we have $\wedge(n)\log n + \sum_{d|n} \wedge(d)\wedge(\frac{n}{d}) = \sum_{d|n} \mu(d)\log^2(\frac{n}{d})$.

Proof: We know that $\log n = (\wedge * u)(n)$ (refer S.A.Q 3)

$\Rightarrow u(n)\log n = (\wedge * u)(n)$ (since $u(n) = 1$)

$\Rightarrow u^1(n) = (\wedge * u)(n)$ ... (i)

By differentiating on both sides, we get

$u^{11}(n) = (\wedge * u)^1(n)$

$= (\wedge^1 * u)(n) + (\wedge * u^1)(n)$

$= (\wedge^1 * u)(n) + (\wedge * (\wedge * u))(n)$ (by (i))

$= (\wedge^1 * u)(n) + ((\wedge * \wedge)) * u)(n)$

By multiplying on both sides (on right) with $\mu = u^{-1}$ (refer Note 2.1.10) we get

$(u^{11} * \mu)(n) = \wedge^1(n) + (\wedge * \wedge)(n)$

$\Rightarrow \sum_{d|n} \mu(d)u^{11}(\frac{n}{d}) = \wedge(n)\log n + \sum_{d|n} \wedge(d)\wedge(\frac{n}{d})$

$\Rightarrow \sum_{d|n} \mu(d)\log^2(\frac{n}{d}) = \wedge(n)\log n + \sum_{d|n} \wedge(d)\wedge(\frac{n}{d})$

[Verification for $u^{11}(\frac{n}{d}) = \log^2(\frac{n}{d})$ is given below]

Since $u^{11}(\frac{n}{d}) = (u^1(\frac{n}{d}))^1$

$= (u(\frac{n}{d}).\log(\frac{n}{d}))^1$

$= (u(\frac{n}{d}).\log(\frac{n}{d}))\log(\frac{n}{d})$

$= u(\frac{n}{d}).\log^2(\frac{n}{d}) = \log^2(\frac{n}{d})$ (since $u(n) = 1$ for all n)

2.7 SUMMARY

We dealt with the Dirichlet product of arithmetical functions and their inversion formula. We introduced Mangoldt function and Liouvllie's function, related results discussed.

This lesson also dealt with Arithmetical functions such as $\lambda(n)$ and divisor functions $\sigma_\alpha(n)$. We provided the properties inter relations of various functions and their applications. It is observed that the sum for $\varphi(n)$ can be expressed as a product extended over the distinct prime divisors of n; also the properties of the product formula obtained. We also discussed Dirichlet multiplication, a concept which helps to classify inter relationships between various arithmetical functions. Selberg identity is derived from the concept of derivative which is sometimes used as the starting point of an elementary proof of the prime number theorem.

2.8 TECHNICAL TERMS

Dirichlet product: For any two arithmetical functions f and g, the Dirichlet product is defined by the equation $f*g = \sum_{d|n} f(d).g(\frac{n}{d})$ where the summation is over all positive divisors d of n.

Inversion formula: $f(n) = \sum_{d|n} g(d) \Leftrightarrow g(n) = \sum_{d|n} f(d).\mu(\frac{n}{d})$.

Multiplicative function: An arithmetical function f is multiplicative if f is not identically zero. That is., $f \neq 0$ and $f(mn) = f(m).f(n)$ whenever $(m, n) = 1$.

Liouville's function: $\lambda(n) = \begin{cases} 1 & \text{if } n = 1 \\ (-1)^{\alpha_1+\alpha_2+\ldots+\alpha_k} & \text{if } n = p_1^{\alpha_1}.p_2^{\alpha_2}\ldots p_k^{\alpha_k} \end{cases}$

where $p_1, p_2, \ldots, p_k$ are distinct prime numbers and $\alpha_i \geq 1$ for all i.

2.9 ANSWERS TO SELF ASSESSMENT QUESTIONS

1: Consider

$$(I \circ F)(x) = \sum_{k \leq x} I(k).F(\tfrac{x}{k})$$

$$= I(1)F(\tfrac{x}{1}) + \sum_{1<k\leq x} I(k).F(\tfrac{x}{k})$$

$$= F(x) + 0 = F(x) \text{ (since } I(1) = 1 \text{ and } I(n) = 0 \text{ for } n > 1)$$

Therefore $(I \circ F)(x) = F(x)$. Hence I is a left identity.

2: Suppose f = g. Then $f(p^n) = g(p^n)$ for all primes p and all $n \geq 0$. So $f_p(x) = g_p(x)$. Conversely suppose that $f_p(x) = g_p(x)$ for all p, then $f(p^n) = g(p^n)$ for all $n \geq 0$. Since f and g are multiplicative and agree at all prime powers, we have that they agree at all positive integers. So f = g.

3: We know that (by Theorem 2.2.3)

$$\log n = \sum_{d|n} \wedge(d) = \sum_{d|n} \wedge(d).u(\tfrac{n}{d}) \quad (\text{since } u(n) = 1 \text{ for all } n \geq 1)$$

$$= (\wedge * u)(n).$$

Therefore $\log n = (\wedge * u)(n)$.

2.10 MODEL QUESTIONS

1. Define Dirichlet product. Prove that a set of all arithmetical functions f with $f(1) \neq 0$ forms an abelian group with respect to Dirichlet product.
2. State and prove Mobius inversion formula
3. Define Mangoldt function. Prove that for $n \geq 1$, $\log n = \sum_{d|n} \Lambda(d)$.
4. Define Liouville's function and Bell series of f modulo p.
5. State and prove the Selberg's identy.

2.11 REFERENCE BOOKS

1. Chandrasekharan, K. "Introduction to Analytic Number Theory", Springer Verlag .
2. Hardy, G.H. & Wright, E.M. "Introduction to the Theory of Numbers", Fourth Edition, Oxford Publications,
3. Levegue W.J. (1986) "Topics in Number Theory (2 volumes), Addition - Wesley Publ. Co.
4. Rademacher (1964) "Lectures on Elementary Number Theory", New York, Blaisdell Publ. Co.
5. Tom M. Apostol "Introduction to Analytic Number Theory", Springer International Student Edition, Narosa Publishing House, 1995.
6. Uspensky, J.V., and Heaslett, M.A. (1939) "Elementary Number Theory", New York, Mc. Graw - Hill Book. Co.
7. Vinogrador, "Elements of Number Theory", Dover Publications

Name of the Author of this Lesson: **Dr. Kuncham Syam Prasad**

LESSON: 3

ASYMPTOTIC EQUALITY OF FUNCTIONS & EULER'S SUMMATION FORMULA

Objectives

The objectives of this lesson are to:

- introduce the big oh notation
- know about asymptotic equality of functions and some elementary asymptotic formulae
- study the properties of order
- know the significance of Euler's summation formula and related results

Structure

3.0 INTRODUCTION

We describe that the average order of d(n) is log n. Partial sum notation of arithmetical function splays an vital role in the theory of numbers. This lesson aims at the determination of the behavior of the partial sum $\sum_{k\le x} f(k)$ at a function of x especially for large x. We derive a Summation formula of Euler, which gives an exact expression for the error made in an approximation, where the asymptotic value of a partial sum can be obtained by comparing it with an integral.

3.1 PARTIAL SUMS

3.1.1 Definition Let f(n) be an arithmetic function. Then

(i) $\bar{f}(n) = \frac{1}{n}\sum_{k=1}^{n} f(k)$ is called the **arithmetic mean** (for given n).

(ii) $\sum_{k=1}^{n} f(k)$ is called **n^{th} partial sum.**

3.12 Example let f be any arithmetical function defined on N.

Take $n = 3$, then $\sum_{k=1}^{3} f(k)$ denote the 3^{rd} partial sum.

3.1.3 Note If $n \le x < n+1$, then $\sum_{k \le x} f(k) = f(1) + f(2) + \ldots + f(n) = \sum_{k=1}^{n} f(k)$ is called **n^{th} partial sum.** Here it is understood that the index k varies from 1 to [x], the greatest integer not exceeding x.

3.1.4 Example

Take $x = 3.5$, then $n = 3$. Now k varies from 1 to $[3.5] = 3$.

Therefore $\sum_{k \le x} f(k) = f(1) + f(2) + f(3)$

3.2 THE BIG Oh NOTATION

3.2.1 Definition Suppose $g(x) > 0$ for all real values $x \ge a$ and f(x) is a real valued function such that $\frac{f(x)}{g(x)}$ is bounded for $x \ge a$. Then we say that "f(x) is of large order g(x)" or "f(x) is of order g(x)". In this case, we write $f(x) = O(g(x))$ (we read f(x) is big Oh of g(x)).

[Equivalently, we can say that $f(x) = O(g(x))$ if there exists a constant $M > 0$ such that $\left|\frac{f(x)}{g(x)}\right| \le M$ for all $x \ge a$, or $|f(x)| \le M.|g(x)|$ or $|f(x)| \le M.g(x)$ for all $x \ge a$ (since $g(x) > 0$)].

3.2.2 Note (i) $f(x) = h(x) + O\, g(x)$ means that

$f(x) - h(x) = O(g(x)) \Rightarrow |f(x) - h(x)| \le M.g(x)$ for some $M > 0$.

(ii) Suppose $f(t) = O(g(t))$ for $t \ge a$

$\Rightarrow |f(t)| \le M.g(t)$ for $t \ge a$ and for some $M > 0$.

$$\Rightarrow \int_a^x |f(t)|\,dt \le \int_a^x M.g(t)\,dt \Rightarrow \left|\int_a^x f(t)dt\right| \le M\int_a^x g(t)\,dt$$

$$\Rightarrow \int_a^x f(t)dt = O\left(\int_a^x g(t)\,dt\right) \text{ for } x \ge a.$$

Therefore $f(t) = O(g(t))$ for $t \ge a$ implies that $\int_a^x f(t)dt = O\left(\int_a^x g(t)\,dt\right)$ for $x \ge a$.

Self Assessment Question 1: *Show that if $f(x) = O(g(x))$ then $cf(x) = O(g(x))$ for any constant $c>0$.*

3.2.3 Example (i) Write $f(x) = 20x$ and $g(x) = x$.

Then $\dfrac{f(x)}{g(x)} = 20$ which is bounded. Therefore $f(x) = O(g(x))$ or $20x = O(x)$.

(ii) Suppose $f(x) = 10x^2$ and $g(x) = 20x^4$. Then $\dfrac{f(x)}{g(x)} = \dfrac{10x^2}{20x^4} = \dfrac{1}{2x^2} \le 1$

for all $x \ge 1$. Therefore $f(x) = O(g(x))$ or $10x^2 = O(20\,x^4)$.

(iii) Suppose $f(x) = 30x$, $h(x) = 10x$ and $g(x) = x$.

Then $f(x) - h(x) = 30x - 10x = 20x = O(x) = O(g(x))$

$\Rightarrow f(x) - h(x) = O(g(x)) \Rightarrow f(x) = h(x) + O(g(x))$.

3.3 ASYMPTOTIC EQUALITY OF FUNCTIONS

3.3.1 Definition (i) If $\lim_{x\to\infty} \dfrac{f(x)}{g(x)} = 1$ then we say that $f(x)$ and $g(x)$ are of same order (or) $f(x)$ is **asymptotic** to $g(x)$. In this case, we write $f(x) \sim g(x)$ as $x \to \infty$.

(ii) If $\lim_{x\to\infty} \dfrac{f(x)}{g(x)} = 0$, then we say that $f(x)$ is of small order $g(x)$, and we write $f(x) = o(g(x))$. (Here we use small letter o).

3.3.2 Example Write $f(x) = x^3 + x^2 - 5$ and $g(x) = x^3$.

Then $\lim_{x\to\infty} \dfrac{f(x)}{g(x)} = \lim_{x\to\infty} \dfrac{x^3 + x^2 - 5}{x^3} = \lim_{x\to\infty}\left(1 + \dfrac{1}{x} - \dfrac{5}{x^3}\right) = 1$

Therefore $f(x)$ and $g(x)$ are of same order, and so $f(x)$ is asymptotic to $g(x)$.

Self Assessment Question 2: *If $f(x) = x^3 + x^2 - 5$, and $g(x) = x^4$, then $f(x)$ is of small order $g(x)$*

3.3.3 Theorem If $g(x) > 0$ and $\lim_{x\to\infty} \frac{f(x)}{g(x)} = L$ where L is finite, then $f(x)$ is large order of $g(x)$ (that is, $f(x) = O(g(x))$).

Proof: Now $\lim_{x\to\infty} \frac{f(x)}{g(x)} = L$

$\Rightarrow$ given $\varepsilon > 0$, there corresponds x_0 such that $\left|\frac{f(x)}{g(x)} - L\right| < \varepsilon$ for all $x \geq x_0$.

$\Rightarrow \left|\frac{f(x)}{g(x)}\right| < \varepsilon + |L|$ for all $x \geq x_0$.

Let $\varepsilon + |L| = M$. Then $\left|\frac{f(x)}{g(x)}\right| < M$ for all $x \geq x_0$.

$\Rightarrow \frac{f(x)}{g(x)}$ is bounded for all $x \geq x_0$.

By the definition of large order, we have $f(x)$ is of large order $g(x) \Rightarrow f(x) = O(g(x))$.
Hence the theorem.

3.3.4 Corollary If $f(x) > 0$ and $g(x) \sim f(x)$, then $f(x) = O(g(x))$ and $g(x) = O(f(x))$ if $f(x) > 0$.

Proof: Let $f(x) > 0$ and $f(x) \sim g(x)$

Now $\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1$ and $\lim_{x\to\infty} \frac{g(x)}{f(x)} = 1$.

So given $\varepsilon > 0$ there exists x_0 such that $\left|\frac{f(x)}{g(x)}\right| < \varepsilon + 1$ and $\left|\frac{g(x)}{f(x)}\right| < \varepsilon + 1$ for $x \geq x_0$.

$\Rightarrow f(x) = O(g(x))$ and $g(x) = O(f(x))$ (by definition)

3.3.5 Corollary If $g(x) > 0$ and $f(x) = o(g(x))$, then $f(x) = O(g(x))$.

Proof: Suppose $g(x) > 0$, and $f(x)$ are two real valued functions and $f(x) = o(g(x))$.

Then $\lim_{x\to\infty} \frac{f(x)}{g(x)} = 0$ ... (i)

Now we have to prove that $f(x) = O(g(x))$.

By (i), we have that given $\varepsilon > 0$ there exists x_0 such that $\left|\frac{f(x)}{g(x)}\right| < \varepsilon$ for all $x \geq x_0$ $\Rightarrow f(x) = O(g(x))$.

3.3.6 Theorem (i) $O(g(x)) + O(g(x)) = O(g(x))$
(ii) If $f(x) = O(g(x))$ then $O(f(x)) + O(g(x)) = O(g(x))$

Proof: (i) Let f_1 and f_2 are two real valued functions and $g(x) > 0$ is a real valued function such that $f_1(x) = O(g(x))$ and $f_2(x) = O(g(x))$.

By definition of large order, there exist numbers $M_1 > 0$ and $M_2 > 0$ such that $\left|\frac{f_1(x)}{g(x)}\right| \le M_1$

and $\left|\frac{f_2(x)}{g(x)}\right| \le M_2$. Write $M = M_1 + M_2$.

Consider $\left|\frac{f_1(x)+f_2(x)}{g(x)}\right| \le \left|\frac{f_1(x)}{g(x)}\right| + \left|\frac{f_2(x)}{g(x)}\right| \le M_1 + M_2 = M.$

$\Rightarrow \left|\frac{f_1(x)+f_2(x)}{g(x)}\right|$ is bounded $\Rightarrow f_1(x) + f_2(x) = O(g(x))$

$\Rightarrow O(g(x)) + O(g(x)) = O(g(x)).$

(ii) Let f_1 and f_2 be two real valued functions and $g(x) > 0$ is a real valued function such that $f_1(x) = O(f(x))$ and $f_2(x) = O(g(x))$.

Then by def. $\left|\frac{f_1(x)}{f(x)}\right| \le M_1$ where M_1 is a positive number $\Rightarrow |f_1(x)| \le M_1 |f(x)|$ ... (i)

And also $\left|\frac{f_2(x)}{g(x)}\right| \le M_2$ where M_2 is a positive number. $\Rightarrow |f_2(x)| \le M_2 |g(x)|$ ... (ii).

Given that $f(x) = O(g(x))$, we have that

Since $\left|\frac{f(x)}{g(x)}\right| \le M$ where M is a positive number.

$\Rightarrow |f(x)| \le M.|g(x)|$ ... (iii)

Consider $|f_1(x) + f_2(x)| \le |f_1(x)| + |f_2(x)|$

$\le M_1|f(x)| + M_2|g(x)|$ (by (i) and (ii))

$\le M_1|g(x)|.M + M_2|g(x)|$ (by (iii))

$= |g(x)|(M_1.M + M_2)$

$\Rightarrow \left|\frac{f_1(x)+f_2(x)}{g(x)}\right| \le M^*$ where $M^* = M_1.M + M_2$.

$\Rightarrow \left|\frac{f_1(x)+f_2(x)}{g(x)}\right|$ is bounded.

$\Rightarrow f_1(x) + f_2(x) = O(g(x)).$

$\Rightarrow O(f(x)) + O(g(x)) = O(g(x))$

Self Assessment Question 3: *Verify whether* $O(O(f(x)) = O(f(x))$.

3.4 EULER'S SUMMATION FORMULA

3.4.1 Theorem Euler Summation Formula: If $f(x)$ has continuous derivative on $[a, b]$ where $0 < a < b$ (that is $f^{1}(x)$ is in $[a, b]$, $0 < a < b$), then

$$\sum_{a<n\le b} f(n) = \int_a^b f(t)dt + \int_a^b (t-[t])f^{1}(t)dt + f(b)([b] - b) - f(a)([a] - a).$$

Proof: Suppose $f(x)$ has continuous derivative and $f^{1}(x)$ is in the closed interval $[a, b]$ where $0 < a < b$.

Let $[a] = m$ and $[b] = k$ (that is, m is the largest integer less than or equal to a and similarly for k).

Then $\sum_{a<n\le b} f(n) = \sum_{m<n\le k} f(n) = \sum_{n=m+1}^{k} f(n)$ ... (i)

Suppose $(n - 1)$ and n are two integers in $[a, b]$ and t lies between $(n - 1)$ and n.

Then $\int_{n-1}^{n} [t]f^{1}(t)dt = \int_{n-1}^{n} (n-1)f^{1}(t)dt$

$= (n - 1) \int_{n-1}^{n} f^{1}(t)dt = (n - 1)\,[f(t)]_{n-1}^{n}$

$= (n - 1)(f(n) - f(n - 1)) = n.f(n) - f(n) - (n - 1).f(n - 1)$ ... (ii)

Taking summation with $n = m + 1, m + 2, \ldots, k$ on both sides of (ii), we get

$$\sum_{n=m+1}^{k} \int_{n-1}^{n} [t]f^{1}(t)dt = \sum_{n=m+1}^{k} \{nf(n) - f(n) - (n-1)f(n-1)\}$$

$$\Rightarrow \sum_{n=m+1}^{k} \int_{n-1}^{n} [t]f^{1}(t)dt = k.f(k) - m.f(m) - \sum_{n=m+1}^{k} f(n)$$

$$\Rightarrow \sum_{n=m+1}^{k} f(n) = k.f(k) - m.f(m) - \int_{m}^{k} [t]f^{1}(t)dt$$

$$= k.f(k) - m.f(m) - \int_{a}^{b} [t]f^{1}(t)dt$$

$$= k.f(b) - m.f(a) - \int_a^b [t]\, f^1(t)dt \quad \ldots (iii)$$

Now $\int_a^b f(t)dt = \int_a^b 1 \cdot f(t)dt = b\, f(b) - a\, f(a) - \int_a^b t\, f^1(t)dt$ (integration by parts)

$$\Rightarrow \int_a^b f(t)dt - b\, f(b) + a\, f(a) + \int_a^b t\, f^1(t)dt = 0 \quad \ldots (iv)$$

from (iii), $\sum_{n=m+1}^{k} f(n) = k.f(b) - m.f(a) - \int_a^b [t]\, f^1(t)dt + 0.$

Now replace '0' by L.H.S of (iv), we get

$$\sum_{n=m+1}^{k} f(n) = [k.f(b) - m.f(a) - \int_a^b [t]\, f^1(t)dt\,] + [\int_a^b f(t)dt - b\, f(b) + a\, f(a) + \int_a^b t\, f^1(t)dt\,] \ldots (v).$$

Now $\sum_{a<n\le b} f(n) = \sum_{n=m+1}^{k} f(n)$ (by (i))

$$= \int_a^b f(t)dt + \int_a^b (t-[t])f^1(t)dt + f(b)(k - b) - f(a)(m - a) \text{ (by (v))}$$

$$\Rightarrow \sum_{a<n\le b} f(n) = \int_a^b f(t)dt + \int_a^b (t-[t])f^1(t)dt + f(b)([b] - b) - f(a)([a] - a).$$

This completes the proof.

3.4.2 Note $C = \lim_{n\to\infty}\left(1+\frac{1}{2}+\frac{1}{3}+\ldots+\frac{1}{n}-\log n\right) = \lim_{n\to\infty}\left[\left(\sum_{k=1}^{n}\frac{1}{k}\right)-\log n\right]$

$= \lim_{n\to\infty}\left[\left(\sum_{k\le n}\frac{1}{k}\right)-\log n\right]$ is called **Euler's constant.**

3.5 SOME ELEMENTARY ASYMPTOTIC FORMULAE

3.5.1 Theorem If $x \ge 1$, then $\sum_{n\le x}\frac{1}{n} = \log x + C + O(\frac{1}{x})$.

Proof: Consider $f(t) = \frac{1}{t}$. We know that $\int_1^x f(t)dt = \int_1^x \frac{1}{t}dt = \log x$.

Also $f^1(t) = \left(\frac{1}{t}\right)^1 = -\frac{1}{t^2}$ which is continuous in $[1, x]$.

By Euler's summation formula

$$\sum_{1<n\le x} f(n) = \sum_{1<n\le x} \frac{1}{n} = \int_1^x \frac{1}{t}dt + \int_1^x (t-[t])\left(\frac{-1}{t^2}\right)dt + ([x]-x)\frac{1}{x} - f(1)([1]-1) \text{ (by theorem 3.4.1)}$$

$$= \log x - \int_1^x \frac{t-[t]}{t^2}dt + \frac{[x]-x}{x} - 0.$$

$$\Rightarrow \sum_{n\le x}\frac{1}{n} = \frac{1}{1} + \sum_{1<n\le x}\frac{1}{n} = 1 + \log x - \int_1^x \frac{t-[t]}{t^2}dt + \frac{[x]-x}{x}$$

$$= 1 + \log x - \int_1^\infty \frac{t-[t]}{t^2}dt + \int_x^\infty \frac{t-[t]}{t^2}dt + \frac{[x]-x}{x}$$

$$= \log x + A + \int_x^\infty \frac{t-[t]}{t^2}dt + \frac{[x]-x}{x} \quad \ldots \text{(i)} \quad \text{where } A = 1 - \int_1^\infty \frac{t-[t]}{t^2}dt.$$

Since $0 \le x - [x] < 1$, we have $0 \le \frac{x-[x]}{x} < \frac{1}{x}$ for every x

$$\Rightarrow \frac{x-[x]}{x} = O\left(\frac{1}{x}\right) \quad \ldots \text{(ii)}$$

Also for any $t \in [x,)$, $0 \le t - [t] < 1$.

$$\Rightarrow 0 \le \frac{t-[t]}{t^2} < \frac{1}{t^2} \Rightarrow \int_x^\infty \frac{t-[t]}{t^2}dt < \int_x^\infty \frac{1}{t^2}dt = \frac{1}{x}$$

$$\Rightarrow \int_x^\infty \frac{t-[t]}{t^2}dt = O\left(\frac{1}{x}\right) \quad \ldots \text{(iii)}$$

Substituting (ii) and (iii) in (i), we get

$$\sum_{n\le x}\frac{1}{n} = \log x + A + O\left(\frac{1}{x}\right) + O\left(\frac{1}{x}\right) = \log x + A + O\left(\frac{1}{x}\right) \quad \ldots \text{(iv)}$$

(by theorem 3.3.6, $O(g) + O(g) = O(g)$)

$$\Rightarrow \sum_{n\le x}\frac{1}{n} - \log x = A + O\left(\frac{1}{x}\right)$$

$$\Rightarrow \lim_{x\to\infty}\left(\sum_{n\le x}\frac{1}{n} - \log x\right) = \lim_{x\to\infty} A + O\left(\frac{1}{x}\right) \Rightarrow \text{Euler's constant } (C) = A \quad \ldots \text{(v)}$$

From (iv) and (v), we have $\sum_{n\le x}\frac{1}{n} = \log x + C + O\left(\frac{1}{x}\right)$.

3.5.2 Definition For $s > 0$, the **Riemann zeta function** is defined as

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \quad \text{if } s > 1$$

$$= \lim_{x\to\infty}\left(\sum_{n\le x}\frac{1}{n^s} - \frac{x^{1-s}}{1-s}\right) \quad \text{if } 0 < s < 1.$$

*The zeta function $\zeta(s)$ was introduced by Euler into analysis to prove the prime number theory. Euler had restricted the zeta function $\zeta(s)$ to real values of s. Riemann in his momoir uber die Anzahl der Primzahlen unter einer gegebenen Grosse of 1859, recognized the connection between the distribution of primes and the beahviour of $\zeta(s)$ as a function of a complex variable s = a + ib. The Riemann's Explicit formula, relating $\pi(x)$ to the zeroes of $\zeta(s)$ in the s-plane, connected two seemingly **unrelated** things namely, number theory, which is the study of discrete, and complex analsis, which **deals with** continuous process.*

3.5.3 Theorem If $s > 0$ and $s \neq 1$ then for any $x \geq 1$,

$$\sum_{n\le x}\frac{1}{n^s} = \frac{x^{1-s}}{1-s} + \zeta(s) + O\left(\frac{1}{x^s}\right)$$

Proof: We know that the function $f(t) = \frac{1}{t^s}$ has derivative

$f^1(t) = -\frac{s}{t^{s+1}}$ is in $[1, x]$. Therefore by Euler's summation formula

$$\sum_{a<n\le b} f(n) = \int_a^b f(t)dt + \int_a^b (t-[t])f'(t)dt + f(b)([b] - b) - f(a)([a] - a)$$

We have that $\sum_{1<n\le x}\frac{1}{n^s} = \int_1^x \frac{1}{t^s}dt + \int_1^x (t-[t])\left(\frac{-s}{t^{s+1}}\right)dt + ([x]-x)\left(\frac{1}{x^s}\right) - ([1]-1)$

$$= \int_1^x \frac{1}{t^s}dt + \int_1^x (t-[t])\left(\frac{-s}{t^{s+1}}\right)dt + \frac{[x]-x}{x^s} + 0 \quad \ldots \text{(i)}$$

Consider $\sum_{n\le x}\frac{1}{n^s} = \frac{1}{1^s}$ (n = 1 case) + $\sum_{1<n\le x}\frac{1}{n^s}$

$$= 1 + \int_1^x \frac{1}{t^s}dt + \int (t-[t])\left(\frac{-s}{t^{s+1}}\right)dt + \frac{[x]-x}{x^s} \quad \text{(by (i))}$$

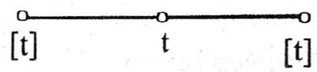
$$= 1 + \left[\frac{t^{-s+1}}{1-s}\right]_1^x - s\int_1^x \frac{t-[t]}{t^{s+1}}dt + \frac{[x]-x}{x^s}$$

$$= 1 + \left[\frac{x^{-s+1}}{1-s} - \frac{1}{1-s}\right] - s\int_1^x \frac{t-[t]}{t^{s+1}}\,dt + \frac{[x]-x}{x^s}$$

$$= \frac{x^{-s+1}}{1-s} + \left[1 - \frac{1}{1-s} - s\int_1^\infty \frac{t-[t]}{t^{s+1}}\,dt\right] + s\int_1^\infty \frac{t-[t]}{t^{s+1}}\,dt - s\int_1^x \frac{t-[t]}{t^{s+1}}\,dt + O\left(\frac{1}{x^s}\right)$$

$$= \frac{x^{-s+1}}{1-s} + A(s) + s\int_x^\infty \frac{t-[t]}{t^{s+1}}\,dt + O\left(\frac{1}{x^s}\right) \quad \dots \text{(ii)}$$

where $A(s) = 1 - \dfrac{1}{1-s} - s\displaystyle\int_1^\infty \frac{t-[t]}{t^{s+1}}\,dt$.

Now $0 \le t - [t] < 1$. (Since )

$$\Rightarrow \frac{t-[t]}{t^{s+1}} < \frac{1}{t^{s+1}} \Rightarrow \int_x^\infty \frac{t-[t]}{t^{s+1}}\,dt < \int_x^\infty \frac{1}{t^{s+1}}\,dt = \left[\frac{t^{-s}}{-s}\right]_x^\infty = 0 - \frac{x^{-s}}{(-s)} = \frac{1}{sx^s}$$

$$\Rightarrow s\int_x^\infty \frac{t-[t]}{t^{s+1}}\,dt < \frac{1}{x^s} \quad \Rightarrow s\int_x^\infty \frac{t-[t]}{t^{s+1}}\,dt = O\left(\frac{1}{x^s}\right) \quad \dots \text{(iii)}$$

By (ii) and (iii) we have $\displaystyle\sum_{n\le x}\frac{1}{n^s} = \frac{x^{-s+1}}{1-s} + A(s) + O\left(\frac{1}{x^s}\right) + O\left(\frac{1}{x^s}\right)$

$$= \frac{x^{-s+1}}{1-s} + A(s) + O\left(\frac{1}{x^s}\right) \quad \dots \text{(iv)}$$

(By Theorem 3.3.6, $O(g(x)) + O(g(x)) = O(g(x))$)

Now it is enough to show that $A(s) = \zeta(s)$.

By applying $\lim\limits_{x\to\infty}$ on both sides in (iv), we get

$$\zeta(s) = \sum_{n=1}^{\infty}\frac{1}{n^s} = \lim_{x\to\infty}\sum_{n\le x}\frac{1}{n^s}$$

$$= \lim_{x\to\infty}\frac{x^{1-s}}{1-s} + \lim_{x\to\infty}A(s) + \lim_{x\to\infty}O\left(\frac{1}{x^s}\right)$$

$$= 0 + \lim_{x\to\infty}A(s) + 0 = A(s) \qquad \text{(because } A(s) \text{ is independent of } x\text{)}$$

[Verification:

Suppose $s > 1$.

Then $\lim_{x\to\infty} \frac{x^{1-s}}{1-s} = \lim_{x\to\infty} \frac{1}{(1-s)x^{s-1}} = 0$. Also $\lim_{x\to\infty} O\left(\frac{1}{x^s}\right) = 0$ [since $x^s \to \infty$].

So, if $s > 1$ we have $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = A(s)$ ... (v)

If $0 < s < 1$, we have $\sum_{n\le x} \frac{1}{n^s} = \frac{x^{1-s}}{1-s} + A(s) + O(\frac{1}{x^s})$

$$\Rightarrow \sum_{n\le x}\left(\frac{1}{n^s} - \frac{x^{1-s}}{1-s}\right) = A(s) + O(\frac{1}{x^s}).$$

Again applying $\lim_{x\to\infty}$ on both sides, we get

$$\lim_{x\to\infty}\left(\sum_{n\le x}\frac{1}{n^s} - \frac{x^{1-s}}{1-s}\right) = \lim_{x\to\infty}\left(A(s) + O\left(\frac{1}{x^s}\right)\right) = A(s) + 0$$

$\Rightarrow \zeta(s) = A(s)$ ... (vi) (by the definition of $\zeta(s)$)]

From (v) and (vi) (in both cases where $s > 1$ and $0 < s < 1$) we have $\zeta(s) = A(s)$ ... (vii)

By using (iv) and (vii) we get $\sum_{n\le x} \frac{1}{n^s} = \frac{x^{1-s}}{1-s} + \zeta(s) + O(\frac{1}{x^s})$.

This completes the proof.

3.5.4 Corollary If $x \ge 1$ and $s > 1$, then $\sum_{n>x} \frac{1}{n^s} = O(x^{1-s})$.

Proof: If $s > 1$, then by theorem 3.5.3, condition (v), $\lim_{x\to\infty} \sum_{n\le x} \frac{1}{n^s} = \lim_{x\to\infty} A(s) = \zeta(s)$.

$\Rightarrow \sum_{n=1}^{\infty} \frac{1}{n^s} = \zeta(s)$ is finite (since $\sum_{n=1}^{\infty} \frac{1}{n^s}$ is convergent series for $0 < s < 1$ and $s > 1$).

Therefore $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \sum_{n\le x} \frac{1}{n^s} + \sum_{n>x} \frac{1}{n^s}$

$$\Rightarrow \sum_{n>x} \frac{1}{n^s} = \zeta(s) - \sum_{n\le x} \frac{1}{n^s}$$

$$= \zeta(s) - [\frac{x^{1-s}}{1-s} + \zeta(s) + O(\frac{1}{x^s})].$$ (By Theorem 3.5.3 ,

$$= -\frac{x^{1-s}}{1-s} - O\left(\frac{1}{x^s}\right)$$

$= -(O(x^{1-s}) + O(x^{-s}))$ [Suppose $f(x) = x^{-s}$ and $g(x) = x^{1-s}$.

Then $\lim_{x\to\infty} \frac{f(x)}{g(x)} = \lim_{x\to\infty} \frac{x^{-s}}{x^{1-s}} = \lim_{x\to\infty} \frac{1}{x} = 0.$

Therefore $f(x) = O(g(x))$

$\Rightarrow O(f(x)) = O(O(g(x))) = O(g(x)) \Rightarrow O(x^{-s}) = O(x^{1-s})$]

$$= O(x^{1-s}) + O(x^{1-s}) = O(x^{1-s}).$$

Hence $\sum_{n>x} \frac{1}{n^s} = O(x^{1-s})$. This completes the proof.

3.5.5 Theorem If $\alpha \geq 0$, then for any $x \geq 1$, we have $\sum_{n\leq x} n^\alpha = \frac{x^{\alpha+1}}{\alpha+1} + O(x^\alpha)$.

Proof: Let $f(t) = t^\alpha$ and $f^1(t) = \alpha.t^{\alpha-1}$ are continuous in [1, x].

By Eulers summation formula, we have

$$\sum_{1<n\leq x} n^\alpha = \int_1^x t^\alpha\, dt + \int_1^x (t-[t])\alpha.t^{\alpha-1}dt + ([x]-x)x^\alpha - (1-[1])f(1)$$

$$= \left[\frac{t^{\alpha+1}}{\alpha+1}\right]_1^x + \alpha\int_1^x (t-[t]).t^{\alpha-1}dt + ([x]-x)x^\alpha + 0.$$

By including the case $n = 1$ we get

$$\sum_{n\leq x} n^\alpha = 1 + \sum_{1<n\leq x} n^\alpha = 1 + \left[\frac{x^{\alpha+1}}{\alpha+1} - \frac{1}{\alpha+1} + \alpha\int_1^x (t-[t]).t^{\alpha-1}dt + O(x^\alpha)\right] \ldots \text{(i)}$$

(by (ii) given below)

[reason: $0 \leq |[x] - x| < 1 \Rightarrow ([x] - x)x^\alpha < x^\alpha \Rightarrow ([x] - x)x^\alpha = O(x^\alpha)$] ... (ii)

Consider $\left|1 - \frac{1}{\alpha+1}\right| = \left|\frac{\alpha}{\alpha+1}\right| < 1 \Rightarrow 1 - \frac{1}{\alpha+1} = O(1)$ ... (iii)

Consider $0 \leq t - [t] < 1 \Rightarrow (t - [t])t^{\alpha-1} < t^{\alpha-1}$

$$\Rightarrow \int_1^x (t-[t]).t^{\alpha-1}dt < \int_1^x t^{\alpha-1}dt = \left[\frac{t^\alpha}{\alpha}\right]_1^x = \frac{x^\alpha}{\alpha} - \frac{1}{\alpha} = O(x^\alpha) \ldots \text{(iv)}$$

By substituting (iii) and (iv) in (i), we get

$$\sum_{n\le x} n^{\alpha} = \frac{x^{\alpha+1}}{\alpha+1} + O(1) + O(x^{\alpha}) + O(x^{\alpha})$$

$$= \frac{x^{\alpha+1}}{\alpha+1} + O(1) + O(x^{\alpha}) \text{ (since } O(x^{\alpha}) + O(x^{\alpha}) = O(x^{\alpha}))$$

Hence $\sum_{n\le x} n^{\alpha} = \frac{x^{\alpha+1}}{\alpha+1} + O(x^{\alpha})$.

3.5.6 Problem Use Euler's summation formula to deduce the following for $n \ge 2$.

$$\sum_{n\le x} \frac{\log n}{n} = \frac{1}{2}\log^2 x + A + O\left(\frac{\log x}{x}\right) \text{ where } A \text{ is a constant.}$$

Solution: Consider $f(t) = \frac{\log t}{t}$ and $f^{1}(t) = \frac{1-\log t}{t^2}$ in $[1, x]$.

By Euler's summation formula, we have

$$\sum_{1<n\le x} \frac{\log n}{n} = \int_1^x \frac{\log t}{t}\,dt + \int_1^x (t-[t])\left(\frac{1-\log t}{t^2}\right)dt + ([x]-x)\frac{\log x}{x} + (1-[1])\left(\frac{\log 1}{1}\right) \quad \dots (i)$$

[Note that $\log 1 = 0 \Rightarrow$ the last term of RHS of (i) is zero].

Put $\log t = y$. Then $dy = \frac{1}{t}dt$.

Also $1 \le t \le x \Rightarrow \log 1 \le \log t \le \log x \Rightarrow 0 \le y \le \log x$

Now consider

$$\int_1^x \frac{\log t}{t}\,dt = \int_0^{\log x} y\,dy = \left[\frac{y^2}{2}\right]_0^{\log x} = \frac{(\log x)^2}{2} \quad \dots (ii)$$

Consider $0 \le |[x] - x| < 1 \Rightarrow |[x] - x|\frac{\log x}{x} < \frac{\log x}{x} = O\left(\frac{\log x}{x}\right) \quad \dots (iii)$

Consider $0 \le t - [t] < 1 \Rightarrow 0 \le (t - [t])\left(\frac{1-\log t}{t^2}\right) \le \frac{1-\log t}{t^2}$

$$\Rightarrow \left|\int_x^{\infty} (t-[t])\left(\frac{1-\log t}{t^2}\right)dt\right| \le \int_x^{\infty} \frac{1-\log t}{t^2}\,dt$$

$$\leq \int_x^{\infty} \frac{1-\log x}{t^2}\, dt \quad (\text{since } t \in [x,] \Rightarrow x \leq t \Rightarrow \log x \leq \log t$$

$$\Rightarrow 1 - \log x \geq 1 - \log t)$$

$$=(1 - \log x) \int_x^{\infty} \frac{1}{t^2}\, dt$$

$$= \frac{1-\log x}{x} \quad \left(\text{Since } \int_x^{\infty} \frac{1}{t^2}\, dt = \left[\frac{t^{-2+1}}{-2+1}\right]_x^{\infty} = -\left(\frac{1}{t}\right)_x^{\infty} = -\left(-\frac{1}{x}\right) = \frac{1}{x}\right)$$

$$= O\left(\frac{\log x}{x}\right).$$

Therefore $\int_x^{\infty} (t-[t])\left(\frac{1-\log t}{t^2}\right) dt = O\left(\frac{\log x}{x}\right)$ ... (iv)

Now consider (i) . That is,

$$\sum_{1<n\leq x} \frac{\log n}{n} = \int_1^x \frac{\log t}{t}\, dt + \int_1^x (t-[t])\left(\frac{1-\log t}{t^2}\right) dt + ([x]-x)\frac{\log x}{x}$$

$$= \frac{(\log x)^2}{2} + \int_1^x (t-[t])\left(\frac{1-\log t}{t^2}\right) dt + O\left(\frac{\log x}{x}\right) \quad \text{(by (ii) and (iii))}$$

$$= \frac{(\log x)^2}{2} + A - \int_x^{\infty} (t-[t])\left(\frac{1-\log t}{t^2}\right) dt + O\left(\frac{\log x}{x}\right)$$

where $A = \int_1^{\infty} (t-[t])\left(\frac{1-\log t}{t^2}\right) dt$

$$= \frac{(\log x)^2}{2} + A + O\left(\frac{\log x}{x}\right) + O\left(\frac{\log x}{x}\right) \quad \text{(by (iv))}$$

$$= \frac{1}{2}\log^2 x + A + O\left(\frac{\log x}{x}\right).$$

3.5.7 Problem Use Euler's summation formula to deduce the following for $n \geq 2$.

$$\sum_{2\leq n\leq x} \frac{1}{n \log n} = \log(\log x) + B + O\left(\frac{1}{x \log x}\right).$$

Solution: Consider $f(t) = \dfrac{1}{t\log t}$ and $f^{1}(t) = \dfrac{-(1+\log t)}{t^2 \log^2 t}$ which are continuous in (1,).

By Euler's summation formula, we have

$$\sum_{2\le n\le x} \frac{1}{n\log n} = \int_1^x \frac{1}{t\log t}\,dt + \int_1^x (t-[t])\frac{-(1+\log t)}{t^2\log t}\,dt + ([x]-x)\frac{1}{x\log x} \quad \ldots \text{(i)}$$

(we are not using last term, since log 1 = 0)

Consider $\displaystyle\int_1^x \frac{1}{t\log t}\,dt = \int_0^{\log x} \frac{1}{y}\,dy$ [Reason: Take $\log t = y$. $1 < t < x$

$\Rightarrow \log 1 \le \log t \le \log x \Rightarrow 0 < y \le \log x$.

Also $\dfrac{1}{t}dt = dy$]

$$= [\log y]_0^{\log x} = \log(\log x) - \log 0 = \log(\log x) - \log(\log 1) \ldots \text{(ii)}$$

Now consider $0 \le x - [x] < 1 \Rightarrow 0 \le \dfrac{x-[x]}{x\log x} < \dfrac{1}{x\log x} \Rightarrow \dfrac{x-[x]}{x\log x} = O\left(\dfrac{1}{x\log x}\right) \ldots$ (iii)

Since $0 \le t - [t] < 1$, we have $0 \le (t-[t])\,\dfrac{1+\log t}{t^2\log^2 t} \le 1.\dfrac{(1+\log t)}{t^2\log^2 t}$

$$\Rightarrow \int_x^\infty \frac{(t-[t])(1+\log t)}{t^2\log^2 t}\,dt \le \int_x^\infty \frac{(1+\log t)}{t^2\log^2 t}\,dt = -\int_x^\infty \frac{d}{dt}\left(\frac{1}{t\log t}\right)dt = \left[\frac{-1}{t\log t}\right]_x^\infty = \frac{1}{x\log x}$$

Therefore $\displaystyle\int_x^\infty \frac{(t-[t])(1+\log t)}{t^2\log^2 t}\,dt = O\left(\frac{1}{x\log x}\right) \ldots$ (iv)

Using (ii), (iii), (iv) in (i), we get that

$$\sum_{2\le n\le x} \frac{1}{n\log n} = [\log(\log x) - \log(\log 1)] - \int_1^\infty \frac{(t-[t])(1+\log t)}{t^2\log^2 t}\,dt$$

$$+ \int_x^\infty \frac{(t-[t])(1+\log t)}{t^2\log^2 t}\,dt + O\left(\frac{1}{x\log x}\right).$$

$$= \log(\log x) + B + O\left(\frac{1}{x\log x}\right) + O\left(\frac{1}{x\log x}\right)$$

where $B = -\log(\log 1) - \displaystyle\int_1^\infty \frac{(t-[t])(1+\log t)}{t^2\log^2 t}\,dt$ is a constant.

Hence $\sum_{2\le n\le x} \frac{1}{n\log n} = \log(\log x) + B + O\left(\frac{1}{x\log x}\right)$.

3.6. SUMMARY

This lesson dealt with the asymptotic equality of functions. We provided a Euler's summation formula to compare the asymptotic value of a partial sum with an integral. Some consequences of Euler's summation formulae which may be regarded as elementary asymptotic formulae, were obtained.

3.7. TECHNICAL TERMS

partial sum: $\sum_{k=1}^{n} f(k)$

big oh notation: "f(x is of order g(x)" if there exists M > 0 such that $|f(x)| \le M\,|g(x)|$, $g(x) > 0$.

asymptotic: "f(x) is asymptotic g(x)" provided $\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1$.

Euler's Summation formula:

$$\sum_{a<n\le b} f(n) = \int_a^b f(t)dt + \int_a^b (t-[t])f'(t)dt + f(b)([b]-b) - f(a)([a]-a),$$

where f(x) has continuous derivative on [a, b], 0 < a < b.

Euler's constant: $C = \lim_{n\to\infty}\left((\sum_{k\le n} \frac{1}{k}) - \log n \right)$

Riemann Zeta function: $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$ if $s > 1$

$$= \lim_{x\to\infty}\left(\sum_{n\le x} \frac{1}{n^s} - \frac{x^{1-s}}{1-s} \right) \text{ if } 0 < s < 1.$$

3.8. ANSWERS TO SELF ASSESSMENT QUESTIONS

1: Suppose $f(x) = O(g(x))$.

Then by definition, we have $\frac{f(x)}{g(x)} < M$ for some $M > 0$.

$\Rightarrow c\,\frac{f(x)}{g(x)} < c\,M = M^1$ (Say)

$\Rightarrow c\,f(x) = O(g(x))$.

2: Write $f(x) = x^3 + x^2 - 5$ and $g(x) = x^4$.

Then $\lim_{x\to\infty}\frac{f(x)}{g(x)} = \lim_{x\to\infty}\frac{x^3+x^2-5}{x^4} = \lim_{x\to\infty}\left(\frac{1}{x}+\frac{1}{x^2}-\frac{5}{x^4}\right) = 0$

Therefore $f(x)$ is of small order $g(x)$. That is, $f(x) = o(g(x))$.

3: Let $f_1(x) = O(f(x))$ and $f_2(x) = O(f_1(x))$ where f_1 and f_2 are two real valued functions and $f(x) > 0$.

$\Rightarrow$ there exists two positive constants M_1 and M_2 such that

$$\left|\frac{f_1(x)}{f(x)}\right| \le M_1 \text{ and } \left|\frac{f_2(x)}{f_1(x)}\right| \le M_2.$$

$\Rightarrow |f_1(x)| < M_1|f(x)|$ and $|f_2(x)| < M_2|f_1(x)|$

$\Rightarrow |f_2(x)| < M_2|f_1(x)| \le M_2.M_1|f(x)|$

$\Rightarrow \left|\frac{f_2(x)}{f(x)}\right| \le M_2M_1 \Rightarrow \frac{f_2(x)}{f(x)}$ is bounded $\Rightarrow f_2(x) = O(f(x))$

$O(f_1(x)) = O(f(x)) \Rightarrow O(O(f(x)) = O(f(x))$.

3.9. MODEL QUESTIONS

1. Define asymptotic equality of functions.
2. Prove the Euler's summation formula.
3. If $s > 0$ and $s \neq 1$, then show that for any $x \ge 1$, $\sum_{n\le x}\frac{1}{n^s} = \frac{x^{1-s}}{1-s} + \zeta(s) + O(\frac{1}{x^s})$

3.10. REFERENCE BOOKS

1. Chandrasekharan, K. "Introduction to Analytic Number Theory", Springer Verlag .
2. Hardy, G.H. & Wright, E.M. "Introduction to the Theory of Numbers", Fourth Edition, Oxford Publications,
3. Levegue W.J. (1986) "Topics in Number Theory (2 volumes), Addition - Wesley Publ. Co.
4. Rademacher (1964) "Lectures on Elementary Number Theory", New York, Blaisdell Publ. Co.
5. Tom M. Apostol "Introduction to Analytic Number Theory", Springer International Student Edition, Narosa Publishing House, 1995.
6. Uspensky, J.V., and Heaslett, M.A. (1939) "Elementary Number Theory", New York, Mc. Graw - Hill Book. Co.
7. Vinogrador, "Elements of Number Theory", Dover Publications

Name of the Author of this Lesson: **Dr. Kuncham Syam Prasad**

LESSON – 4

AVERAGES OF ARITHMETICAL FUNCTIONS

Objectives

The objectives of this lesson are to:

- find the average order of various arithmetical functions
- discuss different identities satisfied by arithmetical functions such as $\mu(n)$, $\varphi(n)$, $\lambda(n)$ and the divisor function
- study the behavior of these functions and other arithmetical functions f(n) for large values of n
- discuss an application of the asymptotic formula for the partial sums of $\varphi(n)$, to a theorem concerning the distribution of lattice points.

Structure

4.0 INTRODUCTION

We had already familiar with the arithmetical functions like Mobius, Euler, divisor, and studied their asymptotic equality using big oh notation. In this lesson, we discuss the average orders of some arithmetical functions such as d(n), σ_α (n), $\varphi(n)$, $\mu(n)$ and $\wedge(n)$. Also we will deal an interesting application of the asymptotic formula for the partial sums of $\varphi(n)$ to a theorem concerning the distribution of lattice points in the plane which are visible from the origin.

4.1 THE AVERAGE ORDER OF d(n)

4.1.1 Definition: A point (d, f) in the plane is said to be a **lattice point** if d and f are both integers. [For example, (1, 2), (-3, 4), (5, 6) are lattice points.]

4.1.2 Note: (i) $x.C = O(x)$ where C is a constant. (ii) $x.O\left(\frac{1}{x}\right) = O(1)$.

[**Verification:** (i) Suppose $f(x) = x.C$ and $g(x) = x$.

Consider $\lim_{x\to\infty} \frac{f(x)}{g(x)} = \frac{xC}{x} = C \Rightarrow f(x) = O(g(x)) \Rightarrow x.C = O(x)$.

(ii) Take $g(x) = O\left(\frac{1}{x}\right) \Rightarrow \frac{g(x)}{(\frac{1}{x})} \le M$ for some $M > 0$. $\Rightarrow x.g(x) \le M$

$\Rightarrow \frac{x.g(x)}{1} \le M \Rightarrow x.g(x) = O(1) \Rightarrow x.O\left(\frac{1}{x}\right) = O(1)$.]

4.1.3 Theorem: If $d(n)$ is the number of positive divisors of n, then for any $x \ge 1$ we have $\sum_{n\le x} d(n) = x \log x + O(x)$.

Proof: Since $d(n) = \sum_{d|n} 1$, we have

$$\sum_{n\le x} d(n) = \sum_{n\le x}\sum_{d|n} 1$$

$$= \sum_{d\delta\le x}\sum_{d|n} 1 \text{ (since } d \mid n \text{ we have } n = d.\delta \text{ for some } \delta \Rightarrow d.\delta = n \le x)$$

$$= \sum_{\substack{(d,\delta) \\ d\delta\le x}} 1 \quad \ldots \text{(i)}$$

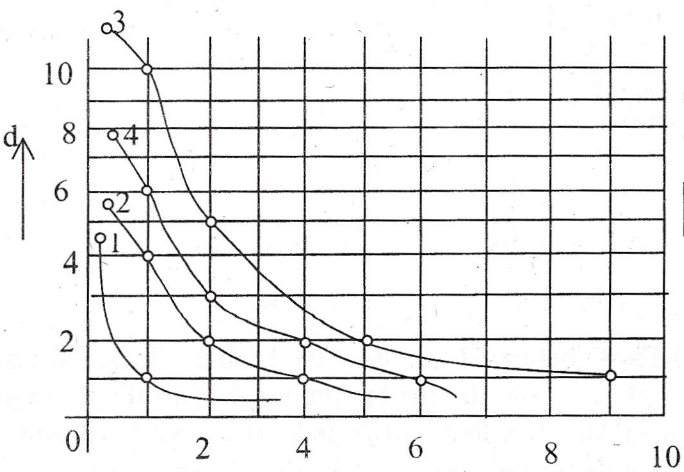


Fig-4.1.3

[Here the summation runs over all those ordered pairs (d, δ) of positive integers d, δ with $d\delta < x$. That is, the sum on the right hand side is taken over all these lattice points in the first quadrant of the $d\delta$ plane. Observe the figure- 4.1.3 given.].

Observation: Curve-1 $qd = 1$; curve-2 $qd = 4$; curve-3 $qd = 10$; curve-4 $qd = 6$.

If $n = 1$, then $(d, \delta) = (1, 1)$.

If $n = 2$, then $(d, \delta) \in \{(2, 1), (1, 2)\}$

If $n = 6$, then $(d, \delta) \in \{(1, 6), (2, 3), (3, 2), (6, 1)\}$

If $n = 10$, then $(d, \delta) \in \{(1, 10), (2, 5), (5, 2), (10, 1)\}$

These points (d, δ)'s lies on the hyperbolas $d\delta = n \in \{1, 2, 3, \ldots, [x]\}$.

Thus $\sum_{n \le x} d(n)$ gives the number of lattice points in the first quadrant that do not lie on the axis and those lie below the hyperbola $d\delta \le x$.

For any fixed point d with $d \le x$, all the lattice points on the vertical through d below the hyperbola are only those (d, δ) with $1 \le \delta \le \frac{x}{d}$ (since $1 \le \delta = \frac{n}{d} \le \frac{x}{d}$)

Thus (i) becomes $\sum_{n \le x} d(n) = \sum_{1 \le d \le x} \sum_{1 \le \delta \le x/d} 1$ ... (ii)

By theorem 3.5.5, (statement: $\sum_{n \le x} n^{\alpha} = \frac{x^{\alpha+1}}{\alpha+1} + O(x^{\alpha})$ if $\alpha \ge 0$)

we get (by taking $\alpha = 0$) $\sum_{n \le x} 1 = \frac{x}{1} + O(1)$ ... (iii)

From (ii) and (iii), we have [in (iii), take $\frac{x}{d}$ in place of x]

$$\sum_{n \le x} d(n) = \sum_{1 \le d \le x} \left\{\frac{x}{d} + O(1)\right\} = x \sum_{1 \le d \le x} \frac{1}{d} + \sum_{1 \le d \le x} O(1) = x \sum_{1 \le d \le x} \frac{1}{d} + O(x) \quad \ldots \text{(iv)}$$

[Verification for $\sum_{1 \le d \le x} O(1) = O(x)$:

Consider $\sum_{1 \le d \le x} O(1) = [x].O(1) = O(x).O(1) = O(x.1) = O(x)$]

Also by Theorem 3.5.1, $\sum_{n \le x} \frac{1}{n} = \log x + C + O\left(\frac{1}{x}\right)$ ....(v) where C is the Euler's constant.

From (iv) and (v) we have (take d in place of n in (v))

$$\sum_{n \le x} d(n) = x\{\log x + C + O\left(\frac{1}{x}\right)\} + O(x)$$

$$= x \log x + x.C + x.O\left(\frac{1}{x}\right) + O(x) = x \log x + O(x) + O(1) + O(x)$$

$$= x \log x + O(x) \quad (\text{since } O(x) + O(1) + O(x) = O(x))$$

Hence $\sum_{n \le x} d(n) = x \log x + O(x)$. This completes the proof.

4.1.4 Corollary: The average order of $d(n)$ is $\log n$.

Proof: Let $\bar{d}(n)$ is the average function of $d(n)$.

Then $\bar{d}(n) = \frac{1}{n} \sum_{k=1}^{n} d(k) = \frac{1}{n} \sum_{k \le n} d(k) = \frac{1}{n}\{n \log n + O(n)\}$ (by Theorem 4.1.3)

$$= \log n + \frac{1}{n} O(n) = \log n + O(1)$$

$$\Rightarrow \frac{\bar{d}(n)}{\log n} = \frac{\log n}{\log n} + \frac{O(1)}{\log n} = 1 + \frac{O(1)}{\log n} \Rightarrow \lim_{n\to\infty} \frac{\bar{d}(n)}{\log n} = 1 + 0 = 1 \Rightarrow \lim_{x\to\infty} \frac{\bar{d}(n)}{\log n} = 1$$

Therefore the average order of $d(n)$ is $\log n$.

4.1.5 Theorem: Dirichlet Asymptotic formula: If $d(n)$ is the divisor function, then for all $x \geq 1$, $\sum_{n\leq x} d(n) = x \log x + (2C - 1)x + O(\sqrt{x})$, where C is the Euler's constant.

Proof:

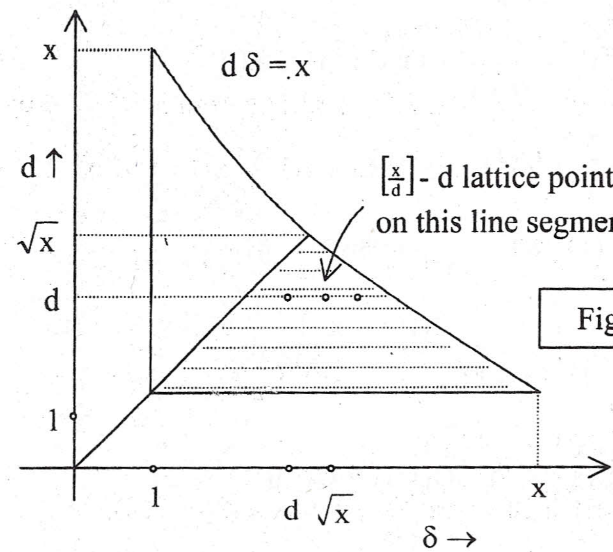


Fig-4.1.5

Consider $\sum_{n\leq x} d(n) = \sum_{n\leq x} \sum_{d|n} 1$ (since $d(n) = \sum_{d|n} 1$)

$= \sum_{d\delta\leq x} 1$ where $\frac{n}{d} = \delta$. (see point (1) of Theorem 4.1.3)

Here the RHS sum is over all those ordered pairs (d, δ) of positive integers with $d\delta \leq x$.

Clearly the RHS sum is equal to the number of lattice points in the first quadrant of the $d\delta$-plane which is not on the coordinate axis and that lie below the hyperbola $d\delta = x$.

So $\sum_{d\delta\leq x} 1$ is the number of lattice points (d, δ) with $d\delta \leq x$.

The hyperbola $d\delta = x$ is symmetrical about the line $d = \delta$.

So $\sum_{d\delta\leq x} 1$ = the number of lattice points in the region.

= 2 ×(the number of such points below the line $d = \delta$
+ (the number of lattice points on the line $d = \delta$)

Therefore $\sum_{n\leq x} d(n) = \sum_{\substack{d\delta\leq x \\ (d,\delta)}} 1$ (from earlier steps)

$$= 2 \sum_{d \le \sqrt{x}} \left\{ \left[\frac{x}{d} \right] - d \right\} + [\sqrt{x}]$$

[Since the number of lattice points on the line $d = \delta$ are $[\sqrt{x}]$]

$$= 2 \sum_{d \le \sqrt{x}} \left\{ \frac{x}{d} + O(1) - d \right\} + O(\sqrt{x})$$

[Since $O(\sqrt{x}) = [\sqrt{x}]$ and $[\frac{x}{d}] = O(1) + \frac{x}{d}$ (verify!)]

$$= 2x \sum_{d \le \sqrt{x}} \frac{1}{d} - 2 \sum_{d \le \sqrt{x}} d + 2. \sum_{d \le \sqrt{x}} O(1) + O(\sqrt{x})$$

[by Theorem 3.5.1 and Theorem 3.5.5, and by the proof of Theorem 4.1.3 $\sum_{n \le x} O(1) = O(x)$.]

$$= 2x\{\log \sqrt{x} + C + O(\frac{1}{\sqrt{x}}) - 2\left\{ \frac{(\sqrt{x})^{1+1}}{1+1} + O(\sqrt{x}) \right\} + 2O(\sqrt{x}) + O(\sqrt{x})$$

$$= 2x \log \sqrt{x} + 2xC + 2x. O(\frac{1}{\sqrt{x}}) - x - 2.O(\sqrt{x}) + 2O(\sqrt{x}) + O(\sqrt{x})$$

$$= 2x \log \sqrt{x} + (2C - 1)x + 2\, O(\sqrt{x}) + O(\sqrt{x})$$

[since $x \cdot O(\frac{1}{\sqrt{x}}) = O(\sqrt{x})$(verify !)]

$$= 2x \log \sqrt{x} + (2C - 1)x + O(\sqrt{x})$$

Therefore $\sum_{n \le x} d(n) = 2x \log(x)^{1/2} + (2C - 1)x + O(\sqrt{x})$

Hence $\sum_{n \le x} d(n) = x \log x + (2C - 1)x + O(\sqrt{x})$.

Self Assessment Question 1: *Verify (i)* $O(\sqrt{x}) = [\sqrt{x}]$ *(ii)* $[\frac{x}{d}] = O(1) + (\frac{x}{d})$

Self Assessment Question 2: *Verify* $x \cdot O(\frac{1}{\sqrt{x}}) = O(\sqrt{x})$

4.2 THE AVERAGE ORDER OF THE DIVISOR FUNCTION $\sigma_\alpha(n)$

In the above theorem, we considered the case $\alpha = 0$. Next we consider $\alpha > 0$. We consider the case $\alpha = 1$ separately.

4.2.1 Theorem: If $\sigma(n)$ is the sum of the positive divisors of n, then for any $x \ge 1$ we have $\sum_{n \le x} \sigma(n) = \frac{1}{2}.\zeta(2).x^2 + O(x \log x)$.

Proof: Since $\sigma(n) = \sum_{d|n} d$ we have

$$\sum_{n\le x}\sigma(n) = \sum_{n\le x}\sum_{d|n} d = \sum_{d\delta\le x} d$$

$$= \sum_{d\le x}\left(\sum_{\delta\le \frac{x}{d}} \delta\right)$$

[Take $\alpha = 1$, $n = \delta$ and $x = \frac{x}{d}$ in the theorem 3.5.5. Then we get $\sum_{\delta\le\frac{x}{d}}\delta = \left(\frac{1}{2}\left(\frac{x}{d}\right)^2 + O\left(\frac{x}{d}\right)\right)$]

$$= \sum_{d\le x}\left(\frac{1}{2}\left(\frac{x}{d}\right)^2 + O\left(\frac{x}{d}\right)\right) = \frac{x^2}{2}\sum_{d\le x}\frac{1}{d^2} + O\left(x\sum_{d\le x}\frac{1}{d}\right)$$

[Put $n = d$ and $s = 2$ in Theorem 3.5.3.

Then we get $\sum\frac{1}{d^2} = \frac{x^{1-2}}{1-2} + \zeta(2) + O(\frac{1}{x^2})$

and put $n = d$ in Theorem 3.5.1]

$$= \frac{x^2}{2}\left[\frac{x^{1-2}}{1-2} + \zeta(2) + O(x^{-2})\right] + O(\,x\,(\log x + C + O(\tfrac{1}{x})\,)\,)$$

$$= \frac{x^2}{2}.\frac{x^{-1}}{-1} + \frac{x^2}{2}\zeta(2) + \frac{x^2}{2}\,(O(x^{-2})) + O(x.\log x + xC + x\,O(\tfrac{1}{x}))$$

$$= -\frac{1}{2}x + \frac{x^2}{2}\zeta(2) + \frac{x^2}{2}O(x^{-2}) + O(x\log x + xC + x.\,O(\tfrac{1}{x}))$$

[Since (i) $\frac{x^2}{2}O(x^{-2}) = O(1)$. (ii) $xC = O(x)$, $x.\,O(\frac{1}{x}) = O(1)$ [by Note 4.1.2]

$\Rightarrow O(x) + O(1) = O(x)$]

$$= -\frac{1}{2}x + \frac{x^2}{2}\zeta(2) + O(1) + O(x\log x + O(x))$$

[We know that $\lim_{x\to\infty}\frac{O(x)}{x\log x} \sim \lim_{x\to\infty}\frac{1}{x\log x} = 0.$

$\Rightarrow O(x) = O(x\log x) \Rightarrow x\log x + O(x) = O(x\log x)$]

$$= -\frac{1}{2}x + \frac{x^2}{2}\zeta(2) + O(1) + O(x\log x)$$

[Since $Cx = O(x)$, $O(x) + O(1) = O(x)$ and $O(x) + O(x\log x) = O(x\log x)$]

$$= \frac{x^2}{2}\zeta(2) + O(x\log x)$$

Therefore $\sum_{n\leq x}\sigma(n) = \frac{1}{2}.\zeta(2).x^2 + O(x \log x)$.

4.2.2 Note: It can be shown that $\zeta(2) = \sum_{n=1}^{\infty}\frac{1}{n^2} = \frac{\pi^2}{b}$

(proof is out of scope of the book)
We use this fact in the next Corollary.

4.2.3 Corollary: The average order of $\sigma(n)$ (or $\sigma_1(n)$) is $\frac{\pi^2 n}{12}$.

Proof: By the definition of the average order, we have that

$$\bar{\sigma}(n) = \frac{1}{n}\sum_{k=1}^{n}\sigma(k) = \frac{1}{n}\sum_{k\leq n}\sigma(k) = \frac{1}{n}\left[\frac{1}{2}n^2\zeta(2) + O(n\log n)\right] \text{ (by Theorem 4.2.1)}$$

$$= \frac{1}{2}n\zeta(2) + \frac{1}{n}O(n\log n) = \frac{1}{2}n\frac{\pi^2}{6} + O(\log n)$$

(by Note 4.2.2 . Use $\frac{1}{n}O(n\log n) = O(\log n)$)

$$= \frac{\pi^2 n}{12} + O(\log n).$$

Consider $\lim_{n\to\infty}\frac{\bar{\sigma}(n)}{\left(\frac{\pi^2 n}{12}\right)} = \lim_{n\to\infty} 1 + \lim_{n\to\infty}\frac{O(\log n)}{\left(\frac{\pi^2 n}{12}\right)} = 1 + 12\lim_{n\to\infty}\left(\frac{O(\log n)}{\pi^2 n}\right) = 1 + 0 = 1.$

Hence the average order of $\sigma(n) = \frac{\pi^2 n}{12}$.

4.2.4 Theorem: If $x \geq 1$ and $\alpha > 0$, $\alpha \neq 1$, then $\sum_{n\leq x}\sigma_\alpha(n) = \frac{\zeta(\alpha+1)}{\alpha+1}.x^{\alpha+1} + O(x^\beta)$ where $\beta = \max\{1, \alpha\}$.

Proof: Since $\sigma_\alpha(n) = \sum_{d|n} d^\alpha = \sum_{d\delta=n} d^\alpha = \sum_{d\delta=n}\delta^\alpha$ (by replacing d and δ)

We have $\sum_{n\leq x}\sigma_\alpha(n) = \sum_{n\leq x}\sum_{d\delta=n}\delta^\alpha = \sum_{d\leq x}\left(\sum_{\delta\leq\frac{x}{d}}\delta^\alpha\right)$.

$$= \sum_{d\leq x}\left\{\frac{1}{\alpha+1}\left(\frac{x}{d}\right)^{\alpha+1} + O\left(\frac{x}{d}\right)^\alpha\right\}$$ [Since $\sum_{n\leq x} n^\alpha = \frac{x^{\alpha+1}}{\alpha+1} + O(x^\alpha)$, by theorem 3.5.5

Here take $\frac{x}{d}$ in place of x and δ in place of n.]

$$= \frac{x^{\alpha+1}}{\alpha+1}\sum_{d\leq x}\frac{1}{d^{\alpha+1}} + O\left(x^\alpha\sum_{d\leq x}\frac{1}{d^\alpha}\right)$$

$$= \frac{x^{\alpha+1}}{\alpha+1}\left(\frac{x^{1-(\alpha+1)}}{1-(\alpha+1)}+\zeta(\alpha+1)+O\left(x^{-(1+\alpha)}\right)\right) + O\left[x^{\alpha}\left(\frac{x^{1-\alpha}}{1-\alpha}\right)+\zeta(\alpha)+O\left(\frac{1}{x^{\alpha}}\right)\right]$$

[Since $\sum_{n\le x}\frac{1}{n^s} = \frac{x^{1-s}}{1-s} + \zeta(s) + O(\frac{1}{x^s})$, by Theorem 3.5.3, take d in place of n and $(\alpha + 1)$ in place of s and for the second part take α in place of s.]

$$= \frac{-x}{\alpha(\alpha+1)} + \frac{x^{\alpha+1}}{\alpha+1}\zeta(\alpha+1) + \frac{x^{\alpha+1}}{1+\alpha}\cdot O(x^{-(1+\alpha)}) + O\left(\frac{x}{1-\alpha}+x^{\alpha}\zeta(\alpha)+x^{\alpha}\left(O\left(\frac{1}{x^{\alpha}}\right)\right)\right)$$

[Since $\frac{x^{\alpha+1}}{\alpha+1}\cdot\frac{x^{1-(\alpha+1)}}{1-(\alpha+1)} = \frac{x^{\alpha+1}}{\alpha+1}\cdot\frac{x^{-\alpha}}{-\alpha} = \frac{x^{\alpha+1}.x^{-\alpha}}{-\alpha(\alpha+1)} = \frac{-x}{\alpha(\alpha+1)}$]

$$= \frac{-x}{\alpha(\alpha+1)} + \frac{x^{\alpha+1}}{\alpha+1}\zeta(\alpha+1) + O(1) + O(x^{\beta}) \text{ where } \beta = \max\{1, \alpha\}$$

[We know that. (i) $x.O(\frac{1}{x}) = O(1)$. So $x^{\alpha+1}.O(x^{-(1+\alpha)}) = O(1)$.

Also constant $\times.O(1) = O(1)$. Last term of above step= $O\left[\frac{x}{1-\alpha}+x^{\alpha}\zeta(\alpha)+O(1)\right]$

$= O(x) + O(x^{\alpha}) + O(1) = O(x^{\beta})$,

where $\beta = \max\{1, \alpha\}$]

$$= \frac{-x}{\alpha(\alpha+1)} + \frac{x^{\alpha+1}}{\alpha+1}\zeta(\alpha+1) + O(1) + O(x^{\beta})$$

$$= O(x) + \frac{x^{\alpha+1}}{\alpha+1}\zeta(\alpha+1) + O(1) + O(x^{\beta}).$$

$$= \frac{x^{\alpha+1}}{\alpha+1}\zeta(\alpha+1) + O(x^{\beta})$$ [Observe $[O(x) + O(1)] + O(x^{\beta}) = O(x) + O(x^{\beta}) = O(x^{\beta})$]

Hence we proved that $\sum_{n\le x}\sigma_{\alpha}(n) = \frac{\zeta(\alpha+1)}{\alpha+1}.x^{\alpha+1} + O(x^{\beta})$ where $\beta = \max\{1, \alpha\}$.

4.2.5 Theorem: If $\beta > 0$ and $\delta = \max\{0, 1-\beta\}$, then for $x > 1$, we have

$$\sum_{n\le x}\sigma_{-\beta}(n) = \begin{cases}\zeta(\beta+1)x + O(x^{\delta}) & \text{if } \beta \ne 1\\ \zeta(2)x + O(\log x) & \text{if } \beta = 1\end{cases}$$

Proof: Case-(i): Let $\beta \ne 1$ and $x > 1$.

Consider $\sigma_{-\beta}(n) = \sum_{d|n} d^{-\beta} = \sum_{d|n}\frac{1}{d^{\beta}}$

Now $\sum_{n\le x}\sigma_{-\beta}(n) = \sum_{n\le x}\sum_{d|n}\frac{1}{d^{\beta}}$

$$= \sum_{d\le x}\sum_{\delta\le \frac{x}{d}} \frac{1}{d^{\beta}} = \sum_{d\le x}\frac{1}{d^{\beta}}\sum_{\delta\le\frac{x}{d}} 1.$$

$$= \sum_{d\le x}\frac{1}{d^{\beta}}\left\{\frac{x}{d}+O(1)\right\} \quad [\text{Since } \sum_{\delta\le\frac{x}{d}} 1 = \left[\frac{x}{d}\right] = \frac{x}{d}+O(1)\,]$$

$$= x\sum_{d\le x}\frac{1}{d^{\beta+1}} + \sum_{d\le x}\frac{1}{d^{\beta}}.O(1)$$

$$= x\sum_{d\le x}\frac{1}{d^{\beta+1}} O\left(\sum_{d\le x}\frac{1}{d^{\beta}}\right) \quad \ldots \text{(i) (say)}$$

$$= x\left[\frac{x^{1-(\beta+1)}}{1-(\beta+1)}+\zeta(\beta+1)+O\left(x^{-\beta-1}\right)\right] + O\left[\frac{x^{1-\beta}}{1-\beta}+\zeta(\beta)+O\left(x^{-\beta}\right)\right] \quad \ldots \text{(ii) (say)}$$

[Take d in place of n and $\beta + 1$ in place of α, in theorem 3.5.3]

$$= \frac{x^{1-\beta}}{-\beta} + x.\zeta(\beta+1) + x.O\left(x^{-\beta-1}\right) + O\left\{O\left(x^{1-\beta}\right)\right\}$$

$$[\text{ Since } \frac{x^{1-\beta}}{1-\beta}+\zeta(\beta)+O\left(x^{-\beta}\right) = O\left(x^{1-\beta}\right) \text{ (verify !) }]$$

$$= \frac{x^{1-\beta}}{-\beta} + x.\zeta(\beta+1) + O\left(x^{-\beta}\right) + O\left(x^{1-\beta}\right)$$

$$= O(x^{1-\beta}) + x.\zeta(\beta+1) + O\left(x^{-\beta}\right) + O\left(x^{1-\beta}\right). \quad [\text{Since } \frac{x^{1-\beta}}{-\beta} = O(x^{1-\beta})]$$

$$= x.\zeta(\beta+1) + O\left(x^{1-\beta}\right) + O(x^{\beta}) \quad [\text{ Since } O(x^{1-\beta}) + O(x^{1-\beta}) = O(x^{1-\beta}) \text{ and } O(x^{-\beta}) = O(x^{1-\beta})]$$

Therefore $\sum_{n\le x}\sigma_{-\beta}(n) = x.\zeta(\beta+1) + O\left(x^{1-\beta}\right) = x.\zeta(\beta+1) + O\left(x^{\delta}\right)$ where $\delta = \max\{\beta, 1-\beta\}$

[Since $O(x^{1-\beta}) = O(x^{\delta})$, where $\delta = \max\{\beta, 1-\beta\}$(verify !)]

Hence the result is proved for case-(i): $\beta \neq 1$.

Case-(ii): Suppose $\beta = 1$. Put $\beta = 1$ in (i) of the above part, then we get

$$\sum_{n\le x}\sigma_{-1}(n) = x\sum_{d\le x}\frac{1}{d^{2}} + O\left(\sum_{d\le x}\frac{1}{d}\right).$$

[Next we use the following:

(i) By Theorem 3..5.3, $\sum_{n\le x}\frac{1}{n^{\alpha}} = \frac{x^{1-\alpha}}{1-\alpha} + \zeta(\alpha) + O(x^{-\alpha})$

Take d in place of n and $\alpha = 2$ in the first term. Then

$$\sum_{d\le x}\frac{1}{d^2} = \frac{x^{1-2}}{1-2} + \zeta(2) + O(x^{-2}) = \frac{-1}{x} + \zeta(2) + O(x^{-2})$$

(ii) By Theorem 3.5.1, $\sum_{n\le x}\frac{1}{n} = \log x + C + O(\frac{1}{x})$.

Take d in place of n for second term of the above.]

$$= x\left(\frac{-1}{x} + \zeta(2) + O(x^{-2})\right) + O\left(\log x + C + O(\tfrac{1}{x})\right)$$

$$= -1 + x.\zeta(2) + x.O(x^{-2}) + O\left(\log x + C + O(\tfrac{1}{x})\right)$$

$$= -1 + x.\zeta(2) + x.O(x^{-2}) + O(\log x)$$

[Since $\lim_{x\to\infty}\frac{(\log x + C + O(\frac{1}{x}))}{\log x} = 1$, we have $[\log x + C + O(\frac{1}{x})] = O(\log x)$]

$= -1 + x.\zeta(2) + O(\frac{1}{x}) + O(\log x)$ [since $x.O(x^{-2}) = O(\frac{1}{x})$]

$= -1 + x.\zeta(2) + O(\log x)$ [Since $O(\frac{1}{x}) + O(\log x) = O(\log x)$]

$= x.\zeta(2) + O(\log x)$ (since, constant + $O(f(x)) = O(f(x))$)

Thus if $\beta = 1$, we have $\sum_{n\le x}\sigma_{-\beta}(n) = \sum_{n\le x}\sigma_{-1}(n) = x.\zeta(2) + O(\log x)$.

Self Assessment Question 3: *Verify* $\frac{x^{1-\beta}}{1-\beta} + \zeta(\beta) + O(x^{-\beta}) = O(x^{1-\beta})$

Self Assessment Question 4: *Verify* $O(x^{1-\beta}) = O(x^{\delta})$, *where* $\delta = \max\{\beta, 1-\beta\}$

Self Assessment Question 5: *Verify* $O(\frac{1}{x}) + O(\log x) = O(\log x)$

4.3 THE AVERAGE ORDER OF φ (n)

4.3.1. Note:

(i). Consider $\sum_{n=1}^{\infty}\frac{\mu(n)}{n^2}$. Since $\mu(n) \le 1$ by the def. of Mobius function, $\left|\frac{\mu(n)}{n^2}\right| \le \frac{1}{n^2}$.

Therefore $\sum_{n=1}^{\infty}\frac{\mu(n)}{n^2}$ is absolutely convergent.

(ii) $\sum_{n=1}^{\infty}\frac{\mu(n)}{n^2} = \frac{1}{\zeta(2)} = \frac{6}{\pi^2}$. [Proof is out of the scope of the book].

(iii) Similarly $\sum_{n=1}^{\infty}\frac{\mu(n)}{n^s} = \frac{1}{\zeta(s)}$

4.3.2 Theorem: (i) $\sum_{n\le x}\frac{\mu(n)}{n^s} = \frac{1}{\zeta(s)} + O(x^{1-s})$ and in particular

(ii) $\sum_{n\le x}\frac{\mu(n)}{n^2} = \frac{6}{\pi^2} + O(\frac{1}{x})$.

Proof: (i) By the above Note 4.3.1, we have $\sum_{n=1}^{\infty}\frac{\mu(n)}{n^s} = \frac{1}{\zeta(s)}$

$$\Rightarrow \sum_{n\le x}\frac{\mu(n)}{n^s} + \sum_{n>x}\frac{\mu(n)}{n^s} = \frac{1}{\zeta(s)} \Rightarrow \sum_{n\le x}\frac{\mu(n)}{n^s} = \frac{1}{\zeta(s)} - \sum_{n>x}\frac{\mu(n)}{n^s}.$$

Therefore $\sum_{n\le x}\frac{\mu(n)}{n^s} = \frac{1}{\zeta(s)} + O(x^{1-s})$.

[since $\mu(n) \le 1$ and $\sum_{n>x}\frac{1}{n^s} = O(x^{1-s})$ (by Corollary 3.5.4)]

(ii) Take $s = 2$ in (i), then

$$\sum_{n\le x}\frac{\mu(n)}{n^2} = \frac{1}{\zeta(2)} + O(x^{1-2})$$

$= \frac{6}{\pi^2} + O(\frac{1}{x})$. (since $\zeta(2) = \sum_{n=1}^{\infty}\frac{1}{n^2} = \frac{\pi^2}{6}$). This completes the proof.

4.3.3 Theorem: For $x > 1$, we have

(i) $\sum_{n\le x}\varphi(n) = \frac{3}{\pi^2}x^2 + O(x\log x)$; and (ii) The average order of $\varphi(n)$ is $\frac{3n}{\pi^2}$.

Proof: We know that $\varphi(n) = \sum_{d|n}\mu(d).\frac{n}{d} \Rightarrow \sum_{n\le x}\varphi(n) = \sum_{n\le x}\sum_{d|n}\mu(d).\frac{n}{d}$. [By Th. 1.5.14]

Then $\sum_{n\le x}\varphi(n) = \sum_{d\le x}\sum_{\delta\le\frac{x}{d}}\mu(d)\delta$ (Here $n = d\,\delta$)

$$= \sum_{d\le x}\mu(d)\sum_{\delta\le\frac{x}{d}}\delta$$

[Now we use Theorem 3.5.5, $\sum_{n\le x}n^\alpha = \frac{x^{\alpha+1}}{\alpha+1} + O(x^\alpha)$.]

$$= \sum_{d\le x}\mu(d)\left\{\frac{1}{2}\left(\frac{x}{d}\right)^2 + O\left(\frac{x}{d}\right)\right\} = \frac{x^2}{2}\sum_{d\le x}\frac{\mu(d)}{d^2} + O\left(x\sum_{d\le x}\frac{\mu(d)}{d}\right)$$

[Now we use, for 1st term: above Theorem 4.3.2 (ii) use d in place of n.

for second term: $|\mu(d)| \leq 1 \Rightarrow \left|\frac{\mu(d)}{d}\right| \leq \frac{1}{d}$

$$\Rightarrow O\left(x\sum_{d\leq x}\frac{\mu(d)}{d}\right) = O\left(x\sum_{d\leq x}\frac{1}{d}\right) \quad]$$

$$= \frac{x^2}{2}\left(\frac{6}{\pi^2} + O\left(\frac{1}{x}\right)\right) + O\left(x\sum_{d\leq x}\frac{1}{d}\right)$$

$$= \frac{3x^2}{\pi^2} + \frac{x^2}{2}.O\left(\tfrac{1}{x}\right) + O\left(x\left[\log x + C + O\left(\tfrac{1}{x}\right)\right]\right)$$

[Since $\sum_{n\leq x}\frac{1}{n} = \log x + C + O\left(\frac{1}{x}\right)$, by Theorem 3.5.1]

$$= \frac{3x^2}{\pi^2} + O(x) + O(x\log x + xC + O(1))$$

$$= \frac{3x^2}{\pi^2} + O(x) + O(x\log x)$$

$$= \frac{3x^2}{\pi^2} + O(x\log x).$$

(ii) The average order of $\varphi(n)$

$$\overline{\varphi(n)} = \frac{1}{n}\sum_{k=1}^{n}\varphi(k)$$

$$= \frac{1}{n}\sum_{k\leq n}\varphi(k).$$

Therefore $\sum_{n\leq x}\varphi(n) = \frac{3x^2}{\pi^2} + O(x\log x).$

$$= \frac{1}{n}\left[\frac{3n^2}{\pi^2} + O(n\log n)\right] = \frac{3n}{\pi^2} + O(\log n)$$

Consider $\lim_{n\to\infty}\frac{\overline{\varphi(n)}}{\left(\frac{3n}{\pi^2}\right)} = \lim_{n\to\infty}\frac{\left(\frac{3n}{\pi^2}\right)}{\left(\frac{3n}{\pi^2}\right)} + \lim_{n\to\infty}\frac{O(\log n)}{\left(\frac{3n}{\pi^2}\right)}$

$$= 1 + \lim_{n\to\infty}\left(\frac{O(\log n)}{3n}\right).\pi^2 = 1 + 0 = 1$$

Therefore by the definition of average order, we get that average order of $\varphi(n)$ is $\frac{3n}{\pi^2}$.

4.4 AN APPLICATION TO THE DISTRIBUTION OF LATTICE POINTS VISIBLE FROM THE ORIGIN

4.4.1 Definition: Two lattice points P and Q are said to be **mutually visible** if the line segment which joins P and Q contains no lattice points other than the end points P and Q.

4.4.2 Definition: A lattice point P(a, b) is said to be **visible from the origin** if the line segment joining the origin and the point P has no lattice points other than origin and P.

4.4.3 Example: (1, 1), (2, 3), (3, 2), (2, 1) are visible points from origin. (2, 2) is not a visible point from the origin.

4.4.4 Theorem: A lattice point (a, b) is visible from the origin ⇔ a and b are relatively prime.

Proof: Suppose (a, b) is visible lattice point from the origin.
Now we have to show that a and b are relatively prime. Suppose (a, b) = d.

In a contrary way suppose that d > 1. Then $\left(\frac{a}{d}, \frac{b}{d}\right)$ is also a lattice point on the line segment joining (0, 0) to (a, b), a contradiction. Therefore d = 1.
Hence a and b are relatively prime numbers.

Converse: Suppose (a, b) = 1. In a contrary way assume that (a, b) is not a visible point from the origin. Then there exists a lattice point say (a^1, b^1) on the line segment joining (0, 0) and (a, b). This means there exists a rational number t with $0 < t < 1$ such that $a^1 = ta$ and $b^1 = tb$. (Note that t can not be an integer). Suppose $t = r/s$ where r and s are integers (r, s) = 1 and $s \neq 0$.

Then $a^1 = \frac{ra}{s}$, $b^1 = \frac{rb}{s}$ ⇒ s / ra , s / rb (since a^1, b^1 are integers)

⇒ s / a, s / b (since r and s are relatively prime numbers)
⇒ s = 1 (since g.c.d of a and b is 1)
⇒ t = r and so t is an integer, a contradiction.
Therefore (a, b) is a visible point from origin.

4.4.5 Theorem: Two lattice points (a, b) and (m, n) are mutually visible
⇔ a - m and b - n are relatively prime.

Proof: Suppose (a, b) and (m, n) are mutually visible
⇔ (a - m, b - n) and (m -m, n - n) are mutually visible (by shifting the origin to (m, n))
⇔ (a - m, b - n) and (0, 0) are mutually visible
⇔ a - m, and b - n are relatively prime (by Theorem 4.4.4).
This completes the proof.

4.4.6 Definition: For any r > 0, let N(r) be the number of lattice points in the (square) $\{(x, y) / |x|, |y| \leq r\}$ and $N^1(r)$ is the number of the lattice points which are visible from the origin. $\lim_{n\to\infty} \frac{N^1(r)}{N(r)}$ is called the **density** of the lattice points visible from the origin.

4.4.7 Theorem: The set of lattice points visible from the origin has density $\frac{6}{\pi^2}$.

Proof: We know that, by Theorem 4.4.4, the lattice point (a, b) is visible from the origin $\Leftrightarrow$ a, b are relatively prime.

Part-(i): To find $N^1(r)$:

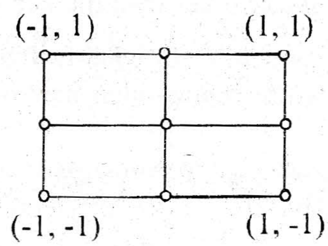


Fig - 4.4.7 A

Let $r \geq 1$ and $S_r = \{(x, y) / |x| \leq r, |y| \leq r\}$.

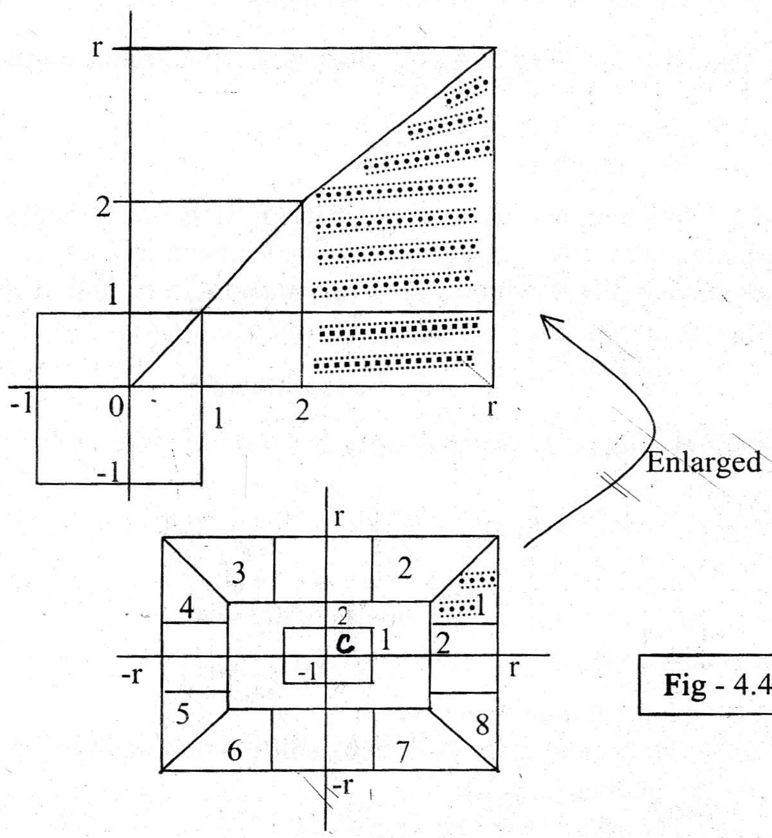


Fig - 4.4.7 B

The notation used is

N(r) = the number of lattice points in the square S.

$N^1(r)$ = the number of visible lattice points from the origin in the square S.

If r = 1, then S_r contains the eight visible lattice points from the origin, these are
(1, 1), (0, 1), (0, -1), (0, -1), (-1, -1), (-1, 0), (-1, 1), (0, 1)

Therefore $N(1) = 8 = N^1(1)$. Observe the figure. in general (for any r)
$N^1(r)$ = Number of lattice points visible from the origin in $S_1 + 8 \times$ (number of lattice points is the shaded region of the figure)

$= 8 + 8 \times$ (number of lattice points in $\{(x, y) / 2 \le x \le r,\ 1 \le y \le x\}$ that are visible from the origin)

$= 8 + 8 \times$ (number of lattice points in $\{(x, y) / 2 \le x \le r,\ 1 \le y \le x\}$ such that x, y are relatively prime) (by Theorem 4.4.4)

$$= 8 + 8 \sum_{2 \le x \le r} \varphi(x)\ (x, y) = 1$$

$$= 8.\ \varphi(1) + 8 \sum_{2 \le x \le r} \varphi(x) \quad \left[\text{We know that } \varphi(n) = \sum_{\substack{k=1 \\ (k,n)=1}}^{n} 1 . \Rightarrow \varphi(1) = 1\right]$$

Here we use Euler's totient function.

$$= 8. \sum_{n=1}^{r} \varphi(n)$$

$$= 8. \sum_{n \le r} \varphi(n) = 8\left\{\frac{3r^2}{\pi^2} + O(r \log r)\right\} \text{ (by Theorem 4.3.3)}$$

$$= \frac{24r^2}{\pi^2} + O(r \log r)$$

Therefore $N^1(r) = \dfrac{24r^2}{\pi^2} + O(r \log r)$ ... (i)

Part-(ii): (To find N(r)): Consider the part of X-axis and part of Y-axis inside S_r.

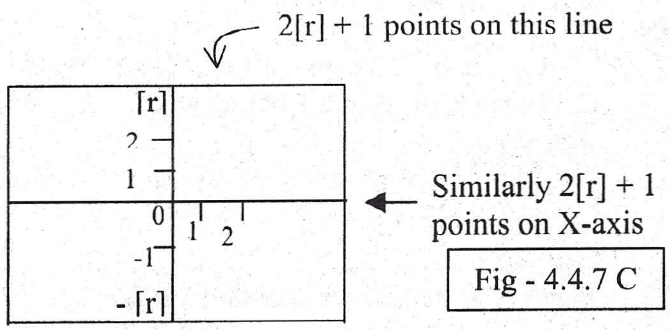


Fig - 4.4.7 C

These two contains $2[r] + 1$ integers.
So the lattice points are $(2[r] + 1) \times (2[r] + 1) = (2[r] + 1)^2$ in number.
Therefore $N(r) = (2[r] + 1)^2 = (2(r + O(1)) + 1)^2 = 4r^2 + O(r)$
Therefore $N(r) = 4r^2 + O(r)$ ... (ii)
Part-(iii): From (i) and (ii) we get

$$\frac{N^1(r)}{N(r)} = \frac{\frac{24r^2}{\pi^2} + O(r\log r)}{4r^2 + O(r)} = \frac{\frac{6}{\pi^2} + O\left(\frac{\log r}{r}\right)}{1 + O\left(\frac{1}{r}\right)}. \text{ Now } \lim_{r\to\infty} \frac{N^1(r)}{N(r)} = \frac{\frac{6}{\pi^2}+0}{1+0} = \frac{6}{\pi^2}.$$

Hence the density of lattice points visible from the origin is $\frac{6}{\pi^2}$. Hence the theorem.

4.5 THE AVERAGE ORDER OF $\mu(n)$ AND $\wedge(n)$

4.5.1 Note: (i) Finding the average orders of $\mu(n)$ and $\wedge(n)$ are more difficult than that of $\phi(n)$ and the divisor function. It is known that $\mu(n)$ has average order 0 and $\wedge(n)$ has the average order 1.

That is., $\lim_{x\to\infty} \frac{1}{x}\sum_{n\le x}\mu(n) = 0$ and $\lim_{x\to\infty} \frac{1}{x}\sum_{n\le x}\wedge(n) = 1$

(ii) These results (given (i)) are equivalent to the prime number theorem $\lim_{x\to\infty} \frac{\pi(x)\log x}{x} = 1$ where $\pi(x)$ is the number of primes $\le x$.

4.6 SUMMARY

In this lesson, an attempt has been made for finding average orders of certain arithmetic functions: Mobius, Liouville's, Euler and divisor function. Also provided applications, computing techniques involving arithmetic functions, particularly to the distribution of lattice points visible from the origin

4.7 TECHNICAL TERMS

Lattice point : Coordinates (d, f) in the plane, wh... and f are both integers.

Dirichlet Asymptotic formula: $\sum_{n\le x} d(n) = x\log x + (2C - 1)x + O(\sqrt{x})$, where C is the Euler's constant $x \ge 1$.

Average order of $\sigma_\alpha(n)$: $\sum \sigma_\alpha(n) = \frac{\zeta(\alpha+1)}{\alpha+1} \cdot x^{\alpha+1} + O(x^\beta)$, $x \ge 1$, $\alpha > 0, \alpha \ne 1, \beta = \{1, \alpha\}$.

The average order of $\varphi(n)$: $\frac{3n}{\pi^2}$. (Since $\sum_{n\le x}\varphi(n) = \frac{3}{\pi^2}\cdot x^2 + O(x\log x)$.)

Visible from the origin: Lattice point p(a, b) is said to be visible from the origin if there are no lattice points on the segment PQ.

Density: $\lim_{n\to\infty} \frac{N^1(r)}{N(r)}$ where N(r) = number of lattice points in $\{(x, y) / |x|, |y| \le r\}$; $N^1(r)$ = number of lattice points which are visible from the origin.

4.8 ANSWERS TO SELF ASSESSMENT QUESTIONS

1: Since $[x] \le x$, we have $\left(\frac{[x]}{x}\right) \le 1$, for any x. So $[x] = O(x.)$

Therefore in particular we have $O(\sqrt{x}) = [\sqrt{x}\,]$.

Take $y = \frac{x}{d}$.

Consider $\lim_{y\to\infty} \frac{y + O(1)}{y} = 1 + \lim_{y\to\infty} \frac{O(1)}{y} = 1 + 0 = 1$

This implies $O(y) = O(1) + y$. We know that $[y] = O(y)$

Therefore $[y] = O(1) + y$.

2: Suppose $f(x) = O\left(\frac{1}{\sqrt{x}}\right)$

$\Rightarrow \frac{f(x)}{\frac{1}{\sqrt{x}}} < M$ for some constant $M > 0$. $\Rightarrow \sqrt{x}\,.f(x) < M \Rightarrow \frac{x \cdot f(x)}{\sqrt{x}} < M.$

$\Rightarrow x\cdot f(x) = O(\sqrt{x})$. That is., $x\cdot O\left(\frac{1}{\sqrt{x}}\right) = O(\sqrt{x})$.

3: Consider $\lim_{x\to\infty} \frac{\frac{x^{1-\beta}}{1-\beta} + \zeta(\beta) + O(x^{-\beta})}{x^{1-\beta}} = \frac{1}{1-\beta} + 0 + 0 = \frac{1}{1-\beta}$

$$\Rightarrow \frac{x^{1-\beta}}{1-\beta} + \zeta(\beta) + O(x^{-\beta}) = O(x^{1-\beta}).$$

4: For this consider, $1 - \beta \le \max\{\beta, 1 - \beta\} = \delta$.

$$\Rightarrow \lim_{x\to\infty} \frac{x^{1-\beta}}{x^{\delta}} = \begin{cases} 0 \text{ if } 1 - \beta < \delta. \\ 1 \text{ if } 1 - \beta = \delta. \end{cases}$$

So $x^{1-\beta} = O(x^{\delta}) \Rightarrow O(x^{1-\beta}) = O(O(x^{\delta})) = O(x^{\delta})$.

5: $\lim_{x\to\infty} (\frac{1}{x})/\log x = \lim_{x\to\infty} \frac{1}{x \log x} = 0.$

So $\frac{1}{x} = O(\log x) \Rightarrow O(\frac{1}{x}) = O(\log x) \Rightarrow O(\frac{1}{x}) + O(\log x) = O(\log x)$.

4.9 MODEL QUESTIONS

1. Define lattice point. Show that if $d(n)$ is the number of positive divisors of n, then for any $x \geq 1$ we have $\sum_{n\leq x} d(n) = x \log x + O(x)$.
2. State and prove Dirichlet Asymptotic formula.
3. Show that if $\sigma(n)$ is the sum of the positive divisors of n, then for any $x \geq 1$ we have $\sum_{n\leq x} \sigma(n) = \frac{1}{2}.\zeta(2).x^2 + O(x \log x)$.
4. Show that if $x \geq 1$ and $\alpha > 0$, $\alpha \neq 1$, then $\sum_{n\leq x} \sigma_\alpha(n) = \frac{\zeta(\alpha+1)}{\alpha+1}.x^{\alpha+1} + O(x^{\beta})$ where $\beta = \max\{1, \alpha\}$.
5. Show that for $x > 1$, (i) $\sum_{n\leq x} \phi(n) = \frac{3}{\pi^2}x^2 + O(x \log x)$; and
(ii) The average order of $\phi(n)$ is $\frac{3n}{\pi^2}$.
6. A lattice point (a, b) is visible from the origin $\Leftrightarrow$ a and b are relatively prime.

4.10 REFERENCE BOOKS

1. Chandrasekharan, K. "Introduction to Analytic Number Theory", Springer Verlag .
2. Hardy, G.H. & Wright, E.M. "Introduction to the Theory of Numbers", Fourth Edition, Oxford Publications,
3. Levegue W.J. (1986) "Topics in Number Theory (2 volumes), Addition - Wesley Publ. Co.
4. Rademacher (1964) "Lectures on Elementary Number Theory", New York, Blaisdell Publ. Co.
5. Tom M. Apostol "Introduction to Analytic Number Theory", Springer International Student Edition, Narosa Publishing House, 1995.
6. Uspensky, J.V., and Heaslett, M.A. (1939) "Elementary Number Theory", New York, Mc. Graw - Hill Book. Co.
7. Vinogrador, "Elements of Number Theory", Dover Publications

Name of the Author of this Lesson: **Dr. Kuncham Syam Prasad**

LESSON - 5

THE PARTIAL SUMS OF A DIRICHLET PRODUCT

Objectives

The Objectives of this lesson are to:

- understand Dirichlet product
- to know applications of Mobius function $\mu(n)$ and Mangold's function $\wedge(n)$
- analyze the partial sums of a Dirichlet product

Structure

5.0 INTRODUCTION

In the previous lessons we derived some elementary identities involving $\mu(n)$ and $\wedge(n)$ which are useful to study the distribution of primes. Now we obtain them from a general formula relating the partial sums of arbitrary arithmetical functions f and g with those of their Dirichlet product f * g. We examine the applications to $\mu(n)$ and $\wedge(n)$. We observed that the factorial of integral part of $x \geq 1$ is the product of primes, called the Legendre's identity. We use Euler's summation formula to determine an asymptotic for log [x]! and find another identity for the partial sums of a Dirichlet product.

5.1 THE PARTIAL SUMS OF DIRICHLET PRODUCT

5.1.1 Theorem: Suppose f and g are two arithmetical functions and $h = f*g$, the Dirichlet product of f and g.

Suppose $F(x) = \sum_{n \leq x} f(n)$, $G(x) = \sum_{n \leq x} g(n)$ and $H(x) = \sum_{n \leq x} h(n)$.

Then $H(x) = \sum_{n \leq x} f(n)\, G(\frac{x}{n}) = \sum_{n \leq x} g(n)\, F(\frac{x}{n})$

Proof: We know that $(f*g)(n)=\sum_{d|n} f(d)\, g(\frac{n}{d})$ and $(f\circ g)(x)=\sum_{n\le x} f(n)\, g(\frac{x}{n})$

Now f, g and h are arithmetical functions.

Consider the function $u(x)=\begin{cases}0 & \text{if } 0<x<1\\ 1 & \text{if } x\ge 1\end{cases}$

We have to prove that $H=f\circ G=g\circ F$.

Consider $F(x)=\sum_{n\le x} f(n)=\sum_{n\le x} f(n)\, u(\frac{x}{n})=(f\circ u)(x)$

$G(x)=\sum_{n\le x} g(n).1=\sum_{n\le x} g(n)\, u(\frac{x}{n})=(g\circ u)(x)$ .... (i) and

$H(x)=\sum_{n\le x} h(n)=\sum_{n\le x} h(n)\, u(\frac{x}{n})=(h\circ u)(x)$ ....(ii)

Consider $(f\circ G)(x)=[f\circ(g\circ u)](x)=[(f*g)\circ u](x)$ (We know that in general $g\circ(h\circ f)=(g*h)\circ f$)

$=(h\circ u)(x)$ (since $h=f*g$)

$=H(x)$ (by (ii)).

Therefore $H(x)=(f\circ G)(x)$

Consider $(g\circ F)(x)=[g\circ(f\circ u)](x)$ (since $f=f\circ u$)

$=[(g*f)\circ u](x)=(h\circ u)(x)$ (since $h=f*g$) $=H(x)$.

Therefore $H(x)=(f\circ G)(x)=(g\circ F)(x)$. Hence $H=f\circ G=g\circ F$.

5.1.2 Corollary: If $g(n)=1$ for all n, then $G(x)=[x]$.

Proof: From above $G(x)=\sum_{n\le x} g(n)=\sum_{n\le x} 1=[x]$.

5.1.3 Theorem: If $F(x)=\sum_{n\le x} f(n)$, then $\sum_{n\le x}\sum_{d|n} f(d)=\sum_{n\le x} f(n)[\frac{x}{n}]=\sum_{n\le x} F(\frac{x}{n})$.

Proof: Consider the statement of Theorem 5.1.1.

Take $g(n)=1$ for all n. Then by Corollary 5.1.2, we have that $G(x)=[x]$ .... (i)

Theorem 5.1.1, says that $H(x)=\sum_{n\le x} f(n)\, G(\frac{x}{n})=\sum_{n\le x} g(n).F(\frac{x}{n})$ .... (ii)

From (ii) $H(x)=\sum_{n\le x} f(n)\, G(\frac{x}{n})=\sum_{n\le x} f(n).\left[\frac{x}{n}\right]$ (by (i)) .... (iii)

From (ii) $H(x)=\sum_{n\le x} g(n)\, F(\frac{x}{n})=\sum_{n\le x} 1\cdot F\left(\frac{x}{n}\right)$ (by def. g) $=\sum_{n\le x} F(\frac{x}{n})$ .... (iv)

See statement of Theorem 5.1.1, $H(x)=\sum_{n\le x} h(n)$ and $h=f*g$.

Now $h(n)=\sum_{d|n} f(d)\, g(\frac{x}{d})=\sum_{d|n} f(d).1$ (since $g(n)=1$ for all n) $=\sum_{d|n} f(d)$ .... (v)

Therefore $H(x)=\sum_{n\le x} h(n)=\sum_{n\le x}\sum_{d|n} f(d)$ ... (vi) (from (v))

From (iii), (iv), (vi) we have that

$$\sum_{n\le x}\sum_{d|n} f(d) = \sum_{n\le x} f(n)\left[\tfrac{x}{n}\right] = \sum_{n\le x} F\left(\tfrac{x}{n}\right).$$

Hence the Theorem.

5.2 APPLICATIONS TO $\mu(n)$ AND $\wedge(n)$

5.2.1 Theorem: For $x \ge 1$, we have

$$\sum_{n\le x}\mu(n)\left[\tfrac{x}{n}\right] = 1 \text{ and } \sum_{n\le x}\wedge(n)\left[\tfrac{x}{n}\right] = \log([x]!)$$

(These sums are regarded as weighted averages of $\mu(n)$ and $\wedge(n)$).

Proof: From Theorem 5.1.3, we have

$$\sum_{n\le x}\sum_{d|n} f(d) = \sum_{n\le x} f(n)\left[\tfrac{x}{n}\right] = \sum_{n\le x} F\left(\tfrac{x}{n}\right) \quad \ldots \text{(i)}$$

Part-(i): In $\sum_{n\le x} f(n)\left[\tfrac{x}{n}\right] = \sum_{n\le x}\sum_{d\le n} f(d)$, $f(n) = \mu(n)$.

Then we have $\sum_{n\le x}\mu(n)\left[\tfrac{x}{n}\right] = \sum_{n\le x}\left(\sum_{d|n}\mu(d)\right)$

$$= \sum_{n\le x}\left[\frac{1}{n}\right] = \left[\frac{1}{1}\right]+\left[\frac{1}{2}\right]+\ldots+\left[\frac{1}{[x]}\right] = 1+0+\ldots+0 = 1$$ (Since $\sum_{d/n}\mu(d) = I(n) = \left[\frac{1}{n}\right]$ (by theorem 1.5.7 and by definition of I(n)))

Therefore $\sum_{n\le x}\mu(n)\left[\tfrac{x}{n}\right] = 1$.

Part-(ii): We know that Mangoldt function $\wedge(n) = \begin{cases} \log p, & \text{if } n = p^m,\ m \ge 1 \text{ and} \\ 0, & \text{otherwise.}\end{cases}$

Taking $f(n) = \wedge(n)$ in (i) we get

$$\sum_{n\le x}\wedge(n)\left[\tfrac{x}{n}\right] = \sum_{n\le x}\sum_{d|n}\wedge(d).$$

$$= \sum_{n\le x}\log n \text{ [by theorem 2.2.3]}$$

$$= \log 1 + \log 2 + \ldots + \log [x]$$

$$= \log(1\times 2\times \ldots \times [x])$$

$$= \log([x]!)$$

5.2.2 Theorem: Legendre's identity: For every $x \ge 1$, we have $[x]! = \prod_{p\le x} p^{\alpha(p)}$ where the product is extended over all primes $\le x$ and $\alpha(p) = \sum_{m=1}^{\infty}\left[\frac{x}{p^m}\right]$.

Proof: We know that

$$\wedge(n) = \begin{cases} \log p & \text{if } n = p^m \text{ for some prime } p, m \geq 1 \\ 0 & \text{otherwise} \end{cases}$$

Consider $\log([x]!) = \sum_{n \leq x} \wedge(n)\left[\frac{x}{n}\right]$ (by Theorem 5.2.1 part (ii))

$$= \sum_{p \leq x} \sum_{m=1}^{\infty} \log p \left[\frac{x}{p^m}\right] \quad \text{[since } \wedge(n) = 0 \text{ if } n \neq p^m \text{ for some } m\text{]}$$

$$= \sum_{p \leq x} \left[\left(\sum_{m=1}^{\infty} \left[\frac{x}{p^m}\right]\right) \log p\right] = \sum_{p \leq x} \alpha(p) \log p, \text{ where } \alpha(p) = \sum_{m=1}^{\infty} \left[\frac{x}{p^m}\right].$$

$$= \sum_{p \leq x} \log\left(p^{\alpha(p)}\right) = \prod_{p \leq x} (p^{\alpha(p)})$$

Therefore $\log([x]!) = \log \prod_{p \leq x} \left(p^{\alpha(p)}\right) \Rightarrow [x]! = \prod_{p \leq x} \left(p^{\alpha(p)}\right)$

5.2.3 Theorem: For all $x \geq 1$, we have $\left|\sum_{n \leq x} \frac{\mu(n)}{n}\right| \leq 1$

(Moreover, $\sum_{n \leq x} \frac{\mu(n)}{n} = 1$ only if $x < 2$).

Proof: Suppose $x < 2$. Then $\sum_{n \leq x} \frac{\mu(n)}{n} = \frac{\mu(1)}{1} = \frac{1}{1} = 1$, and so $\left|\sum \frac{\mu(n)}{n}\right| = 1$.

Assume that $x \geq 2$.
For any real y we use the notation: $\{y\} = y - [y]$.
(clearly $0 < \{y\} < 1$) then $y = [y] + \{y\}$
We have $1 = \sum_{n \leq x} \mu(n)\left[\frac{x}{n}\right]$ (by Theorem 5.2.1, weighted average of $\mu(n)$)

$$= \sum_{n \leq x} \mu(n)\left(\frac{x}{n} - \left\{\frac{x}{n}\right\}\right) = x \sum_{n \leq x} \frac{\mu(n)}{n} - \sum_{n \leq x} \mu(n)\left\{\frac{x}{n}\right\}.$$

$$\Rightarrow x \sum_{n \leq x} \frac{\mu(n)}{n} = 1 + \sum_{n \leq x} \mu(n)\left\{\frac{x}{n}\right\}$$

$$\Rightarrow x\left|\sum_{n \leq x} \frac{\mu(n)}{n}\right| = \left|1 + \sum_{n \leq x} \mu(n)\left\{\frac{x}{n}\right\}\right| = \left|1 + \mu(1)\left\{\frac{x}{1}\right\} + \sum_{2 \leq n \leq x} \mu(n)\left\{\frac{x}{n}\right\}\right|$$

$$= \left|1 + \{x\} + \sum_{2 \leq n \leq x} \mu(n)\left\{\frac{x}{n}\right\}\right|$$

$$\leq 1 + \{x\} + \left|\sum_{2 \leq n \leq x} \mu(n)\left\{\frac{x}{n}\right\}\right|.$$

$$= 1 + \{x\} + \sum_{\substack{2 \le n \le x \\ n \text{ is square free}}} \left\{\frac{x}{n}\right\}$$ [If n is not square free then $\mu(n) = 0$.

If n is square free, then $|u(n)| = |(\pm 1)| = 1$]

Now, $\sum_{2 \le n \le x} \left\{\frac{x}{n}\right\} = \left\{\frac{x}{2}\right\} + \left\{\frac{x}{3}\right\} + \ldots + \left\{\frac{x}{[x]}\right\}$

$\le 1 + 1 + \ldots + 1$ ([x] - 1 times) (since $\{y\} \le 1$ for all y) = [x] - 1

Therefore $x\left|\sum_{n \le x} \frac{\mu(n)}{n}\right| \le 1 + \{x\} + ([x] - 1) = x = 1 + x - [x] + [x] - 1 = x$

(Since $\{x\} = x - [x]$)

Therefore $x\left|\sum_{n \le x} \frac{\mu(n)}{n}\right| \le x$. Hence $\left|\sum_{n \le x} \frac{\mu(n)}{n}\right| \le 1$.

5.2.4 Theorem: For $x \ge 2$, we have

$$\log [x]! = x \log x - x + O(\log x) \text{ and } \sum_{n \le x} \wedge (n)\left[\tfrac{x}{n}\right] = x \log x - x + O(\log x)$$

Proof: By Theorem 5.2.1, we have $\sum_{n \le x} \wedge (n)\left[\tfrac{x}{n}\right] = \log [x]!$

$$= \log(1 \times 2 \times \ldots \times [x]) = \log 1 + \log 2 + \ldots + \log[x] = \sum_{n \le x} \log n \quad \ldots \text{(i)}$$

Now let $f(t) = \log t$ be a function having continuous derivative in $[1, x]$ for any $x \ge 1$.
By Euler's summation formula:

$$\sum_{a < n \le b} f(n) = \int_a^b f(t)dt + \int_a^b (t - [t]) f'(t)dt + f(b)([b] - b) - f(a)([a] - a)$$

we have, $\sum_{1 < n \le x} \log n = \int_1^x \log t dt + \int_1^x (t - [t]) f'(t)dt + ([x] - x) \log x - ([1] - 1) \log 1$

$$= [t \log t - t]_1^x + \int_1^x \frac{(t - [t])}{t} dt + O(\log x) \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \text{(ii)}$$

[Since (i) $f^1(t) = (\log (t))^1 = \frac{1}{t}$; (ii) $0 \le |[x] - x| < 1$

$\Rightarrow |([x] - x) \log x| < \log x \Rightarrow ([x] - x) \log x = O(\log x)$]

Now $0 \le t - [t] < 1 \Rightarrow \frac{t - [t]}{t} < \frac{1}{t} \Rightarrow \int_1^x \frac{(t - [t])}{t} dt < \int_1^x \frac{1}{t} dt = \log x$ (since $\log 1 = 0$)

$$\Rightarrow \int_1^x \frac{(t - [t])}{t} dt < \log x \quad \Rightarrow \int_1^x \frac{(t - [t])}{t} dt = O(\log x) \quad \ldots\ldots\ldots\ldots\ldots\ldots \text{(iii)}$$

and $[t \log t - t]_1^x = [x \log x - x] - [1.\log 1 - 1] = [x \log x - x] + 1 \quad \ldots\ldots\ldots\ldots\ldots\ldots \text{(iv)}$

From (ii), (iii) and (iv) we get,

6)

$$\sum_{1<n\le x} \log n = (x \log x - x + 1) + O(\log x) + O(\log x) = x \log x - x + O(\log x)$$

Since $\log 1 = 0$, we have $\sum_{1<n\le x} \log n = \sum_{n\le x} \log n$.

So, $\sum_{n\le x} \log n = x \log x - x + O(\log x)$.

By (i) we have $\sum_{n\le x} \wedge(n)\left[\frac{x}{n}\right] = \sum_{n\le x} \log n$

Therefore $\sum_{n\le x} \wedge(n)\left[\frac{x}{n}\right] = x \log x - x + O(\log x)$.

This completes the proof.

5.2.5 Theorem: For $x \ge 2$,we have $\sum_{p\le x}\left[\frac{x}{p}\right]\log p = x \log x + O(x)$ where the sum is extended over all primes $p \le x$.

Proof: By Theorem 5.2.4, we have $\sum_{n\le x} \wedge(n)\left[\frac{x}{n}\right] = x \log x - x + O(\log x)$

We know that Mongoldt function $\wedge$ defined by $\wedge(n) = \begin{cases} \log p & \text{if } n = p^m, m \ge 1 \\ 0 & \text{otherwise} \end{cases}$

So, $\sum_{n\le x} \wedge(n)\left[\frac{x}{n}\right] = \sum_{p\le x}\sum_{m=1}^{\infty} \wedge(p^m)\left[\frac{x}{p^m}\right]$ (with $p^m \le x$)

$$= \sum_{p\le x}\sum_{m=1}^{\infty} (\log p)\left[\frac{x}{p^m}\right] \quad (\text{with } p^m \le x)$$

$$= \sum_{p\le x} (\log p)\left[\frac{x}{p}\right] + \sum_{p\le x}\sum_{m=2}^{\infty} (\log p)\left[\frac{x}{p^m}\right] \quad (\text{with } p^m \le x)$$

$$\Rightarrow \sum_{p\le x} (\log p)\left[\frac{x}{p}\right] = \sum_{n\le x} \wedge(n)\left[\frac{x}{n}\right] - \sum_{p\le x}\sum_{m=2}^{\infty} (\log p)\left[\frac{x}{p^m}\right] \quad \ldots\ldots\ldots\ldots\ldots\ldots \text{(i)}$$

Note that all the following p 's are with $p^m \le x$.

Consider $\sum_{p\le x}\sum_{m=2}^{\infty} (\log p)\left[\frac{x}{p^m}\right] \le \sum_{p\le x}\sum_{m=2}^{\infty} (\log p)\frac{x}{p^m}$ (since $[x] \le x$)

$$= x\sum_{p\le x} (\log p)\left(\sum_{m=2}^{\infty} \frac{1}{p^m}\right)$$

$$= x\sum_{p\le x} (\log p)\left(\frac{1}{p(p-1)}\right) \quad (\text{using G.P. formula})$$

$$\le x\sum_{n\le x} \frac{\log n}{n(n-1)} \le x\sum_{n=2}^{\infty} \frac{\log n}{n(n-1)}.$$

Therefore by this ratio test, it is clear that $\sum_{n=2}^{x} \frac{\log n}{n(n-1)}$ converges (verify !).

So this sum is finite quantity.

Therefore from the above we get that $x\left(\sum_{n\le x} \frac{\log n}{n(n-1)}\right) = O(x)$ .... (ii)

We know that by Theorem 5.2.4, $\sum_{n\le x} \wedge(n)[\frac{x}{n}] = x \log x - x + O(\log x)$ .... (iii)

From (i), (ii) and (iii) we get

$$\sum_{p\le x} (\log p)[\tfrac{x}{p}] = (x \log x - x + O(\log x)) + O(x)$$

$$= x \log x + O(x) + O(x) + O(x) = x \log x + O(x)$$

[Since $\log x \le x \Rightarrow \frac{\log x}{x} \le 1$ $\log(x) = O(x) \Rightarrow O(\log x) = O(O(x)) = O(x)$.]

Hence $\sum_{p\le x} (\log p)[\frac{x}{p}] = x \log x + O(x)$.

Self Assessment Question 1 : *Verify that* $\sum_{n=2}^{\infty} \frac{\log n}{n(n-1)}$ *converges* .

5.3 ANOTHER IDENTITY FOR THE PARTIAL SUMS OF A DIRICHLET PRODUCT

5.3.1 Note: (i) (Refer Theorem 5.1.1) The statement is as follows:

If $h = f * g$, the Dirichlet product of f and g, $F(x) = \sum_{n\le x} f(n)$, $G(x) = \sum_{n\le x} g(n)$ and $H(x) = \sum_{n\le x} h(n)$.

Then we have $H(x) = \sum_{n\le x} f(n)\, G(\frac{x}{n}) = \sum_{n\le x} g(n)\, F(\frac{x}{n})$

(ii) $H(x) = \sum_{n\le x} f(n)\, G(\frac{x}{n}) = \sum_{n\le x}\sum_{d|n} f(d)\, g(\frac{n}{d})$

Self Assessment Question 2: *Verify* $H(x) = \sum_{n\le x} f(n)\, G(\frac{x}{n}) = \sum_{n\le x}\sum_{d|n} f(d)\, g(\frac{n}{d})$, *by taking* $x = 3.5$

(iii) $H(x) = \sum_{n\le x}\sum_{d|n} f(d)\, g(\frac{n}{d}) = \sum_{\substack{n\le x \\ d|n}} f(d)\, g(\frac{n}{d}) = \sum_{qd\le x} f(d)\, g(q)$.

5.3.2 Theorem: Let $F(x) = \sum_{n\le x} f(n)$, $G(x) = \sum_{n\le x} g(n)$ and

$H(x) = \sum_{n\le x} (f * g)(n)$. If a and b are positive real numbers such that $ab = x$, then

$$\sum_{qd\le x} f(d)\, g(q) = \sum_{n\le a} f(n)\, G(\tfrac{n}{n}) + \sum_{n\le b} g(n)\, F(\tfrac{n}{n}) - F(a)G(b).$$

Proof:

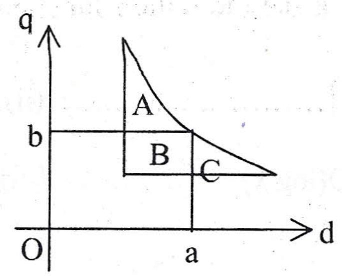


Fig - 5.3.2

By Note 5.3.1 (iii), we have $H(x) = \sum_{qd\le x} f(d)\, g(q)$ ... (i)

The curve is for $ab = x$. Observe the Fig-5.3.2, given here.

All the d, q participated in the sum on right side of (i) satisfy $dq \le x$. So the point (d, q) lies below the curve. The point (d, q) participated in the sum of (i) are lattice points belongs to the region A or B or C.

We split this sum into two parts, one part over the lattice points in $A\cup B$ (that sum is $\sum_{d\le a}\sum_{q\le \frac{x}{d}} f(d)g(q)$) and

the other over the lattice points in $B\cup C$ (That sum is $\sum_{q\le b}\sum_{d\le \frac{x}{d}} f(d)g(q)$).

The lattice points in B are covered twice (That is, in both the parts) so we have to subtract the sum over lattice points in B. [(That sum is $\sum_{d\le a}\sum_{q\le \frac{x}{q}} f(d)g(q)$) and the other over the lattice point in $B\cup C$

(that sum is $\sum_{q\le b}\sum_{d\le \frac{x}{q}} f(d)g(q)$). The lattice points in B are covered twice (that is, in both the parts),

so we have to subtract the sum over lattice points in B (that sum is $\sum_{d\le a}\sum_{q\le b} f(d)g(q)$)]

Hence $H(x) = \sum_{dq\le x} f(d).g(q)$

$$= \sum_{d\le a}\sum_{q\le \frac{x}{d}} f(d)g(q) + \sum_{q\le b}\sum_{d\le \frac{x}{d}} f(d)g(q) - \sum_{d\le a}\sum_{q\le b} f(d)g(q) \quad \text{.......................... (i)}$$

$$= \sum_{d\le a} f(d) \sum_{q\le \frac{x}{d}} g(q) + \sum_{q\le b} g(q) \sum_{d\le \frac{x}{q}} f(d) - \sum_{d\le a} f(d) \sum_{q\le b} g(q)$$

$$= \sum_{d\le a} f(d).G(\tfrac{x}{d}) + \sum_{g\le b} g(q).F(\tfrac{x}{q}) - F(a)G(b)$$

By replacing d by n in first term, q by n in second term, we get

$$= \sum_{n\le a} f(n).G(\tfrac{x}{n}) + \sum_{n\le b} g(n).F(\tfrac{x}{n}) - F(a)G(b).$$

This completes the proof of the theorem.

5.3.3 Problem: Prove that $\sum_{n\le x}\lambda(n)\left[\frac{x}{n}\right] = [\sqrt{x}\,]$ where $\lambda(n)$ is the Liouville's function.

Solution: Theorem 5.1.3, states that $\sum_{n\le x}\sum_{d|n} f(d) = \sum_{n\le x} f(n)\left[\frac{x}{n}\right]$........................(i)

In this, take $f(n) = \lambda(n)$.

Then R.H.S $= \sum_{n\le x}\lambda(n)\left[\frac{x}{n}\right] = \sum_{n\le x}\sum_{d|n}\lambda(d)$ [by (i)]

$$= \sum_{n\le x}\left(\sum_{d|n}\lambda(d)\right) = \sum_{\substack{n\le x \\ n \text{ is square}}} 1 \quad \text{(by reason (ii))}$$

[Reason(ii): $\sum_{d|n}\lambda(d) = \begin{cases} 1 & \text{if } n \text{ is a square} \\ 0 & \text{otherwise} \end{cases}$ (by Theorem 2.3.4 of Lesson-2)]

$= [\sqrt{x}\,]$ (by reason (iii))

[Reason (iii): Note that the number of squares $\le x$ are $1, 2, \ldots [\sqrt{x}\,]$].

Hence $\sum_{n\le x}\lambda(n)\left[\frac{x}{n}\right] = [\sqrt{x}\,]$ where λ is the Liouville's function.

5.4 SUMMARY

In this lesson, we obtained some identities involving arithmetic functions. An exercise has been made in the partial sums of arbitrarily arithmetical functions f and g with their Dirichlet product $f*g$. Further applications of $\mu(n)$ and $\wedge(n)$ were identified. We also proved the Legendre's identity, the computation for factorial of an integral part of some greater than or equal to 1. Some related consequences also obtained.

5.5 TECHNICAL TERMS

Legendre inequality: For every $x \ge 1$, we have $[x]! = \prod_{p\le x} p^{\alpha(p)}$ and

$$\alpha(p) = \sum_{m=1}^{\infty}\left[\frac{x}{p^m}\right]$$

Partial sums of a Dirichlet product: $H(x) = \sum_{n\le x} f(n)G\left(\frac{x}{n}\right) = \sum_{n\le x} g(n)F\left(\frac{x}{n}\right)$, where f, g are arithmetical functions , $h = f * g$, $F(x) = \sum_{n \le x} f(n)$,

$G(x) = \sum_{n \le x} g(n)$, $H(x) = \sum_{n \le x} h(n)$

5.6 ANSWERS TO SELF ASSESSMENT QUESTIONS

1: Now we use ratio test:

Let $U_n = \frac{\log n}{n(n-1)}$ and $U_{n+1} = \frac{\log(n+1)}{n(n+1)}$

$$\Rightarrow \lim_{n\to\infty} \frac{U_{n+1}}{U_n} = \lim_{n\to\infty} \frac{\log(n+1)}{n(n+1)} \times \frac{n(n-1)}{\log n} = \lim_{n\to\infty} \frac{\log(n+1-n)}{(n+1)} \times (n-1)$$

$$= \lim_{n\to\infty} \frac{\log(1)}{(n+1)} \times (n-1) = \lim_{n\to\infty} 0.\frac{(n-1)}{(n+1)} = 0.$$

Therefore by ratio test, it is clear that $\sum_{n=2}^{\infty} \frac{\log n}{n(n-1)}$ converges.

2: Take $x = 3.5$ then $n = 1, 2, 3$

$$\text{L.H.S} = \sum_{n \le x} f(n)\, G(\tfrac{x}{n}) = f(1)\, G(\tfrac{3.5}{1}) + f(2)\, G(\tfrac{3.5}{2}) + f(3)\, G(\tfrac{3.5}{3})$$

$$= f(1)[g(1) + g(2) + g(3)] + f(2)[g(1)] + f(3)[g(1)].$$

$$\text{R.H.S} = \sum_{n \le x} \sum_{d|n} f(d)\, g(\tfrac{n}{d})$$

$$= \underbrace{f(1)g(1)}_{n=1\,\text{case}} + \underbrace{f(1)g(2) + f(2)[g(1)]}_{n=2\ \text{case}} + \underbrace{f(1)g(3) + f(3)g(1)}_{n=3\ \text{case}} = \text{L.H.S.}$$

5.7 MODEL QUESTIONS

1. State and prove Legendre's identity.

2. For $x \ge 1$, show that $\sum_{n \le x} \mu(n)[\tfrac{x}{n}] = 1$ and $\sum_{n \le x} \wedge(n)[\tfrac{x}{n}] = \log([x]!)$.

3. For $x \ge 2$,we have $\sum_{p \le x} \left[\frac{x}{p}\right] \log p = x \log x + O(x)$ where the sum is extended over all primes $p \le x$.

4. For $x \ge 2$, show that $\log [x]! = x \log x - x + O(\log x)$ and

$$\sum_{n\le x} \wedge(n)\left[\frac{x}{n}\right] = x \log x - x + O(\log x).$$

5.8 REFERENCE BOOKS

1. Chandrasekharan, K. "Introduction to Analytic Number Theory", Springer Verlag .
2. Hardy, G.H. & Wright, E.M. "Introduction to the Theory of Numbers", Fourth Edition, Oxford Publications,
3. Levegue W.J. (1986) "Topics in Number Theory (2 volumes), Addition - Wesley Publ. Co.
4. Rademacher (1964) "Lectures on Elementary Number Theory", New York, Blaisdell Publ. Co.
5. Tom M. Apostol "Introduction to Analytic Number Theory", Springer International Student Edition, Narosa Publishing House, 1995.
6. Uspensky, J.V., and Heaslett, M.A. (1939) "Elementary Number Theory", New York, Mc. Graw - Hill Book. Co.
7. Vinogrador, "Elements of Number Theory", Dover Publications

Name of the Author of this Lesson: **Dr. Kuncham Syam Prasad**

LESSON - 6

SOME ELEMENTARY THEOREMS ON THE DISTRIBUTION OF PRIME NUMBERS

Objectives

The objectives of this lesson are to:

- understand the notion $\pi(x)$
- observe the relations between $\psi(x)$ and $\vartheta(x)$
- know the relations between $\vartheta(x)$ and $\pi(x)$
- identify the equivalent forms of prime numbers

Structure

6.0 Introduction
6.1. Chebyshev's functions $\psi(x)$ and $\vartheta(x)$
6.2. Relations connecting $\vartheta(x)$ and $\pi(x)$
6.3. Some equivalent forms of the prime number theorem
6.4 Summary
6.5 Technical terms
6.6 Answers to Self Assessment Questions
6.7 Model Questions
6.8 Reference Books

6.0 INTRODUCTION

Let $x > 0$ and $\pi(x)$ denote the number of primes not exceeding x. We know that the number of distinct prime numbers is infinite. So $\pi(x) \to \infty$ as $x \to \infty$. Inspection of tables of prime numbers led Gauss (1792) and Legendre (1798) to conjecture that $\pi(x)$ is asymptotic to $\frac{x}{\log x}$, that is., $\lim\limits_{x\to\infty} \frac{\pi(x)\log x}{x} = 1$. This conjecture was first proved in 1896 by Hadamard and de la Vallee Poussin and is known as the **Prime Number Theorem**.

We obtain some results relating to $\vartheta(x)$ and $\pi(x)$, which are useful in showing that the prime number theorem is equivalent to the relation : $\lim\limits_{x\to\infty} (\vartheta(x)/x) = 1$.

This lesson is mainly concerned with elementary theorems on primes. We show that the prime number theorem can be expressed as several equivalent forms. For example, we will show that the prime number theorem is equivalent to the asymptotic formula

$$\sum_{n\leq x} \Lambda(n) \sim x \text{ as } x \to \infty.$$

6.1 CHEBYSHEV'S FUNCTIONS $\psi(x)$ AND $\vartheta(x)$

6.1.1 Definition: For $x > 0$, we define $\pi(x)$ by $\pi(x) = \sum_{p \le x} 1$, where the summation is over all primes $p \le x$. (That is., $\pi(x)$ denotes the number of primes not exceeding x. Here $\pi(x) \to x$ as $x \to \infty$)

6.1.2 Definition: For $x > 0$, we define **Chebyshev's ψ-function** by the formula $\psi(x) = \sum_{n \le x} \wedge(n)$

[We know that the Mangoldt function $\wedge(n)$ is defined by

$$\wedge(n) = \begin{cases} \log p & \text{if } n = p^m, \text{ p is prime} \\ 0 & \text{otherwise} \end{cases}$$

6.1.3 Note: Since $\wedge(n) = 0$ unless n is a prime power,

$$\psi(x) = \sum_{n \le x} \wedge(n) = \sum_{m=1}^{\infty} \sum_{p^m \le x} \wedge(p^m) \text{ (since } \wedge(n) = 0 \text{ if } n \ne p^m)$$

$$= \sum_{m=1}^{\infty} \sum_{p^m \le x} \log p \text{ ,where } p \text{ is a prime number.}$$

[The number of m's that satisfy $p^m \le x$ is finite.
Hence the sum on right side is a finite sum]

$$= \sum_{m=1}^{\infty} \sum_{p \le x^{1/m}} \log p$$

***Self Assessment Question 1:** Verify* $\sum_{m=1}^{\infty} \sum_{p \le x^{1/m}} \log p = \sum_{m \le \log_2 x}^{\infty} \sum_{p \le x^{1/m}} \log p$

$$= \sum_{m \le \log_2 x}^{\infty} \sum_{p \le x^{1/m}} \log p .$$

Hence $\psi(x) = \sum_{m \le \log_2 x}^{\infty} \sum_{p \le x^{1/m}} \log p .$

6.1.4 Definition: If $x \ge 0$, we define the **Chebyschev's ϑ function** by the equation $\vartheta(x) = \sum_{p \le x} \log p$, where the sum runs over all prime numbers p less than or equal to x.

6.1.5 (Relation between $\psi(x)$ and $\vartheta(x)$):

We know that, by 6.1.3, $\psi(x) = \sum_{m \le \log_2 x} \sum_{p \le x^{1/m}} (\log p)$

$$= \sum_{m \le \log_2 x} \vartheta(x^{1/m}) \text{ (by Definition 6.1.4)}$$

Therefore $\psi(x) = \sum_{m \le \log_2 x} \vartheta(x^{1/m})$.

6.1.6 Theorem: For any $x \ge 1$, we have

$$\psi(x) = \sum_{m \le \log_2 x} \vartheta(x^{1/m}) = \vartheta(x) + \vartheta(x^{1/2}) + \ldots + \vartheta(x^{1/m}) \text{ where } m = \left(\frac{\log x}{\log 2}\right) = \log_2 x.$$

Proof: We know that

$$\psi(x) = \begin{cases} \sum_{n \le x} \wedge(n) = 0 \text{ if } n \text{ is not equal to power of a prime.} \\ \sum_{n \le x} \log p, \text{ if } n = p^m \text{ where } p \text{ is a prime number.} \end{cases}$$

$$\Rightarrow \psi(x) = \sum_{m=1}^{\infty} \sum_{p^m \le x} \log p \quad (p \text{ is prime})$$

$$= \sum_{m=1}^{\infty} \vartheta(x^{1/m}) = \vartheta(x) + \vartheta(x^{1/2}) + \ldots + \vartheta(x^{1/m}) + \ldots$$

If $x < 2$, then $x = 1$ and so $\vartheta(x) = \sum_{p \le 1} \log p = \log 1 = 0$.

So $\vartheta(x) = 0$ if $x < 2$.

This series on the right has non-zero terms, if $(x^{1/m}) \ge 2$

$$\Rightarrow m \le \frac{\log x}{\log 2} \quad \Rightarrow m \le \left[\frac{\log x}{\log 2}\right].$$

Therefore $\psi(x) = \vartheta(x) + \vartheta(x^{1/2}) + \ldots + \vartheta(x^{1/m})$ where $m = \left[\frac{\log x}{\log 2}\right] = \log_2 x$.

In other words, $\psi(x) = \sum_{m \le \log_2 x}^{\infty} \vartheta(x^{1/m})$.

6.1.7 Theorem: (i) For $x > 0$, we have

$$0 \le \psi(x)/x - \vartheta(x)/x \le \frac{(\log x)^2}{2\sqrt{x}\log 2}$$

(ii) $\lim_{x \to \infty} \{ (\psi(x)/x) - (\vartheta(x)/x) \} = 0$

(iii) If one of $\psi(x)/x$ or $\vartheta(x)/x$ tends to a limit then so does the other. Also the two limits are equal.

Proof: By Theorem 6.1.6, we have

$$\psi(x) = \sum_{m \le \log_2 x} \vartheta(x^{1/m}) = \vartheta(x) + \sum_{2 \le m \le \log_2 x} \vartheta(x^{1/m}).$$

$$\Rightarrow \psi(x) - \vartheta(x) = \sum_{2\le m\le \log_2 x} \vartheta(x^{1/m}) \ge 0 \quad \ldots (i)$$

From the definition of $\vartheta(x)$, we have $\vartheta(x) = \sum_{p\le x} \log p$ where p is a prime number. Consider $\vartheta(x) = \sum_{p\le x} \log x$

$= \log 1 + \log 2 + \ldots + \log p + \ldots$

(sum runs over all prime numbers $\le x$)

$\le \log 1 + \log 2 + \ldots + \log [x]$ (sum runs over all positive integers $\le x$)

$\le \log x + \log x + \ldots + \log x$ (since $\log a \le \log b$ if $a \le b$)

$= [x] \log x \le x \log x$ (the number of terms here is $[x]$)

Therefore $\vartheta(x) \le x \log x$ .... (ii)

From (ii), we have $\vartheta(x^{1/m}) \le x^{1/m}.\log x^{1/m}$ .... (iii)

From (i) and (iii) we get

$$0 \le \psi(x) - \vartheta(x) = \sum_{2\le m\le \log_2 x} \vartheta(x^{1/m})$$

$$\le \sum_{2\le m\le \log_2 x} x^{1/m} \log x^{1/m}$$

$$\le \sum_{2\le m\le \log_2 x} \sqrt{x} \log \sqrt{x} \quad \text{(verify!))}$$

$$\le (\log_2 x)(\sqrt{x} \log \sqrt{x})$$

(Observe $\sum_{2\le m\le a} y = \sum_{2\le m\le [a]} y = y + y + \ldots + y$ ([a] times) $= [a]\, y \le ay$)

$$= \left(\frac{\log x}{\log 2}\right) \sqrt{x}\, \tfrac{1}{2} \log x$$

$$= \left(\frac{1}{2\log 2}\right) \sqrt{x} (\log x)^2 = \frac{(\log x)^2 \sqrt{x}}{2\log 2}$$

Therefore $0 \le (\psi(x) - \vartheta(x))/x = \dfrac{(\log x)^2 \sqrt{x}}{2\log 2} \dfrac{1}{x}$

$$\Rightarrow 0 \le \psi(x)/x - \vartheta(x)/x = \frac{(\log x)^2}{2\sqrt{x}\log 2}$$

This completes (i).

(ii) By taking $x \to \infty$, we have $\sqrt{x} \to \infty$ and so $\dfrac{(\log x)^2}{2\sqrt{x}\log 2} \to 0$.

Hence we have $0 \le \lim_{x\to\infty} (\psi(x) - \vartheta(x))/x = 0$

This shows that $\lim_{x\to\infty} (\psi(x) - \vartheta(x))/x = 0$

(iii) If one of the limits tends to a limit, then

$$0 = \lim_{x\to\infty} (\psi(x) - \vartheta(x))/x = \lim_{x\to\infty} \psi(x)/x - \lim_{x\to\infty} \vartheta(x)/x$$

$$\Rightarrow \lim_{x\to\infty} \psi(x)/x = \lim_{x\to\infty} \vartheta(x)/x$$

Self Assessment Question 2: Verify $\sum_{2\le m\le \log_2 x} x^{1/m} \log x^{1/m} \le \sum_{2\le m\le \log_2 x} \sqrt{x} \log\sqrt{x}$ for $m \ge 2$.

6.2 RELATIONS CONNECTING ϑ(X) AND π(X)

6.2.1 Remark: The functions $\pi(x) = \sum_{p\le x,\, p \text{ is prime}} 1$, and $\vartheta(x) = \sum_{p\le x} \log p$ are step functions with jumps at prime numbers. Observe the following:

x	Primes	$\pi(x)$	$\vartheta(x)$
$0 \le x < 2$	Nil	0	0
$2 \le x < 3$	2	1	log 2
$3 \le x < 5$	2, 3	2	log 2 + log 3
$5 \le x < 7$	2, 3, 5	3	log 2 + log 3 + log 5
$7 \le x < 11$	2, 3, 5, 7	4	log 2 + log 3 + log 5 + log 7
$11 \le x < 13$	2, 3, 5, 7, 11	5	log 2 + log 3 + log 5 + log 7 + log 11

6.2.2 Theorem: Abel's Identity: For any arithmetic function a(n), define $A(x) = \sum_{n\le x} a(n)$, where $A(x) = 0$ if $x < 1$. Assume that f has a continue derivative on the interval [y, x], where $0 < y < x$. Then we have

$$\sum_{y<n\le x} a(n)f(n) = A(x)f(x) - A(y)f(y) - \int_y^x A(t)f'(t)dt.$$

Proof: Suppose $[y] = k$ and $[x] = m$ so that $A(y) = A(k)$ and $A(x) = A(m)$.

Consider $\sum_{y<n\le x} a(n)f(n) = \sum_{n=k+1}^{m} a(n)f(n)$.

[By the definition of $A(x)$ we have $a(n) = A(n) - A(n-1)$]

$$= \sum_{n=k+1}^{m} \{A(n) - A(n-1)\}f(n)$$

$$= \sum_{n=k+1}^{m} A(n)f(n) - \sum_{n=k+1}^{m} A(n-1)f(n)$$

$$= \sum_{n=k+1}^{m} A(n)f(n) - \sum_{n=k}^{m-1} A(n)f(n+1)$$

$$= \left\{\sum_{n=k+1}^{m-1} A(n)f(n) + A(m)f(m)\right\} - \left\{A(k)f(k+1) + \sum_{n=k+1}^{m-1} A(n)f(n+1)\right\}$$

$$= \sum_{n=k+1}^{m-1} A(n)\{f(n) - f(n+1)\} + A(m).f(m) - A(k).f(k+1)$$

$$= -\sum_{n=k+1}^{m-1} A(n)\int_n^{n+1} f^1(t)dt + A(m)f(m) - A(k)f(k+1)$$

[Since $\int_n^{n+1} f^1(t)dt = [f(t)]_n^{n+1} = f(n+1) - f(n)$, we have

$f(n+1) - f(n) = \int_n^{n+1} f^1(t)dt \Rightarrow f(n) - f(n+1) = -\int_n^{n+1} f^1(t)dt$]

$$= \sum_{n=k+1}^{m-1} \int_n^{n+1} A(n)f^1(t)dt + A(m)f(m) - A(k)f(k+1)$$

$$= -\sum_{n=k+1}^{m-1} \int_n^{n+1} A(t)f^1(t)dt + A(m)f(m) - A(k)f(k+1) \text{..........................} \quad \text{(i)}$$

(If $n < t < n+1$, then $A(n) = A(t)$)

Since $m = [x]$, there is no integer lies between m and x.
Therefore $A(x) = A(m)$.

Now $A(x)f(x) - \int_m^x A(t)f^1(t)dt = A(m)f(x) - \int_m^x A(m)f^1(t)dt$

$= A(m)f(x) - A(m)\int_m^x f^1(t)dt$

$= A(m)f(x) - A(m)\{f(x) - f(m)\}$

$= A(m)f(x) - A(m)f(x) + A(m)f(m) = A(m)f(m)$

$\Rightarrow A(m)f(m) = A(x)f(x) - \int_m^x A(t)f^1(t)dt$ .... (ii)

And also we have $k = [y]$ so that $A(k) = A(y)$

Now $\int_y^{k+1} A(t)f^1(t)dt = \int_y^{k+1} A(y)f^1(t)dt$

$= A(y)\int_y^{k+1} f^1(t)dt$

$= A(y)\{f(k+1) - f(y)\}$

$= -A(y)f(y) + A(y)f(k+1)$

$= -A(y) f(y) + A(k) f(k+1)$

$= -A(y)f(y) + A(k)f(k+1)$ (since $A(y) = A(k)$)

$\Rightarrow A(k)f(k+1) = A(y)f(y) + \int_y^{k+1} A(t)f^1(t)dt$ .... (iii)

From (i), (ii) and (iii) we have

$$\sum_{y<n\le x} a(n)f(n) = -\sum_{n=k+1}^{m-1} \int_n^{n+1} A(t)f^1(t)dt + \left\{A(x)f(x) - \int_m^x A(t)f^1(t)dt\right\}$$

$$- \left\{A(y)f(y) + \int_y^{k+1} A(t)f^1(t)dt\right\}$$

[Observe that $\sum_{n=k+1}^{m-1} \int_{n}^{n+1} A(t)f^1(t)dt = \int_{k+1}^{m} A(t)f^1(t)dt$]

$= A(x)f(x) - A(y)f(y) - \{ \int_{y}^{k+1} A(t)f^1(t)dt + \int_{k+1}^{m} A(t)f^1(t)dt + \int_{m}^{x} A(t)f^1(t)dt \}$

$= A(x)f(x) - A(y)f(y) - \int_{y}^{x} A(t)f^1(t)dt$.

This completes the proof.

6.2.3 Corollary: (Euler's Summation formula for Abel's identity)

If $a(n) = 1 = U(n)$ for all n, then

$$\sum_{y<n\le x} f(n) = \int_y^x f(t)dt + \int_y^x (t-[t])f^1(t)dt + (y - [y])f(y) - (x - [x])f(x).$$

Proof: Let $a(n) = U(n) = 1$ for all n .... (i)

We know that by Abel's identity,

$$\sum_{y<n\le x} a(n)f(n) = A(x)f(x) - A(y)f(y) - \int_y^x f^1(t)A(t)dt$$

$$= [x]f(x) - [y]f(y) - \int_y^x f^1(t)[t]dt.$$

(Since $A(x) = \sum_{n\le x} a(n) = \sum_{n\le x} 1 = [x]$. Similarly $A(y) = [y]$)

Since $a(n) = 1$, we have $\sum_{y<n\le x} f(n) = [x]f(x) - [y]f(y) - \int_y^x f^1(t)[t]dt$ .... (ii)

By using integration by parts, we get

$$\int_y^x t f^1(t)dt = [t f(t)]_y^x - \int_y^x f(t)dt = (xf(x) - yf(y)) - \int_y^x f(t)dt$$

$\Rightarrow \int_y^x f(t)dt = xf(x) - yf(y) - \int_y^x t f^1(t)dt$ .... (iii)

Subtracting (iii) from (ii), we get

$$\sum_{y<n\le x} f(n) - \int_y^x f(t)dt = [x]f(x) - [y]f(y) - \int_y^x f^1(t)[t]dt - x\cdot f(x) + yf(y) + \int_y^x t f^1(t)dt$$

$$= ([x] - x)f(x) + (y - [y])f(y) + \int_y^x (t-[t])f^1(t)dt$$

(Take the L.H.S. second term to right side)

$$\Rightarrow \sum_{y<n\le x} f(n) = ([x] - x)f(x) + (y - [y])f(y) + \int_y^x (t-[t])f^1(t)dt + \int_y^x f(t)dt.$$

6.2.4 Theorem: For $x \ge 2$, we have (a) $\vartheta(x) = \pi(x)\log x - \int_2^x \frac{\pi(t)dt}{t}$ and

(b) $\pi(x) = [\vartheta(x)/\log x] + \int_2^x [\vartheta(t)/(t \log^2 t)]dt$

Proof: (i) Assume $a(n)=\begin{cases}1 & \text{if n is a prime number}\\ 0 & \text{other wise}\end{cases}$ .... (i)

We know that $A(x) = \sum_{n\le x} a(n) = \sum_{p\le x} 1 = \pi(x)$ (that is the number of primes $\le x$)

$\Rightarrow A(x) = \pi(x)$ .... (ii)

$\Rightarrow \sum_{1<n\le x} a(n)\log n = \sum_{1<p\le x} a(p)\log p$ (since $a(n) = 0$ if $n \ne p$, a prime number)

$= \sum_{1<p\le x} \log p$ (since $a(p) = 1$ if p is prime)

$= \sum_{p\le x} \log p = \vartheta(x)$ .... (iii)

Consider the Abel's identity given in Theorem 6.2.2,

$$\sum_{y<n\le x} a(n)f(n) = A(x)f(x) - A(y)f(y) - \int_y^x A(t)f'(t)dt.$$

Take $\log n$ in place of $f(n)$ and $y = 1$.

Then $\sum_{1<n\le x} a(n)\log n = A(x)\log x + A(1)\log 1 - \int_1^x A(t)\log^1(t)\,dt.$

$$= \pi(x)\log x + 0 - \int_1^x \pi(t)\tfrac{1}{t}dt \text{ ....(iv)}$$

[use $A(x) = \pi(x)$, $\log^1(t) = 1/t$, $\log 1 = 0$]

From (iii) and (iv), we have $\vartheta(x) = \sum_{1<n\le x} a(n)\log n = \pi(x)\log x - \int_1^x \frac{\pi(t)dt}{t}$.

Therefore $\vartheta(x) = \pi(x)\log x - \int_2^x \frac{\pi(t)dt}{t}$. [Since $t < 2$, the number of primes less than $2 = \pi(t) = 0$.]

(b) Consider $a(n)$ as above, that is., $a(n)=\begin{cases}1 & \text{if n is a prime}\\ 0 & \text{otherwise}\end{cases}$

Let $b(n) = a(n).\log n$. Now $\pi(x) = \sum_{p\le x} 1 = \sum_{n\le x} a(n)$

$$= a(1) + \sum_{1.5<n\le x} a(n) = 0 + \sum_{1.5<n\le x} a(n)$$

Therefore $\pi(x) = \sum_{1.5<n\le x} a(n)$ .... (i)

Consider $\vartheta(x) = \sum_{p\le x} \log p = \sum_{p\le x} 1.\log p$

$= \sum_{p\le x} a(p)\log p = \sum_{n\le x} a(n)\log n$ (since $a(n) = 0$ if n is not prime)

Therefore $\vartheta(x) = \sum_{n \le x} a(n)\log n = \sum_{n \le x} b(n)$ .... (ii)

Now consider the Abel's identity,

$$\sum_{y<n\le x} a(n)f(n) = A(x)f(x) - A(y)f(y) - \int_y^x A(t)f'(t)dt \quad \text{where } A(x) = \sum_{n\le x} a(n).$$

Take b(n) in place of a(n) and $\frac{1}{\log x}$ in place of f(x) and y = 3/2.

Then we get $\sum_{\frac{3}{2}<n\le x} b(n)\frac{1}{\log n} = A(x)\frac{1}{\log x} - A\left(\frac{3}{2}\right)\frac{1}{\log\left(\frac{3}{2}\right)} - \int_{3/2}^{x} A(t)\left(\frac{1}{\log t}\right)' dt.$

$$\Rightarrow \sum_{\frac{3}{2}<n\le x} \frac{a(n)\log n}{\log n} = \frac{A(x)}{\log x} - \frac{A(3/2)}{\log(3/2)} + \int_{1.5}^{x} \frac{A(t)}{t\log^2 t}dt$$

$$\left[\text{ Since } b(n) = a(n)\log n,\ \left(\frac{1}{\log t}\right)' = \frac{-1}{t(\log t)^2} = \frac{-1}{t\log^2 t}\ \right]$$

$$\Rightarrow \sum_{\frac{3}{2}<n\le x} a(n) = \frac{A(x)}{\log x} - \frac{A(3/2)}{\log(3/2)} + \int_{1.5}^{x} \frac{A(t)}{t\log^2 t}dt$$

$$\Rightarrow \pi(x) = \vartheta(x)/\log x - 0 + \int_2^x \frac{A(t)}{t\log^2 t}dt.$$

$\left[\text{ Since (i) } \pi(x) = \sum_{\frac{3}{2}<n\le x} a(n),\ \text{(ii) } A(x) = \sum_{n\le x} b(n) = \vartheta(x) \text{ (see (ii) above)}\right.$

$\left.\text{(iii) } A(3/2) = \sum_{n\le\frac{3}{2}} b(n) = b(1) = a(1)\log 1 = 0\ \right]$

Hence $\pi(x) = \vartheta(x)/\log x + \int_2^x \frac{A(t)}{t\log^2 t}dt.$

6.3 SOME EQUIVALENT FORMS OF THE PRIME NUMBER THEOREM

6.3.1 Note: We know that the prime number theorem is :

$$\lim_{x\to\infty} \frac{\pi(x)\log x}{x} = 1 \Rightarrow \pi(x) = O\left(\frac{x}{\log x}\right) \text{ or } \frac{\pi}{x} \sim \frac{x}{\log x} \text{ as } x \to \infty.$$

6.3.2 Theorem: The following statements are equivalent:

(a) $\lim_{x\to\infty} \frac{\pi(x)\log x}{x} = 1$; (b) $\lim_{x\to\infty} [\vartheta(x)/x] = 1$; and (c) $\lim_{x\to\infty} \frac{\psi(x)}{x} = 1.$

Proof: We know by Theorem 6.2.4 that

$$\vartheta(x) = \pi(x)\log x - \int_2^x \frac{\pi(t)}{t}dt \quad \text{.......... (i) and}$$

$$\pi(x) = [\vartheta(x)/\log x] + \int_2^x [\vartheta(t)/(t\log^2 t)]dt \quad \text{.......... (ii)}$$

$$\text{and } 0 \le (\psi(x)/x) - (\vartheta(x)/x) \le \frac{(\log x)^2}{2\sqrt{x}\log 2} \quad \text{.......... (iii) (by Theorem 6.1.7)}$$

(a) ⇒ (b): Divide by x on both sides of (i)

Then we get $\vartheta(x)/x = \dfrac{\pi(x)\log x}{x} - \dfrac{1}{x}\displaystyle\int_2^x \frac{\pi(t)}{t}dt.$

$$\lim_{x\to\infty} \vartheta(x)/x = \lim_{x\to\infty}\frac{\pi(x)\log x}{x} - \lim_{x\to\infty}\frac{1}{x}\int_2^x \frac{\pi(t)}{t}dt$$

$$= 1 - \lim_{x\to\infty}\frac{1}{x}\int_2^x \frac{\pi(t)}{t}dt \text{ (since by (a))} \quad \text{.......... (iv)}$$

From (a) we have, $\displaystyle\lim_{x\to\infty}\frac{\pi(x)\log x}{x} = 1$

$$\Rightarrow \frac{\pi(x)}{x} = O\left(\frac{1}{\log x}\right) \Rightarrow \int_2^x \frac{\pi(t)}{t}dt = O\left(\int_2^x \frac{1}{\log t}dt\right)$$

$$\Rightarrow \frac{1}{x}\left(\int_2^x \frac{\pi(t)}{t}dt\right) = O\left(\frac{1}{x}\int_2^x \frac{1}{\log t}dt\right) \quad \text{.......... (v)}$$

Consider $\displaystyle\int_2^x \frac{1}{\log t}dt = \int_2^{\sqrt{x}} \frac{1}{\log t}dt + \int_{\sqrt{x}}^x \frac{1}{\log t}dt.$

$$\le \int_2^{\sqrt{x}} \frac{1}{\log 2}dt + \int_{\sqrt{x}}^x \frac{1}{\log\sqrt{x}}dt \quad \left[\text{ since (i) } \log 2 \le \log t \text{ for } 2 \le t \Rightarrow \frac{1}{\log t} \le \frac{1}{\log 2}.\right.$$

$$\left.\text{(ii) } \sqrt{x} \le t \Rightarrow \log\sqrt{x} \le \log t \Rightarrow \frac{1}{\log t} \le \frac{1}{\log\sqrt{x}}\right]$$

$$= \frac{1}{\log 2}\int_2^{\sqrt{x}} 1\,dt + \frac{1}{\log\sqrt{x}}\int_{\sqrt{x}}^x 1\,dt$$

$$= \frac{1}{\log 2}[t]_2^{\sqrt{x}} + \frac{1}{\log\sqrt{x}}[t]_{\sqrt{x}}^x$$

$$= \frac{\sqrt{x}-2}{\log 2} + \frac{x-\sqrt{x}}{\log\sqrt{x}} < \frac{\sqrt{x}}{\log 2} + \frac{x-\sqrt{x}}{\log\sqrt{x}}$$

$$\Rightarrow \int_2^x \frac{1}{\log t}dt < \frac{\sqrt{x}}{\log 2} + \frac{x-\sqrt{x}}{\log\sqrt{x}} = \frac{\sqrt{x}}{\log 2} + \frac{x}{\log\sqrt{x}} - \frac{\sqrt{x}}{\log\sqrt{x}}$$

$$\Rightarrow \frac{1}{x}\int_2^x \frac{1}{\log t}dt < \frac{1}{\sqrt{x}\log 2} + \frac{1}{\log\sqrt{x}} - \frac{1}{\sqrt{x}\log\sqrt{x}}$$

$$\Rightarrow \lim_{x\to\infty}\left(\frac{1}{x}\int_2^x \frac{1}{\log t}dt\right) \le \lim_{x\to\infty}\left(\frac{1}{\sqrt{x}\log 2}\right) + \lim_{x\to\infty}\left(\frac{1}{\log\sqrt{x}}\right) - \lim_{x\to\infty}\left(\frac{1}{\sqrt{x}\log\sqrt{x}}\right)$$

$= 0 + 0 + 0 = 0$

$$\Rightarrow \lim_{x\to\infty}\left(\frac{1}{x}\int_2^x \frac{1}{\log t}dt\right) = 0 \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (vi)$$

From (v) and (vi) we get, $\lim_{x\to\infty}\left(\frac{1}{x}\int_2^x \frac{\pi(t)}{t}dt\right) = 0.$

By substituting this fact in (iv), we get that $\lim_{x\to\infty} (\mathcal{T}(x) / x) = 1.$

This completes the proof of (a) $\Rightarrow$ (b)

(b) $\Rightarrow$ (a): From (ii) we have, $\pi(x) = (\mathcal{T}(x) / \log x) + \int_2^x (\mathcal{T}(x) / t \log^2 t)\, dt$

Multiplying on both sides by $\frac{\log x}{x}$, we get

$$\frac{\pi(x)\log x}{x} = (\mathcal{T}(x) / x) + \frac{\log x}{x}\int_2^x (\mathcal{T}(t) / t\log^2 t)\, dt$$

$$\Rightarrow \lim_{x\to\infty}\frac{\pi(x)\log x}{x} = \lim_{x\to\infty} (\mathcal{T}(x) / x) + \lim_{x\to\infty}\frac{\log x}{x}\int_2^x (\mathcal{T}(t) / t\log^2 t)\, dt$$

$$= 1 + \lim_{x\to\infty}\frac{\log x}{x}\int_2^x (\mathcal{T}(t) / t\log^2 t)\, dt \quad \ldots\ldots\ldots\ldots (vii)$$

Now we have to show that $\lim_{x\to\infty}\frac{\log x}{x}\int_2^x (\mathcal{T}(t) / t\log^2 t)\, dt = 0.$

Now $$\frac{\log x}{x}\int_2^x \frac{O(t)\,dt}{t\log^2 t} = O\left(\frac{\log x}{x}\int_2^x \frac{dt}{\log^2 t}\right) \quad \ldots\ldots\ldots\ldots\ldots\ldots (viii)$$

Consider $$\int_2^x \frac{dt}{\log^2 t} = \int_2^{\sqrt{x}} \frac{dt}{\log^2 t} + \int_{\sqrt{x}}^x \frac{dt}{\log^2 t}$$

$$\le \frac{1}{(\log 2)^2}\int_2^{\sqrt{x}} dt + \frac{1}{(\log\sqrt{x})^2}\int_{\sqrt{x}}^x dt \quad \text{[as in the above part]}$$

$$= \frac{\sqrt{x}-2}{(\log 2)^2} + \frac{x-\sqrt{x}}{(\log\sqrt{x})^2} < \frac{\sqrt{x}}{(\log 2)^2} + \frac{x-\sqrt{x}}{(\log\sqrt{x})^2} \quad \ldots\ldots\ldots\ldots\ldots (ix)$$

From (viii) and (ix) we get that

$$\frac{\log x}{x}\int_2^x \frac{dt}{\log^2 t} = \frac{\log x}{\sqrt{x}\,(\log 2)^2} + \frac{\log x}{(\log\sqrt{x})^2} - \frac{\log x}{\sqrt{x}\,(\log\sqrt{x})^2}$$

$$= \frac{\log x}{\sqrt{x}\,(\log 2)^2} + \frac{2}{\log\sqrt{x}} - \frac{2}{\sqrt{x}\log\sqrt{x}} \to 0 \text{ as } x\to\infty.$$

[since $\log x = \log(\sqrt{x}\,.\sqrt{x}) = \log\sqrt{x} + \log\sqrt{x} = 2\log\sqrt{x}$]

Hence $\lim_{x\to\infty} \frac{\log x}{x} \int_2^x \frac{1}{\log^2 t}\, dt = 0$ .... (x)

From (viii) and (x) we get $\lim_{x\to\infty} \frac{\log x}{x} \int_2^x (\mathcal{G}(t) / t \log^2 t)\, dt = 0$

By substituting this fact in (vii) we get $\lim_{x\to\infty} \frac{\pi(x)\log x}{x} = 1.$

This completes the proof of (b) ⇒ (a)

(b) ⇒ (c): By Theorem 6.1.7, we know that

$$\lim_{x\to\infty} \left(\frac{\psi(x)}{x} - (\mathcal{G}(x) / x)\right) = 0 \Leftrightarrow \lim_{x\to\infty} \frac{\psi(x)}{x} = \lim_{x\to\infty} (\mathcal{G}(x) / x).$$

Therefore $\lim_{x\to\infty} \frac{\psi(x)}{x} = 1 \Leftrightarrow \lim_{x\to\infty} (\mathcal{G}(x) / x).$

Hence the theorem.

6.3.3 Theorem: If p_n denotes the n^{th} prime, then the following three statements are equivalent: (a) $\lim_{x\to\infty} \frac{\pi(x)\log x}{x} = 1$; (b) $\lim_{x\to\infty} \frac{\pi(x)\log \pi(x)}{x} = 1$; (c) $\lim_{x\to\infty} \frac{p_n}{n \log n} = 1.$

Proof: (a) ⇒ (b):- Given $\lim_{x\to\infty} \frac{\pi(x)\log x}{x} = 1.$

Taking "log" on both sides, we get

$$\lim_{x\to\infty} (\log \pi(x) + \log(\log x) - \log x) = \log 1 = 0.$$

Dividing by "log x" on both sides, we get

$$\lim_{x\to\infty} \left(\frac{\log \pi(x)}{\log x} + \frac{\log(\log x)}{\log x} - 1\right) = 0 \Rightarrow \lim_{x\to\infty} \frac{\log \pi(x)}{\log x} + \lim_{x\to\infty} \frac{\log(\log x)}{\log x} = 1.$$

$$\Rightarrow \lim_{x\to\infty} \frac{\log \pi(x)}{\log x} + 0 = 1 \Rightarrow \log \pi(x) \sim \log x.$$

[Put $y = \log x$. Then $\lim_{x\to\infty} \frac{\log(\log x)}{\log x} = \lim_{y\to\infty} \frac{\log y}{y} = 0$]

$$\Rightarrow \log \pi(x) \sim \log x \sim \frac{x}{\pi(x)}$$

[since $\lim_{x\to\infty} \frac{\pi(x)\log(x)}{x} = 1 \Rightarrow \frac{\pi(x)}{x} \sim \frac{1}{\log x} \Rightarrow \log x \sim \frac{x}{\pi(x)}$]

$$\Rightarrow \log \pi(x) \sim \frac{x}{\pi(x)}$$

$\Rightarrow \lim_{x\to\infty} \frac{\pi(x)\log \pi(x)}{x} = 1.$ This completes (a) ⇒(b)

(b) ⇒ (a):- Given that $\lim_{x\to\infty} \frac{\pi(x)\log\pi(x)}{x} = 1$.

Taking "log" on both sides $\lim_{x\to\infty} (\log\pi(x) + \log(\log\pi(x)) - \log x) = \log 1 = 0$.

Dividing by $\log\pi(x)$ on both sides, we get

$$\lim_{x\to\infty}\left(\frac{\log\pi(x)}{\log\pi(x)} + \frac{\log(\log\pi(x))}{\log\pi(x)} - \frac{\log x}{\log\pi(x)}\right) = 0$$

$$\Rightarrow \lim_{x\to\infty}\left(1 + \frac{\log(\log\pi(x))}{\log\pi(x)} - \frac{\log x}{\log\pi(x)}\right) = 0$$

$$\Rightarrow \lim_{x\to\infty}\frac{\log(\log\pi(x))}{\log\pi(x)} - \lim_{x\to\infty}\frac{\log x}{\log\pi(x)} = -1$$

Therefore $0 - \lim_{x\to\infty}\frac{\log x}{\log\pi(x)} = 1$

[Take $y = \pi(x)$. Then $\lim_{x\to\infty}\frac{\log(\log\pi(x))}{\log\pi(x)} = \lim_{y\to\infty}\frac{\log y}{y} = 0$]

$$\Rightarrow \lim_{x\to\infty}\frac{\log x}{\log\pi(x)} = 1 \Rightarrow \log x \sim \log\pi(x) \text{ as } x \to \infty.$$

Given that $\lim_{x\to\infty}\frac{\pi(x)\log\pi(x)}{x} = 1 \Rightarrow \log\pi(x) \sim \frac{x}{\pi(x)}$

Therefore $\log x \sim \log\pi(x) \sim \frac{x}{\pi(x)} \Rightarrow \log x \sim \frac{x}{\pi(x)}$ as $x \to \infty \Rightarrow \lim_{x\to\infty}\frac{\log x\,\pi(x)}{x} = 1$. This completes (b) ⇒ (a).

(b) ⇒ (c):- We know that $\pi(x) = \sum_{p\le x} 1$ = the number of prime numbers $\le x$.

Let p_n be the n^{th} prime number. Then $\pi(p_n) = n$.

[since there are n primes which are $\le p_n$]

By taking $x = p_n$, we get $\lim_{x\to\infty}\frac{\pi(p_n)\log\pi(p_n)}{p_n} = 1$.

$$\Rightarrow \lim_{x\to\infty}\frac{n\log n}{p_n} \qquad \text{[since } \pi(p_n) = n] = 1$$

$$\Rightarrow \lim_{x\to\infty}\frac{p_n}{n\log n} = 1.$$

(c) ⇒ (b):- Given $\lim_{n\to\infty}\frac{p_n}{n\log n} = 1$.

Choose n such that $p_n \le x < p_{n+1}$.

Now $\pi(p_n) = n$ when p_n is the n^{th} prime number, p_{n+1} is the $(n+1)^{th}$ prime number. So $p_n \le x \le p_{n+1}$

$$\Rightarrow \frac{p_n}{n\log n} \le \frac{x}{n\log n} < \frac{p_{n+1}}{n\log n}$$

$$\Rightarrow \lim_{n\to\infty}\frac{p_n}{n\log n} \le \lim_{n\to\infty}\frac{x}{n\log n} \le \lim_{n\to\infty}\frac{p_{n+1}}{n\log n}.$$

$$\Rightarrow 1 \le \lim_{n\to\infty}\frac{x}{n\log n} \le \lim_{n\to\infty}\frac{p_{n+1}}{n\log n} \quad \text{[by the given condition } \lim_{n\to\infty}\frac{p_n}{n\log n} = 1\text{]}.$$

.... (i)

Consider $\lim_{n\to\infty}\frac{p_{n+1}}{n\log n} = \lim_{n\to\infty}\frac{p_{n+1}}{(n+1)\log(n+1)}\,\frac{(n+1)\log(n+1)}{n\log n}$

$$= \lim_{n\to\infty}\frac{p_{n+1}}{(n+1)\log(n+1)}\cdot\lim_{n\to\infty}\frac{(n+1)\log(n+1)}{n\log n}$$

$= 1.\ \lim_{n\to\infty}\frac{(n+1)\log(n+1)}{n\log n}$ [In the given condition, take $n+1$ in place of n, then we get $\lim_{n\to\infty}\frac{p_{n+1}}{(n+1)\log(n+1)}$]

$= 1.$

Therefore $\lim_{n\to\infty}\frac{p_{n+1}}{n\log n} = 1$ ....(ii)

From (i) and (ii) we have $1 \le \lim_{n\to\infty}\frac{x}{n\log n} \le 1$.

Therefore $\lim_{n\to\infty}\frac{x}{n\log n} = 1$.

[By the solution of n, we have $p_n \le x < p_{n+1} \Rightarrow p_n$ is n^{th} prime and there are n primes before x $\Rightarrow \pi(x) = \pi(p_n) = n$. Also $x \to \infty$ as $n \to \infty$]

$$\Rightarrow \lim_{x\to\infty}\frac{x}{\pi(x)\log\pi(x)} = 1 \Rightarrow \lim_{x\to\infty}\frac{\pi(x)\log\pi(x)}{x} = 1.$$ This completes the proof of (c) $\Rightarrow$ (b).

6.4 SUMMARY

In this lesson, we defined Chebysheve's **functions** $\psi(x)$ and $\vartheta(x)$, and obtained some inequalities involving Chebysheve's functions and Logarithmic functions. We proved a Theorem relates the two quotients $\psi(x)/x$ and $\vartheta(x)/x$. We also proved some identities namely, Abel's identity and deduced Euler's Summation formula from Abel's identity. Using the notion $\pi(x)$ $(x > 0)$, (the number of primes not exceeding x), some logically equivalent forms of prime number theorems were obtained. We observed that $\psi(x)$ is "about the same as" $\vartheta(x)$ in magnitude when x is large. We formulated a theorem which relates the "prime number theorem" to the asymptotic value of the n^{th} prime.

6.5 TECHNICAL TERMS

Chebyshev's ψ - function: The Chebyshev's ψ-function given by the formula $\psi(x) = \sum_{n \le x} \wedge(n)$, $x > 0$.

Chebyshev's ϑ - function: For $x \ge 0$, the Chebyschev's ϑ function by the equation $\vartheta(x) = \sum_{p \le x} \log p$, where the sum runs over all prime numbers p less than or equal to x

Abel's identity: For any arithmetic function a(n), define $A(x) = \sum_{n \le x} a(n)$, where $A(x) = 0$ if $x < 1$. Assume that f has a continuous derivative on the interval [y, x] where $0 < y < x$. Then we have

$$\sum_{y<n\le x} a(n)f(n) = A(x)f(x) - A(y)f(y) - \int_y^x A(t)f^1(t)dt.$$

Euler's Summation formula for Abel's identity: If $a(n) = 1 = U(n)$ for all n, then

$$\sum_{y<n\le x} f(n) = \int_y^x f(t)dt + \int_y^x (t-[t])f^1(t)dt + (y - [y])f(y) - (x - [x])f(x).$$

Relation between $\psi(x)$ and $\vartheta(x)$: $\psi(x) = \sum_{m \le \log_2 x} \vartheta(x^{1/m})$.

6.6 ANSWERS TO SELF ASSESSMENT QUESTIONS

1: Observe this sum. Consider the primes p involved in the sum. If $x^{1/m} < 2$, then there exists no prime p such that $p \le x^{1/m} < 2$. Therefore the sum runs over all m such that $x^{1/m} \ge 2$. Now $x^{1/m} \ge 2 \Rightarrow x \ge 2^m \Rightarrow \log x \ge \log 2^m \Rightarrow \log x \ge m \log 2 \Rightarrow \frac{\log x}{\log 2} \ge m \Rightarrow \log_2 x \ge m$ or $m \le \log_2 x$

2: For $m \ge 2$, we have $\frac{1}{m} \le \frac{1}{2} \Rightarrow x^{1/m} \log x^{1/m} \le x^{1/2} \log x^{1/2}$

$x^{1/m} \log x^{1/m} \le \sqrt{x} \log \sqrt{x}$.

6.7 MODEL QUESTIONS

1. Define Chebyshev's ϑ function and prove (i) For $x > 0$, we have

$$0 \leq \frac{\psi(x)}{x} - \vartheta(x)/x \leq \frac{(\log x)^2}{2\sqrt{x}\log 2}$$

(ii) $\lim_{x\to\infty} (\psi(x)/x - \vartheta(x)/x) = 0$

(iii) If one of $\psi(x)/x$ or $\vartheta(x)/x$ tends to a limit then so does the other. Also the two limits are equal.

2. State and prove Abel's identity.

3. Prove that the following statements are equivalent:

(a) $\lim_{x\to\infty} \frac{\pi(x)\log x}{x} = 1$; (b) $\lim_{x\to\infty} \vartheta(x)/x = 1$; and (c) $\lim_{x\to\infty} \frac{\psi(x)}{x} = 1$.

4. If p_n denotes the n^{th} prime, then prove that the following three statements are equivalent: (a) $\lim_{x\to\infty} \frac{\pi(x)\log x}{x} = 1$; (b) $\lim_{x\to\infty} \frac{\pi(x)\log\pi(x)}{x} = 1$; (c) $\lim_{x\to\infty} \frac{p_n}{n\log n} = 1$.

6.8 REFERENCE BOOKS

1. Chandrasekharan, K. "Introduction to Analytic Number Theory", Springer Verlag .
2. Hardy, G.H. & Wright, E.M. "Introduction to the Theory of Numbers", Fourth Edition, Oxford Publications,
3. Levegue W.J. (1986) "Topics in Number Theory (2 volumes), Addition - Wesley Publ. Co.
4. Rademacher (1964) "Lectures on Elementary Number Theory", New York, Blaisdell Publ. Co.
5. Tom M. Apostol "Introduction to Analytic Number Theory", Springer International Student Edition, Narosa Publishing House, 1995.
6. Uspensky, J.V., and Heaslett, M.A. (1939) "Elementary Number Theory", New York, Mc. Graw - Hill Book. Co.
7. Vinogrador, "Elements of Number Theory", Dover Publications

Name of the Author of this Lesson: **Dr. Kuncham Syam Prasad**

LESSON - 7

SHAPIRO'S TAUBERIAN THEOREM

Objectives

The the objectives of this lesson are to :

- learn about the notions $\pi(n)$ and P_n.
- know about Shapiro's Tauberian theorem
- understand the applications of Shapiro's Tauberian Theorem.
- Appreciate the usefulness of asymptotic formula for the partial sums

Structure

7.0 INTRODUCTION

Gauss and Legendre gave a conjecture that $\pi(x)$ is asymptotic to x/log x. In 1896, Hadamard and deVallee Poussin first proved this conjecture which is now known as prime number theorem, namely $\frac{\pi(x)\log x}{x} = 1$. In other words, prime number theorem states that $\pi(n) \sim n/\log n$ as $n \to \infty$. We deal with the inequalities for $\pi(n)$ and p_n to show that n/log n is the correct order of magnitude of $\pi(n)$. We obtain upper and lower bounds on the size of the n^{th} prime. We discuss a Tauberian theorem proved by A.N. Shapiro in 1950 which relates the sums of the form $\sum_{n \le x} a(n)$ with those of the form $\sum_{n \le x} a(n)\,[x/n]$ for non - negative a(n) and its applications in detail. We also obtain an asymptotic formula to the divergent series $\sum_{p \le x}(1/p)$ for its partial sums.

7.1 INEQUALITIES FOR $\pi(n)$ AND p_n

7.1.1 Lemma: If n is a positive integer, then $2^n \le {}^{(2n)}C_n < 4^n$.

Proof: **Part-(i)**: In this part (by induction) we prove that $2^n \le {}^{(2n)}C_n$ for all positive integer n.
If $n = 1$, then ${}^{(2n)}C_n = {}^{2}C_1 = 2 \ge 2 = 2^n$.
Induction Hypothesis: Suppose ${}^{(2k)}C_k \ge 2^k$.

Consider $${}^{2(k+1)}C_{(k+1)} = \frac{(2(k+1))!}{(k+1)!\,(k+1)!} = \frac{(2k+2)!}{(k+1)[k!](k+1)(k!)}$$

$$= \frac{(2k+2)(2k+1)[(2k)!]}{(k+1)^2\,(k!\,k!)} = \frac{(2k+2)(2k+1)}{(k+1)^2}\,\frac{(2k)!}{(k!\,k!)}$$

$$= \frac{(2k+2)(2k+1)}{(k+1)^2}\,{}^{(2k)}C_k \ge \frac{(2k+2)(2k+1)}{(k+1)^2}\,2^k \text{ (by Induction Hypothesis)}$$

$$= \frac{2\,(k+1)(2k+1)}{(k+1)^2}\,2^k = 2^{k+1}\frac{(2k+1)}{(k+1)} \ge 2^{k+1}.1 = 2^{k+1}$$

This completes the proof of part (i).
Part-(ii): Now we prove that ${}^{(2n)}C_n < 4^n$.
Consider $4^n = (2)^{2n}$ = sum of binomial coefficient for index $2n$
$= {}^{(2n)}C_0 + {}^{(2n)}C_1 + \ldots + {}^{(2n)}C_n + \ldots + {}^{(2n)}C_{2n} > {}^{(2n)}C_n$.
This completes the proof of part (ii).

7.1.2 Theorem: For every integer $n \ge 2$, we have $\frac{1}{6}\frac{n}{\log n} < \pi(n) < \frac{6.n}{\log n}$

(or $\frac{1}{6} < \frac{\pi(n)\log n}{n} < 6$)

Proof: **Part-(i)**: By Lemma 7.1.1, we have $2^n \le {}^{(2n)}C_n < 4^n$.
By taking "log" on both sides, we get $n \log 2 \le \log({}^{2n}C_n) < n \log 4$
$\Rightarrow n \log 2 \le \log((2n)!) - 2\log(n!) < n \log 4$ .... (i)

[since $\log({}^{2n}C_n) = \log\left(\frac{2n!}{n!n!}\right) = \log(2n!) - \log n! - \log n! = \log 2n! - 2 \log n!$]

By Legendre's identity, we have $[x]! = \prod_{p \le x} p^{\alpha(p)}$, where $\alpha(p) = \sum_{m=1}^{\infty}\left[\frac{x}{p^m}\right]$

$$\Rightarrow n! = \prod_{p \le n} p^{\alpha(p)} \text{ where } \alpha(p) = \sum_{m=1}^{\infty}\left[\frac{n}{p^m}\right].$$

If $p^m > n$, then $0 < \frac{n}{p^m} < 1 \Rightarrow \left[\frac{n}{p^m}\right] = 0 \Rightarrow \alpha(p) = \sum_{\substack{m=1 \\ p^m < n}} \frac{n}{p^m}$

$$\Rightarrow \alpha(p) = \sum_{m=1}^{\left[\frac{\log n}{\log p}\right]} \left[\frac{n}{p^m}\right]. \qquad \text{[Now } p^m < n \Rightarrow m \log p < \log n \Rightarrow m < \frac{\log n}{\log p}$$

$$\Rightarrow m \le \frac{\log n}{\log p}]$$

Therefore $n! = \prod_{p \le n} p^{\alpha(p)}$ where $\alpha(p) = \sum_{m=1}^{\left[\frac{\log n}{\log p}\right]} \left[\frac{n}{p^m}\right]$ .... (ii)

By taking logarithm on both sides, we get $\log n! = \sum_{p \le m} \alpha(p) \log p$ .... (iii)

Part-(ii): By substituting (iii) in left side part of (i), we get

$$n \log 2 \le \sum_{p \le 2n} \alpha(p) \log p - 2 \sum_{p \le n} \alpha(p) \log p$$

$$\Rightarrow n \log 2 \le \sum_{p \le 2n} \left(\sum_{m=1}^{\left[\frac{\log 2n}{\log p}\right]} \left[\frac{2n}{p^n}\right] \right) \log p - 2 \sum_{p \le n} \left(\sum_{m=1}^{\left[\frac{\log n}{\log p}\right]} \left[\frac{n}{p^m}\right] \right) \log p \quad \text{[By using (ii)]}$$

$$= \sum \sum_{m=1}^{\left[\frac{\log 2n}{\log p}\right]} \left(\left[\frac{2n}{p^m}\right] - 2\left[\frac{n}{p^m}\right] \right) \log p .$$

[Reason: If $p^m > n$, then $\left[\frac{n}{p^m}\right] = 0$. So $\sum_{m=1}^{\left[\frac{\log n}{\log p}\right]} \left[\frac{n}{p^m}\right] = \sum_{m=1}^{\left[\frac{\log 2n}{\log p}\right]} \left[\frac{n}{p^m}\right]$. The newly added terms are equal to zero]

$$\le \sum_{p \le 2n} \sum_{m=1}^{\left[\frac{\log 2n}{\log p}\right]} (1.\log p) = \sum_{p \le 2n} \left[\frac{\log 2n}{\log p}\right] \log p$$

[since for any x, we have that $[2x] - 2[x]$ is either 0 or 1.Therefore $\left(\frac{2n}{p^m} - 2\left(\frac{n}{p^m}\right)\right) \le 1$]

$$\le \sum_{p \le 2n} \log 2n = \pi(2n).\log 2n.$$

[the number of primes $\le 2n$ is $\pi(2n)$]

Therefore $n \log 2 \le \pi(2n).\log 2n$.

$$\Rightarrow \pi(2n) \geq \frac{n\log 2}{\log 2n} = \frac{2n}{\log 2n} \cdot \frac{\log 2}{2}.$$

$$\Rightarrow \pi(2n) \geq \frac{\log 2n}{\log 2n} \cdot \frac{1}{4} = \frac{1}{4}\frac{2n}{\log 2n} \text{ ....(iv)}$$

[since $\log 2 > \frac{1}{2}$, we have $\frac{\log 2}{2} > \frac{1}{4}$]

Case-(i): Suppose k is an even number. Then $k = 2n$ for some n.

From (iv) $\pi(k) = \pi(2n) \geq \frac{1}{4}\frac{2n}{\log 2n} \geq \frac{1}{4}\frac{k}{\log k} \geq \frac{1}{6}\frac{k}{\log k}$.

Therefore $\frac{1}{6}\frac{k}{\log k} \leq \pi(k)$ is true for all even integers k .... (v)

Suppose k is odd. Then $k = 2n + 1$ for some n.

Consider $\pi(k) = \pi(2n+1) \geq \pi(2n) > \frac{1}{4}\frac{2n}{\log 2n}$ (by (iv))

$$\geq \frac{1}{4}\frac{2n}{\log(2n+1)} = \frac{1}{4}\frac{2n}{2n+1} \cdot \frac{2n+1}{\log(2n+1)} = \frac{1}{4}\frac{2n}{(2n+1)}\frac{k}{\log k}$$

$$\geq \frac{1}{4}\frac{2}{3}\frac{k}{\log k} \quad \left[\text{for any } n, \frac{2n}{2n+1} \geq \frac{2}{3}\right]$$

$$= \frac{1}{6}\frac{k}{\log k} \text{ .... (vi)}$$

From (v) and (vi) we get that, for any integer $k \geq 2$, we have $\frac{1}{6}\frac{k}{\log k} < \pi(n)$.

Part-(iii): From (ii) and (iii) we get that

$$\log(2n)! - 2\log n! = \sum_{p\leq 2n}\sum_{m=1}^{\left[\frac{\log 2n}{\log p}\right]}\left[\frac{2n}{p^m}\right]\log p - 2\sum_{p\leq n}\sum_{m=1}^{\left[\frac{\log n}{\log p}\right]}\left[\frac{n}{p^m}\right]\log p$$

$$\geq \sum_{p\leq 2n}\left[\frac{2n}{p}\right]\log p - 2\sum_{p\leq n}\left[\frac{n}{p}\right]\log p$$

$$\geq \sum_{p\leq 2n}\left[\frac{2n}{p}\right]\log p - 2\sum_{p\leq 2n}\left[\frac{n}{p}\right]\log p$$

$$= \sum_{p\leq 2n}\left(\left[\frac{2n}{p}\right] - 2\left[\frac{n}{p}\right]\right)\log p \geq \sum_{n<p\leq 2n}\left(\left[\frac{2n}{p}\right] - 2\left[\frac{n}{p}\right]\right)\log p$$

$$= \sum_{n<p\leq 2n} 1.\log p \quad \left[\text{for those primes p with } n < p \leq 2n, \left[\frac{2n}{p}\right] - 2\left[\frac{n}{p}\right] = 1 \text{ (verify!)}\right]$$

$$= \sum_{p\leq 2n}\log p - \sum_{p\leq n}\log p$$

$= \vartheta(2n) - \vartheta(n)$. [By definition of $\vartheta(x) = \sum_{p\le x} \log p$ (p is prime)]

Therefore $\vartheta(2n) - \vartheta(n) \le \log(2n)! - 2\log(n!) < n \log 4$ (by (i))

$\Rightarrow \vartheta(2n) - \vartheta(n) < n \log 4$.

Taking $n = 2^r$ in this inequality, we get

$\vartheta(2^{r+1}) - \vartheta(2^r) < 2^r \log 4 = 2^r . 2 \log 2 = 2^{r+1}\log 2$

$$\Rightarrow \sum_{r=0}^{k} (\vartheta(2^{r+1}) - \vartheta(2^r)) < \sum_{r=0}^{k} 2^{r+1} \log 2$$

$$\Rightarrow \vartheta(2^{k+1}) - \vartheta(2^0) < (\log 2)\left(\sum_{r=0}^{k} 2^{r+1}\right) = \log 2(2^{k+2} - 2) < (\log 2).2^{k+2} = 2^{k+2}\log 2.$$

$\Rightarrow \vartheta(2^{k+1}) < 2^{k+2} \log 2$ .... (vii)(since $\vartheta(2^0) = \log 1 = 0$)

Select k such that $2^k \le n < 2^{k+1}$.

Then we obtain $\vartheta(n) \le \vartheta(2^{k+1}) < 2^{k+2} \log 2$ (by (vii))

$\le 4n \log 2$ [since $2^k \le n$, we have $2^k.4 \le n.4 \Rightarrow 2^{k+2} \le 4n$]

$\Rightarrow \vartheta(n) \le 4n \log 2$ .... (viii)

Part-(iv): If $0 < \alpha < 1$ and $n^\alpha < p \le n$, then $\log n^\alpha < \log p$

$\Rightarrow \log p > \log n^\alpha$.

$$\Rightarrow \sum_{n^\alpha < p \le n} \log p > \sum_{n^\alpha < p \le n} \log n^\alpha = \log(n^\alpha) \sum_{n^\alpha < p \le n} 1$$

$$= \log n^\alpha \left(\sum_{p\le n} 1 - \sum_{p \le n^\alpha} 1 \right) = \log n^\alpha(\pi(n) - \pi(n^\alpha))$$

$$= (\pi(n) - \pi(n^\alpha))\cdot \log n^\alpha \text{ .... (ix)}$$

Therefore $(\pi(n) - \pi(n^\alpha))\cdot \log n^\alpha < \sum_{n^\alpha < p \le n} \log p$ (by (ix))

$$< \sum_{p \le n} \log p = \vartheta(n) \le 4n \log 2 \text{ (by (viii))}$$

Therefore $(\pi(n) - \pi(n^\alpha)) \log n^\alpha \le 4n \log 2$

$\Rightarrow \pi(n) \log n^\alpha \le 4n \log 2 + \pi(n^\alpha) \log n^\alpha$

$$\Rightarrow \pi(n) < \frac{4n \log 2}{\log n^\alpha} + \pi(n^\alpha)$$

$$\le \frac{4n \log 2}{\alpha \log n} + n^\alpha \quad [\text{since } \pi(n^\alpha) = n^\alpha]$$

$$= \frac{n}{\log n}\left(\frac{4 \log 2}{\alpha} + \frac{(\log n) n^\alpha}{n}\right) = \frac{n}{\log n}\left(\frac{4 \log 2}{\alpha} + \frac{(\log n)}{n^{1-\alpha}}\right)$$

Therefore $\pi(n) < \dfrac{n}{\log n}\left(\dfrac{4\log 2}{\alpha} + \dfrac{(\log n)}{n^{1-\alpha}}\right)$ .... (x)

If $c > 0$ and $x \geq 1$, then the function $f(x) = x^{-c}\log x$ attains its maximum value at $x = e^{1/c}$

Therefore $x^{-c}\log x \leq$ max value $= (e^{1/c})^{-c}\log(e^{1/c}) = e^{-1}\dfrac{1}{c}\log e = \dfrac{e^{-1}}{c} = \dfrac{1}{ce}$.

Therefore $x^{-c}\log x \leq \dfrac{1}{ce}$ .... (xi)

Taking $\alpha = \dfrac{2}{3}$ in (x) we get

$$\pi(n) < \frac{n}{\log n}\left(\frac{4\log 2}{2/3} + \frac{\log n}{n^{1-(2/3)}}\right)$$

$$= \frac{n}{\log n}\left(6\log 2 + \frac{\log n}{n^{1/3}}\right)$$

$$= \frac{n}{\log n}\left(6\log 2 + \frac{3}{e}\right) \quad \left[\text{Since } \frac{\log n}{n^{1/3}} = n^{-1/3}\log n \leq \frac{1}{\frac{1}{3}e} = \frac{3}{e} \text{ (by (xi))}\right]$$

$$< \frac{n}{\log n}(6).$$

Therefore $\pi(n) < \dfrac{6n}{\log n}$.

This completes the proof of this theorem.

***Self Assessment Question 1:** Verify that* $\left[\dfrac{2n}{p}\right] - 2\left[\dfrac{n}{p}\right] = 1$ *for primes p with* $n < p \leq 2n$.

7.1.3 Theorem: For $n \geq 1$, then n^{th} prime p_n satisfies the following inequality

$$\frac{n\log n}{6} < p_n < 12\left(n\log n + n\log\frac{12}{e}\right)$$

Proof: Part-(i): Let $k = p_n$ is the n^{th} prime

$\Rightarrow \pi(k) = \pi(p_n) = n$ .... (i)

By Theorem 7.1.2, we have that

$$\frac{n}{6\log n} < \pi(n) < \frac{6n}{\log n} \quad \text{.......................................} \text{(ii)}$$

Taking $n = k$ on the right side part of (ii), we get (use (i) also)

$$n = \pi(k) < \frac{6k}{\log k} = \frac{6p_n}{\log p_n}$$

$$\Rightarrow n < \frac{6p_n}{\log p_n} \Rightarrow p_n > \frac{n\log p_n}{6} > \frac{n\log n}{6}$$

[Observe the table

N	1	2	3	4	5	6
N^{th} prime	2	3	5	7	11	13

Clearly $p_n > n \Rightarrow \log p_n > \log n$]

Therefore $p_n > \dfrac{n\log n}{6}$ or $\dfrac{n\log n}{6} < p_n$ .... (iii)

This completes the proof for the left hand part of the required inequality.

Part-(ii): Consider the left part of (ii). That is., $\dfrac{n}{6\log n} < \pi(n)$.

Take $n = k$ in this inequality. Then we get

$n = \pi(k) > \dfrac{k}{6\log k} = \dfrac{p_n}{6\log p_n}$ (since by (i), we have $n = \pi(k)$)

$\Rightarrow n > \dfrac{p_n}{6\log p_n} \Rightarrow 6n.\log p_n > p_n$

$\Rightarrow p_n < 6n \log p_n$ .... (iv)

From the proof of the Theorem 7.1.2, we know that $x^{-c}\log x \le \dfrac{1}{ce}$ .... (v)

Taking $c = \dfrac{1}{2}$, we get $x^{-1/2}\log x \le \dfrac{1}{\frac{1}{2}e} \Rightarrow \dfrac{\log x}{\sqrt{x}} \le \dfrac{2}{e}$.

Taking $x = p_n$ in this we get

$$\frac{\log p_n}{\sqrt{p_n}} \le \frac{2}{e} \Rightarrow \log p_n \le \frac{2\sqrt{p_n}}{e} \Rightarrow (6n)\log p_n \le \frac{(6n).2\sqrt{p_n}}{e}.$$

By using (iv) we get, $p_n < 6n \log p_n \le \dfrac{6n.2\sqrt{p_n}}{e} \Rightarrow p_n < \dfrac{12n}{e}\sqrt{p_n}$

$\Rightarrow \sqrt{p_n} < \dfrac{12n}{e}$

Taking "log" on both sides, we get $\dfrac{1}{2}\log p_n < \log n + \log\left(\dfrac{12}{e}\right)$ .... (vii)

From (iv) and (vii) we get that

$p_n < 6n \log p_n < 6n\,(2 \log n + 2 \log(12/e))$

$\Rightarrow p_n < 12\,(n \log n + n \log(12/e))$

This completes the proof of right hand part of the required inequality

7.2 SHAPIRO'S TAUBERIAN THEOREM

7.2.1 Result: Show that "$\dfrac{1}{x}\sum_{n\le x}\wedge(n) \sim 1$ as $x \to \infty$" is equivalent to prime number theorem.

Proof: Result 6.1.2 shows that

$\psi(x) = \sum_{n\le x}\wedge(x)$ (Here $\wedge$ is the Mongoldt function, $\wedge(n) = \begin{cases}\log p & \text{if } n = p^m \text{ (p prime)}\\ 0 & \text{otherwise}\end{cases}$

Result 6.3.2, states that the prime number theorem is equivalent to $\lim_{x\to\infty} \frac{\psi(x)}{x} = 1$.

Now $\frac{\sum_{n\le x} \wedge(n)}{x} = \frac{\psi(x)}{x}$.

Now "$\frac{1}{x}\sum_{n\le x} \wedge(n) = \frac{\psi(x)}{x} \sim 1$ as $x \to \infty$ is equivalent to prime number theorem.

7.2.2 Note: Consider $\frac{1}{x}\sum_{n\le x} \wedge(n) \sim 1$ as $x \to \infty$............................... (i)

Theorem 5.2.4 states that $\sum_{n\le x} \wedge(n)\left[\frac{x}{n}\right] = x \log x - x + O(\log x)$ .... (ii)

Both sums (i) and (ii) are weighted averages of the function $\wedge(n)$.

Each term $\wedge(n)$ is multiplied by a weight factor $\frac{1}{x}$ in (i) and by $\left[\frac{x}{n}\right]$ in (ii).

Theorems relating to different weighted averages of the same function are called **Tauberian Theorems.**

Hence forth, we present the proofs for important results only.

7.2.3 Theorem: Shapiro's Tauberian:- Suppose $\{a(n)\}$ is non-negative sequence such that

$\sum_{n\le x} a(n)\left[\frac{x}{n}\right] = x \log x + O(x)$ for all $x \ge 1$.......(i), then

(a) For $x \ge 1$, we have $\sum \frac{a(n)}{n} = \log x + O(1)$.

[In other words, in (i) if we remove square brackets then we get $\sum_{n\le x} a(n)\frac{x}{n} = x \log(x) + O(x)$ and divide by x to get $\sum_{n\le x} \frac{a(n)}{n} = \log x + O(1)$].

(b) There exists a constant $A > 0$ such that $\sum_{n\le x} a(n) \le A(x)$ for all $x \ge 1$.

(c) There exists a constant $B > 0$ and $x_0 > 0$ such that $\sum_{n\le x} a(n) \ge B(x)$ for all $x \ge x_0$.

Proof: Write $S(x) = \sum_{n\le x} a(n)$ and $T(x) = \sum_{n\le x} a(n)\left[\frac{x}{n}\right]$ .... (ii)

Part-(i): In this part we prove that $S(x) - S\left(\frac{x}{2}\right) \le T(x) - 2T\left(\frac{x}{2}\right)$ .... (iii)

For this consider $T(x) - 2T\left(\frac{x}{2}\right) = \sum_{n\le x} a(n)\left[\frac{x}{n}\right] - 2\sum_{n\le \frac{x}{2}} a(n)\left[\frac{x}{2n}\right]$

$$= \sum_{n\le \frac{x}{2}} a(n)\left[\frac{x}{n}\right] + \sum_{\frac{x}{2}<n\le x} a(n)\left[\frac{x}{n}\right] - 2\sum_{n\le \frac{x}{2}} a(n)\left[\frac{x}{2n}\right]$$

$$= \sum_{n\le \frac{x}{2}} a(n)\left(\left[\frac{x}{n}\right] - 2\left[\frac{x}{2n}\right]\right) + \sum_{\frac{x}{2}<n\le x} a(n)\left[\frac{x}{n}\right].$$

$$= 0 + \sum_{\frac{x}{2}<n\le x} a(n)\left[\frac{x}{n}\right] = \sum_{\frac{x}{2}<n\le x} a(n)\left[\frac{x}{n}\right].$$ [We know that $[2y] - 2[y] = 0$ or 1 which is ≥ 0.

Taking $y = \frac{x}{2n}$ in this we get $\left[\frac{x}{n}\right] - 2\left[\frac{x}{2n}\right] = 0$]

$$= \sum_{\frac{x}{2}<n\le x} a(n)$$ [since $\left[\frac{x}{n}\right] = 1$ as (i) $\frac{x}{2} < n \Rightarrow \frac{x}{n} < 2 \Rightarrow \left[\frac{x}{n}\right] \le 1$

& (ii) $n < x \Rightarrow \frac{x}{n} > 1 \Rightarrow \left[\frac{x}{n}\right] \ge 1$]

$$= \sum_{n\le x} a(n) - \sum_{n\le \frac{x}{2}} a(n) = S(x) - S\left(\tfrac{x}{2}\right)$$

$\Rightarrow T(x) - 2T\left(\frac{x}{2}\right) \ge S(x) - S\left(\frac{x}{2}\right)$ or $S(x) - S\left(\frac{x}{2}\right) \le T(x) - 2T\left(\frac{x}{2}\right)$ .... (iii)

Part-(ii): In this part we prove (b).

In the hypothesis, it is given that $\sum_{n\le x} a(n)\left[\frac{x}{n}\right] = x\log x + O(x)$ for all $x \ge 1$...(*1)

$$T(x) - 2T\left(\tfrac{x}{2}\right) = \sum_{n\le x} a(n)\left[\frac{x}{n}\right] - 2\sum_{n\le x} a(n)\left[\frac{x}{2n}\right]$$

$$= (x\log x + O(x)) - 2\left(\frac{x}{2}\log\frac{x}{2} + O\left(\frac{x}{2}\right)\right)$$ (by (*1))

$$= x\log x + O(x) = 2\frac{x}{2}\log\frac{x}{2} - 2O\left(\frac{x}{2}\right)$$

$= (x\log x + O(x)) - (x\log x - x\log 2) - O(x)$ [since $2\,\frac{x}{2}\log\frac{x}{2} = x\log\frac{x}{2}$

$= x(\log x - \log 2) = x\log x - x\log 2\,]$

$= x\log 2 + O(x) + O(x) = x\log 2 + O(x) = O(x)\log 2 + O(x) = O(x) + O(x) = O(x)$

Therefore $T(x) - 2T\left(\frac{x}{2}\right) = O(x)$ .... (iv)

From (iii) and (iv), we have that $O(x) = T(x) - 2T\left(\frac{x}{2}\right) > S(x) - S\left(\frac{x}{2}\right)$

$\Rightarrow S(x) - S\left(\frac{x}{2}\right) < O(x) = kx$ for all x, where k is a constant.

In this, take in place of x, the expressions, $x, \frac{x}{2}, \frac{x}{2^2} \ldots$

Then $S(x) - S\left(\frac{x}{2}\right) < kx$; $S(x) - S\left(\frac{x}{2}\right) - S\left(\frac{x}{2^2}\right) < k\frac{x}{2}$;

$S\left(\frac{x}{2^2}\right) - S\left(\frac{x}{2^3}\right) < k\cdot\frac{x}{2^2}, \ldots\ldots\ldots, S\left(\frac{x}{2^n}\right) - S\left(\frac{x}{2^{n+1}}\right) < k\left(\frac{x}{2^n}\right).$

By adding all these, we get $S(x) - S\left(\frac{x}{2^{n+1}}\right) \le kx\left(1 + \frac{1}{2} + \frac{1}{2^2} + \cdots + \frac{1}{2^n}\right)$

$\Rightarrow S(x) \le 2kx.$ [as $n \to \infty$ we get $S\left(\frac{x}{2^{n+1}}\right) = 0$ and $1 + \frac{1}{2} + \frac{1}{2^2} + \cdots + \frac{1}{2^n} = 2$]

Hence we get $\sum_{n\le x} a(n) = S(x) < Ax$ where $A = 2k$, a constant .... (v)

This completes the proof of (b)

Part-(iii): Now we prove (a)

By (ii), we have $T(x) = \sum_{n\le x} a(n)\left[\frac{x}{n}\right] = \sum_{n\le x} a(n)\left[\frac{x}{n} + O(1)\right]$

$$= \sum_{n\le x} a(n)\frac{x}{n} + \left(\sum_{n\le x} a(n)\right)O(1)$$

$$= \sum_{n\le x} a(n)\frac{x}{n} + O\left(\sum_{n\le x} a(n)\right)$$

$= x\sum_{n\le x}\frac{a(n)}{n} + O(x)$ [By (v) we have $\sum_{n\le x} a(n) \le Ax$

$\Rightarrow \sum_{n\le x} a(n) = O(x)$].................. (vi)

From (i) and (vi) we have $x\log x + O(x) = T(x) - x\sum_{n\le x}\frac{a(n)}{n} + O(x)$

$\Rightarrow x\sum_{n\le x}\frac{a(n)}{n} = x\log x + O(x) - O(x) = x\log x + O(x)$

B)

Dividing by x we get that $\sum_{n\le x}\frac{a(n)}{n} = \log x + O(1)$ .... (vii)

This completes the proof of (a)

Part-(iv): In this part we prove (c).

By (vii) we get that $A(x) = \sum_{n\le x}\frac{a(n)}{n} = \log x + O(1)$

$\Rightarrow A(x) = \log x + R(x)$ where $R(x) = O(1)$ .... (viii)

Note that $R(x) = O(1) \Rightarrow \left|\frac{R(x)}{1}\right| \le M$ for some fixed number ....(ix)

Take α with $0 < \alpha < 1$ and

consider $A(x) - A(\alpha x) = \sum_{n\le x}\frac{a(n)}{n} - \sum_{n\le \alpha x}\frac{a(n)}{n}$

$= (\log x + R(x)) - (\log(\alpha x) + R(\alpha x))$ (by (viii))

$= (\log x + R(x)) - (\log \alpha - \log x + R(\alpha x))$

$= -\log \alpha + R(x) - R(\alpha x) \ge -\log \alpha - |R(x)| - |R(\alpha x)|$

$\ge -\log \alpha - 2M$ (where M is given by (ix)).......................(x)

Now we choose α such that $-\log \alpha - 2m = 1$. That is., $-\log \alpha = 1 + 2m$

$\Rightarrow \log \alpha = -2m - 1 \Rightarrow \alpha = e^{-2m-1}$.

Therefore if $\alpha = e^{-2m-1}$, then $-\log \alpha - 2m = 1$ and so $A(x) - A(\alpha x) \ge 1$ .....(xi)

Now $\alpha = \exp(-2m - 1) = \frac{1}{e^{2m+1}} < 1 \Rightarrow \alpha \in (0, 1) \Rightarrow 0 < \alpha < 1$.

$\Rightarrow 0 < \alpha x < x$.

so far $0 < \alpha < 1$ and $\alpha = \exp(-2m - 1)$ we have $A(x) - A(\alpha x) \ge 1$ (from (xi)).

Therefore $1 \le A(x) - A(\alpha x) = \sum_{n\le x}\frac{a(n)}{n} - \sum_{n\le \alpha x}\frac{a(n)}{n}$

$$= \sum_{\alpha x < n \le x}\frac{a(n)}{n}$$

$$< \frac{1}{\alpha x}\sum_{\alpha x < n \le x} a(n) \quad \left[\text{Since } \alpha x < n \text{ we have } \frac{1}{\alpha x} > \frac{1}{n}\right]$$

$$< \frac{1}{\alpha x}\sum_{n\le x} a(n)$$

$\Rightarrow 1 < \frac{1}{\alpha x}\sum_{n\le x} a(n) \Rightarrow \sum_{n\le x} a(n) \ge \alpha x$ for all $x \ge 1/\alpha$.

$\Rightarrow \sum_{n\le x} a(n) \ge Bx$ for all $x \ge x_0$ where $B = \alpha$ and $x_0 = 1/\alpha$.

This completes the proof of the theorem.

7.3 APPLICATIONS OF SHAPIRO'S THEOREM

7.3.1 Theorem: (i) For all $x \geq 1$, we have $\sum_{n\leq x} \frac{\wedge(n)}{n} = \log x + O(1)$.

(ii) Also there exists positive constants c_1, c_2 such that $\psi(x) \leq c_1 x$ for all $x \geq 1$ and $\psi(x) \geq c_2 x$ for all sufficiently large x.

(iii) Define $\wedge_1(n) = \begin{cases} \log p & \text{if } n \text{ is prime} \\ 0 & \text{otherwise} \end{cases}$. Then $\sum_{n\leq x} \Lambda_1(n)\left[\frac{x}{n}\right] = x \log x + O(x)$

Proof: (i) By Theorem 5.2.4., we have $\sum_{n\leq x} \Lambda(n)\left[\frac{x}{n}\right] = x \log x - x + O(\log x)$

By using Theorem 7.2.3(i) we get, $\sum_{n\leq x} \frac{\wedge(n)}{n} = \log x + O(1)$ [Take $a(n) = \wedge(n)$]

(ii) From Theorem 7.2.3 (b) and (c), taking $a(n) = \wedge(n)$ we can conclude that there exists $c_1 = B > 0$ and $c_2 = A > 0$ such that $\sum_{n\leq x} \wedge(n) \leq c_1 x$ and $\sum_{n\leq x} \wedge(n) \geq c_2 x$ for sufficiently large x.

(iii) By Theorem 5.2.5, we have $\sum_{p\leq x} \left[\frac{x}{p}\right] \log p = x \log x + O(x)$

Consider $\wedge_1(n)$ defined in the statement.

Then $\sum_{n\leq x} \wedge_1(n)\left[\frac{x}{n}\right] = \sum_{p\leq x} \wedge_1(p)\left[\frac{x}{p}\right]$ where p is prime

[since $\wedge_1(n) = 0$ if n is not prime]

$= \sum_{p\leq x} (\log p)\left[\frac{x}{p}\right] = x \log x + O(x)$ [by Theorem 5.2.5]

Therefore $\sum_{n\leq x} \wedge_1(n)\left[\frac{x}{n}\right] = x \log x + O(x)$.

7.3.2 Theorem: (a) For all $x \geq 1$, we have $\sum_{p\leq x} \frac{\log p}{p} = \log x + O(1)$.

(b) There exist positive constants c_1 and c_2 such that $\vartheta(x) \leq c_1 x$ for all $x \geq 1$ and $\vartheta(x) \geq c_2 x$ for all sufficiently large x.

Proof: (a). By Theorem 7.3.1(iii), we have $\sum_{n\leq x} \wedge_1(n)\left[\frac{x}{n}\right] = x \log x + O(x)$.

By taking $a(n) = \wedge_1(n)$ in Shapiro's Theorem 7.2.3, we conclude that

$$\sum_{n\leq x} \frac{\wedge_1(n)}{n} = \log x + O(1) \quad \dots (i)$$

Since $\wedge_1(n) = 0$ if n is not prime, we have $\sum_{n \le x} \frac{\wedge_1(n)}{n} = \sum_{p \le x} \frac{\log p}{n}$ ....(ii).

From (i) and (ii) we get $\sum_{p \le x} \frac{\log p}{p} = \log x + O(1)$

(b) By the definition of $\mathcal{G}(x)$, we have $\mathcal{G}(x) = \sum_{p \le x} \log p$.

Therefore $\mathcal{G}(x) = \sum_{p \le x} \log p = \sum_{p \le x} \wedge_1(p) = \sum_{n \le x} \wedge_1(n)$

(since $\wedge_1(n) = 0$ if n is not prime)
Consider Part-(ii), (iii) of Theorem 7.2.3.
If $a(n) = \wedge_1(n)$, then $\sum a(n) = \sum \wedge_1(n) = \mathcal{G}(x)$.

Therefore there exists $c_1 = B > 0$ and $c_2 = A > 0$ such that $\mathcal{G}(x) \le c_1 x$ for all $x \ge 1$ and $\mathcal{G}(x) \ge c_2 x$ for all sufficiently large x.

7.3.3 Theorem: For all $x \ge 1$, we have

(a) $\sum_{n \le x} \psi\left(\frac{x}{n}\right) = x \log x - x + O(\log x)$

(b) $\sum_{n \le x} \mathcal{G}\left(\frac{x}{n}\right) = x \log x + O(x)$

Proof: By Theorem 5.1.3, we have

$$\sum_{n \le x} f(n)\left[\frac{x}{n}\right] = \sum_{n \le x} F\left[\frac{x}{n}\right] \text{ where } F(x) = \sum_{n \le x} f(n) \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (i)$$

(a) By 6.1.2, we know that $\psi(x) = \sum_{n \le x} \wedge(n)$

In (i) take $f = \wedge$, and $F = \psi$.

Then $\sum_{n \le x} \psi\left(\frac{x}{n}\right) = \text{RHS of (i)} = \text{LHS of (i)} = \sum_{n \le x} \wedge(n)\left[\frac{x}{n}\right]$

$= x \log x - x + O(\log x)$ (by Theorem 5.2.4)

(b) As in above Theorem proof part-(ii), we can observe that
$\mathcal{G}(x) = \sum_{p \le x} \log p = \sum_{p \le x} \wedge_1(p) = \sum_{n \le x} \wedge_1(n)$.

Therefore $\mathcal{G}(x) = \sum_{n \le x} \wedge_1(n)$. [In (i) take $f = \wedge_1$, then $F = \mathcal{G}$.]

Consider $\sum_{n \le x} \mathcal{G}\left(\frac{x}{n}\right) = \text{RHS of (i)} = \text{LHS of (i)} = \sum_{n \le x} \wedge_1(n)\left[\frac{x}{n}\right]$

$= x \log x + O(x)$ for all $x \ge 1$.

[By taking $a(n) = \wedge_1(n)$ in Shapiro's Theorem 7.2.3]

7.4 AN ASYMPTOTIC FORMULA FOR THE PARTIAL SUMS $\sum_{p \le x} \frac{1}{p}$

7.4.1 Theorem: There exists a constant A such that $\sum_{p \le x} \frac{1}{p} = \log(\log x) + A + O\left(\frac{1}{\log x}\right)$ for all $x \ge 2$.

Proof: Consider the function $a(n) = \frac{\log n}{n}$ if n is a prime number.
$= 0$ otherwise.

Clearly $a(n) \ge 0$ for all $n \ge 1$.
Write $A(x) = \sum_{n \le x} a(n)$.

Then $A(x) = \sum_{n \le x} a(n) = \sum_{p \le x} a(p)$ (since $a(n) = 0$ if n is not prime)

$= \sum_{p \le x} \frac{\log p}{p} = \log x + O(1)$ (by Theorem 7.3.2)

$\Rightarrow A(x) = \log x + O(1)$ .... (i)

By Abel's Theorem 6.2.2, we have

$$\sum_{y < n \le x} a(n) f(n) = A(x)f(x) - A(y)f(y) - \int_y^x A(t) f^1(t)\,dt$$

[In this take $f(t) = \frac{1}{\log t}$ for $t > 1$.

Then $f^1(t) = \frac{-1}{t \log^2 t}$ exists and continuous in $[1, x]$.

Also observe that $a(n) = 0$ if n is not prime. If $y = 1$, then
$A(y) = A(1) = \log 1 + O(1) = 0$]

Now

$$\sum_{1 < p \le x} \left(\frac{\log p}{p}\right)\left(\frac{1}{\log p}\right) = (\log(x) + O(1))\left(\frac{1}{\log x}\right) - A(y)f(y) - \int_1^x A(t) \frac{-1}{t \log^2 t} dt$$

$$\Rightarrow \sum_{1 < p \le x} \frac{1}{p} = \frac{\log x + O(1)}{\log x} - 0.f(y) + \int_1^x \frac{A(t)}{t \log^2 t} dt$$

$$= \frac{\log x}{\log x} + \frac{O(1)}{\log x} + \int_1^x \frac{\log(t) + O(1)}{t \log^2 t} dt \text{ (since } A(t) = \log t + O(1), \text{ by (i))}$$

$$= 1 + O\left(\frac{1}{\log x}\right) + \int_2^x \frac{\log t}{t \log^2 t} dt + \int_2^x \frac{O(1)\,dt}{t \log^2 t}$$

[since $\log 1 = 0$, we take integral from 2 to x]

$$= 1 + O\left(\frac{1}{\log x}\right) + \int_2^x \frac{dt}{t\log t} + \int_2^x \frac{O(1)dt}{t\log^2 t}$$

$$= 1 + O\left(\frac{1}{\log x}\right) + (\log(\log t))_2^x + \int_2^\infty \frac{O(1)dt}{t\log^2 t} - \int_x^\infty \frac{O(1)dt}{t\log^2 t}$$

[since $\frac{d}{dt}(\log(\log t)) = \frac{1}{t\log t}$]

$$= 1 + O\left(\frac{1}{\log x}\right) + \log(\log x) - \log(\log 2) + \int_2^\infty \frac{O(1)dt}{t\log^2 t} - \int_x^\infty \frac{O(1)dt}{t\log^2 t}$$

$$= A + O\left(\frac{1}{\log x}\right) + \log(\log x) - O(1)\int_x^\infty \frac{dt}{t\log^2 t}$$

[where $A = 1 - \log(\log 2) + \int_2^\infty \frac{O(1)dt}{t\log^2 t}$]

$$= A + O\left(\frac{1}{\log x}\right) + \log(\log x) - O(1).\left(\frac{-1}{\log x}\right).$$

[since $\int_x^\infty \frac{dt}{t\log^2 t} - \int_x^\infty \left(\frac{1}{\log t}\right)^1 dt = \left[\frac{1}{\log t}\right]_x^\infty = 0 - \frac{1}{\log x}$.]

$$= A + \log(\log x) + O\left(\frac{1}{\log x}\right).$$

7.5 SUMMARY

In this lesson, we dealt with further inequalities of $\pi(n)$ and P_n $(n > 0)$, the n^{th} prime. We have also shown that the prime number theorem is equivalent to the asymptotic formula which leads to Shapiro's Tauberian theorem. We proved that n/logn is the correct order of magnitude of $\pi(n)$. We derived an asymptotic formula for the partial sums $\sum(1/p)$. As applications of Shapiro's theorem, some asymptotic formulae were deduced from it.

7.6 TECHNICAL TERMS

Shapiro's Tauberian Theorem: Let $\sum_{n\le x} a(n)\left[\frac{x}{n}\right] = x\log x + O(x)$ for all $x \ge 1$, where $\{a(n)\}$ is a non - negative sequence. Then

(a) For $x \ge 1$, we have $\sum \frac{a(n)}{n} = \log x + O(1)$.

(b) There is a constant $B > 0$ such that $\sum_{n\le x} a(n) \le B(x)$ for all $x \ge 1$.

(c) There is a constant $A > 0$ and $x_0 \geq 0$ such that

$$\sum_{n \le x} a(n) \ge A(x) \quad \text{for all } x \ge x_0.$$

Inequalities in $\pi(n)$ and p_n: (i). $\frac{1}{6}\frac{n}{\log n} < \pi(n) < \frac{6 \cdot n}{\log n}$ $(n \ge 2)$

(ii). $\frac{n \log n}{6} < p_n < 12\left(n \log n + n \log \frac{12}{e}\right)$

7.7 ANSWERS TO SELF ASSESSMENT QUESTIONS

1: Let p be a prime with $n < p \le 2n$. Then we have

(i) $\frac{n}{p} < 1 \le \frac{2n}{p} \Rightarrow \left[\frac{n}{p}\right] = 0$ and $\left[\frac{2n}{p}\right] \ge 1$

(ii) $n < p \Rightarrow 2n < 2p \Rightarrow \left[\frac{2n}{p}\right] < 2.$

Now $1 \le \left[\frac{2n}{p}\right] < 2 \Rightarrow \left[\frac{2n}{p}\right] = 1.$

Therefore $\left[\frac{2n}{p}\right] - 2\left[\frac{n}{p}\right] = 1 - 2\times 0 = 1$ for all $n < p \le 2n$.

7.8 MODEL QUESTIONS

1. Prove that for every integer $n \ge 2$, we have $\frac{1}{6}\frac{n}{\log n} < \pi(n) < 6.\frac{n}{\log n}$.
2. Prove that for all $x \ge 1$, $\sum_{n \le x} \frac{\Lambda(n)}{n} = \log x + O(1)$.
3. Prove that there is a constant A such that $\sum_{p \le x} \frac{1}{p} = \log \log x + A + O\left(\frac{1}{\log x}\right)$.

7.9 REFERENCE BOOKS

1. Chandrasekharan, K. "Introduction to Analytic Number Theory", Springer Verlag .
2. Hardy, G.H. & Wright, E.M. "Introduction to the Theory of Numbers", Fourth Edition, Oxford Publications,
3. Levegue W.J. (1986) "Topics in Number Theory (2 volumes), Addition - Wesley Publ. Co.
4. Rademacher (1964) "Lectures on Elementary Number Theory", New York, Blaisdell Publ. Co.
5. Tom M. Apostol "Introduction to Analytic Number Theory", Springer International Student Edition, Narosa Publishing House, 1995.
6. Uspensky, J.V., and Heaslett, M.A. (1939) "Elementary Number Theory", New York, Mc. Graw - Hill Book. Co.
7. Vinogrador, "Elements of Number Theory", Dover Publications

Name of the Author of this Lesson: **Dr. Kuncham Syam Prasad**

LESSON – 8

THE PARTIAL SUMS OF THE MOBIUS FUNCTION AND SELBERG'S ASYMPTOTIC FORMULA

Objectives

The objectives of this lesson are to:

- understand partial sums of the Mobius function
- know brief sketch of elementary proof of the prime number theorem
- analyze the Selberg's asymptotic formula

Structure

8.0 INTRODUCTION

In previous lessons, we had familiar with various arithmetical functions. In this lesson, we provided the detailed proofs of some implication of prime number theorem, we introduce the notion, and the proof of Selberg's asymptotic formula. Using this we discussed the sketch of elementary proof of prime number theorem.

8.1 THE PARTIAL SUMS OF THE MOBIUS FUNCTION

8.1.1 Definition: If $x \geq 1$, we define $M(x) = \sum_{n \leq x} \mu(n)$.

[Mobius function $\mu(n) = \begin{cases} 1 & \text{if } n = 1 \\ (-1)^k & \text{if } n = p_1 p_2 \ldots p_k \text{ (square free)} \\ 0 & \text{other wise} \end{cases}$]

8.1.2 Note: (i) The exact order of Magnitude of $M(x)$ is not known. Numerical evidence suggests that $|M(x)| < \sqrt{x}$ if $x > 1$. But this inequality, known as **Mertens conjecture**, has not been proved nor disproved.

(ii) The best O- result obtained to date is $M(x) = O(x \cdot \delta(x))$ where $\delta(x) = \exp\{-A \log^{(3/5)} x \, (\log\log x)^{-1/5}\}$ for some positive constant A.

(iii) In this section, we prove that the statement $\lim_{x\to\infty} \frac{M(x)}{x} = 0$ is equivalent to the prime number theorem.

8.1.3 Definition: If $x \geq 1$, we define $H(x) = \sum_{n \leq x} \mu(n)\log n$.

8.1.4 Theorem: (i) $\lim_{x\to\infty}\left(\frac{M(x)}{x} - \frac{H(x)}{x\log x}\right) = 0.$

(ii) If one of $\frac{M(x)}{x}$ or $\frac{H(x)}{x\log x}$ tends to a finite limit, the other also tends to same limit.

Proof: By Abel's identity (Theorem 6.2.2), if $a(n)$, is an arithmetical function, and $A(n) = \sum_{n\leq x} a(n)$, then $\sum_{y<n\leq x} a(n)f(n) = A(x)f(x) - A(y)f(y) - \int_y^x A(t)f^1(t)dt$

In this Abel's identity, take $a(n) = \mu(n)$ and $f(t) = \log t$ which is differentiable in $[1, x]$.

$A(x) = \sum_{n\leq x} a(n) = \sum_{n\leq x}\mu(n) = M(x)$.

Now by substituting these, in Abel's identity we get

$$\sum_{1<n\leq x}\mu(n)\log n = M(x)\log x - A(1)\log 1 - \int_1^x M(t)\frac{1}{t}dt \quad \text{.............................} \quad (i)$$

By definition of $H(x)$ (refer 8.1.3), we have

$$H(x) = \sum_{1<n\leq x}\mu(n)\log n = \mu(1)\log 1 + \sum_{1<n\leq x}\mu(n)\log n$$

$$= 0 + \sum_{1<n\leq x}\mu(n)\log n$$

$$= M(x)\log x - A(1)\log 1 - \int_1^x M(t)\frac{1}{t}dt$$

$$= M(x)\log x - 0 - \int_1^x M(t)\frac{1}{t}dt$$

Dividing by $x \log x$, we get

$$\Rightarrow \frac{H(x)}{x\log x} = \frac{M(x)}{x} - \frac{1}{x\log x}\int_1^x \frac{M(t)}{t}dt$$

$$\Rightarrow \frac{H(x)}{x\log x} - \frac{M(x)}{x} = -\frac{1}{x\log x}\int_1^x \frac{M(t)}{t}dt$$

$$\Rightarrow \lim_{x\to\infty}\left(\frac{H(x)}{x\log x}-\frac{M(x)}{x}\right) = -\lim_{x\to\infty}\frac{1}{x\log x}\int_1^x \frac{M(t)}{t}dt \quad \text{.............................. (ii)}$$

Consider $\int_1^x \frac{M(t)dt}{t} = \int_1^x \frac{\left(\sum_{n\le t}\mu(t)\right)}{t}dt$ (by definition of M(t))

[since $\mu(t) = 1$ or (-1) we have $\mu(t) \le 1$]

$$\le \int_1^x \left(\frac{\sum_{n\le t} 1}{t}\right)dt = \int_1^x \frac{[t]}{t}dt$$

$$\le \int_1^x 1\,dt \text{ (since } [t]\le t) = [x]_1^x = x - 1.$$

Dividing on both sides by x log x, we get

$$\frac{1}{\log x}\int_1^x \frac{M(t)dt}{t} = \frac{x-1}{x\log x} = \frac{1}{\log x} - \frac{1}{x\log x}$$

$$\Rightarrow \lim_{x\to\infty} \frac{1}{x\log x}\int_1^x \frac{M(t)dt}{t} = \lim_{x\to 0}\frac{1}{\log x} - \lim_{x\to 0}\frac{1}{x\log x} = 0$$

By substituting this in (ii), we get $\lim_{x\to\infty}\left[\frac{H(x)}{x\log x}-\frac{M(x)}{x}\right] = 0$

(b) From above steps we have $\lim_{x\to\infty}\frac{H(x)}{x\log x} - \lim_{x\to\infty}\frac{M(x)}{x} = 0.$

$$\Rightarrow \lim_{x\to\infty}\frac{H(x)}{x\log x} = \lim_{x\to\infty}\frac{M(x)}{x}$$

Therefore if one of $\frac{H(x)}{x\log x}$ or $\frac{M(x)}{x}$ tends to a finite limit then the other also tends to the same limit.

8.1.5 Theorem: The prime number theorem implies $\lim_{x\to\infty}\frac{M(x)}{x} = 0.$

Proof: First we prove that, $\lim_{x\to\infty}\frac{\psi(x)}{x} = 1$ implies $\lim_{x\to\infty}\frac{H(x)}{x\log x} = 0.$

Part-(i): Suppose $\lim_{x\to\infty}\frac{\psi(x)}{x} = 1$

$\Rightarrow$ for $\varepsilon > 0$, there exist a positive number A such that $\left[\frac{\psi(x)}{x}-1\right] < \varepsilon/2$ for all $x \ge A$.

$$\Rightarrow |\psi(x) - x| < \frac{x\varepsilon}{2} \text{ for all } x \ge A \quad \text{.. (i)}$$

By Theorem 2.2.3, we have that, $\log n = \sum_{d|n} \wedge(d)$ .... (ii)

where Mangoldt function is $\wedge(n) = \begin{cases} \log p & \text{if } n = p^m \\ 0 & \text{otherwise} \end{cases}$

By Theorem 2.2.4, we have $\wedge(n) = -\sum_{d|n} \mu(d)\log d$ .... (iii)

We know that the Mobius inversion formula (Theorem 2.1.11) is

$f(n) = \sum_{d|n} g(d) \Leftrightarrow g(n) = \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right)$.

In this take $f(n) = \wedge(n)$ and $g(n) = -\mu(n)\log n$.

Then we get $\wedge(n) = \sum_{d|n} \mu(d)\log d \Leftrightarrow -\mu(n)\log n = \sum_{d|n} \mu(d)\wedge\left(\frac{n}{d}\right)$ .... (iv)

From (iii), we have $\wedge(n) = \sum_{d|n} \mu(d)\log d$

$\Rightarrow -\mu(n)\log n = \sum_{d|n} \mu(d)\wedge\left(\frac{n}{d}\right)$ (by (iv))

Taking sum $\le x$ on both sides, we get $-\sum_{n\le x} \mu(n)\log n = \sum_{n\le x} \sum_{d|n} \mu(d)\Lambda\left(\frac{n}{d}\right)$

$\Rightarrow -H(x) = -\sum_{n\le x} \mu(n)\log n$ [By definition 8.1.3 of H(x)]

$= \sum_{n\le x} \sum_{d|n} \mu(d)\wedge\left(\frac{n}{d}\right) = \sum_{n\le x} (\mu * \wedge)$.

$= \sum_{n\le x} \mu(n)\psi\left(\frac{x}{n}\right)$ (verify ! SAQ 1)

Therefore $-H(x) = \sum_{n\le x} \mu(n)\psi\left(\frac{x}{n}\right)$.

Put $y = \left[\frac{x}{A}\right]$ where A is taken as in (i)

$\Rightarrow -H(x) = \sum_{n\le y} \mu(n)\psi\left(\frac{x}{n}\right) + \sum_{y<n\le x} \mu(n)\psi\left(\frac{x}{n}\right)$ .... (v)

Part-(ii): Consider $\sum_{n\le y} \mu(n)\psi\left(\frac{x}{n}\right) = \sum_{n\le y} \mu(n)\left(\frac{x}{n} + \psi\left(\frac{x}{n}\right) - \frac{x}{n}\right)$

$= x\sum_{n\le y} \frac{\mu(n)}{n} + \sum_{n\le y} \mu(n)\left(\psi\left(\frac{x}{n}\right) - \frac{x}{n}\right)$

$\Rightarrow \left|\sum_{n\le y} \mu(n)\psi\left(\frac{x}{n}\right)\right| \le x\left|\sum_{n\le y} \frac{\mu(n)}{n}\right| + \left|\sum_{n\le y} \psi\left(\frac{x}{n}\right) - \frac{x}{n}\right|$

$< x \cdot 1 + \sum_{n \le y} \left(\frac{x}{n}\right)\frac{\varepsilon}{2}$ [since, (i) Theorem 5.2.3 is $\left|\sum \frac{\mu(n)}{n}\right| \le 1$

(ii) Form (i) we get $\left|\psi\left(\frac{x}{n}\right) - \frac{x}{n}\right| \le \left(\frac{x}{n}\right)\frac{\varepsilon}{2}$]

$< x + \frac{\varepsilon}{2}\sum_{n \le y}\left(\frac{x}{n}\right) = x + \frac{\varepsilon x}{2}\sum_{n \le y}\frac{1}{n}$

$= x + \frac{\varepsilon}{2} \cdot x(\log y + c + O(y))$

[Since by Theorem 3.5.1 we know that $\sum_{n \le x}\frac{1}{n} = \log x + c + O(x)$]

$= x + \frac{\varepsilon x}{2}(\log y + O(1))$ (since y is constant, $O(y) = O(1)$)

$= x + \frac{\varepsilon x}{2}(\log y + 1) = x + \frac{\varepsilon x}{2}\log y + \frac{\varepsilon x}{2}$

Therefore $\sum_{n \le y}\mu(n)\psi\left(\frac{x}{n}\right) \le x + \frac{\varepsilon x}{2}\log y + \frac{\varepsilon x}{2}$ .... (vi)

Consider the second part of R.H.S of (v).

That is, $\sum_{y < n \le x}\mu(n)\psi\left(\frac{x}{n}\right) = \sum_{\frac{x}{n} < n \le x}\mu(n)\psi\left(\frac{x}{n}\right)$

$< \sum_{\frac{x}{n} < n \le x}\mu(n)\psi(A)$ (verify! SAQ 2)

$= \psi(A)\sum_{\frac{x}{n} < n \le x}\mu(n)$

$\le \psi(A).x$ .... (vii)

[since by definition of $\mu(n)$, $\mu(n) = 1$ or 0. Therefore $\sum_{n < x}\mu(x) \le x$]

Part-(iii): From (v), (vi), (vii) we get that

$-H(x) \le \left(x + \frac{\varepsilon x}{2}\log y + \frac{\varepsilon x}{2}\right) + (\psi(A).x)$

Dividing by x log x and taking modulus, we get

$$\left|\frac{H(x)}{x\log x}\right| \le \left|\frac{x\left(1 + \frac{\varepsilon}{2}\log y + \frac{\varepsilon}{2} + \psi(A)\right)}{x\log x}\right| = \frac{1}{\log x}\left(1 + \frac{\varepsilon}{2} + \frac{\varepsilon}{2}\log y + \psi(A)\right)$$

Consider $\log y = \log\left(\frac{x}{A}\right) \leq \log\left(\frac{x}{A}\right) = \log x - \log a$

$$\Rightarrow \frac{\log y}{\log x} = \frac{\log x - \log A}{\log x} = 1 - \frac{\log A}{\log x}$$

$$\Rightarrow \lim_{x\to\infty} \frac{\log y}{\log x} = 1 - \lim_{x\to\infty} \frac{\log A}{\log x} = 1 - 0 = 1.$$

$$\text{So, } \lim_{x\to\infty} \left|\frac{H(x)}{x\log x}\right| \leq \lim_{x\to\infty} \frac{\left(1+\frac{\varepsilon}{2}+\psi(A)\right)}{\log x} + \frac{\varepsilon}{2}.\frac{\log y}{\log x} = 0 + \frac{\varepsilon}{2}.1 = \frac{\varepsilon}{2}.$$

This is true for any $\varepsilon > 0$.

$$\text{Hence } \lim_{x\to\infty} \left|\frac{H(x)}{x\log x}\right| = 0 \Rightarrow \lim_{x\to\infty} \frac{H(x)}{x\log x} = 0.$$

Now by Theorem 8.1.4 (ii), $\lim_{x\to\infty} \frac{M(x)}{x} = 0.$

Self Assessment Question 1: *Verify* $\sum_{n\leq x}(\mu * \wedge) = \sum_{n\leq x}\mu(n)\psi\left(\frac{x}{n}\right)$

Self Assessment Question 2: *Verify* $\psi\left(\frac{x}{n}\right) \leq \psi(A)$, *where* $y < n \leq x$

8.1.6 Definition: (i) $f(x) = o(g(x))$ as $x \to \infty$ (read: f(x) is little oh of g(x)) means that $\lim_{x\to\infty} \frac{f(x)}{g(x)} = 0.$

(ii) An equation $f(x) = h(x) + o(g(x))$ as $x \to \infty$ means that $f(x) - h(x) = o(g(x))$ as $x \to \infty$

8.1.7 Note: (i) Consider the asymptotic relation $f(x) \sim g(x)$ as $x \to \infty$

$$\Rightarrow \lim_{x\to\infty} \frac{f(x)}{g(x)} = 1 = \lim_{x\to\infty} \frac{g(x)}{g(x)}$$

$$\Leftrightarrow \lim_{x\to\infty} \frac{f(x)}{g(x)} - \lim_{x\to\infty} \frac{g(x)}{g(x)} = 1 - 1 = 0$$

$$\Leftrightarrow \lim_{x\to\infty} \frac{f(x)-g(x)}{g(x)} = 0 \Leftrightarrow f(x) - g(x) = o(g(x)) \Leftrightarrow f(x) = g(x) + o(g(x)).$$

Therefore $f(x) \sim g(x)$ as $x \to \infty$ is equivalent to $f(x) = g(x) + o(g(x))$.

(ii) By Definition 8.1.6, we have the following:

Prime Number Theorem $\Rightarrow \lim_{x\to\infty} \frac{M(x)}{x} = 0 \Rightarrow M(x) = o(x)$

(iii) By Theorem 6.3.2 (c), we have

Prime Number Theorem $\Rightarrow \lim_{x\to\infty} \frac{\psi(x)}{x} = 1$

$$\Rightarrow \lim_{x\to\infty} \frac{\psi(x)}{x} - 1 = 0 \Rightarrow \lim_{x\to\infty} \frac{\psi(x)}{x} - \lim_{x\to\infty} \frac{x}{x} = 0$$

$$\Rightarrow \lim_{x\to\infty} \frac{\psi(x)-x}{x} = 0 \Rightarrow \psi(x) - x = o(x)$$

$$\Rightarrow \psi(x) = x + o(x).$$

Self Assessment Question 3: *Show that* $f(x) = o(1) \Rightarrow f(x) = o(x)$ *as* $x \to \infty$.

8.1.8 Note: The relation $M(x) = o(x)$ as $x \to \infty$ implies that $\psi(x) \sim x$ as $x \to \infty$.

8.1.9 Theorem: If $\frac{M(x)}{x} \to 0$ as $x \to \infty$ then the prime number theorem is true (In other words, $M(x) = o(x) \Rightarrow \psi(x) = x + o(x)$).

Proof: Suppose $M(x) = o(x) \Rightarrow \lim_{x\to\infty} \frac{M(x)}{x} = 0.$

By Theorem 8.1.4, we have that $\psi(x) \sim x$ as $x \to \infty \Rightarrow \lim_{x\to\infty} \frac{\psi(x)}{x} = 1.$

Now by Theorem 6.3.2, we have that $\lim_{x\to\infty} \frac{\pi(x)\log x}{x} = 1.$

Thus the prime number theorem is true.

8.1.10 Theorem: If $A(x) = \sum_{n\le x} \frac{\mu(n)}{n}$, then the relation $A(x) = o(1)$ as $x \to \infty$ implies that the prime number theorem.

[In other words, the prime number theorem is a consequence of the statement that the series $\sum_{n=1}^{\infty} \frac{\mu(n)}{n}$ converges and has sum 0].

8.1.11 Note: The converse of this Theorem 8.1.10 is also true. But this is out of the scope of this book.

8.2 BRIEF SKETCH OF AN ELEMENTARY PROOF OF THE PRIME NUMBER THEOREM

This section gives a very brief sketch of an elementary proof of the prime number theorem.

Using Selberg's asymptotic formula: $\psi(x) \log x + \sum_{n\le x} \Lambda(n)\psi\left(\frac{x}{n}\right) = 2x \log x + O(x).$

(given in Section 8.3), we discuss the proof of prime number theorem.

First, Selberg's formula, will be brought in a convenient form, which involves the function $\sigma(x) = e^{-x}\psi(e^x) - 1$.

Selberg's formula implies an integral inequality of the form

$$|\sigma(x)|x^2 \le 2\cdot\int_0^x\int_0^y|\sigma(u)|\,du\,dy + O(x)\ldots\ldots\ldots\ldots(i).$$

and the prime number theorem is equivalent to showing that $\sigma(x) \to 0$ as $x \to \infty$

Therefore, if we take $C = \limsup_{x\to\infty}|\sigma(x)|$, the prime number theorem is equivalent to showing that $C = 0$.

In a contrary way, assume that $C > 0$.

From the definition of C, we have $|\sigma(x)| \le C + g(x)$..................(ii)

where $g(x) \to 0$ as $x \to \infty$.

If $C > 0$ then this inequality, together with (i), gives another inequality of the same type, $|\sigma(x)| \le C^1 + h(x)$..................................(iii)

where $0 < C^1 < C$ and $h(x) \to 0$ as $x \to \infty$.

The deduction of (iii) from (i) and (ii) is so lengthy part of the proof.

Letting $x \to \infty$ in (iii) we find that $C \le C^1$, a contradiction which completes the proof.

8.3 SELBERG'S ASYMPTOTIC FORMULA

8.3.1 Theorem: Let F be a real or complex valued function defined on $(0,)$ and let $G(x) = \log x \sum_{n\le x} F\left(\frac{x}{n}\right)$. Then $F(x)\log x + \sum_{n\le x} F\left(\frac{x}{n}\right)\Lambda(n) = \sum_{d\le x}\mu(d)G\left(\frac{x}{d}\right)$.

Proof: Consider $F(x)\log x = \sum_{n\le x}\left[\frac{1}{n}\right]F\left[\frac{x}{n}\right]\log\left(\frac{x}{n}\right)$.[since $\left[\frac{1}{n}\right] = 0$ if $n > 1$]

$$= \sum_{n\le x}F\left(\frac{x}{n}\right)\log\left(\frac{x}{n}\right)\left(\sum_{d|n}\mu(d)\right)$$

[By Theorem 1.5.7, we know that $\left[\frac{1}{n}\right] = \sum_{d|n}\mu(d)$]

$$= \sum_{n\le x}\sum_{d|n}\log\left(\frac{x}{n}\right)\mu(d)F\left(\frac{x}{n}\right)\ldots\ldots\ldots\ldots(i)$$

By Theorem 2.2.3, we know that $\log n = \sum_{d|n}\Lambda(d)$ ....(ii)

By Mobius inversion formula (Theorem 2.1.11), we have

$$f(n) = \sum_{d|n}g(d) \Leftrightarrow g(n) = \sum_{d|n}f(d)\mu\left(\tfrac{n}{d}\right) = \sum_{d|n}\mu(d)f\left(\tfrac{n}{d}\right)$$

Taking $f(n) = \log n$ and $g(d) = \Lambda(d)$ in the Mobius inversion formula, we get

$$\log n = \sum_{d|n}\Lambda(d) \Leftrightarrow \Lambda(n) = \sum_{d|n}\mu(d)\log\left(\tfrac{n}{d}\right)\ldots\ldots\ldots\ldots(iii)$$

From (ii) and (iii) we get that $\wedge(n) = \sum_{d|n} \mu(d)\log\left(\frac{n}{d}\right)$ .... (iv)

By multiplying with $F\left(\frac{x}{n}\right)$ on both sides, we get

$$F\left(\tfrac{x}{n}\right)\wedge(n) = \sum_{d|n} \mu(d)\log\left(\tfrac{n}{d}\right) F\left(\tfrac{x}{n}\right)$$

$$\Rightarrow \sum_{n\le x} F\left(\tfrac{x}{n}\right)\wedge(n) = \sum_{n\le x}\sum_{d|n} \mu(d)\log\left(\tfrac{n}{d}\right) F\left(\tfrac{x}{n}\right) \quad \text{.................................. (v)}$$

By adding (i) and (v) we get

$$F(x)\log x + \sum_{n\le x} F\left(\tfrac{x}{n}\right)\wedge(n) = \sum_{n\le x}\sum_{d|n} \mu(d)\log\left(\tfrac{x}{n}\right) F\left(\tfrac{x}{n}\right) + \sum_{n\le x}\sum_{d|n} \mu(d) F\left(\tfrac{x}{n}\right)\log\left(\tfrac{n}{d}\right)$$

$$= \sum_{n\le x}\sum_{d|n} \mu(d) F\left(\tfrac{x}{n}\right)\left(\log\left(\tfrac{x}{n}\right) + \log\left(\tfrac{n}{d}\right)\right)$$

$$= \sum_{n\le x}\sum_{d|n} \mu(d) F\left(\tfrac{x}{n}\right)\log\left(\tfrac{x}{d}\right) \qquad \left[\text{since } \log\left(\tfrac{x}{n}\right) + \log\left(\tfrac{n}{d}\right) = \log\left(\tfrac{x}{d}\right)\right]$$

$$= \sum_{d\delta\le x}\sum_{\delta\le \frac{x}{d}} F\left(\tfrac{x}{d\delta}\right)\mu(d)\log\left(\tfrac{x}{d}\right)$$

$$= \sum_{d\delta\le x} \mu(d)\log\left(\tfrac{x}{d}\right)\sum_{\delta\le \frac{x}{d}} F\left(\tfrac{x}{d\delta}\right)$$

$$= \sum_{d\delta\le x} \mu(d)\left(\log\left(\tfrac{x}{d}\right)\sum_{\delta\le \frac{x}{d}} F\frac{\left(\left(\frac{x}{d}\right)\right)}{\delta}\right)$$

$$= \sum_{d\delta\le x} \mu(d)\, G\left(\tfrac{x}{d}\right) \quad \text{(G is given in hypothesis)}$$

$$= \sum_{d\le x} \mu(d)\, G\left(\tfrac{x}{d}\right).$$

This completes the proof.

8.3.2 Theorem: (***selberg's asymptotic formula***): For $x > 0$ we have $\psi(x)\log x + \sum_{n\le x} \wedge(n)\,\psi\left(\frac{x}{n}\right) = 2x\log x + O(x)$.

Proof: **Part-(i)**: Write $F_1(x) = \psi(x)$ and $G_1(x) = \log x \sum_{n\le x} F_1\left(\frac{x}{n}\right)$.

Then $G_1(x) = \log x \sum_{n\le x} F_1\left(\frac{x}{n}\right)$

$= \log x \sum_{n\le x} \psi\left(\frac{x}{n}\right)$ (since $F_1 = \psi$)

$= \log x\,(x \log x - x + O(\log x))$ [by 7.3.3, $\sum_{n\le x}\psi(n) = x\log x - x + O(\log(x))$.]

$\Rightarrow G_1(x) = x \log^2 x - x\log x + O(\log^2 x)$ .... (i)

Write $F_2(x) = x - C - 1$ where C is Euler's constant and $G_2(x) = \log x \sum_{n\le x} F_2\left(\frac{x}{n}\right)$.

Then $G_2(x) = \log x \sum_{n\le x} F_2\left(\frac{x}{n}\right)$

$= \log x \sum_{n\le x}\left(\frac{x}{n} - C - 1\right)$

$= (\log x)\left(x\sum_{n\le x}\frac{1}{n} - C\sum_{n\le x}1 - \sum_{n\le x}1\right)$

$= \log x\,(x(\log x + C + O(\frac{1}{x})) - C[x] - [x])$

[by Theorem 3.5.1, $\sum_{n\le x}\frac{1}{n} = \log x + C + O(\frac{1}{x})$]

$= \log x\,(x\log x + Cx + O(1) - C(x + O(1)) - x - O(1))$ [since $[x] = x + O(1)$]

$= \log x\,(x\log x - C.O(1) - x)$

$= x\log^2 x - O(\log x) - x\log x$.[since $C\cdot O(1) = O(1)$ & $(\log x)\,O(1) = O(\log x)$]

Therefore $G_2(x) = x\log^2 x + O(\log x) - x\log x$ .... (ii)

Part-(ii): By Theorem 8.3.1, we have

$F(x)\log x + \sum_{n\le x} F\left(\frac{x}{n}\right)\wedge(n) = \sum_{n\le x}\mu(d)G\left(\frac{x}{d}\right)$ .... (iii)

Taking $F_1(x)$, $G_1(x)$ in place of $F(x)$ and $G(x)$ in (iii) we get

$F_1(x)\log x + \sum_{n\le x} F_1\left(\frac{x}{n}\right)\wedge(n) = \sum_{n\le x}\mu(d)G_1\left(\frac{x}{n}\right) = \sum_{n\le x}\mu(n)G_1\left(\frac{x}{n}\right)$ .... (iv)

Taking $F_2(x)$, $G_2(x)$ in place of $F(x)$, and $G(x)$ in (iii) we get

$F_2(x)\log x + \sum_{n\le x} F_2\left(\frac{x}{n}\right)\wedge(n) = \sum_{n\le x}\mu(d)G_2\left(\frac{x}{n}\right)$ .... (v)

Subtracting (v) from (iv) we have

$(F_1(x) - F_2(x))\log x + \sum_{n\le x}\left(F_1\left(\frac{x}{n}\right) - F_2\left(\frac{x}{n}\right)\right)\wedge(n) = \sum_{n\le x}\mu(d)\left(G_1\left(\frac{x}{n}\right) - G_2\left(\frac{x}{n}\right)\right)$ ....(*)

Now, $F_1(x) - F_2(x) = \psi(x) - (x - C - 1) = \psi(x) - x + C + 1$

$F_1\left(\frac{x}{n}\right) - F_2\left(\frac{x}{n}\right) = \psi\left(\frac{x}{n}\right) - \frac{x}{n} + C + 1$

$G_1(x) - G_2(x) = (x\log^2 x - x\log x + O(\log^2 x)) - (x\log^2 x + O(\log x) - x\log x)$

$= O(\log^2 x) - O(\log x)$

$G_1\left(\frac{x}{n}\right) - G_2\left(\frac{x}{n}\right) = O\left(\log^2\frac{x}{n}\right) - O\left(\log\frac{x}{n}\right)$

$= O\left(\log^2\left(\frac{x}{n}\right)\right)$

[Reason: $O(y) + O(y^2) = O(y^2)$ $\lim_{x\to\infty}\frac{y}{y^2} = 0 \Rightarrow y = O(y^2)$]

By substituting these in (*), we get

$$(\psi(x) - x + C + 1) \log x + \sum_{n \le x} \wedge(n)\left(\psi\left(\tfrac{x}{n}\right) - \tfrac{x}{n} + C + 1\right) = \sum_{n \le x} \mu(n)\left(O\left(\log^2\left(\tfrac{x}{n}\right)\right)\right)$$

So, $(\psi(x)\log x - x \log x + O(1)\log(x)) + \sum_{n \le x} \wedge(n)\psi\left(\tfrac{x}{n}\right) - x \sum_{n \le x} \frac{\wedge(n)}{n} + \sum_{n \le x} \wedge(n)(C+1)$

$$= \sum_{n \le x} \mu(n) o\left(\sqrt{\tfrac{x}{n}}\right). \quad \left[\text{Since } O\left(\log^2\left(\tfrac{x}{n}\right)\right) = O\left(\sqrt{\frac{x}{n}}\right) \text{ (Verify! SAQ 4) }\right]$$

[In the next step we use (i). Theorem 7.3.1, $\sum_{n \le x} \frac{\wedge(n)}{n} = \log x + O(1)$

(ii). We know $O(1) \log x = O(\log x)$

(iii). $\sum_{n \le x} \Lambda(n)(C+1) = (C + 1) \sum_{n \le x} \Lambda(n) = (C + 1)\, \psi(x)$ (by definition of $\psi(x)$)]

So, $\psi(x)\log x - x \log x + O(\log x) + \sum_{n \le x} \wedge(n)\psi\left(\tfrac{x}{n}\right) - x(x \log x + O(1)) + (C + 1)\psi(x)$

$$= \sum_{n \le x} \mu(n) O\left(\sqrt{\tfrac{x}{n}}\right)$$

$$= \sqrt{x} \sum_{n \le x} \mu(n)\left(O\left(\tfrac{1}{\sqrt{n}}\right)\right) = \sqrt{x} \cdot O\left(\sum_{n \le x} \frac{\mu(n)}{\sqrt{n}}\right)$$

[In the next step we use

(i) Theorem 6.3.2 : Prime number theorem $\Rightarrow \lim_{x \to \infty} \frac{\psi(x)}{x} = 1 \Rightarrow \psi(x) = O(x)$

$$\Rightarrow (c + 1)\psi(x) = (c + 1)O(x) = O(x)$$

(ii) By definition $\mu(n) = 0$ or $\pm 1 \Rightarrow \mu(n) \le 1$ for all n

$$\Rightarrow \frac{\mu(n)}{\sqrt{n}} \le \frac{1}{\sqrt{n}} \Rightarrow \sum_{n \le x} \frac{\mu(n)}{\sqrt{n}} \le \sum_{n \le x} \frac{1}{\sqrt{n}} \Rightarrow O\left(\sum_{n \le x} \frac{\mu(n)}{\sqrt{n}}\right) = O\left(\sum_{n \le x} \frac{1}{\sqrt{n}}\right)$$]

So, $\psi(x) \log x + \sum_{n \le x} \wedge(n)\psi\left(\tfrac{x}{n}\right) - 2x \log x - O(x) + O(\log x) + O(x)$

$$= \sqrt{x} \sum_{n \le x} \mu(n) O\left(\tfrac{1}{\sqrt{n}}\right) = \sqrt{x} \cdot O\left(\sum_{n \le x} \frac{1}{\sqrt{n}}\right)$$

[Take $s = \frac{1}{2}$ in Theorem 3.5.3 : $\sum_{n \le x} \frac{1}{n^s} = \frac{x^{1-s}}{1-s} + \zeta(s) + O\left(\frac{1}{x^s}\right)$.

Then we get $\sum_{n\le x}\frac{1}{\sqrt{n}} = \frac{\sqrt{x}}{\left(1-\frac{1}{2}\right)} + \zeta\left(\frac{1}{2}\right) + O\frac{1}{\sqrt{x}} \quad = 2\sqrt{x} + \zeta\left(\frac{1}{2}\right) + O\left(\frac{1}{\sqrt{x}}\right)$

$$= 2\sqrt{x} + O(1) + O\left(\frac{1}{\sqrt{x}}\right)$$

Now $\sqrt{x}\cdot O\left(\sum_{n\le x}\frac{1}{\sqrt{n}}\right) = \sqrt{x}\cdot O\left(2\sqrt{x} + O(1) + O\left(\frac{1}{\sqrt{x}}\right)\right)$

$$= O(2x + O(1)\sqrt{x} + O(1))$$
$$= O(2x + O(x) + O(1)) = O(x) + O(1) = O(x) \;]$$

So, $\psi(x)\log x + \sum_{n\le x}\Lambda(n)\psi\left(\frac{x}{n}\right)$

$= 2x\log x + O(x) - O(\log x) - O(x) + O(x)$

$= 2x\log x + O(x) + O(x) + O(x)$

$$[\; \lim_{x\to\infty}\frac{\log x}{x} = 0 \Rightarrow \log x = O(x) \Rightarrow O(\log x) = O(O(x)) = O(x)]$$

$= 2x\log x + O(x)$

Therefore $\psi(x)\log x + \sum_{n\le x}\Lambda(n)\psi\left(\frac{x}{n}\right) = 2x\log x + O(x).$

This completes the proof.

Self Assessment Question 4: *Verify* $O\left(\log^2\left(\frac{x}{n}\right)\right) = O\left(\sqrt{\frac{x}{n}}\right)$.

8.4 SUMMARY

In this lesson, we defined partial sum representations of the Mobius function, related results, properties were discussed. We also obtained the Selberg's asymptotic formula and its consequences. We also provided the sketch of an elementary proof of Prime Number Theorem using Selberg's asymptotic formula.

8.5 TECHNICAL TERMS

Merten's Conjecture: $|M(x)| < \sqrt{x}$, if $x > 1$.

Selberg's asymptotic formula: For $x > 0$ we have $\psi(x)\log x + \sum_{n\le x}\Lambda(n)\psi\left(\frac{x}{n}\right) = 2x\log x + O(x).$

8.6 ANSWERS TO SELF ASSESSMENT QUESTIONS

1: Consider Theorem 5.1.1

This states that if $h = f*g$, $F(x) = \sum_{n\le x} f(n)$, $G(x) = \sum_{n\le x} g(n)$, then

$\sum_{n\le x} h(n) = \sum_{n\le x} f(n)G(\frac{x}{n})$. In this, take $f = \mu$ and $g = \Lambda$, then $h = \mu * \Lambda$.

Consider $G(\frac{x}{n}) = \sum_{d\le \frac{x}{n}} g(d) = \sum_{d\le \frac{x}{n}} \wedge(d) = \psi(\frac{x}{n})$ (by point 6.1.2)

So $\sum_{n\le x}(\mu * \wedge)(n) = \sum_{n\le x} h(n) = \sum_{n\le x} f(n)G(\frac{x}{n}) = \sum_{n\le x}\mu(n)G(\frac{x}{n}) = \sum_{n\le x}\mu(n)\psi(\frac{x}{n})$.

2: Consider $y < n \le x$

$$\Rightarrow n \ge y+1 \Rightarrow \frac{1}{n} \le \frac{1}{y+1} \Rightarrow \frac{x}{n} \le \frac{x}{y+1} \Rightarrow \frac{x}{n} \le \frac{x}{y+1} \le \frac{x}{y}$$

$$\Rightarrow \frac{x}{n} \le \frac{x}{y+1} < A \Rightarrow \frac{x}{n} < A \Rightarrow \psi\left(\frac{x}{n}\right) \le \psi(A).$$

3: Suppose $f(x) = o(1)$

$$\Rightarrow \lim_{x\to\infty}\frac{f(x)}{1} = 0 \Rightarrow \lim_{x\to\infty} f(x) = 0$$

$$\Rightarrow \lim_{x\to\infty} f(x) \lim_{x\to\infty}\frac{1}{x} = 0.0 = 0$$

$$\Rightarrow \lim_{x\to\infty}\frac{f(x)}{x} = 0 \Rightarrow f(x) = o(x)$$

4:Consider $\lim_{x\to\infty}\frac{\log^2(\frac{x}{n})}{\sqrt{\frac{x}{n}}} = \lim_{y\to\infty}\frac{2\log(y)^2}{y}$ (where $y = \sqrt{\frac{x}{n}}$)

$$= \lim_{y\to\infty} 4\frac{\log y}{y} = 4\lim_{y\to\infty}\frac{\log y}{y} = 4.0 = 0.$$

Therefore $O(\log^2(\frac{x}{n})) = O\left(\sqrt{\frac{x}{n}}\right)$

8.7 MODEL QUESTIONS

1. Prove that $\lim_{x\to\infty}\left(\frac{M(x)}{x}-\frac{H(x)}{x\log x}\right)=0$.

2. State and prove Selberg's Asymptotic formula.

3. Assuming the prime number theorem, prove that $\lim_{x\to\infty}\frac{M(x)}{x}=0$.

8.8 REFERENCE BOOKS

1. Chandrasekharan, K. "Introduction to Analytic Number Theory", Springer Verlag .
2. Hardy, G.H. & Wright, E.M. "Introduction to the Theory of Numbers", Fourth Edition, Oxford Publications,
3. Levegue W.J. (1986) "Topics in Number Theory (2 volumes), Addition - Wesley Publ. Co.
4. Rademacher (1964) "Lectures on Elementary Number Theory", New York, Blaisdell Publ. Co.
5. Tom M. Apostol "Introduction to Analytic Number Theory", Springer International Student Edition, Narosa Publishing House, 1995.
6. Uspensky, J.V., and Heaslett, M.A. (1939) "Elementary Number Theory", New York, Mc. Graw - Hill Book. Co.
7. Vinogrador, "Elements of Number Theory", Dover Publications

Name of the Author of this Lesson: Dr. Kuncham Syam Prasad

LESSON – 9

PRELIMINARIES IN GRAPH THEORY

Objectives

After reading this lesson, the reader should able to:

- appreciate the relevance of Graph Theory in real life situation
- understand different fundamental definitions
- observe the difference between different concepts defined through the examples presente
- understand some techniques used in proving simple theorems

Structure

9.0 INTRODUCTION

Graph theory was born in 1736 with Euler's paper in which he solved the Kongsberg Bridges problem. No development made during the next 100 years. In 1847, G.R. Kirchhoff (1824 - 87) developed the theory of trees to applications in electrical networks. After 10 years, A.Cayley discovered trees while he was trying to enumerate the isomers of ($C_n H_{2n+2}$).

Mobius (1790 - 1868) solved the four color problem. D. Morgan discussed about it. Later, Cayley gave a lecture on this topic in 1879. Hamilton (1805 - 1865) invented a puzzle in 1920's. D. Konig worked for the development of graph theory.

The last three decades have witnessed more interest in Graph Theory, particularly among applied mathematicians and engineers. Graph Theory has a surprising number of applications in many developing areas. The Graph Theory is also intimately related to many branches of mathematics including Group Theory, Matrix Theory, Automata and Combinatorics. One of the features of Graph Theory is that it depends very little on the other branches of mathematics. Graph Theory serves as a mathematical model for any system involving a binary relation. One of the attractive features of Graph Theory is its inherent pictorial character. The development of high-speed computers is also one of the reasons for the recent growth of interest in Graph Theory.

9.1 DEFINITIONS

9.1.1 Definition: A **linear graph** (or simply a **graph**). $G = (V, E)$ consists of a nonempty set of objects, $V = \{v_1, v_2, \ldots\}$ called **vertices** and another set, $E = \{e_1, e_2, \ldots\}$ of elements called **edges** such that each edge 'e_k' is identified with an unordered pair $\{v_i, v_j\}$ of vertices. The vertices v_i, v_j associated with edge e_k are called the **end vertices** of e_k.

9.1.2 Note: (i) A graph is also called a **linear complex** (or) **1-complex** (or) **one-dimensional complex**. (ii) A vertex is also called as: a **node** (or) **junction** (or) **point** (or) **0-cell** (or) **0-simplex**. (iii) Edge is also called as: **branch** (or) **line** (or) **element** (or) **1-cell** (or) **arc** (or) **1-simplex**.

9.1.3 Definition: An edge associated with a vertex pair $\{v_i, v_i\}$ is called a **loop (or) selfloop.**

9.1.4 Definition: If there are more than one edge associated with a given pair of vertices, then these edges are called **parallel edges** (or) **multiple edges**.

9.1.5 Example: Consider the graph given here.

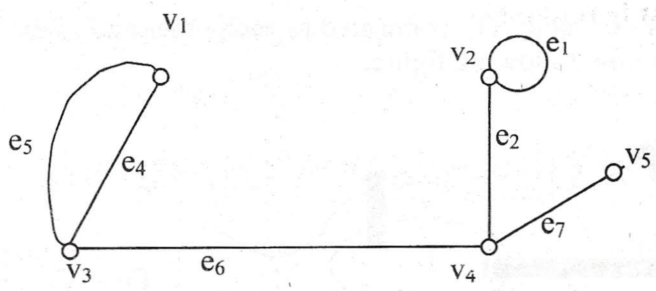


Fig-9.1.5

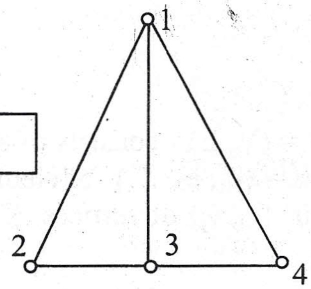
This is a graph with five vertices and six edges. Here $G = (V, E)$ where $V = \{v_1, v_2, v_3, v_4, v_5\}$ and $E = \{e_1, e_2, e_4, e_5, e_6, e_7\}$.
The identification of edges with the unordered pairs of vertices is given by
$e_1 \leftrightarrow \{v_2, v_2\}$, $e_2 \leftrightarrow \{v_2, v_4\}$, $e_4 \leftrightarrow \{v_1, v_3\}$, $e_5 \leftrightarrow \{v_1, v_3\}$, $e_6 \leftrightarrow \{v_3, v_4\}$.
Here 'e_1' is a loop and e_4, e_5 are parallel edges.

9.1.6 Definition: A graph that has neither self-loops nor parallel edges is called a **simple graph.**

9.1.7 Note: Graph containing either parallel edges or loops is also referred as **general graph**.

9.1.8 Example: It can be observed that the two graphs given in Figures 9.1.8A and B are one and the same.

Fig-9.1.8A



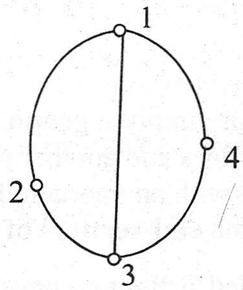


Fig-9.1.8B

9.2 APPLICATIONS OF GRAPHS

Graph theory has wide range of applications in engineering, medical, physical, social, biological sciences. A graph can be used to represent almost any physical situation involving discrete objects and a relation ship among them. In the following, we present few such examples.

9.2.1 Konigsberg Bridges Problem: This is one of the best known examples of graph theory. This problem was solved by Leonhard Euler (1707 - 1783) in 1736 by using the concepts of Graph Theory. He is the originator of graph theory.

[Problem: There were two islands 'C' and 'D' connected to each other and to the banks 'A' and 'B' with seven bridges as shown in the following figure.

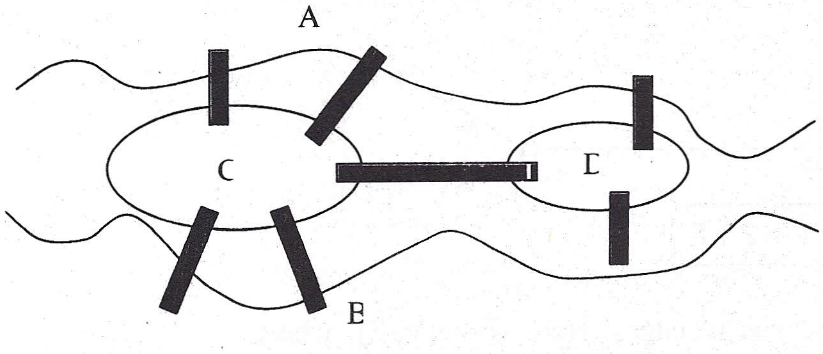
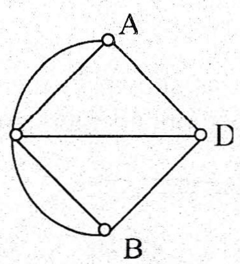


Fig-9.2.1

The problem was to start at any of the four land areas of the city A, B, C, D walk over each of the seven bridges once and only once, and returns to the starting point.]

Euler represented this situation by means of a graph as given in the following figure.



Euler proved that a solution for this problem does not exist.

9.2.2 Note: The Konigsberg Bridges Problem is same as drawing a figures without lifting the pen from the paper and without retracing a line. The same situation can be observed with the following for graphs/figures.

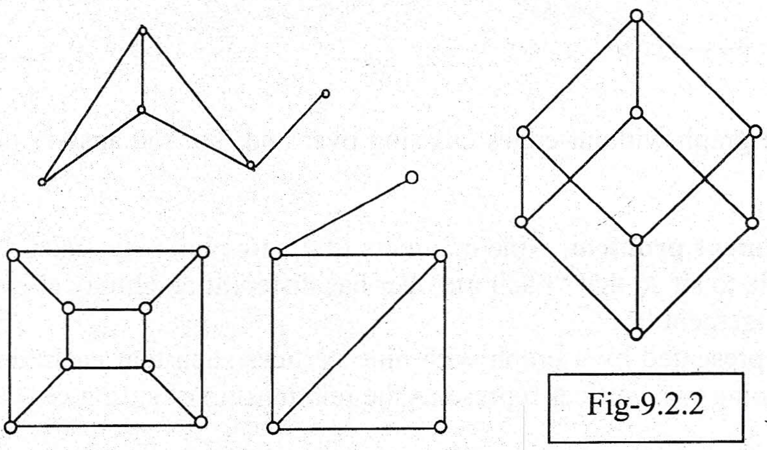


Fig-9.2.2

9.2.3 Utilities problem: There are three houses H_1, H_2, H_3 each to be connected to each of the three utilities water (w), Gas (G), Electricity (E) by means of conduits as shown in the following figure.

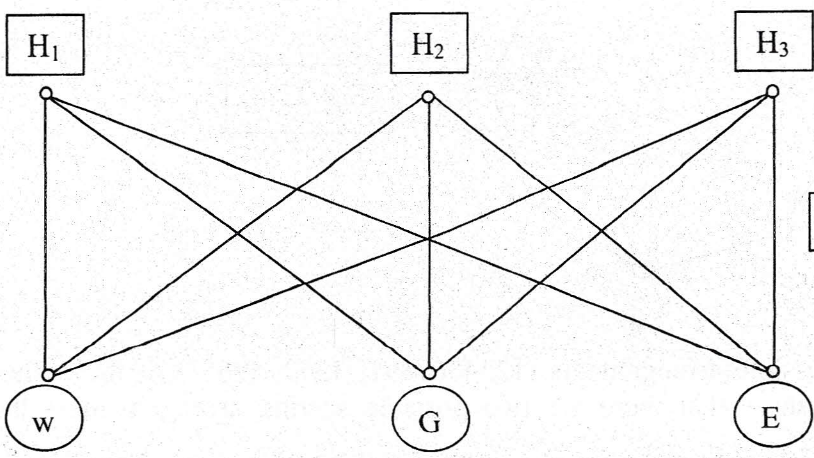
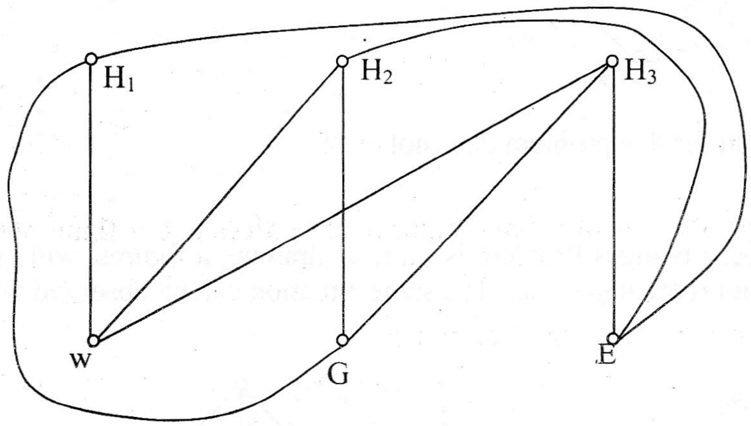


Fig - 9.2.3

The Problem is - "Is it possible to make such connections without any crossovers of the conduits" ?

This problem can be represented by the graph as shown in the following figure. Here the conducts are shown as edges, and the houses and utility supply centers are vertices.



But we cannot trace the graph without edges crossing over and so the answer to this problem is 'NO'

9.2.4 Seating Arrangement problem: Nine members of a new club meet each day for lunch at a round table. They decide to sit so that "Each member has different neighbors at each lunch". How many days can this arrangement last?
This situation can be represented by a graph with nine vertices such that each vertex represents a member and an edge joining two vertices represents the relationship of sitting next to each other.

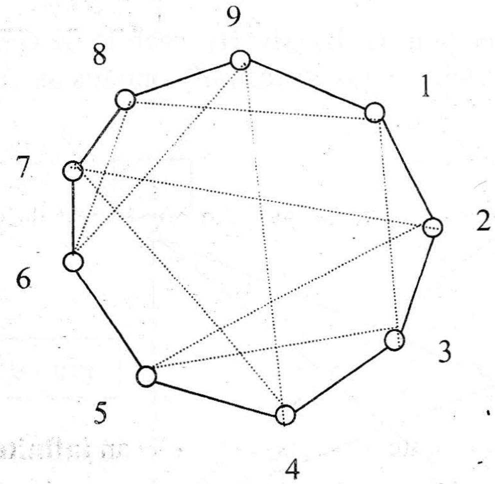


Fig-9.2.4

The above figure has two possible arrangements (1234567891, 1352749681) at the dinner table. From this figure, we can observe that there are two possible seating arrangements - those are 1234567891 and 1352749681.

It can be shown by Graph - theoretic considerations that there are only two more arrangements possible - these are 1 5 7 3 9 2 8 4 6 1 and 1 7 9 5 8 3 6 2 4 1.

In general, for 'n' people the number of such possible arrangements is

$= \dfrac{n-1}{2}$ if 'n' is odd (refer later lessons)

$= \dfrac{n-2}{2}$ if 'n' is even.

9.3 FINITE GRAPHS

9.3.1 Definition: A graph 'G' with a finite number of vertices and a finite number of edges is called a **finite graph**.

9.3.2 Example: Consider the following three graphs

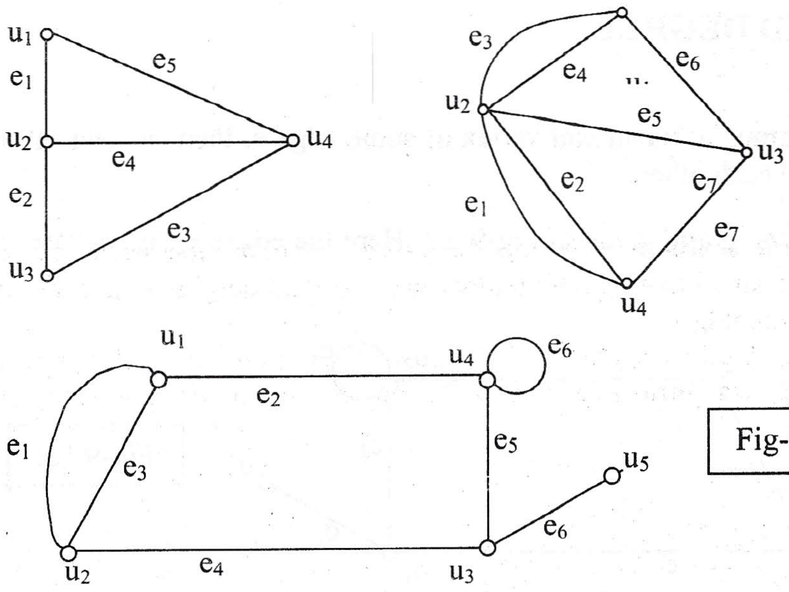


Fig-9.3.2

It can be observed that the number of vertices, and the number of edges are finite. Hence these three graphs are finite graphs.

9.4 INFINITE GRAPHS

9.4.1 Definition: A graph 'G' that is not a finite graph is said to be an **infinite graph**.

9.4.2 Examples: Consider the two graphs given here. It can be understood that the number of vertices of these two graphs is not finite. So we conclude that these two figures represent infinite graphs.

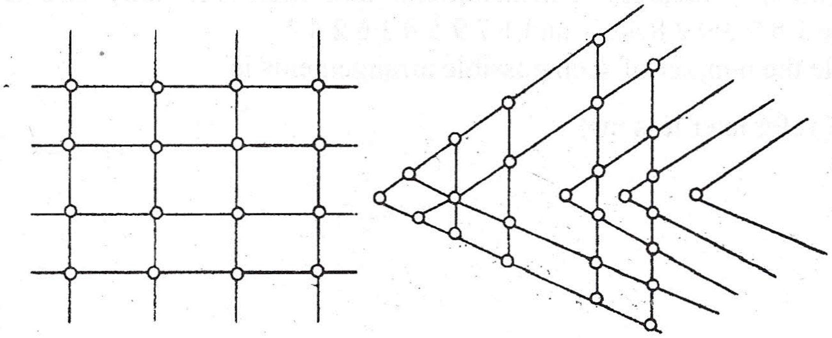


Fig-9.4.2

9.4.3 Note: Henceforth, we place our attention on the study of **finite graphs**. So we use the term 'graph' for 'finite graph'.

9.5 INCIDENCE AND DEGREE

9.5.1 Definition: If a vertex v is an end vertex of some edge e, then v and e are said to be **incident** with (or on, or to) each other.

9.5.2 Example: Consider the graph given in Fig-9.5.2. Here the edges e_2, e_6, e_7 are incident with the vertex u_4.

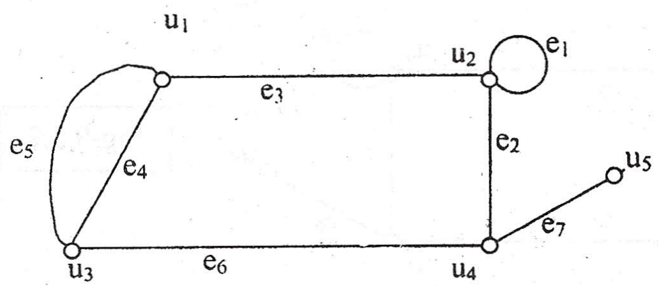


Fig-9.5.2

9.5.3 Definitions: (i) Two non-parallel edges are said to be **adjacent** if they are incident on a common vertex.

(ii) Two vertices are said to be **adjacent** if they are the end vertices of the same edge.

9.5.4 Example: Consider the graph given in Fig-9.5.2. Here the vertices u_4, u_5 are adjacent. The vertices u_1 and u_4 are not adjacent. The edges e_2 and e_3 are adjacent.

9.5.5 Definition: The number of edges incident on a vertex v is called the **degree** (or **valency**) of v. The degree of a vertex v is denoted by d(v). It is to be noted that a self-loop contributes two to the degree of the vertex.

9.5.6 Example: Consider the graph given in Fig-9.5.6. Here $d(u_1) = 2$; $d(u_2) = 1$;

$d(u_3) = 3$; $d(u_4) = 2$; $d(u_5) = 2$; $d(u_6) = 2$; $d(u_7) = 1$; $d(u_8) = 3$; $d(u_9) = 2$; $d(u_{10}) = 2$.

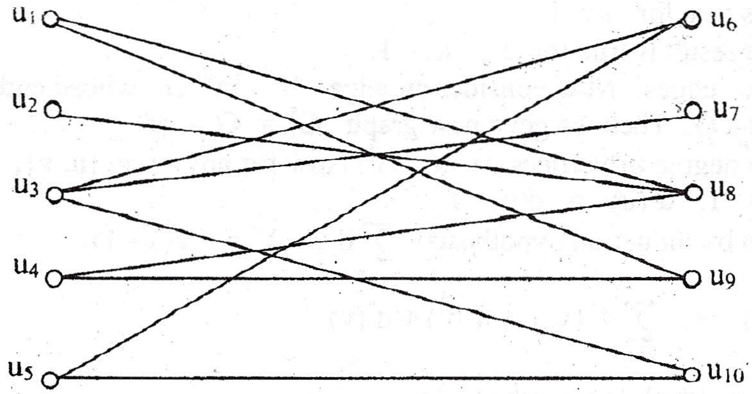


Fig-9.5.6

9.5.7 Observation: Consider the graph given in Fig-9.5.7.

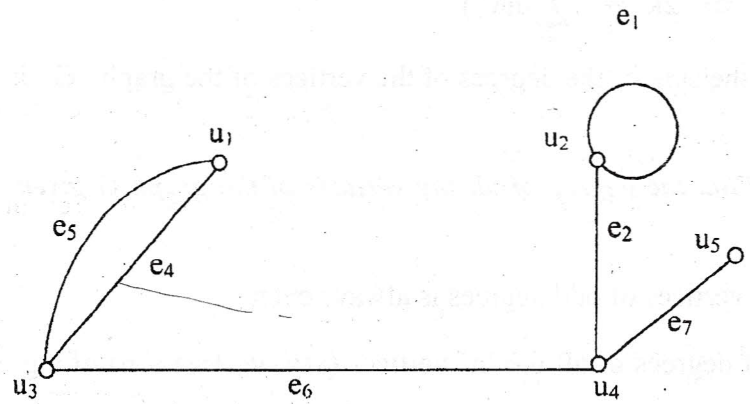


Fig-9.5.7

Here $d(u_1) = 2$, $d(u_3) = d(u_4) = 3$; $d(u_2) = 3$; $d(u_5) = 1$

So, $d(u_1) + d(u_2) + d(u_3) + d(u_4) + d(u_5) = 2 + 3 + 3 + 3 + 1 = 12 = 2(6) = 2e$, where e denotes the number of edges. Hence we can observe that

$d(u_1) + d(u_2) + d(u_3) + d(u_4) + d(u_5) = 2e$ (that is, the sum of the degrees of all vertices is equal to twice the number of edges).

9.5.8 Theorem: The sum of the degrees of the vertices of a graph G is twice the number of edges. That is, $\sum_{v_i \in V} d(v_i) = 2e$. (Here e is the number of edges).

Proof: (The proof is by induction on 'e').

Case-(i): Suppose $e = 1$. Suppose f is the edge in G with $f = uv$.

Then $d(v) = 1$, $d(u) = 1$

Therefore $\sum_{x \in V} d(x) = \sum_{x \in V \setminus \{u,v\}} d(x) + d(u) + d(v) = 0 + 1 + 1 = 2 = 2 \times 1$

= 2 × (number of edges).

Hence the given statement is true for n = 1.

Now we can assume that the result is true for e = k - 1.

Take a graph G with k edges. Now consider an edge 'f' in G whose end points are u and v. Remove f from G. Then we get a new graph $G^* = G - \{f\}$.

Suppose $d^*(v)$ denotes the degree of vertices v in G^*. Now for any $x \notin \{u, v\}$, we have $d(x) = d^*(x)$, and $d^*(v) = d(v) - 1$, $d^*(u) = d(u) - 1$.

Now G^* has k - 1 edges. So by induction hypothesis $\sum_{v_i \in V} d^*(v_i) = 2(k - 1)$.

$$\text{Now } 2(k-1) = \sum_{v_i \in V} d^*(v_i) = \sum_{v_i \notin \{u,v\}} d^*(v_i) + d^*(u) + d^*(v)$$

$$= \sum_{v_i \notin \{u,v\}} d(v_i) + (d(u) - 1) + (d(v) - 1)$$

$$= \sum_{v_i \notin \{u,v\}} d(v_i) + d(u) + d(v) - 2 = \sum_{v_i \in V} d^*(v_i) - 2$$

$$\Rightarrow 2(k-1) + 2 = \sum_{v_i \in V} d^*(v_i) \Rightarrow 2k = \sum_{v_i \in V} d(v_i)$$

Hence by induction we get that "the sum of the degrees of the vertices of the graph G is twice the numbers of edges".

Self Assessment Question 1: *Find the degree of all the vertices of the graph G given in Figure 9.3.2 (Incidence and degree)*

9.5.9 Theorem: The number of vertices of odd degrees is always even.

Proof: We know that the sum of degrees of all the 'n' vertices (say, v_i, $1 \leq i \leq n$) of a graph G is twice the number of edges (e) of G. So we have $\sum_{i=1}^{n} d(v_i) = 2e$ --------- (i)

If we consider the vertices of odd degree and even degree separately, then

$$\sum_{i=1}^{n} d(v_i) = \sum_{v_j \text{ is even}} d(v_j) + \sum_{v_k \text{ is odd}} d(v_k) \text{ -------- (ii)}$$

Since the L.H.S of (ii) is even (from (i)) and the first expression on the RHS side is even, we have that the second expression on RHS is always even.

Therefore $\sum_{v_k \text{ is odd}} d(v_k)$ is an even number --------- (iii)

In (iii), each $d(v_k)$ is odd. The number of terms in the sum must be even to make the sum an even number. Hence the number of vertices of odd degree is even.

Self Assessment Question 2: *Can a simple graph exist with 15 vertices each of degree five.*

9.5.10 Problem: Show that the number of people who dance (at a dance where the dancing is done in couples) an odd number of times is even.

Solution: Suppose the people are vertices. If two people dance together, then we can consider it as an edge. Then the number of times a person v danced is $\delta(v)$. By Theorem 9.5.9, the number of vertices of odd degree is even. Therefore the number of people who dance odd number of times is even.

9.5.11 Definition: A graph in which all vertices are of equal degree, is called a **regular graph**. (or **simply regular**)

9.5.12 Example Consider the graph G given in Fig-9.6.12. It is easy to observe that the degree of every vertex is equal to 3. Hence the graph G is a regular graph of degree 3.

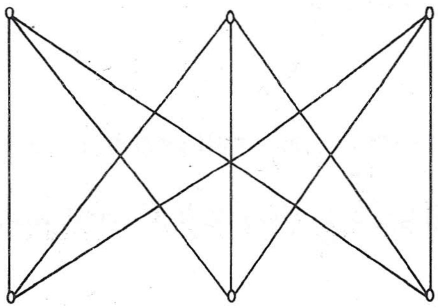


Fig-9.5.12

Self Assessment Question 3: *How many vertices does a regular graph of degree 4 with 10 edges have.*

9.6 ISOLATED VERTEX

9.6.1 Definition: A vertex having no incident edge is called an **isolated vertex**. In other words, a vertex v is said to be an isolated vertex if the degree of v is equal to zero.

9.6.2 Example: Consider the graph given in Fig-9.6.2. The vertices v_4 and v_7 are isolated vertices.

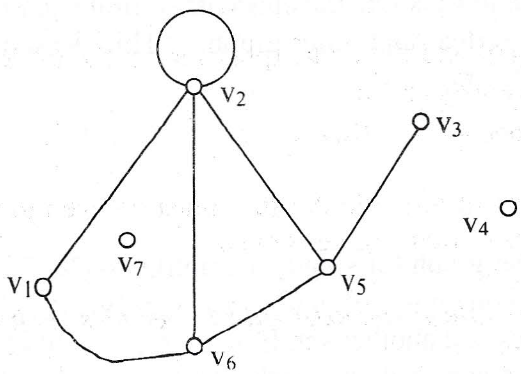


Fig-9.6.2

9.7 PENDENT VERTEX

9.7.1 Definition: A vertex of degree one is called a **pendent vertex** or an **end vertex**.

9.7.2 Example: Consider the graph given in the Example 9.6.2. Here 'v_3' is of degree 1, and so it is a pendent vertex.

9.7.3 Definition: Two adjacent edges are said to be in **series** if their common vertex is of degree two.

9.7.4 Example: In the graph given in Example 9.6.2, two edges incident on v_1 are in series.

9.8 NULL GRAPH

9.8.1 Definition: A graph $G = (V, E)$ is said to be a **null graph** if $E = \phi$.

9.8.2 Example: The graph G given in Fig-9.8.2. The graph G contains no edges and hence G is a null graph.

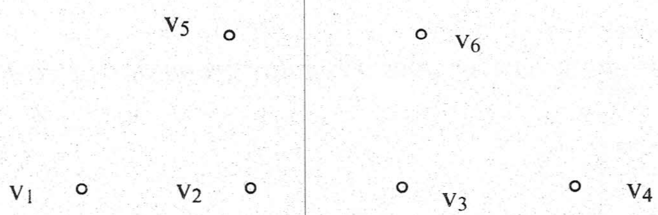


Fig-9.8.2

9.9 SUMMARY

This lesson is meant for beginning your process of learning Graph Theory. It started with the definition of Graph and Move on to illustrate the concepts of finite and infinite graph, incidence, degree, isolated vertex, pendent vertex and null graph. This lesson also initiated various fundamental notions in the Graph Theory.

9.10 TECHNICAL TERMS

Graph: A linear graph (or simply a graph) $G = (V, E)$ consists of a nonempty set of objects, $V = \{v_1, v_2, \ldots\}$ called vertices and another set, $E = \{e_1, e_2, \ldots\}$ of elements called edges such that each edge 'e_k' is identified with an unordered pair $\{v_i, v_j\}$ of vertices. The vertices v_i, v_j associated with edge e_k are called the end vertices of e_k

Finite graph: A graph consists of finite number of vertices and a finite number of edges.

infinite graph: A graph that is not finite

incidence: If a vertex v is an end vertex of some edge e, then v and e are said to be incident with (or on, or to) each other.

degree of a vertex: The number of edges incident on a vertex. The degree of a vertex v is denoted by d(v). It is to be noted that a self-loop contributes two to the degree of the vertex.

isolated vertex: A vertex having no incident edge. In other words, a vertex v is said to be an isolated vertex if the degree of v is equal to zero.

pendent vertex: A vertex of degree one.

null graph: A graph with edge set $E = \phi$.

9.11 ANSWERS TO SELF ASSESSMENT QUESTIONS

1: Here $d(u_1) = 3$; $d(u_2) = 4$; $d(u_3) = 3$; $d(u_4) = 3$; and $d(u_5) = 1$

Now $\sum_{i=1}^{5} u_i = 3 + 4 + 3 + 3 + 1 = 14$. $|E| = 7$.

So $\sum_{i=1}^{5} d(u_i) = 2\,|E|$

Therefore the sum of degrees of all the vertices of a graph G is twice the number of edges in G

2: No, since the sum of the degrees of the vertices cannot be odd.

3: Let G be a regular graph of degree 4 with 10 edges and let 'n' be the number of vertices in G. Then $\sum_{u \in V} d(u) = 2 \times 10 = 20$.

$\Rightarrow n \cdot 4 = 20. \Rightarrow n = 5.$

9.12 MODEL QUESTIONS

1. Define the terms: Graph, finite graph, infinite graph, incidence, degree, isolated vertex, pendent vertex, null graph
2. Explain the Koingsberg Bridges problem.
3. Explain the Seating Arrangement Problem.
4. Show that the sum of the degrees of the vertices of a finite graph G is twice the number of edges.
5. Show that the number of vertices of odd degree is always even.
6. Show that an infinite graph with finite number of edges must have an infinite number of isolated vertices.
7. Show that the maximum degree of any vertex in a simple graph is (n - 1).
8. Show that the maximum number of edges in a simple graph with n vertices is $\frac{n(n-1)}{2}$.

9.13 REFERENCE BOOKS

1. Bondy J.A and Murty U.S.R, "Graph Theory with applications", North Holland, New York (1976).

2. Douglas B. West "Introduction to Graph Theory", Second Edition, Prentice Hall of India, New Delhi, 2002.

3. Harary Frank. "Graph Theory", Addison - Wesley Publishing Company, Inc., Reading, Mass., 1969.

4. John Clark and Derek Allan Holton, "A first look at Graph Theory" Allied Publishers, 1995

5. Narsingh Deo "Graph theory with applications to Engineering and Computer Science", Prentice Hall of India Pvt., Ltd., New Delhi, 1993.

6. Satyanarayana Bhavanari and Syam Prasad Kuncham "Graph Theory for Beginners", Satyasri Maths Study Centre, Guntur, AP, 2003.

Name of the Author of this Lesson: Dr. Kuncham Syam Prasad

LESSON-10

SUBGRAPHS

Objectives

The objectives of this lesson are to:

- understand the concept of isomorphism between two graphs
- identify whether a given graph is a subgraph of another graph
- find out a method to solve the puzzle: Instant Insanity
- learn about walks, paths and circuits in a graph

Structure

10.0 INTRODUCTION

In this lesson, we introduce some additional concepts and terms in Graph Theory and provide a variety of examples. We study isomorphism between graphs like congruent figures. Two graphs are thought of as equivalent and called isomorphic if they have identical behavior in terms of graph theoretic properties.

Some times we need only a part of a graph to solve some problems. When some edges and vertices are removed from a graph without removing end points of remaining edges, a smaller graph is obtained and such a graph is called subgraph of the original graph. Walks, paths, circuits in graph G are its subgraphs with special properties.

A puzzle, which involves stacking four multi-colored cubes, will be solved. In this lesson we see with examples that how some general problems can be converted into problems of graph theory and solved.

10.1 ISOMORPHISM

10.1.1 Definition: Two graphs G and G^1 are said to be **isomorphic** to each other if there is a one-to-one correspondence between their vertices and a one-to-one correspondence between their edges such that the incident relationship must be preserved.
[In other words, two graphs $G = (V, E)$ & $G^1 = (V^1, E^1)$ are said to **be isomorphic** if there exist bijections $f : V \to V^1$ and $g : E \to E^1$ such that $g(v_iv_j) = f(v_i)f(v_j)$ for any edge v_iv_j in G].

10.1.2 Note: Except the labeling of their vertices and edges of the isomorphic graphs, they are same, perhaps may be drawn differently.

10.1.3 Example: Consider the two graphs given in Figures 10.1.3A and B. Observe that these are isomorphic. The correspondence between these two graphs is as follows.
$f(a_i) = v_i$ for $1 \le i \le 5$ and $g(i) = e_i$ for $1 \le i \le 5$.

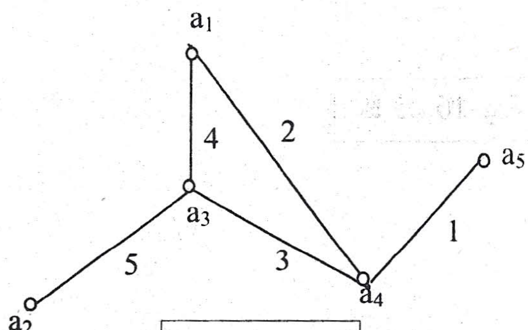


Fig-10.1.3A

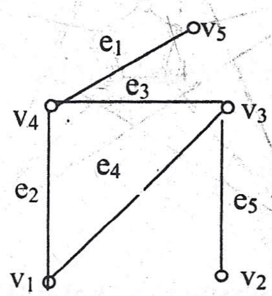
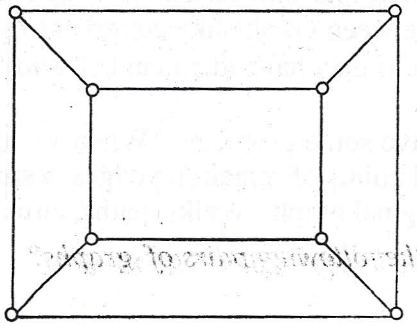


Fig-10.1.3 B

10.1.4 Example: Observe that the two graphs given in Figures 10.1.4A and B are isomorphic.

Fig-10.1.4 A



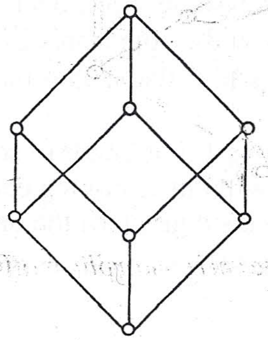


Fig-10.1.4 B

10.1.5 Example: Observe that the three graphs given in Figures 10.1.5A, B and C are isomorphic.

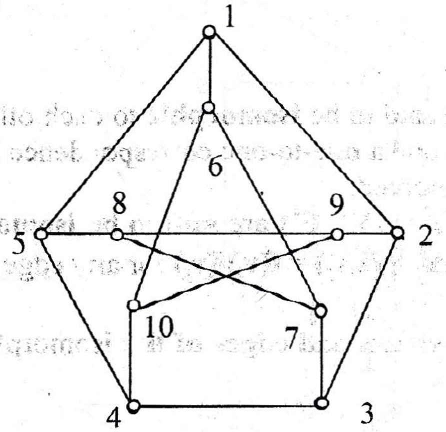


Fig-10.1.5 A

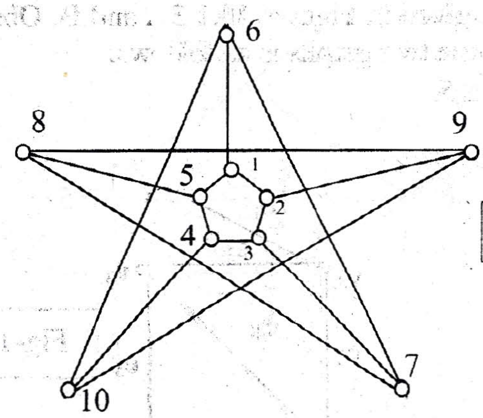


Fig-10.1.5 B

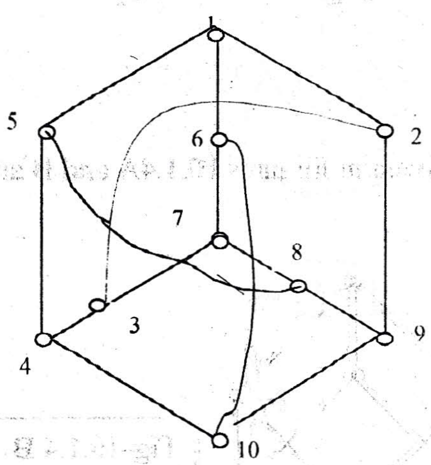
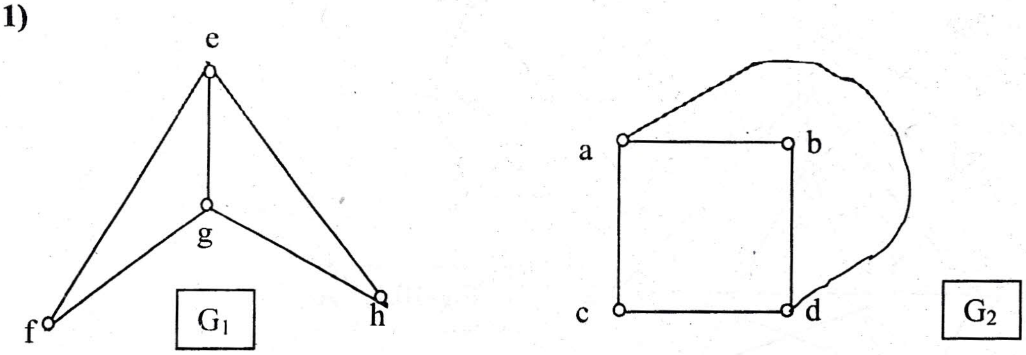


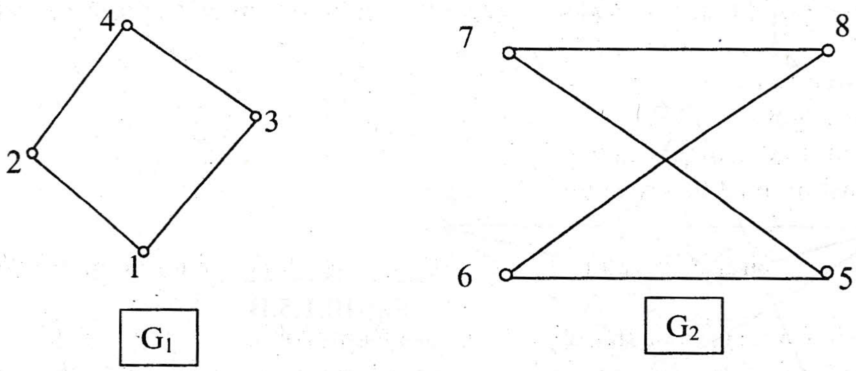
Fig-10.1.5 C

Self Assessment Question1: *Write an isomorphism of the following pairs of graphs?*

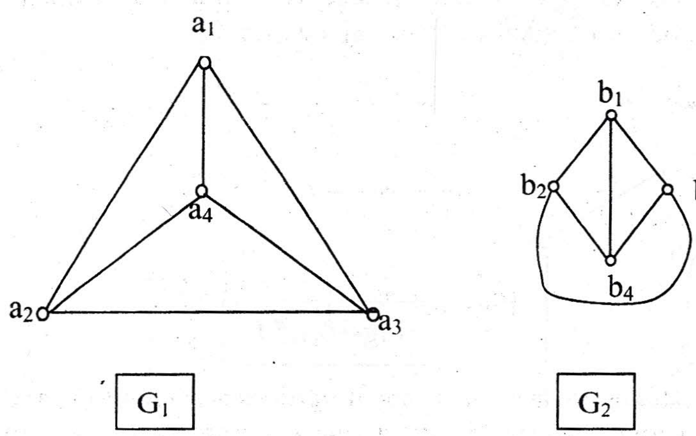
1)



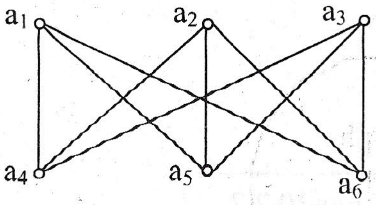
2)



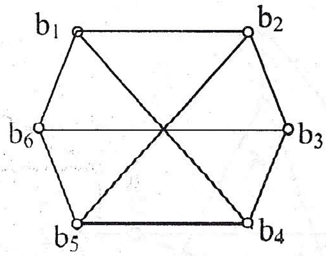
3)



4)



G_1



G_2

10.1.6 Note: It can be observed that if there is an isomorphism between two graphs G and H, then G and H must have :

(i) The same number of vertices

(ii) The same number of edges

(iii) An equal number of vertices of a given degree

(iv) The incident relationship must be preserved.

10.1.7 Note: Consider the two Graphs given in Figures 10.1.7A and B. These two graphs are not isomorphic.

[**verification**: In a contrary way, suppose that the graphs are isomorphic.

Then $\delta(a)$ =degree of a =3 and $\delta(y)$ = degree of u = 3 and there is no vertex other than a and u whose degree is 3. So a and u are to be associated. In such a case, the number of pendent vertices adjacent to a must be equal to the number of pendent vertices adjacent to u.

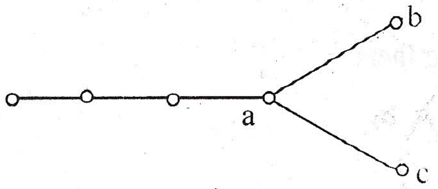


Fig-10.1.7 A

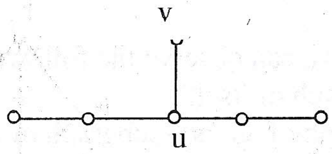


Fig-10.1.7 B

Observing the graphs, we can conclude that there are two pendent vertices adjacent to a, and there is only one pendent vertex adjacent to u, a contradiction. So the given two graphs are not isomorphic].

10.2 SUB GRAPHS

10.2.1 Definition: A graph 'g' is said to be a **subgraph** of a graph G if all the vertices and all the edges of 'g' are in G, and each edge of 'g' has the same end vertices in g as in G. We denote this fact by $g \subset G$.

10.2.2 Example: The graph-2 and graph-3 are subgraphs of graph-1.

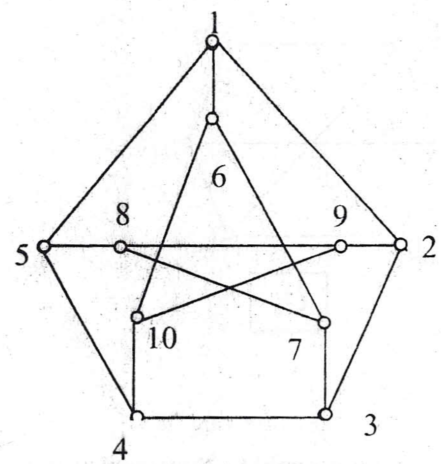


Fig-10.2.2
Graph-1

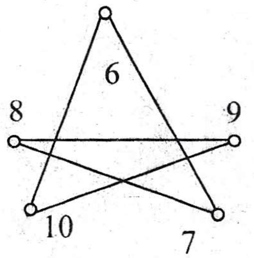


Fig-10.2.2 B
Graph-2

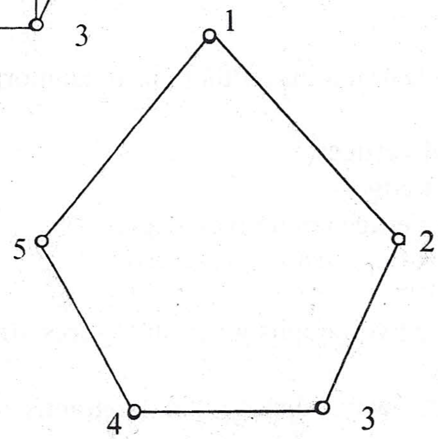


Fig-10.2.2 C
Graph-3

10.2.3 Observations: Here we can observe the following facts :

(i) Every graph is a sub graph of itself.

(ii) A subgraph of a subgraph of G is a subgraph of G.

(iii) A single vertex in a graph G is a subgraph of G.

(iv) A single edge in G together with its end vertices is a subgroup of G.

10.2.4 Definition: Two subgraphs g_1 and g_2 of a graph 'G' are said to be **edge-disjoint** if g_1 and g_2 do not have any edges in common.

10.2.5 Example: Observe the two graphs given in Figures 10.2.5A and B. These two graphs are subgraphs of the graph given in the Figure-10.2.5C. There are no common edges in these two subgraphs. Hence these two subgraphs are edge disjoint subgraphs.

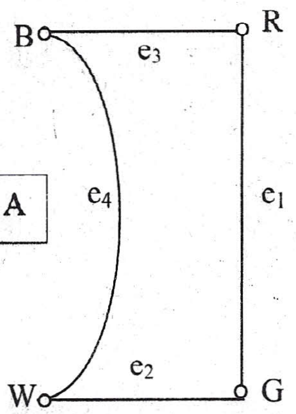


Fig-10.2.5 A

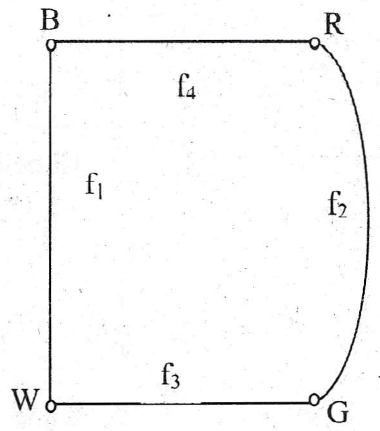


Fig-10.2.5 B

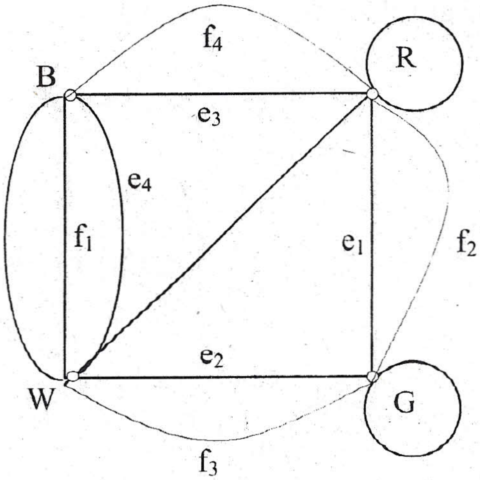


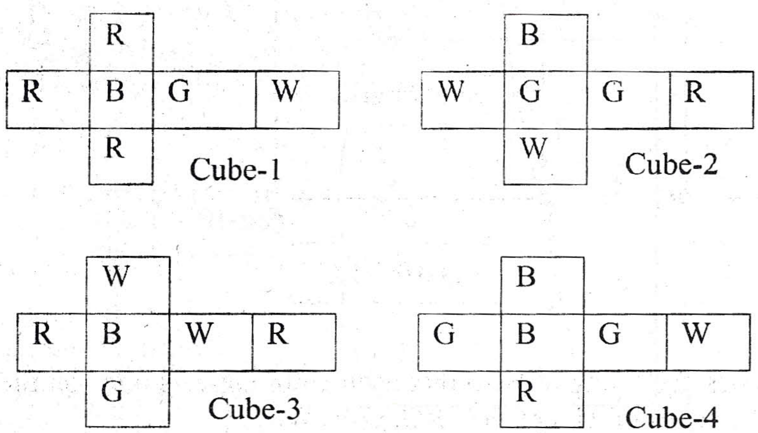
Fig-10.2.5 C

10.2.6 Definition: The subgraphs that do not have vertices in common are said to be **vertex disjoint**.

10.3 A PUZZLE WITH MULTI COLORED CUBES

Now we are going to solve a puzzle called "**Instant Insanity Puzzle**"

10.3.1 Problem: We are given four cubes. The six faces of every cube are variously colored with colors: Blue (B), Red (R), Green (G), white (W).
Now the problem is: 'Is it possible to stack all the four cubes one on the top of another to form a column so that no color appears twice on any of the four sides of this column'.



Solution: Step-(i): (Construction of the graph):

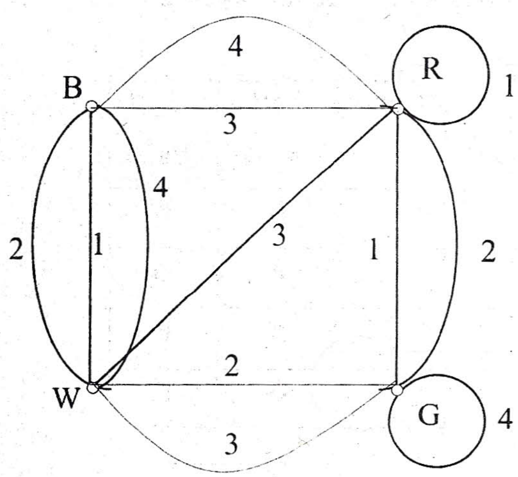


Fig-10.3.1A

Construct a graph with four vertices one corresponding to each of the four colors. We draw an edge between two vertices if the corresponding colors are on opposite sides of a cube. Label the edges with the number of the cube to which that particular edge belongs.

The graph of the above four cubes is given in Figure-10.3.1A.

Step-(ii): (To find two edge disjoint spanning regular subgraphs of degree 2): In this step we have to find two edge disjoint spanning regular subgraphs H and L of degree 2. For this problem, two such subgraphs H and L were given in the Figures 10.3.1B and C.

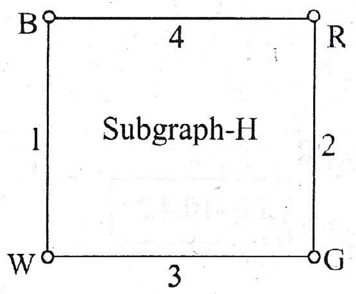


Fig-10.3.1 B

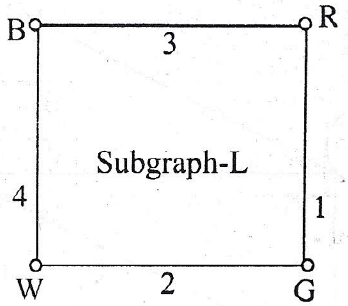


Fig-10.3.1 C

Step-(iii): First we stack the cubes according to H so that each color appears once on the front and one on the back of the stack. The edges of H are BR, RG, GW, WB.
Using these edges, we form table-1. Now L determines the colors on the sides of the stack. Since each cube can be rotated about an axis through the front and back, there is no problem in arranging the colors so that the left and right sides correspond with the table - 2.

Cube	Front (North)	Back (South)
4	B	R
2	R	G
3	G	W
1	W	B

Table-1

Cube	Left (West)	Right (East)
4	B	W
2	W	G
3	R	B
1	G	R

Table-2

10.3.2 Note: Observe that a solution for the above puzzle exists ⇔ there exists two spanning edge disjoint regular subgraphs H and L of degree two.

10.4 WALKS

10.4.1 Definition: A finite alternating sequence of vertices and edges (no repetition of edge allowed) beginning and ending with vertices such that each edge is incident with the vertices preceding and following it, is called a **walk** (or **edge train** or **chain**).

10.4.2 Example: (i) From the above definition, it is clear that no edge appears more than once in a walk.

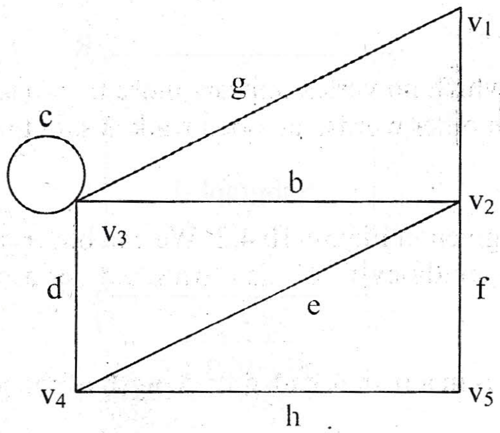


Fig-10.4.2

(ii) Consider the graph given in Figure 10.4.2. We can observe that " $v_1av_2bv_3cv_3d\ v_4e\ v_2f\ v_5$" is a walk.

10.4.3 Note: The set of vertices and edges constituting a given walk in a graph G forms a subgraph of G.

10.4.4 Definition: Vertices with which a walk begins and ends are called the **terminal vertices** (or) **terminal points** of the given walk. The remaining vertices in the walk are called **intermediate vertices** (or) **intermediate points** of the walk.

10.4.5 Definition: A walk is said to be a **closed walk** if the terminal points are same.

10.4.6 Example: Consider the graph given in Figure 10.4.6.
The walk "$v_1av_2bv_3cv_1$" is a closed walk.

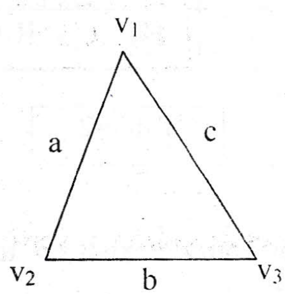


Fig-10.4.6

10.4.7 Definition: A walk which is not closed, is called an **open walk.** [In other words, a walk is said to be an **open walk** if the terminal points are different].

10.4.8 Example: Consider the graph given in Figure 10.4.2. In this graph, the walk "$v_1av_2bv_3dv_4ev_2fv_5$" is an open walk.

10.5 PATHS

10.5.1 Definition: An open walk in which no vertex appears more than once, is called a **path** (or) **simple path** (or) **elementary path**. In other words, an open walk is said to be a **path** if it does not intersects itself.

10.5.2 Example: Consider the graph given in Figure-10.4.2. We can observe that "$v_1av_2bv_3dv_4$" is a path, and "$v_1av_2bv_3cv_3dv_4ev_2f\, v_5$" is a walk but not a path (because this walk contains a repeated vertex v_2).

10.5.3 Definition: The number of edges in a path is called the **length** of the path.

10.5.4 Note: (i) Consider the graph given in Figure 10.4.2. The path "$v_1av_2bv_3dv_4$" is of length 3.

(ii) An edge that is not a self-loop is a path of length one.

(iii) A self-loop is a walk but not a path.

(iv) Consider a path as a subgraph. With respect to the subgraph, we have that terminal vertices of the path are of degree one and the rest of the vertices (these are called intermediate vertices) are of degree two.

For example, consider the path $v_1av_2bv_3dv_4$ (refer the graph given in Figure 10.4.2). With respect to this path $d(v_1) = 1$, $d(v_2) = 2$, $d(v_3) = 2$, $d(v_4) = 1$.

10.5.5 Note: Consider the graph given in Figure 10.5.5. We can observe the following facts.

(i) If there is no repetition of vertices in a walk. then the walk is a non-intersecting walk.

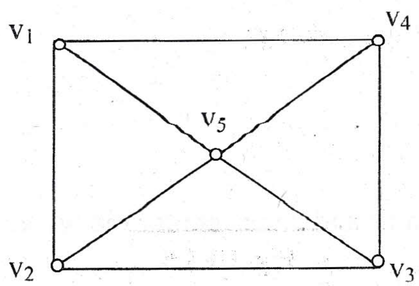


Fig-10.5.5

(ii) Observe that a walk is intersecting $\Leftrightarrow$ there lies repetition of vertices.

(iii) v_1v_5, v_5v_3, v_3v_4, v_4v_5, v_5v_2 is a walk.

10.6 CIRCUITS

10.6.1 Definition: A closed walk in which no vertex (except the initial vertex and the final vertex) appears more than once is called a **circuit**. (or) **cycle** (or) **elementary cycle** (or) **circular path** (o)r **polygon** (or) **loop**. In other words, a closed and non-intersecting walk is called a **circuit**.

10.6.2 Example: (i) Consider the graph given in Figure 10.4.2. The walk v_2 b v_3 d v_4 e v_2 is a circuit.

(ii) Consider the three graphs given in Figures 10.6.2 A, B and C. These three graphs represent three different circuits.

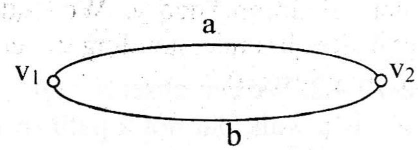


Fig-10.6.2 A

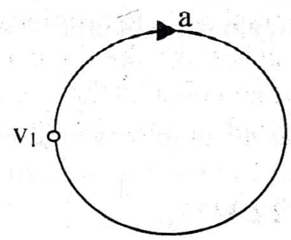


Fig-10.6.2 B

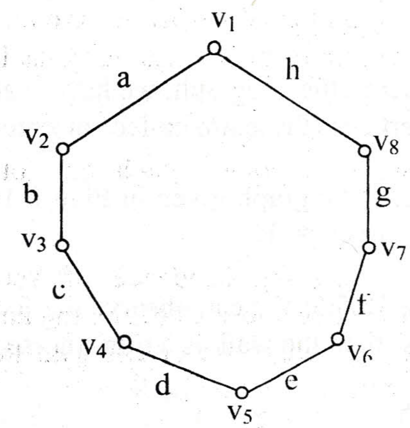
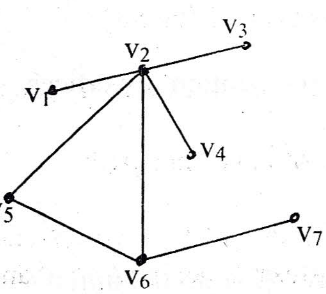


Fig-10.6.2 C

Self Assessment Question-2: Find any two paths and one cycle for the given graph.



10.6.3 Note: (i) Every vertex in a circuit, is of degree 2.
(ii) Every self-loop is a circuit, but every circuit is not a self-loop.

10.7 SUMMARY

In this lesson, we learnt that two isomorphic graphs must have the same number of vertices, same number of edges, & equal number of vertices with a given degree. We discussed terms like subgraphs, Edge disjoint subgraphs, vertex disjoint subgraphs; we also learnt, to convert the given four cubes problem in to a problem of Graph Theory. We studied some basic concepts like walks, paths and circuits that are prerequisites in understanding the concepts Euler graphs and Hamiltonian graphs (that appear in the coming lesson).

10.8 TECHNICAL TERMS

1.Isomorphism between two graphs: An one-to-one correspondence between their vertices and their edges such that the incident relation ship must be preserved.

2. Subgraph: A graph'g' is said to be a subgraph of a graph G if all the vertices and all the edges of 'g' are in G, and each edge of 'g' has the same end vertices in g as in G. We denote this fact by $g \subset G$.

3. Edge-disjoint: Subgraphs of a graph which do not have any edges in common.

4. Walk/edge-train/chain: A finite alternating sequence of vertices and edges (no repetition of edge allowed) beginning and ending with vertices such that each edge is incident with the vertices preceeding and following it.

5. Terminal vertices: Vertices with which a walk begins and ends

6. Intermediate vertices: The vertices which are not terminal vertices, in the walk.

7. Open walk: A walk which is not closed. [In other words, a walk whose terminal points are different].

8. Path/Simple path/Elementary path: An open walk in which no vertex appears more than once.

9. Length: The number of edges in a path.

10. Circuit/Cycle/Loop: A closed walk in which no vertex (except the initial vertex and the final vertex) appears more than once. [In other words, a closed and non-intersecting walk is called a circuit].

10.9 ANSWERS TO SELF ASSESSMENT QUESTIONS

1. The two graphs G_1 and G_2 in (1) are isomorphic and the isomorphism is given by

$a \to e$, $b \to h$, $c \to f$, $d \to g$,

The two graphs G_1 and G_2 in (2) are isomorphic under the correspondence: $1 \to 7$, $2 \to 5$, $3 \to 8$, $4 \to 6$.

The two graphs G_1 and G_2 in (3) are isomorphic and the isomorphism is given by $a_1 \to b_1$, $a_2 \to b_2$, $a_3 \to b_3$, $a_4 \to b_4$.

The two graphs G_1 and G_2 in (4) are isomorphic and the isomorphism is given by the correspondence: $a_1 \to b_1$, $a_2 \to b_2$, $a_3 \to b_3$, $a_4 \to b_4$, $a_5 \to b_5$, $a_6 \to b_6$.

2: (v_6 v_5 v_2 v_4) and (v_7 v_6 v_2 v_1) are two paths.
(v_5 v_6 v_2 v_5) is a cycle.

10.10 MODEL QUESTIONS

1. Explain the isomorphism between two graphs and give an example?
2. Define subgraph of a graph and give an example.?
3. Define the terms: Walk, Path ,Open Walk, Closed walk and give an example of each.
4. When will you say that two subgraphs are edge disjoint?
5. State and solve the Instant Insanity Puzzle.

10.11 REFERENCE BOOKS

1. Bondy J.A and Murty U.S.R, "Graph Theory with Applications", North Holland, New York (1976).

2. Douglas B. West "Introduction to Graph Theory", Second Edition, Prentice Hall of India, New Delhi, 2002.

3. Harary Frank. "Graph Theory", Addison - Wesley Publishing Company, Inc., Reading, Mass., 1969.

4. John Clark and Derek Allan Holton, "A first look at Graph Theory" Allied Publishers, 1995

5. Narsingh Deo "Graph theory with applications to Engineering and Computer Science", Prentice Hall of India Pvt., Ltd., New Delhi, 1993.

6. Satyanarayana Bhavanari and Syam Prasad Kuncham "Graph Theory for Beginners", Satyasri Maths Study Centre, Guntur, AP, 2003.

Name of the Author of this Lesson: Dr. Kuncham Syam Prasad

LESSON - 11

CONNECTED GRAPHS

Objectives

The objectives of this lesson are to:

- learn the concepts of connected graphs & disconnected graphs.
- analyze the components of disconnected graphs.
- study a method to find all the components of a graph G.
- knowing different examples of the connected graphs.

Structure

11.0 INTRODUCTION

One of the most important elementary properties of a graph, is that of connectedness. Intuitively, the concept of connectedness is obvious. A connected graph is in "one piece", so that we can reach any point from any other vertex point by travelling along the edges. In this lesson we develop the basic properties of connected, disconnected graphs and components. We also obtain some elementary results and examples.

11.1 CONNECTED GRAPHS

11.1.1 Definition: A graph G is said to be **connected** if there is at least one path between every pair of vertices in G.

11.1.2 Example: The graph given in Figure 11.1.2 is connected.

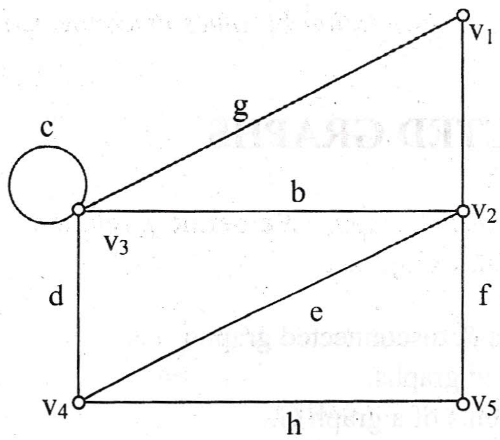


Fig-11.1.2

11.1.3 Example: Observe the graph given in Figure 11.1.3

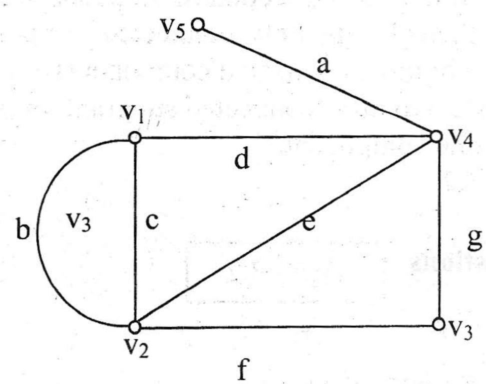


Fig11.1.3

The graph given in Figure 11.1.3 is a connected graph

11.2 DISCONNECTED GRAPHS

11.2.1 Definition: A graph 'G' is said to be a **disconnected graph** if it is not a connected graph.
11.2.2 Example: The graph given in Figure 11.2.2 is a disconnected graph (observe that there is no path from v_4 to v_2).

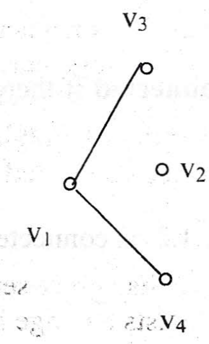


Fig11.2.2

***Self Assessment Question 1:** Draw a connected graph that becomes disconnected when any edge is removed from it ?*

11.3 COMPONENTS

11.3.1 Note: Let G = (V, E) be a disconnected graph. We define a relation ~ on the set of vertices as follows: $v \sim u \Leftrightarrow$ there is a walk from v to u.
Then this relation ~ is an equivalence relation.
Let $\{V_i\}_{i\in\Delta}$ be the collection of all equivalence classes. Now $V = \bigcup_{i\in\Delta} V_i$.

Write $E_i = \{e \in E$ / an end point of e is in $V_i\}$ for each i.
Then (V_i, E_i) is a connected subgraph of G for every $i\in\Delta$.
This connected subgraph (V_i, E_i) of G is called a **connected component** (or **component**) of G for every $i \in \Delta$.
The collection $\{(V_i, E_i)\}_{i\in\Delta}$ of subgraphs of G is the collection of all connected components of G.
11.3.2 Note:(i) If G is a connected graph, then G is the only connected component of G.
(ii) A disconnected graph G consists of two or more connected components.
(iii) Connected component of a graph G is a maximal connected subgraph of G.
(iv) A graph is connected iff it has exactly one component.
(v) Consider the graph given in Figure 11.3.2.

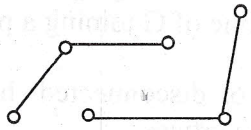


Fig11.3.2

This graph is a disconnected graph with two components.

11.3.3 Formation of components: If G is a connected graph, then G contains only one connected component and it is equal to G.
Now suppose that G is a disconnected graph. Consider a vertex v in G. If each vertex of G is joined by some path to v, then the graph is connected, a contradiction. So there exists at least one vertex which is not joined by any path to v.
The vertex v and all the vertices of G that are joined by some paths to v together with all the edges incident on them form a component (G_1, say).
To find another component, take a vertex u (from G) which is not in G_1. The vertex u and all the vertices of G that are joined by some paths to u together with all the edges incident on them form a component (G_2, say).
Continue this procedure to find the components. Since the graph is a finite graph, the procedure will stop at a finite stage. In this way, we can find all the connected components of G. It is clear that, a component it self is a graph.

11.3.4 Theorem: A graph G is disconnected $\Leftrightarrow$ its vertex set V can be partitioned into two non-empty disjoint subsets V_1 and V_2 such that there exists no edge in G, whose one end-vertex is in V_1 and the other end vertex is in V_2.

Proof: Let $G = (V, E)$ be a graph.
Assume that $V = V_1 \cup V_2$, $V_1 \neq \phi$, $V_2 \neq \phi$ and $V_1 \cap V_2 = \phi$ such that there exists no edge in G whose one end-vertex is in V_1 and another end-vertex is in V_2.
We have to show that G is disconnected.
In a contrary way, assume that G is connected.
Let $a, b \in G$ such that $a \in V_1$ and $b \in V_2$.
Since G is connected there exists a path $a\, e_1\, a_1\, e_2\, a_2 \ldots a_{n-1}\, e_n\, b$ from a to b.
Now $b \notin V_1$. So there exists least number j such that $a_j \notin V_1$.
Now $a_{j-1} \in V_1$, $a_j \in V_2$ and e_j is an edge between a vertex in V_1 and a vertex in V_2, a contradiction. Hence G is disconnected

Converse: Suppose G is disconnected. Let a be a vertex in G. Write
$V_1 = \{v \in V$ / either $a = v$, or a is joined by a walk to $v\}$.
If $V_1 = V$, then all the vertices (other than a) are joined by a path to a, and so the graph is connected, a contradiction.
Hence $V_1 \subsetneq V$. Write $V_2 = V \setminus V_1$. Now V_1, V_2 form a partition for V. If a vertex $x \in V_1$ is joined to $y \in V_2$ by an edge, then y is connected to a (since $x \in V_1$) $\Rightarrow y \in V_1 \Rightarrow y \in V_1 \cap V_2 = \phi$, a contradiction.
Hence no vertex in V_1 is connected to a vertex of V_2 by an edge. This completes the proof.

[In other words, the Theorem 11.3.4 can be stated as : A graph G is connected $\Leftrightarrow$ for any partition v of vertex set in to subsets V_1 and V_2, there is a line of G joining a point of V_1 to a point of V_2].

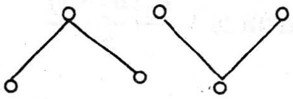
11.3.5 Theorem: If a graph (either connected or disconnected) has exactly two vertices of odd degree, then there exists a path joining these two vertices.

Proof: Let G be a graph and v_1, v_2 be the only two vertices in G whose degrees are odd.

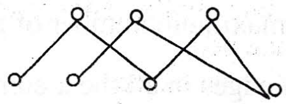
Case-(i): Suppose G is connected. Then by definition, there exists a path between any two vertices.
So there is a path from v_1 to v_2 in G.

Case-(ii): Suppose G is disconnected. Then G has two or more components.
Let G_1 be the component in which v_1 presents.
Now G_1 is a connected subgraph.
If G_1 do not contain v_2, then the number of vertices in G_1 with odd degree is 1 (an odd number), a contradiction (since in any graph, the number of vertices of odd degree is even).
Therefore v_2 is also in G_1.
Hence v_1, v_2 are in the same component.
Since every component is connected, there exists a path from v_1 to v_2 in G.

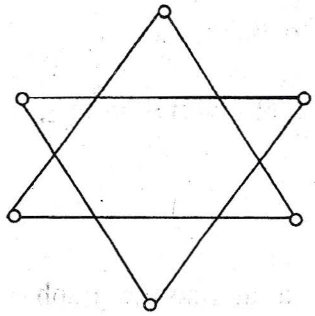
***Self Assessment Question 2:** Determine whether the given graphs are connected.*



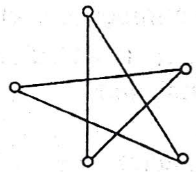
G1



G2



G3



G4

11.3.6 Theorem: A simple graph with 'n' vertices and 'k' components can have at most (n - k) (n -k + 1)/2 edges [or the maximum number of edges in a simple graph with 'n' vertices and 'k' components is (n - k)(n - k + 1)/2].

Proof: Let G be a simple graph [that is, G has no self-loops and no parallel edges] wih 'n' vertices and k components.

Suppose that $G_1, G_2, G_3, \ldots, G_i, \ldots G_k$ are k components and $n_1, n_2, n_3, \ldots n_i, \ldots, n_k$ are the number of vertices in the components $G_1, G_2, G_3, \ldots, G_k$ respectively.

It is clear that $n = n_1 + n_2 + n_3 + \ldots + n_k$ ------ (i)

Now $\sum_{i=1}^{k}(n_i - 1) = \sum_{i=1}^{k} n_i - k = n - k$

Squaring on both sides, we get that $\left[\sum_{i=1}^{k}(n_i - 1)\right]^2 = (n - k)^2$

$$\Rightarrow \sum_{i=1}^{k}(n_i - 1)^2 + 2\prod_{i=1}^{k}\prod_{j=1}^{k}(n_i - 1)(n_j - 1) = n^2 + k^2 - 2nk$$

$$\Rightarrow \sum_{i=1}^{k}(n_i^2 - 2ni + 1) + (\text{some non-negative terms})$$

$$= n^2 + k^2 - 2nk$$

$$\Rightarrow \sum_{i=1}^{k}(n_i^2 - 2n_i) + k \le n^2 + k^2 - 2nk$$

$$\Rightarrow \sum_{i=1}^{k} n_i^2 - 2\sum_{i=1}^{k} n_i + k \le n^2 + k^2 - 2nk$$

$$\Rightarrow \sum_{i=1}^{k} n_i^2 - 2n + k \le n^2 + k^2 - 2nk. \text{ (since } \sum_{i=1}^{k} n_i = n \text{ by (i))}$$

$$\Rightarrow \sum_{i=1}^{k} n_i^2 \le n^2 + k^2 - 2nk + 2n - k \quad \text{----- (ii)}$$

Since G is a simple graph, the i^{th} component G_i is also a simple graph. Since G_i contains n_i vertices and G_i is simple, we have that the maximum number of edges in the i^{th} component is $\frac{n_i(n_i-1)}{2}$

Therefore the maximum number of edges in all the k components is

$$\sum_{i=1}^{k}\frac{n_i(n_i-1)}{2} = \frac{1}{2}\sum_{i=1}^{k} n_i(n_i-1)$$

$$= \frac{1}{2}\sum_{i=1}^{k}(n_i^2-n_i)$$

$$= \frac{1}{2}\left(\sum_{i=1}^{k} n_i^2 - \sum_{i=1}^{k} n_i\right)$$

$$\leq \frac{1}{2}[(n^2+k^2-2nk+2n-k)-n]$$

(from (i) & (ii))

$$= \frac{1}{2}[n^2- nk- nk + k^2 + n - k]$$

$$= \frac{1}{2}[(n-k)n - (n-k)k + (n-k)]$$

$$= \frac{1}{2}(n-k)(n-k+1).$$

This completes the proof.

11.4 SUMMARY

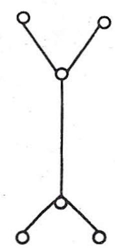
In this lesson, we discussed connected graphs, disconnected graphs and components in a disconnected graph. We also learnt a procedure, to find all the components in a given graph G. We studied an equivalent condition for a graph G to be disconnected. The maximum number of edges in a simple graph with n vertices and k components was found.

11.5 TECHNICAL TERMS

Connected graph: A graph in which every pair of vertices are joined by a path.
Disconnected graph: A graph which is not connected.
Component: maximal connected subgraph of a graph.

11.6 ANSWERS TO SELF ASSESSMENT QUESTIONS

1:



2: Graphs G_1 and G_3 are not connected
Graphs G_2 and G_4 are connected.

11.7 MODEL QUESTIONS

1. Define the terms and provide an example of each. (i) Connected graph (ii) Disconnected graph (iii) Component.
2. Show that a graph G is disconnected $\Leftrightarrow$ its vertex set V can be partitioned into two non-empty disjoint subsets V_1 and V_2 such that there is no edge in G, whose one end-vertex is in V_1 and the other end vertex is in V_2.
3. Show that if a graph (either connected or disconnected) has exactly two vertices of odd degree, then there exists a path joining these two vertices.
4. Show that a simple graph with 'n' vertices and 'k' components can have at most $(n - k)(n - k + 1)/2$ edges [or the maximum number of edges in a simple graph with 'n' vertices and 'k' components is $(n - k)(n - k + 1)/2$].

11.8 REFERENCE BOOKS

1. Bondy J.A and Murty U.S.R, "Graph Theory with applications", North Holland, New York (1976).

2. Douglas B. West "Introduction to Graph Theory", Second Edition, Prentice Hall of India, New Delhi, 2002.

3. Harary Frank. "Graph Theory", Addison - Wesley Publishing Company, Inc., Reading, Mass., 1969.

4. John Clark and Derek Allan Holton, "A first look at Graph Theory" Allied Publishers, 1995

5. Narsingh Deo "Graph theory with applications to Engineering and Computer Science", Prentice Hall of India Pvt., Ltd., New Delhi, 1993.

6. Satyanarayana Bhavanari and Syam Prasad Kuncham "Graph Theory for Beginners", Satyasri Maths Study Centre, Guntur, AP, 2003.

Name of the Author of this Lesson: **Mr. J. L. Ram Prasad**

LESSON - 12

EULER GRAPHS

Objectives

The objectives of this lesson are to:

- learn the concepts of Euler line, Euler graph, Unicursal line and Unicursal graphs.
- learn a beautiful characterization with which Euler solved the Konigs berg bridges problem.
- discuss the operations like union, intersection and ring sum of two graphs.
- know about decomposition of a graph G into subgraphs.
- learn the concepts of arbitrarily traceable graphs.

Structure

12.0 INTRODUCTION

Euler formulated the concept of Eulerian line when he solved the problem of the Konigsberg bridges. The Euler lines mainly deal with the nature of connectivity in graphs. These are used to solve several puzzles and games. In this lesson we discuss the relation between a local property namely degree of a vertex and global properties like the existence of Eulerian cycles. We see that there are well designed characterizations for Eulerian graphs. We also provided some binary operations on graphs.

12.1 EULER GRAPHS

12.1.1 Definition: Let G be a graph. A closed walk running through every edge of the graph G exactly once is called an **Euler line**.

12.1.2 Definition: A graph 'G' that contains Euler line is called an **Euler graph**.

12.1.3 Example: The graphs given in the Figures 12.1.3A and B are Euler graphs.

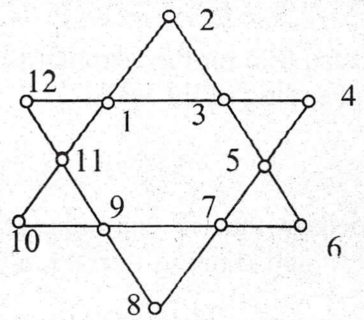


Fig-12.1.3 A
Star of David

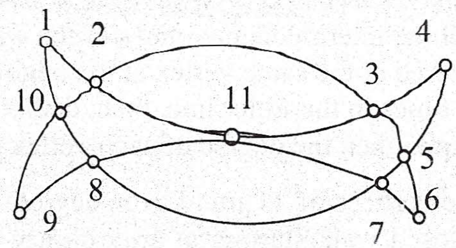


Fig-12.1.3 B
Mohammad's Scimitars

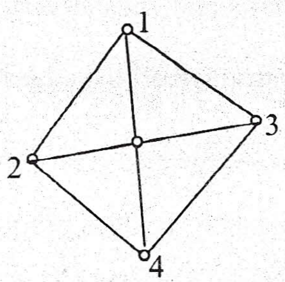
(i) Consider Fig-12.1.3A.

Here 123456789(10)(11)(12)13579(11)1 is an Euler line.

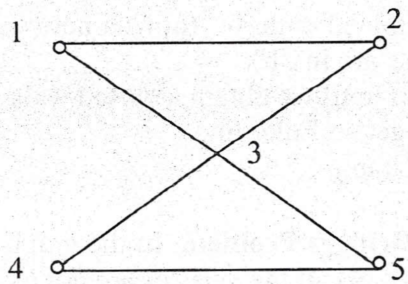
(ii) Consider Fig-12.1.3B.

Here 23456789(10) 12(11)357(11)8(10)2 is an Euler line.

Self Assessment Question 1: *Which of the following is an Euler graph, give reasons ?*



G_1



G_2

12.1.4 Note: An Euler graph may contain isolated vertices. If G is an Euler graph and it contains no isolated vertices, then it is connected.

Here after we consider only those Euler graphs that do not contain isolated vertices. So the Euler graphs those we consider are connected.

12.1.5 Theorem: A given connected graph G is an Euler graph $\Leftrightarrow$ all the vertices of G are of even degree.

Proof: Suppose G is an Euler graph. Then G contains an Euler line. So there exists a closed walk running through all the edges of G exactly once.

Let $v \in V$ be a vertex of G. Now in tracing the walk it goes through two incident edges on v with one entered v and the other exited.

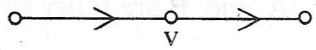


Fig12.1.5

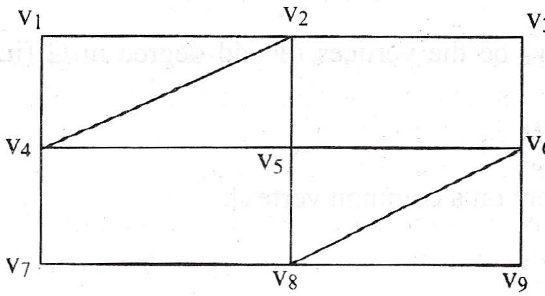
This is true not only for all the intermediate vertices of the walk, but also true for the terminal vertex because we exited and entered at the same vertex at the beginning and ending of the walk.
Therefore if v occurs k times in the Euler line, then $d(v) = 2k$.
Thus if G is an Euler graph, then the degree of each vertex is even.

Converse: Suppose all the vertices of G are of even degree. Now to show that G is a Euler graph, we have to construct a closed walk starting at an arbitrary vertex v and running through all the edges of G exactly once.
To find a closed walk, let us start from the vertex v. Since every vertex is of even degree, we can exist from every vertex we entered, the tracing cannot stop at any vertex but at 'v'.
Since 'v' is also of even degree, we shall eventually reach 'v' when the tracing comes to an end.
If this closed walk (h, say) includes all the edges of G, then G is an Euler graph.
Suppose the closed walk h does not include all the edges. Then the remaining edges form a subgraph h^1 of G.
Since both G and h have all their vertices of even degree, the degrees of the vertices of h^1 are also even.
Moreover, h^1 must touch h atleast one vertex 'a' because
G is connected. Starting from 'a' we can again construct a new walk in graph h^1.
Since all the vertices of h^1 are of even degree, and this walk in h^1 must terminates at the vertex 'a'.
This walk in h^1 combined with h forms a new walk which starts and ends at vertex v and has more edges than those are in 'h'.
We repeat this process until we obtain a closed walk that travels through all the edges of G.
In this way, one can get an Euler line.
Thus G is an Euler Graph.

12.1.6 Konigsberg Bridges Problem: In the graph of the Konigsberg bridges problem, there exist vertices of odd degree. So all the vertices are not of even degree.
Hence by the Theorem 12.1.5, we conclude that "the graph representing the Konigsberg bridges problem" is not an Euler graph.
So we conclude that it is not possible to walk over each of the seven bridges exactly once and return to the starting point.

12.1.7 Note: The concept of Euler graph can be used to solve so many puzzles like: to find how a given picture can drawn in one continuous line without retracing a line and without lifting the pencil from the paper.
For example, consider the two graphs given in Example 12.1.3. Any one of these two graphs can be drawn in one continuous line without retracing a line and without lifting the pencil from the paper.

Self Assessment Question 2: *Let G be the graph given below. Use theorem 12.1.5 to verify that G is an Euler graph.*



12.1.8 Note: In defining an Euler line, some authors drop the requirement that the walk be closed. For example, consider the graph given in Fig-12.1.8. The walk $v_1\, e_1\, v_3\, e_2\, v_4\, e_3\, v_1\, e_4\, v_2\, e_5\, v_4\, e_6\, v_5\, e_7\, v_2$ includes all the edges of the graph and do not contain repetition of edges. Observe that this walk is not closed. (because the initial vertex is 'a' and the final vertex is 'b'). This situation develops a new concept called **unicursal graph.**

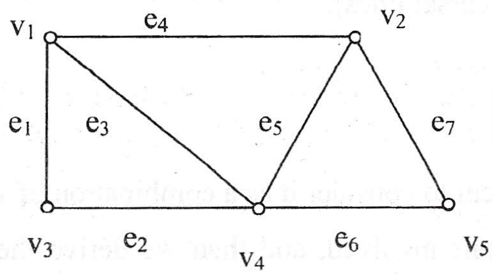


Fig-12.1.8

12.1.9 Definition: Let 'G' be a graph. Then an open walk running through all edges of the graph 'G' exactly once is called an **unicursal line**.

12.1.10 Definition: A connected graph that contains unicursal line is called a **unicursal graph.**

12.1.11 Note: (i) If we add an edge between the initial and final vertices of a unicursal line, then we get an Euler line.

(ii) A connected graph is unicursal $\Leftrightarrow$ it has exactly two vertices of odd degree,

[**Verification**: Let G be an unicursal graph. Then we get a path from v to u with $v \neq u$. If we join a new edge vu, then we get an Euler line. So all the vertices of this new graph $G^* = G \cup \{vu\}$ have degree even.

So in the given graph G, there exists exactly two vertices v and u with odd degree.

Converse: If there exist exactly two vertices u and v of odd degree, then join by uv. So in the new graph, all vertices are of even degree. So by above theorem, the new graph contains an Euler line. Now remove uv from this Euler line to get an unicursal line].

12.1.12 Theorem: In a connected graph 'G' with exactly 2k odd vertices, there exists k edge-disjoint subgraphs such that they together contain all edges of G and that each subgraph is an unicursal graph.

Proof: Let $v_1, v_2, \ldots, v_k, w_1, w_2, \ldots, w_k$ be the vertices of odd degree in G (in some arbitrary order).
Now add k edges between the vertex pairs
$(v_1, w_1), (v_2, w_2), \ldots, (v_k, w_k)$.
[Note that no two of these edges are incident on a common vertex].
Write $G^1 = G \cup \{v_i w_i \,/\, 1 \le i \le k\}$.
Now we got a new graph, say G^1.
Now each vertex of G^1 is of even degree.
Since every vertex of G^1 is of even degree, we have that G^1 consists of an Euler line "P".
If we remove the k edges (just added) from this Euler line P (note that no two of these edges are incident on the same vertex), then this Euler line 'P' will split into k walks, each of which is an unicursal line.
[The first removal will leave a single unicursal line, the second removal will split that into two unicursal lines, and each successive removal will split an unicursal line into two unicursal lines. After removal of k edges, we left with k unicursal lines].
This completes the proof.

12.2. OPERATIONS ON GRAPHS

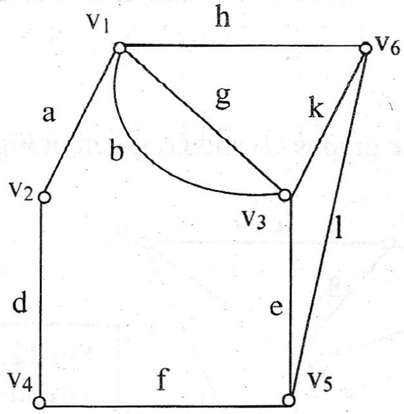
To study a large graph, it is convenient to consider it as a combination of small graphs. First we understand the properties of small graphs involved, and then we derive the properties of the large graphs.

Since graphs are defined by using the concepts of set theory, we use the set theoretical terminology to define operations on graphs. In defining the operations on graphs, we are more concerned about the edge sets.

12.2.1 Definition: Let $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ be any two graphs. Then **union** of G_1 and G_2 is the graph $G = (V, E)$ where
$V = V_1 \cup V_2$ and $E = E_1 \cup E_2$. We write $G = G_1 \cup G_2$.

12.2.2 Example: Consider the following graphs G_1, G_2 and G_3.

Fig12.2.2 A
Graph-G_1



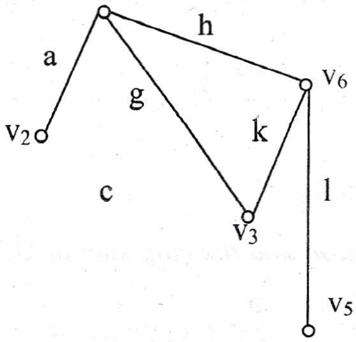


Fig-12.2.2B
Graph-G_2

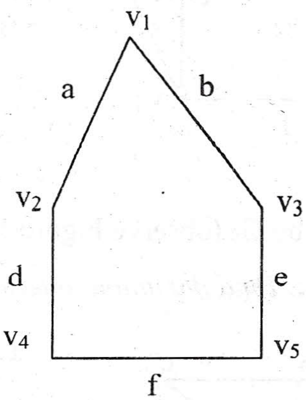


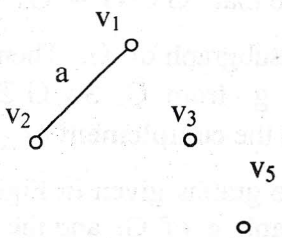
Fig-12.2.2 C
Graph-G_3

It is clear that $G_1 = G_2 \cup G_3$.

12.2.3 Definition: Let $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ **be** any two graphs with $V_1 \cap V_2 \neq \phi$. Then the **intersection** of G_1 and G_2 is defined as the graph $G = (V, E)$ where $V = V_1 \cap V_2$ and $E = E_1 \cap E_2$.
We write $G = G_1 \cap G_2$.

12.2.4 Example: Consider the graphs given in Figures 12.2.2 A, B and C. The intersection of G_2 and G_3 is given below. $G_4 = G_2 \cap G_3$.

Fig-12.2.4
Graph-G_4



12.2.5 Definition: The **ring sum** of two graphs $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ is defined as the graph $G = (V, E)$ where $V = V_1 \cup V_2$ and $E = (E_1 \cup E_2) \setminus (E_1 \cap E_2)$. We write $G = G_1 \oplus G_2$.

12.2.6 Example: Consider the graphs G_2 and G_3 given in Figure 12.2.2 B and C.

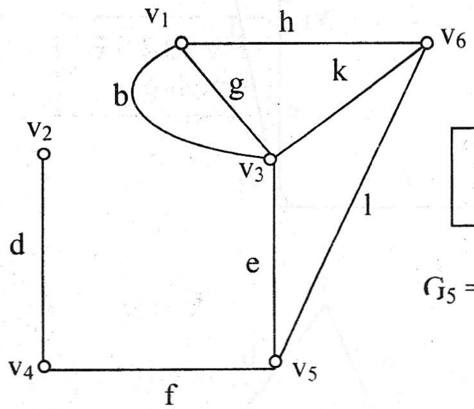
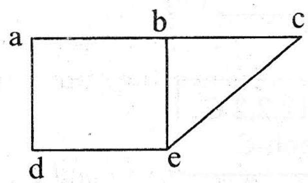


Fig-12.2.6
Graph-G_5

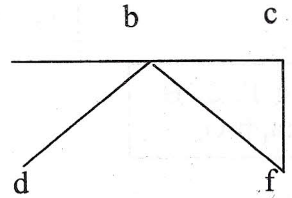
$G_5 = G_2 \oplus G_3$.

The graph $G_2 \oplus G_3$ is given by G_5 (observe Figure 12.2.6).

Self Assessment Question 3: *Find the union, intersection and the ring sum of G_1 and G_2.*



G_1

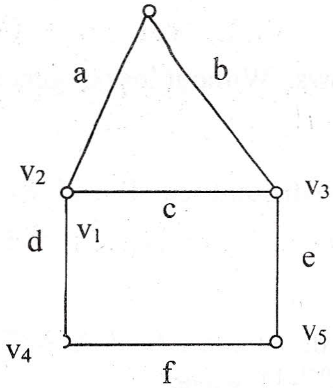


G_2

12.2.7 Note: (i) The three operations (union, intersection and ring sum) on the set of all finite graphs are commutative. That is, $G_1 \cup G_2 = G_2 \cup G_1$, $G_1 \cap G_2 = G_2 \cap G_1$, $G_1 \oplus G_2 = G_2 \oplus G_1$.
(ii) If G_1 and G_2 are edge disjoint, then $G_1 \cap G_2$ is a null graph, and $G_1 \oplus G_2 = G_1 \cup G_2$.
(iii) For any graph G, we have that $G \cup G = G \cap G = G$ and $G \oplus G = \phi$ (a null graph).

12.2.8 Note: Let g be any subgraph of G. Then $G \oplus g$ is a subgraph of G which remains after removing all the edges of g from G. So $G \oplus g$ is written as $G - g$, whenever $g \subseteq G$. So $G \oplus g = G - g$ is often called the **complement** of g in G.

12.2.9 Example: Observe the graphs given in Figures 12.2.9 A, B and C. In these Figures, an example of a graph G, a subgraph g of G, and the complement $G - g$ of g were given.



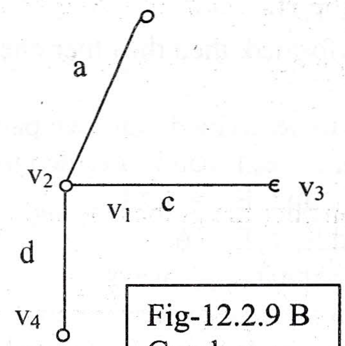


Fig-12.2.9 B
Graph-g

Fig-12.2.9A, Graph-G

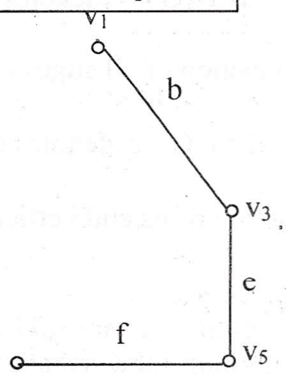


Fig-12.2.9 C
Graph G - g

12.2.10 Definition: A graph G is said to be **decomposed** into two subgraphs g_1 and g_2, if (i) $g_1 \cup g_2 = G$, and (ii) $g_1 \cap g_2 = \phi$ (a null graph).

(Equivalently, a graph G is said to be **decomposed** into two subgraphs g_1 and g_2, if every edge of G occurs either in g_1 or in g_2, but not in both).
However, some of the vertices may occur both in g_1 and g_2. In the decomposition, the isolated vertices are disregarded.

12.2.11 Note: A graph G can be decomposed into more than two subgraphs. A graph G is said to have been **decomposed** into subgraphs $g_1, g_2, \ldots g_n$ if
(i) $g_1 \cup g_2 \cup \ldots \cup g_n = G$, and (ii) $g_i \cap g_j = \phi$ (a null graph), for $i \neq j$.

12.2.12 Problem: Let G be a graph containing m edges. Then G can be decomposed in $(2^{m-1} - 1)$ different ways into pairs of subgraphs g_1, g_2 (which are not null graphs).
Solution: Let $\{e_1, e_2, \ldots, e_m\}$ be the set of all edges in G. Suppose G is decomposed into two of its subgraphs g_1 and g_2 (which are not null graphs) where $G = (V, E)$,
$g_1 = (V_1, E_1)$, $g_2 = (V_2, E_2)$.
Now $E_1 \cup E_2 = E$ and $E_1 \cap E_2 = \phi$.

Note that $E_1 \neq \phi \neq E_2$.
If one of the E_1, E_2 formed, then the other one follows. Without loss of generality, we assume that $e_1 \in E_1$.
Now $\{e_2, \ldots, e_m\}$ is to be divided into two parts.
We know that $\{e_1, e_2, \ldots, e_m\}$ can be divided into two disjoint sets F_1 and F_2 in 2^{m-1} ways.
Write $E_1 = \{e_1\} \cup F_1$ and $E_2 = E \setminus E_1$.
Now $E_1 \cup E_2 = E$ and $E_1 \cap E_2 = \phi$.
This division can be done in 2^{m-1} ways.
Since empty set is not allowed to consider as E_2, this division can be done in $2^{m-1} - 1$ ways.
Thus the subgraphs g_1 and g_2 can be formed in $(2^{m-1}-1)$ ways.
This completes the proof.

12.2.13 Note: (i) If v is a vertex in a graph G, then G - v denotes a subgraph of G obtained by deleting v from G.
(ii) Deletion of a vertex is always implies the deletion of all edges incident on that vertex.

12.2.14 Note: (i) If e is an edge in a graph G, then G - e denotes the subgraph of G obtained by deleting e from G.
(ii) Deletion of an edge does not imply the deletion of its end vertices.
(iii) It is clear that $G - e = G \oplus e$.

12.2.15 Definition: A pair a, b of vertices in a graph G are said to be **fused** (or) **merged** (or) **identified** if the two vertices are replaced by a single new vertex such that every edge that is incident on either 'a' or 'b' or on both is incident on the new vertex. It is clear that the fusion of two vertices does not alter the number of edges, but it reduces the number of vertices by one.

12.2.16 Example :Observe the graphs G and G* given in Figures 12.2.16A and B.
The vertices a and b of G were fused to get the graph G*.

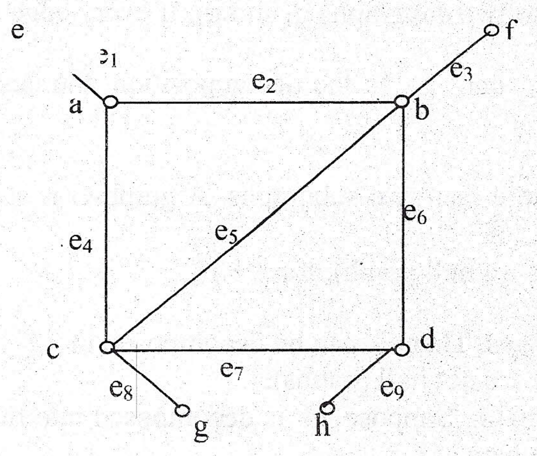


Fig-12.2.16 A
Graph-G

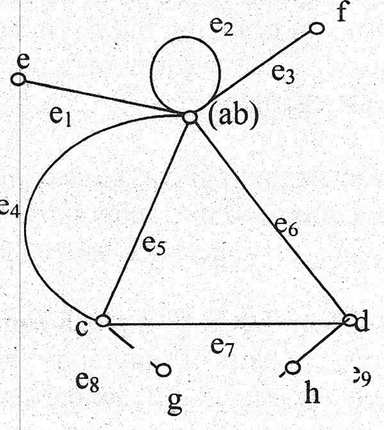


Fig-12.2.16 B
Graph-G*

12.3. FURTHER DISCUSSION ON EULER GRAPHS

12.3.1 Theorem: A connected graph G is an Euler graph $\Leftrightarrow$ it can be decomposed into circuits.
Proof: Let G be a connected graph. Assume that G can be decomposed into circuits.
That is, G is the union of edge-disjoint circuits. Since the degree of every vertex in a circuit is even, we have that the degree of every vertex in G is even. By theorem 12.1.5, we have that G is an Euler graph.

Converse: Suppose that G is an Euler graph.
Then all the vertices of G are of even degree.
Now consider a vertex v_1.
Clearly there are at least two edges incident at v_1.
Suppose that one of these edges is between v_1 and v_2.
Since vertex v_2 is also of even degree, it must have atleast one more edge (say between v_2 and v_3).
Proceeding in this way, we arrive at a vertex that has previously been traversed.
Then we get a circuit say 'Γ_1'.
Now let use remove 'Γ_1' from G. (It is understood that we are removing only the edges of Γ_1 from G). Then all the vertices in the remaining graph must also be of even degree.
Now from the remaining graph, remove another circuit 'Γ_2' in the same way (as we removed 'Γ_1' from G).
Continue this process to get circuits $\Gamma_1, \Gamma_2 \ldots \Gamma_n$ (until no edges are left). Now it is clear that the graph G was decomposed into the circuits $\Gamma_1, \Gamma_2 \ldots \Gamma_n$.
This completes the proof.

12.3.2 Note : Consider the graph G given in Figure 12.3.2. It is an Euler graph. Suppose we start from the vertex 'u' and trace the path uvw. Now at 'w', we have the choice of going to either 'x' or 'y' or 'u'.

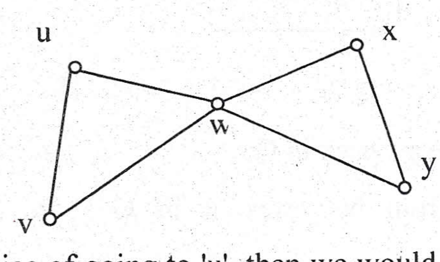


Fig-12.3.2

If we took the choice of going to 'u', then we would only trace the circuit 'uvwu', which is not an Euler line.
Thus we have the following situation:
"Starting from the vertex 'u', we are unable to trace the entire Euler line simply by moving along any edge that has not already been traversed".
Now the following question arises.

"What property must a vertex 'v' in an Euler graph have so that an Euler line is always obtained when one follows any walk from the vertex 'v' according to the single rule that whenever one arrives at a vertex, one shall **select** any edge (which has not been previously traversed)".
For the graph given here, let us consider the vertex 'w'. An Euler line is always obtained when one follows any walk from the vertex 'w' according to the single rule that whenever one arrives at a vertex one shall select any edge which has not been previously traversed. In this case, we say that the graph is an "**arbitrarily traceable graph**" from the vertex 'w'.

One can observe that the graph given above is not arbitrarily traceable from any vertex other than w.

12.3.3 Definition: Let G be a graph and v a vertex. The graph is said to be **arbitrarily traceable graph from the vertex** v if an Euler line is always obtained when one follows any walk from the vertex v according to the single rule that whenever one arrives at a vertex one shall select any edge (which has not been previously traversed).

12.3.4 Example: The graph given in Figure 12.3.4 is an Euler graph. It is not arbitrarily traceable from any vertex.

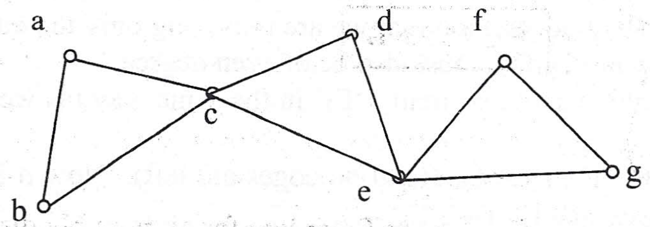


Fig-12.3.4

12.3.5 Example: The graph given in Figure 12.3.5 is an arbitrarily traceable graph from all vertices.

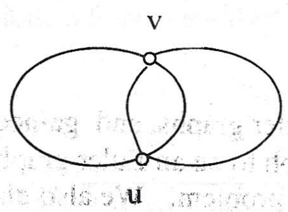


Fig-12.3..5

12.3.6 Theorem: Let G be a graph and v be a vertex in G.

An Euler graph G is arbitrarily traceable from the vertex v in G $\Leftrightarrow$ every circuit in G contains v.

Proof: Let G be an Euler graph.
Suppose that G is arbitrarily traceable from the vertex v.
Now we have to prove that every circuit in G contains v.
In a contrary way, suppose that there exists a circuit C_1 such that v is not in C_1. Since v is in Euler line, v is in a circuit C_2 which is edge disjoint from C_1.
The circuit C_2 provides a closed walk from v to v which is not an Euler line.

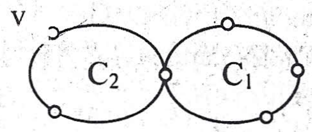


Fig-12.3.6

Now we can get a walk W (of maximum length)starting at v and ending at v which do not contains C_1.
So we get a walk W (of maximum length) which do not contain the edges in C_1 and this walk W is not an Euler line, a contradiction to the fact that G is arbitrarily traceable from v. Hence every circuit contains v.

Converse: Suppose that every circuit in G contains v.
Since G is an Euler graph, there exist finite number of disjoint circuits, say $C_1, C_2, \ldots C_n$.
By converse hypothesis, we have that each of these circuits contains v.
We can cover all the edges of any cycle C_i starting at v and ending at v.

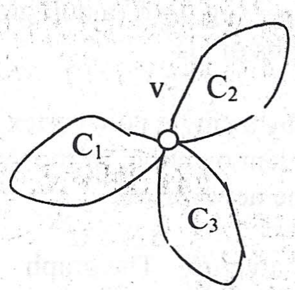


Fig-12.3.6 B

Now the walk given by $v\, C_{i_1}\, v\, C_{i_2}\, v \ldots v\, C_{i_n}\, v$ is an Euler line for all possible distinct values of $i_1, i_2, \ldots, i_n$ such that $\{i_1, i_2, \ldots, i_n\} = \{1, 2, \ldots, n\}$.
Hence G is an arbitrary traceable from v.

12.4 SUMMARY

In this lesson, we learnt the concepts of Euler lines, Euler graphs, and gained knowledge about a necessary and sufficient condition for a connected graph to be an Euler graph. As a consequence of this we obtained a solution for the Konigsbergs bridge problem. We also discussed few binary operations on graphs. The concepts arbitrary traceable graphs and a few characterizations on it were discussed.

12.5 TECHNICAL TERMS

Euler line: A closed walk running through every edge of the graph G exactly once.

Euler graph: A graph that contains an Euler line.

Unicursal line: An open walk running through all edges of the graph exactly once.

Unicursal graph: A connected graph that contains unicursal line.

Union of two graphs G_1 and G_2: $G = (V, E)$ where $V = V_1 \cup V_2$ and $E = E_1 \cup E_2$. We write $G = G_1 \cup G_2$.

Intersection of graphs: $G = (V, E)$ where $\phi \neq V = V_1 \cap V_2$ and $E = E_1 \cap E_2$. We write $G = G_1 \cap G_2$.

Ring sum of graphs: $G = (V, E)$ where $V = V_1 \cup V_2$ and $E = (E_1 \cup E_2) \setminus (E_1 \cap E_2)$. We write $G = G_1 \oplus G_2$

Complement of a graph: Let g be any subgraph of G. Then $G \oplus g$ is a subgraph of G which remains after removing all the edges of g from G. So $G \oplus g$ is written as $G - g$, whenever $g \subseteq G$. So $G \oplus g = G - g$ is often called the complement of g in G.

Decomposition of a graph: (i) $g_1 \cup g_2 = G$, and (ii) $g_1 \cap g_2 = \phi$ (a null graph), where g_1 and g_2 are subgraphs of G.

Fusion of two vertices in a graph: Two vertices are replaced by a single new vertex such that every edge that is incident on either of the vertices or on both is incident on the new vertex.

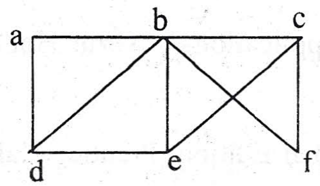
Arbitrarily traceable graph: Let G be a graph and v a vertex. The graph is said to be arbitrarily traceable graph from the vertex v if an Euler line is always obtained when one follows any walk from the vertex v according to the single rule that whenever one arrives at a vertex one shall select any edge (which has not been previously traversed).

12.6 ANSWERS TO SELF ASSESSMENT QUESTIONS

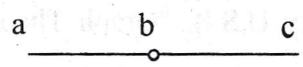
1: G_1: The graph G_1 contains no Euler line. So it is not an Euler graph.
G_2: The graph G_2 has an Euler line "1 3 5 4 3 2 1". So G_2 is an Euler graph.

2: We observe that G is connected and that $d(v_1) = d(v_7) = d(v_3) = d(v_9) = 2$
$d(v_2) = d(v_4) = d(v_8) = d(v_6) = 4$ and $d(v_5) = 6$.
Since the degree of every vertex is even, by Theorem 12.1.5 G is an Euler graph and the Euler line in G is given by: $v_1\ v_2\ v_3\ v_6\ v_9\ v_8\ v_7\ v_4\ v_2\ v_5\ v_8\ v_6\ v_5\ v_4\ v_1$.

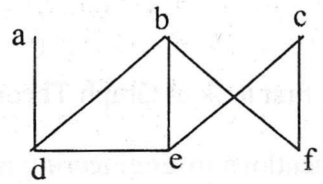
3:



$G_1 \cup G_2$



$G_1 \cap G_2$



$G_1 \oplus G_2$

12.7 MODEL QUESTIONS

1. Explain the terms given below with examples
   (i). Euler line and Euler graph; and (ii). Unicursal line and Unicursal graph.

2. Define the terms given below and provide atleast two examples for each
   (i). Union of graphs; (ii). Intersection of graphs; (iii). Ring sum of graphs; and (iv). Complement of a sub graph in a graph G

3. Explain the terms (i). decomposition of a graph; (ii). Deletion of a vertex from a graph; (iii). fusion of two vertices in a graph; and (iv). arbitrarily traceable graph from a vertex.

4. Prove the a given connected graph G is an Euler graph $\Leftrightarrow$ all the vertices of G are of even degree.

5. Show that the graph of Koningsberg bridges problem is not an Euler graph.

6. Prove that a connected graph G is an Euler graph $\Leftrightarrow$ it can be decomposed into circuits.

7. State and prove a necessary and sufficient condition for an Euler graph G to be arbitrarily traceable from a vertex v in G.

12.8 REFERENCE BOOKS

1. Bondy J.A and Murty U.S.R, "Graph Theory with applications", North Holland, New York (1976).

2. Douglas B. West "Introduction to Graph Theory", Second Edition, Prentice Hall of India, New Delhi, 2002.

3. Harary Frank. "Graph Theory", Addison - Wesley Publishing Company, Inc., Reading, Mass., 1969.

4. John Clark and Derek Allan Holton, "A first look at Graph Theory" Allied Publishers, 1995

5. Narsingh Deo "Graph theory with applications to Engineering and Computer Science", Prentice Hall of India Pvt., Ltd., New Delhi, 1993.

6. Satyanarayana Bhavanari and Syam Prasad Kuncham "Graph Theory for Beginners", Satyasri Maths Study Centre, Guntur, AP, 2003.

Name of the Author of this Lesson: **Mr. J. L. Ram Prasad**

LESSON - 13

HAMILTONIAN GRAPHS

Objectives

The objectives of this lesson are to:

- study different concepts like Hamiltonian circuits and complete graphs and to distinguish Hamiltonian circuits.
- study a necessary and sufficient condition for a simple graph G to have a Hamiltonian circuit.
- study a characterization stating the number of edge disjoint Hamiltonian circuits in a complete graph with odd number of vertices.
- know the application of Hamiltonian circuit, the travelling salesman problem
- know the solution of the seating arrangement problem

Structure

13.0 INTRODUCTION

In the previous lesson, we studied that, the concepts of Euler lines mainly deal with the nature of connectivity in graphs. And also, these concepts have application to the area of puzzles and games. The concept of Hamiltonian circuits came from a game, called the Icosian puzzle (Also called city - route puzzle), invented in 1857 by the Irish Mathematician Sir William Rowan Hamilton. We also studied some applications like travelling salesman problem and seating arrangement problem.

13.1. HAMILTONIAN PATHS AND CIRCUITS

13.1.1 Definition: In a connected graph, a closed walk running through every vertex of G exactly once (except the starting vertex at which the walk terminates) is called a **Hamiltonian circuit**. A graph containing a Hamiltonian circuit is called a Hamiltonian graph.

13.1.2 Example: Observe the graph given in Figure 13.1.2.
In this graph, the walk $e_1, e_2, e_3, e_4, e_5, e_6, e_7, e_8$ is a closed walk running through every vertex of G exactly once.Hence, this walk is a Hamiltonian circuit.

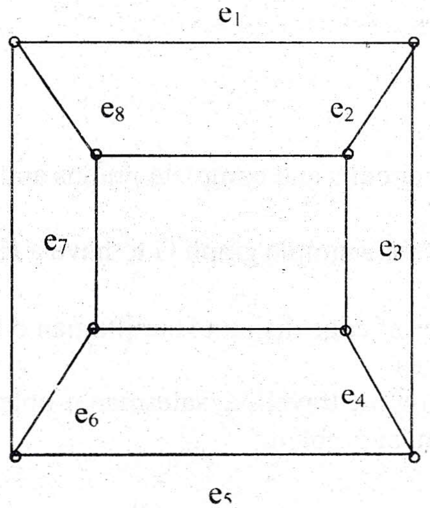


Fig-13.1.2

Hence, this graph is an Hamiltonian graph.

13.1.3 Note (i) A Circuit in a connected graph G is a Hamiltonian circuit ⇔ it includes every vertex of G.
(ii) A Hamiltonian circuit in a graph of 'n' vertices consists of exactly 'n' edges.

13.1.4 Note: Every connected graph may not have a Hamiltonian circuit.

13.1.5 Example: Both the two graphs given in Figures 13.1.5A and B are connected, but they do not have Hamiltonian circuits.

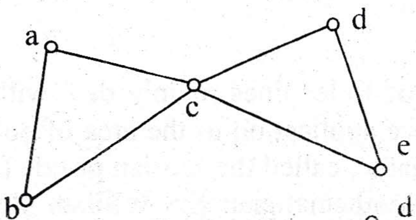


Fig-13.1.5 A

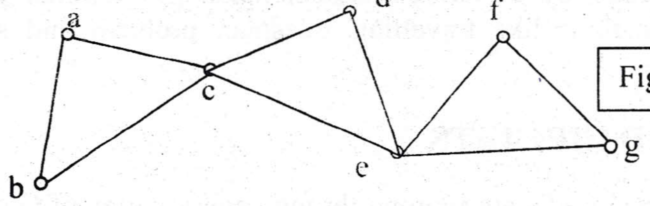
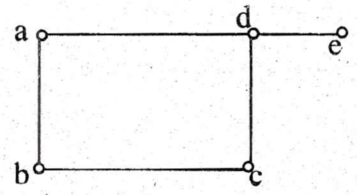
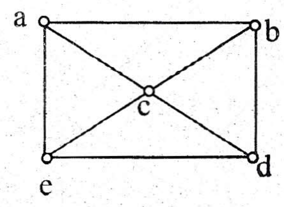


Fig-13.1.5B

Self Assessment Question 1: *Which of the following graphs are Hamiltonian.*



G_1



G_2

13.1.6 City-Route Puzzle: Hamilton made a regular dodecahedron of wood (please see the graph given here) whose 20 corners were marked with the names of cities, and the routes are the edges of the graph.

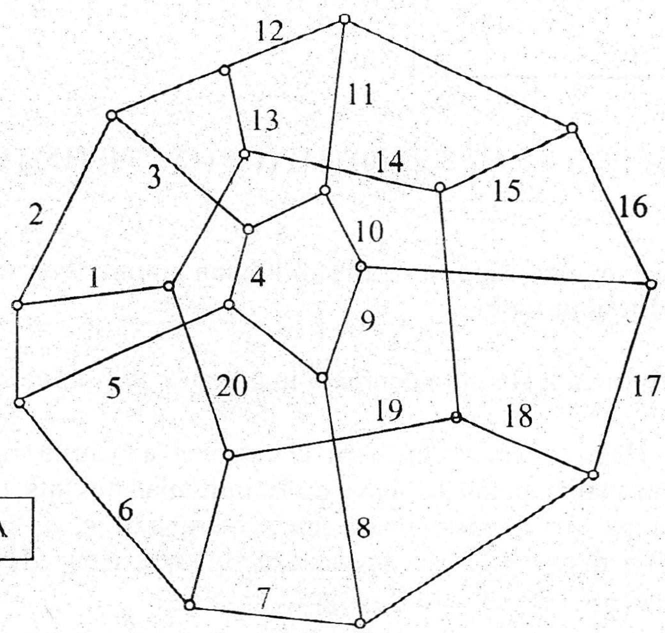


Fig-13.1.6 A

Now the problem is to start from a city and find a route along the edges of the dodecahedron, that passes through every city exactly once and return to the city of origin.
The graph of dodecahedron is given in Fig-13.1.6 A.
This can be represented by the graph given in Fig-13.1.6 B.

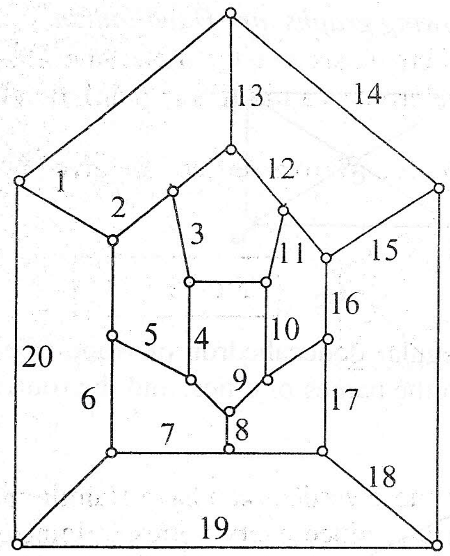


Fig-13.1.6 B

Here the closed walk (of edges) 1 2 3 4 5 6 7 8 9 (10) (11) (12) (13) (14) (15) (16) (17) (18) (19) (20) is a Hamiltonian circuit.

13.1.7 Definition: Ii we remove any one edge from a Hamiltonian circuit, then we are left with a path. This path is called a **Hamiltonian path.**

13.1.8 Note: (i) Clearly by definition, a Hamiltonian path in a graph G traverses through every vertex of G.

(ii) If a graph G that contains a Hamiltonian circuit, then G contains a Hamiltonian path.

(iii) There exists graph with Hamiltonian paths that have no Hamiltonian circuits.

(iv) The length of a Hamiltonian path (if it exists) in a connected graph of n vertices, is 'n-1'.

(v) In a Hamiltonian circuit (or) path every vertex appears exactly once. Hence Hamiltonian circuit (or path) cannot include a self-loop or a set of parallel edges.

Self Assessment Question 2: *Draw a graph with six vertices which is Hamiltonian but not Eulerian.*

13.1.9 Note: (i) Let G be a given graph and we wish to find whether a Hamiltonian circuit exists in G or not.

In such a case, to identify the Hamiltonian circuit (in an easy way), first remove all the self-loops. If there are multiple edges between any two vertices a and b, remove all the edges between a and b except one edge. Then the remaining graph G^* (a subgraph of G) is a simple graph. Now it is easier to identify a Hamiltonian circuit (or path) in G^*. It is clear that Hamiltonian path exists in G^* $\Leftrightarrow$ Hamiltonian path exists in G.

(ii) What is a necessary and sufficient condition for a connected graph G to have a Hamiltonian circuit?

The problem was first posed by the famous Mathematician Sir William Roman Hamiltnion in 1859. and is still unsolved.

13.1.10 Definition: A simple graph in which there exists an edge between every pair of vertices is called a **complete graph**. It is also sometimes referred as a **universal graph or a Clique.**

13.1.11 Example: Complete graphs of two, three, four & five vertices are given in the Fig-13.1.11.

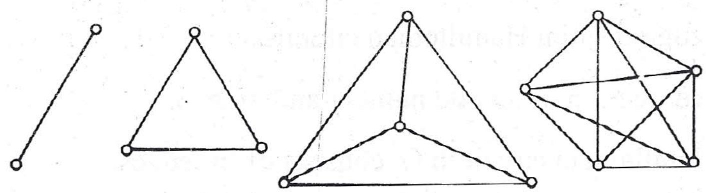


Fig-13.1.11

13.1.12 Note: (i) Complete graphs with three or more vertices can have Hamiltonian circuits.

(ii) Let G be a complete graph with n vertices. Since every vertex is joined with every other vertex and there are no multiple edges, we have that the degree of every vertex is n-1. The total number of edges in G is $\frac{n(n-1)}{2}$.

13.2. FORMATION OF HAMILTONIAN CIRCUITS IN A COMPLETE GRAPH

13.2.1 Note We can construct a Hamiltonian circuit in a complete graph of 'n' vertices (with $n \geq 3$). Suppose the vertices are $v_1, v_2, \ldots, v_n$. Since an edge exists between any two vertices, we can start from v_1 and traverse to v_2, and then from v_2 to v_3, and finally v_n to v_1. Now $\overline{v_1v_2}$, $\overline{v_2v_3}, \ldots, \overline{v_{n-1}v_n}, \overline{v_nv_1}$ is a Hamiltonian circuit.

13.2.2 Note: A given graph may contain more than one Hamiltonian circuits. The determination of the exact number of edge-disjoint Hamiltonian circuits (or paths) in a graph (in general) is an unsolved problem.

13.2.3 Example: Consider the graph given in Fig-13.2.3.

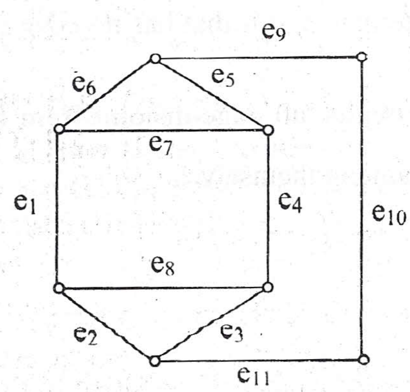


Fig-13.2.3

(i) $e_1, e_7, e_5, e_9, e_{10}, e_{11}, e_3, e_8$ is a Hamiltonian circuit.
(ii) $e_4, e_7, e_6, e_9, e_{10}, e_{11}, e_2, e_8$ is also a Hamiltonian circuit.
(iii) These two Hamiltonian circuits are not edge disjoint.

13.2.4 Theorem: Let G be a complete graph with 'n' vertices, where n is an odd number greater than or equal to 3. Then there are $\frac{(n-1)}{2}$ edge-disjoint Hamiltonian circuits.

Proof: Let G be a complete graph of 'n' vertices, n is an odd number and $n \geq 3$.

Then clearly it has $\frac{n(n-1)}{2}$ edges and a Hamiltonian circuit in G consists of 'n' edges.

Therefore, the number of edge-disjoint Hamiltonian circuits in G cannot exceed $\frac{(n-1)}{2}$.

Now we show that there exists $\frac{(n-1)}{2}$ edge-disjoint Hamiltonian circuits, when 'n' is odd and $n \geq 3$.

The subgraph (of a complete graph of 'n' vertices) given in the Fig-10.4A, is a Hamiltonian circuit.

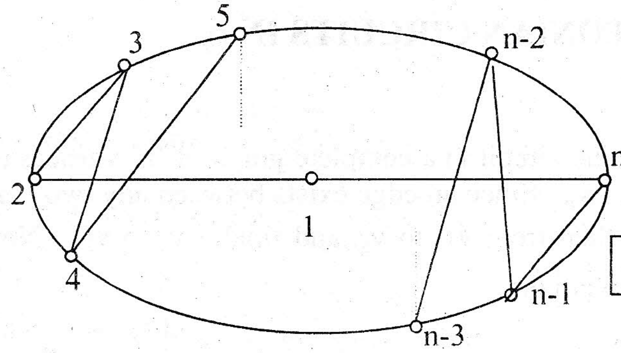


Fig-13.2.4A

Keeping the vertices fixed on a circle, rotate the polygon pattern clockwise by

$$\frac{360}{(n-1)},\ 2.\frac{360}{(n-1)},\ 3.\frac{360}{(n-1)},\ldots,\frac{(n-3)}{2}\frac{360}{(n-1)} \text{ degrees.}$$

Observe that each rotation produces a Hamiltonian circuit that has no edge in common with any of the previous ones.

Thus we have $\frac{(n-3)}{2}$ new Hamiltonian circuits, all edge-disjoint from the Hamiltonian circuit given in Fig-13.2.4A, and also edge-disjoint among themselves.

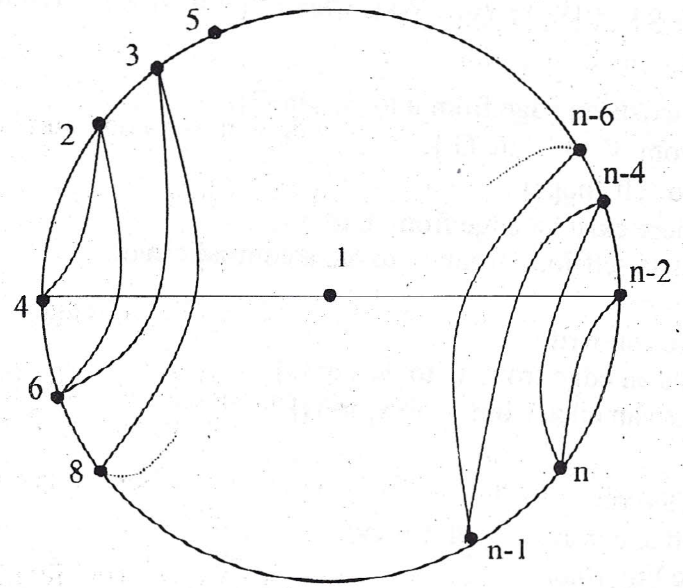


Fig-13.2.4B

Hence the theorem.

13.2.5 Note: This theorem can used to solve "the seating arrangement problem at a Round table" introduced in Chapter1.

13.2.6 Theorem:(Dirac, 1952) If G is a simple graph with n vertices, where $n \geq 3$, and $d(v) \geq \frac{n}{2}$ for every vertex v of G, then G is Hamiltonian.

Proof: part-(i): In a contrary way, we suppose that there exists a graph G which is not a **Hamiltonian graph** with $n \geq 3$ and every vertex has degree at least $\frac{n}{2}$.

Any spanning super graph (that is, with precisely the same vertex set) also has the property that $d(v) \geq \frac{n}{2}$ (because any proper super graph of this form can be obtained by introducing extra edges).

Thus there will be a maximal non-Hamiltonian graph G with n vertices and $d(v)\,) \geq \frac{n}{2}$ for every vertex v in G.

We take such a maximal non-Hamiltonian graph G.

Part-(ii): If G is complete, then by a known result, G is Hamiltonian, a contradiction. There fore G can not be complete. Since G is not complete, there are two non-adjacent vertices u, v in G.

Let G + uv denote the supergraph of G obtained by introducing an edge $\overline{uv}$ from u and v.

Since G is maximal non-Hamiltonian and G + uv is proper supergraph of G, we have that G +uv is Hamiltonian.

Let C be a Hamiltonian circuit in G +uv. Now uv is in C (otherwise, this circuit C is in G $\Rightarrow$ G is Hamiltonian, a contradiction). Suppose C = ($v_1\, v_2\, v_3 \ldots v_n v_1$) where $v_1 = u$, $v_n = v$. (Note that vu = $v_n v_1$).

Part-(iii): Write S = { $v_i \in C$ / there exists an edge from u to v_{i+1} in G}.
T = { $v_j \in C$ / there exists an edge from v to v_j in G }.
Now $v_n = v \notin T$ (since G contains no self-loops).
$v = v_n \notin S$ (If $v = v_n \in S$, then there exist an edge from u to v_{n+1}.
Here in circuit $v_{n+1} = u$. So there exists self-loop from u to u, a contradiction).
$v = v_n \notin S \cup T$. Therefore $|S \cup T| < n$.
Since C contains all vertices of G, we can write
S = {v_i is a vertex in G / there exists an edge from u to v_{i+1} in G}
T = { v_j is a vertex in G / there exists an edge from v to v_j in G}
Therefore $|S| = d(u)$ and $|T| = d(v)$.

Part-(iv): Now we verify that $S \cap T = \phi$.
If $v_k \in S \cap T$, then there exists an edge $e = uv_{k+1}$ and $f = vv_k$.
Then we have the graph given in the Fig-10.8.
Now $C^1 = v_1\, v_{k+1}\, v_{k+2} \ldots v_{n-1}\, v_n\, v_k\, v_{k-1} \ldots v_2 v_1$ is a Hamiltonian cycle in G, a contradiction.
Therefore $S \cap T = \phi$, So $|S \cup T| = |S| + |T|$.
Now $d(u) + d(v) = |S| + |T| = |S \cup T| < n$

$\Rightarrow n > d(u) + d(v) \geq \frac{n}{2} + \frac{n}{2} = n \Rightarrow n > n$, a contradiction.

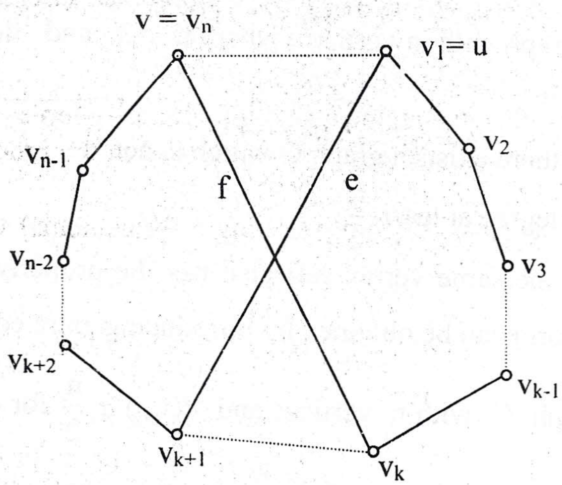


Fig-13.2.6

This completes the proof.

13.2.7 Theorem: Let G be a simple graph with n vertices, and let u and v be non-adjacent vertices in G such that $d(u) + d(v) \geq n$. Let G + uv denotes the super graph of G obtained by joining u and v by an edge. Then G is Hamiltonian $\Leftrightarrow$ G + uv Hamiltonian.

Proof: It is clear that G is Hamiltonian

$\Rightarrow$ it's supergraph $G + uv$ of G is Hamiltonian.

Converse: Suppose that $G + uv$ in Hamiltonian.
In a contrary way, suppose that G is not Hamiltonian. As in the proof of above theorem, we get that $d(u) + d(v) < n$, a contradiction to the hypothesis that $d(u) + d(v) \geq n$.
This shows that G must be Hamiltonian.

Self Assessment Question 3: *Draw a graph with 6 vertices which is Eulerian and non-Hamiltonian*

13.3. THE SEATING ARRANGEMENT PROBLEM

13.3.1: Consider the seating arrangement problem. First we construct the graph of this problem.

(i) Represent a member 'x' by a vertex, and the possibility of sitting next to another member 'y' by an edge between x and y.

(ii) Every member is allowed to sit next to any other member. So G is a complete graph of nine vertices. (Here 'nine' is the number of people to be seated around the table). Clearly every seating arrangement around the table is a Hamiltonian circuit.

(iii) On the first day of their meeting, they can sit in any order, and it will be a Hamiltonian circuit (H_1, say).

On the second day, they are to sit such that every member must have different neighbors. So we have to find another Hamiltonian circuit (H_2, say) in G, with an entirely different set of edges from those in H_1 (that is, H_1 and H_2 are edge-disjoint Hamiltonian circuits).

(iv) But by the Theorem 13.2.4, we know that the number of edge-disjoint Hamiltonian circuits in G is $\frac{(n-1)}{2} = \frac{(9-1)}{2} = 4$.

Therefore we can conclude that there exist 'four' such arrangements among 'nine' people. The Figures 13.3.1 A, B, C and D, were obtained by following the procedure mentioned in the proof of the Theorem 13.2.4. Observe that Fig-13.3.1 E is same as Fig-13.3.1A.
There fore all the four distinct Hamiltonian circuits (that is, different seating arrangements) were shown in the 5 ;ures-13.3.1 A, B, C and D.

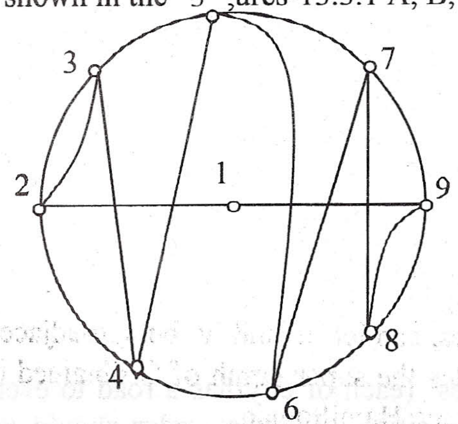


Fig-13.3.1 A

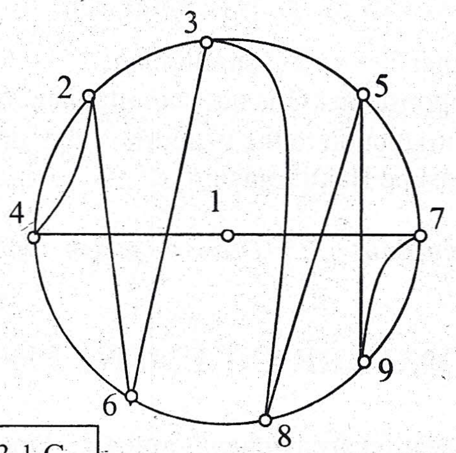


Fig-13.3.1 B

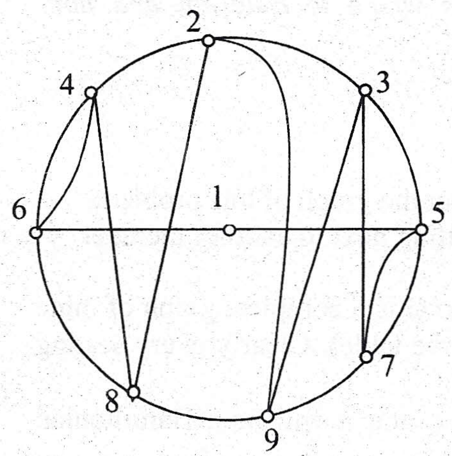


Fig-13.3.1 C

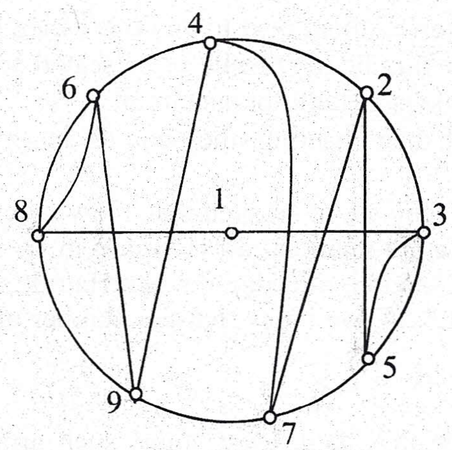


Fig-13.3.1 D

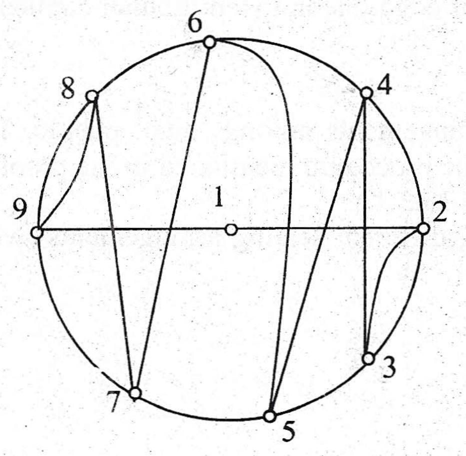


Fig-13.3.1 E

13.4. TRAVELLING - SALESMAN PROBLEM

13.4.1: This problem is related to Hamiltonian circuits.

<u>The Problem</u>: A salesman required to visit a number of cities (each of city has a road to every other city) during his trip. Given the distances between the cities. In what order should the salesman travels so as to visit every city precisely once and return to his home city, with the minimum mileage travelled?

Solution: (i) Represent the cities by vertices, and the roads between them by edges. Then we get a graph. In this graph, for every edge 'e' there corresponds a real number w(e) *(the distance in miles,* say). Such a graph is called a **weighted graph**. Here w(e) is called as the **weight** of the edge 'e'.

(ii) If each of the cities has a road to every other city, we have a complete weighted graph. This graph has numerous Hamiltonian circuits, and we are to select the Hamiltonian circuit that has the smallest sum of distances (or weights).

(iii) The number of different Hamiltonian circuits (may not be edge-disjoint) in a complete graph of 'n' vertices is equal to $\frac{(n-1)!}{2}$.

[**Reason**: Start from a vertex.
To go from the first vertex to second vertex, we can chose any one of the (n-1) edges.
To go from the second vertex to third vertex, we can chose any one of the (n-2) edges.
To go from the third vertex to forth vertex, we can chose any one of the (n-3) edges, and so on. Since these selections are independent, and each Hamiltonian circuit has been counted twice, we have that the number of
Hamiltonian circuits is $\frac{(n-1)(n-2).....2.1}{2} = \frac{(n-1)!}{2}$.

(iv) First we list all the $\frac{(n-1)!}{2}$ Hamiltonian circuits that are possible in the given graph. Next calculate the distance traveled on each of these Hamiltonian circuits. Then select the Hamiltonian circuit with the least distance. This provides a solution for the Travelling salesman problem.

13.5 SUMMARY

In this lesson we discussed Hamiltonian circuit, which is defined as a closed walk that traverses through every vertex exactly once. . Where as Euler line is a closed walk that traverses every edge of the graph exactly once. We also provided a variety of examples for all these concepts. We studied sufficient condition for a simple graph G to have a Hamiltonian circuit and also we studied a Theorem which gives the number of edge disjoint Hamiltonian circuits in a complete graph with odd number 'n' of vertices, and $n \geq 3$. These concepts enables us to find solutions of the city route puzzle, the seating arrangement problem and the travelling salesman problem.

13.6 TECHNICAL TERMS

Hamiltonian circuit: A closed walk running through every vertex of G exactly once, (except the starting vertex at which the walk terminates)

Hamiltonian path: A path obtained on the removal of any edge from a Hamiltonian circuit.

13

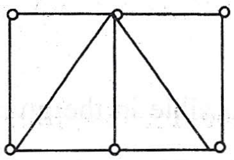
Complete Graph : A simple graph in which there exists an edge between every pair of vertices.

Weighted graph: The graph in which for every edge 'e' there corresponds a real number w(e), called the weight of 'e'.

13.7 ANSWERS TO SELF ASSESSMENT QUESTIONS

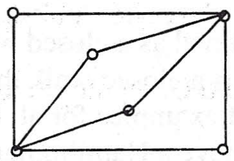
1. G_1: The graph G_1 do not have a Hamiltonian circuit so G_1 is not a Hamiltonian graph..
G_2: The graph G_2 contains a Hamiltonian circuit. So G_2 is a Hamiltonian graph.

2.



Hamiltonian and Non-Eulerian

3.



Eulerian and Non- Hamiltonian

13.8 MODEL QUESTIONS

1. Define the terms and give two examples for each (i). Hamiltonian circuits; (ii). Hamiltonian path; (iii). Complete Graph; and (iv). Weighted graph.

2. Let G be a complete graph with 'n' vertices, where n is an odd number greater than or equal to 3. Then prove that there are $\frac{(n-1)}{2}$ edge-disjoint Hamiltonian

3. If G is a simple graph with n vertices, where $n \geq 3$, and $d(v) \geq \frac{n}{2}$ for every vertex v of G, then prove that G is Hamiltonian.

4. Let G be a simple graph with n vertices, and let u and v be non-adjacent vertices in G such that $d(u) + d(v) \geq n$. Let G + uv denotes the super graph of G obtained by joining u and v by an edge. Then prove tht G is Hamiltonian $\Leftrightarrow$ G + uv Hamiltonian

5. State and find the solutions of
(i). City route puzzle; (ii). The seating arrangement problem; and (iii). Travelling Salesman problem.

13.9 REFERENCE BOOKS

1. Bondy J.A and Murty U.S.R, "Graph Theory with applications", North Holland, New York (1976).

2. Douglas B. West "Introduction to Graph Theory", Second Edition, Prentice Hall of India, New Delhi, 2002.

3. Harary Frank. "Graph Theory", Addison - Wesley Publishing Company, Inc., Reading, Mass., 1969.

4. John Clark and Derek Allan Holton, "A first look at Graph Theory" Allied Publishers, 1995

5. Narsingh Deo "Graph theory with applications to Engineering and Computer Science", Prentice Hall of India Pvt., Ltd., New Delhi, 1993.

6. Satyanarayana Bhavanari and Syam Prasad Kuncham "Graph Theory for Beginners", Satyasri Maths Study Centre, Guntur, AP, 2003.

Name of the Author of this Lesson: **Mr. J. L. Ram Prasad**

LESSON - 14

TREES

Objectives

The objectives of this lesson are to:

- study connected graphs without any circuits (called trees) and some properties of trees.
- know the significance of the terms like "distance", "center", and "diameter" in a tree.
- introduce the "metric" in a connected graph.
- learn about the role of pendant vertices of trees.

Structure

14.0 INTRODUCTION

Trees are extensively used as models in areas like computer science, chemistry, geology, electrical networks and botany etc. We shall now describe such model based on trees. In saturated hydrocarbons, the molecules, where atoms are represented by vertices and bonds between them by edges. In graph models of saturated hydrocarbons, each carbon atom represented by a vertex of degree 4, and hydrogen atom is represented by a vertex of degree 1. So there are 3n + 2 vertices in a graph representing a compound of the form $C_n H_{2n+2}$. Trees are also useful in design of wide range of algorithms.

14.1 TREES

The concept of a 'tree' plays a vital role in the theory of graphs. First we introduce the definition of 'tree', study the some of its properties and its applications. Later, in the next lesson we introduce the concept of 'spanning tree', and study the relationships among circuits and trees.

14.1.1 Definition: A connected graph without circuits is called a **tree.**

14.1.2 Example: Trees with one, two, three and four vertices are given in the Fig-14.1.2.

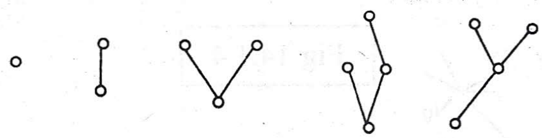


Fig-14.1.2

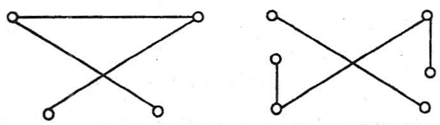
14.1.3 Note: (i) Since a tree is a graph, we have that a tree contains at least one vertex.

(ii) A tree without any edge is referred to as a **null tree.**

(iii) Since we are considering only finite graphs, we have that the trees considered are also finite.

(iv) A tree is always a simple graph.

Self Assessment Question 1: *Which of the following graphs are trees.*



G_1 G_2

14.1.4 Examples: (i) The list of the ancestors of a family, may be represented by a tree. This tree referred to as a **family tree.**

(ii) A river with its tributaries and sub-tributaries may be represented by a tree. This tree is referred to as a **river tree.**

(iii) The sorting of mail according to zip code are done according to a tree. This tree is called **decision tree** (or) **sorting tree.**

The tree given in the Fig-14.1.4, represents the flow of mail. Suppose that all the mail arrives at some local office, say vertex N. For example, take a letter with zip code 522 510.

The most significant digit in the zip code is read at N, and the mail is divided into ten piles $N_0, N_1, N_2, \ldots N_9$ depending on the most significant digit.

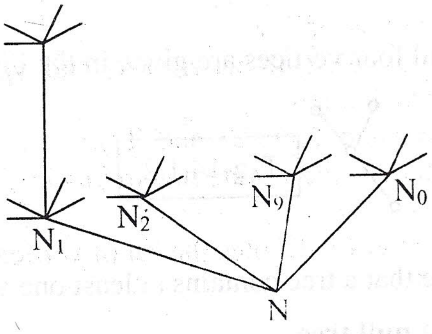


Fig-14.1.4

(For this example, the most significant digit is 5. So this card will be kept in 5^{th} pile).
Each of these piles will be further divided into ten piles according to the second most significant digit, and so on. This will be done up to the mail is subdivided into 10^6 possible piles, each representing a unique six-digit zip code.

***Self Assessment Question 2:** Draw all trees with five vertices*

14.2 SOME PROPERTIES OF TREES

14.2.1 Theorem In a tree T, there is one and only one path between every pair of vertices.
Proof: Suppose T is a tree. Then T is a connected graph and contains no circuits.
Since T is connected, there exists at least one path between every pair of vertices in T.
Suppose that between two vertices a and b of T, there are two distinct paths.
Now, the union of these two paths will contain a circuit in T, a contradiction (since T contains no circuits).
This shows that there exists one and only one path between a given pair of vertices in T.

14.2.2 Theorem: If there is one and only one path between every pair of vertices in G, then G is a tree.
Proof: Let G be a graph.
Assume that there is one and only one path between every pair of vertices in G.
This shows that G is connected.
If possible suppose that G contains a circuit.
Then there is at least one pair of vertices a, b such that there are two distinct paths between a and b. But this is a contradiction to our assumption.
So G contains no circuits. Thus G is a tree.

14.2.3 Theorem: A tree G with 'n' vertices has (n-1) edges.
Proof: We prove this theorem by induction on the number vertices n.
If n = 1, then G contains only one vertex and no edge.
So the number of edges in G is $n - 1 = 1 - 1 = 0$.

Suppose the induction hypothesis that the statement is true for all trees with less than 'n' vertices.
Now let us consider a tree with 'n' vertices.
Let 'e_k' be any edge in T whose end vertices are v_i and v_j.
Since T is a tree, by Theorem 14.2.1, there is no other path between v_i and v_j.
So by removing e_k from T, we get a disconnected graph.
Furthermore, T- e_k consists of exactly two components(say T_1 and T_2).
Since T is a tree, there were no circuits in T and so there were no circuits in T_1 and T_2.
Therefore T_1 and T_2 are also trees.
It is clear that $|V(T_1)| + |V(T_2)| = |V(T)|$ where V(T) denotes the set of vertices in T.

Also $|V(T_1)|$ and $|V(T_2)|$ are less than n.

Therefore by the induction hypothesis, we have

$$|E(T_1)| = |V(T_1)| - 1 \text{ and } |E(T_2)| = |V(T_2)| - 1.$$

Now $|E(T)| - 1 = |E(T_1)| + |E(T_2)| = |V(T_1)| - 1 + |V(T_2)| - 1$

$$\Rightarrow |E(T)| = |V(T_1)| + |V(T_2)| - 1$$

$$= |V(T)| - 1 = n-1.$$

This completes the proof.

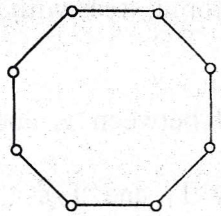
14.2.4 Theorem: Any connected graph with 'n' vertices and n -1 edges is a tree.

Proof: Let 'G' be a connected graph with n vertices and n - 1 edges. It is enough to show that G contains no circuits.
If possible, suppose that G contains a circuit.
Let 'e' be an edge in that circuit.
Since 'e' in a circuit, we have that G - e is still connected.
Now G - e is connected with 'n' vertices, and so it should contain at least n -1 edges, a contradiction (to the fact that G - e contain only (n-2) edges).
So G contains no circuits. Therefore G is a tree.

14.2.5 Definition: A connected graph is said to be **minimally connected** if the removal of any one edge from the graph provides a disconnected graph.

14.2.6 Example: (i) Graph-1 given in Fig-14.2.6A is not minimally connected.
(ii) Graph-2 given in Fig-14.2.6B is minimally connected.
(iii) Any circuit is not minimally connected.
(iv) Every tree is minimally connected.

Fig-14.2.6 A
Graph -1



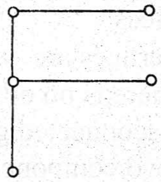


Fig-14.2.6 B
Graph -2

14.2.7 Theorem: A graph G is a tree $\Leftrightarrow$ it is minimally connected.

Proof: Assume that G is a tree.
Now we have to show that G is minimally connected.
In a contrary way, suppose that G is not minimally connected.
Then there exists an edge 'e' such that $G - e$ is connected.
That is, e is in some circuit, which implies G is not a tree, a contradiction.
Hence G minimally connected.
Converse: Suppose that G is minimally connected.
Now it is enough to show that G contains no circuits.
In a contrary way, suppose G contains a circuit.
Then by removing one of the edges in the circuit, we get a connected graph, a contradiction (to the fact that the graph is minimally connected).
This shows that G contains no circuits. Thus G is a tree.

14.2.8 Note: To interconnect 'n' given distinct points, the minimum number of line segments needed is $n - 1$.

14.2.9 Theorem: If a graph G contains n vertices, $n - 1$ edges and no circuits, then G is a connected graph.

Proof: Let G be a graph with 'n' vertices, $n - 1$ edges and contains no circuits.
In a contrary way, suppose that G is disconnected.
G consists of two or more circuitless components (say, $g_1, g_2, \ldots, g_k$).
Now $k \geq 2$. Select a vertex v_i in g_i, for $1 \leq i \leq k$.

Add new edges $e_1, e_2, \ldots, e_{k-1}$ where $e_i = \overline{v_i v_{i+1}}$ to get a new graph G^*.
It is clear that G^* contains no circuits and connected, and so G^* is a tree.
Now G^* contains n vertices and $(n - 1) + (k - 1) = (n + k - 2) \geq n$ edges, a contradiction (since a tree contains $(n - 1)$ edges).
This shows that G is connected.
This completes the proof.

14.2.10 Theorem: For a given graph G, with n vertices the following conditions are equivalent:

(i) G is connected and is circuitless;

(ii) G is connected and has $n-1$ edges;

(iii) G is circuitless and has $n-1$ edges;

(iv) There is exactly one path between every pair of vertices in G;

(v) G is a minimally connected graph; and

(vi) G is a tree.

Proof: (i) $\Leftrightarrow$ (vi) is clear.

(vi) $\Rightarrow$ (ii) and (iii): Theorem 14.2.3

(ii) $\Rightarrow$ (vi): Theorem 14.2.4

(iii) $\Rightarrow$ (vi): Theorem 14.2.9.

(iv) $\Leftrightarrow$ (vi): Theorems 14.2.1 and 14.2.2

(v) $\Leftrightarrow$ (vi): Theorem 14.2.7

14.3 PENDANT VERTICES IN A TREE

Recall that a **pendant vertex** is a vertex of degree 1.

14.3.1 Theorem: If T is a tree (with two or more vertices), then there exists at least two pendant vertices.

Proof: Let T be a tree with $|V| \geq 2$.

Let $v_0e_1v_1e_2v_2e_3 \ldots v_{n-1}e_nv_n$ be a longest path in T (Since T is finite graph, it is possible to find a longest path).

Now we wish to show that $d(v_0) = 1 = d(v_n)$.

If $d(v_0) > 1$, then there exists at least one edge e with end point v_0 such that $e \neq e_1$.

If $e \in \{e_1, e_2, \ldots e_n\}$, then $e = e_i$ for some $i \neq 1$.

So either $v_{i-1} = v_0$ or $v_i = v_0$ $\Rightarrow$ v_0 repeated in the path, a contradiction.

Hence $e \notin \{e_1, e_2, e_3, \ldots e_n\}$.

Now $e, e_1, e_2, e_3, \ldots e_n$ is a path of length $n+1$, a contradiction.

Hence $d(v_0) = 1$.

In a similar way, we can show that $d(v_n) = 1$.

Hence v_0, v_n are two pendant vertices.

14.3.2 Example: (An Application): Given a sequence of integers, no two of which are equal. We have to find the largest monotonically increasing subsequence in it. Suppose that the given sequence is 4, 13, 7, 2, 8, 11. It can be represented by a tree in which

(i) The vertices (except the starting vertex) represent individual numbers in the given sequence, and

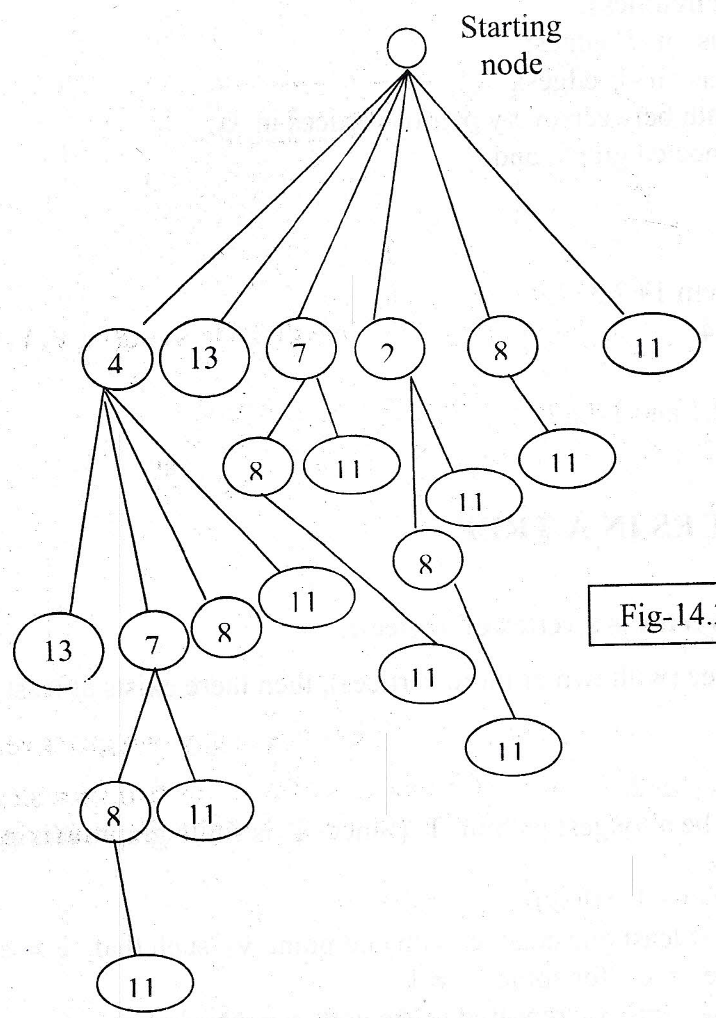


Fig-14.3.2

(ii) a path from the start vertex to a particular vertex 'v' describes the monotonically increasing subsequence terminating in v.

As shown in the Fig-14.3.2, this sequence contains one longest monotonically increasing subsequence (4,7,8,11). It is of length 4. Such a tree used in representing the data is referred to as **data tree** by the computer programmers.

14.4 DISTANCE

14.4.1 Definition: Let G be a connected graph. The **distance** between two vertices v and u is denoted by d(v, u) and is defined as the length of the shortest path [that is, the number of edges in the shortest path] between v and u.

14.4.2 Example: Consider the connected graph given in Fig-14.4.2.

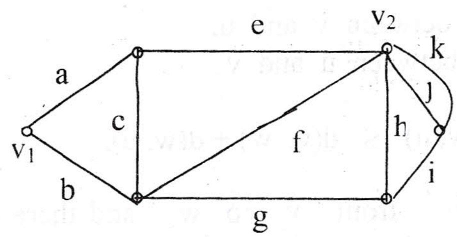


Fig-14.4.2

Here some of the paths between v_1 and v_2 are (a, e), (a, c, f), (b, c, e), (b, f), (b, g, h), (b, g, i, j), (b, g, i, k)
Here there are two shortest paths (a, e) and (b, f) each of length 2. Hence $d(v_1, v_2) = 2$.

14.4.3 Example: Consider the tree given in the Fig-14.4.3.

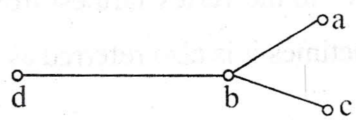


Fig-14.4.3

Here $d(a, b) = 1$, $d(a, c) = 2$, $d(a, d) = 2$, $d(b, d) = 1$.

14.4.4 Note: In a connected graph, we can find the distance between any two given vertices.

14.4.5 Definition: Let X be a set. A real valued function $f(x, y)$ of two variables x and y (that is, $f : X \times X \to R$ where R is the set of all real numbers) is said to be a **metric** on X if it satisfies the following properties.

(i) Non- negativity: $f(x, y) \geq 0$, and $f(x, y) = 0 \Leftrightarrow x = y$

(ii) (Symmetry): $f(x, y) = f(y, x)$.

(iii) (Triangle inequality): $f(x, y) \leq f(x, z) + f(z, y)$ for x, y, z in X.

14.4.6 Theorem: Let G be a connected graph. The distance $d(v, u)$ between two vertices v and u is a metric.

Proof: Let $v, u \in V$
(i) $d(v, u) =$ (the length of the shortest path between v and u)
≥ 0.
Therefore $d(v, u) \geq 0$.
Also $d(v, u) = 0$
$\Leftrightarrow$ there exists a path between v and u of length 0
$\Leftrightarrow v = u$.

[if v is not equal to u, then $d(v, u) \geq 1$, a contradiction.]

So $d(v, u) = 0 \Leftrightarrow v = u$.

(ii) $d(v, u)$ = The length of the shortest path between v and u.

= The length of the shortest path between u and v.

= $d(u, v)$

(iii) Now we show that for any w in V, $d(v, u) \leq d(v, w) + d(w, u)$.

Suppose $n = d(v, w)$ and $m = d(w, u)$.

Then there exists a path of minimum length n from v to w, and there exists a path of minimum length m from w to u. Combining these two paths, we get a path from v to u of length less than or equal to $n + m$.

So $d(v, u) \leq n + m = d(v, w) + d(w, u)$

14.4.7 Definition: Let G be a graph and 'v' be any vertex in G. Then the **eccentricity** of 'v' is denoted by E(v) and is defined as the distance from v to the vertex farthest from 'v' in G. That is, $E(v) = \max \{d(v, u) / u \text{ is a vertex in } G\}$. Sometimes it is also referred as '**associate number**' (or) '**separation**'.

14.4.8 Example: Consider the graph given in Fig-14.4.8.

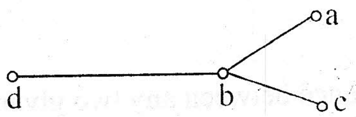


Fig-14.4.8

Here E(a) = 2, because the distance from 'a' to a vertex d farthest from 'a' is d(a, d) = 2.
Similarly E(b) = 1, E(c) = 2, E(d) = 2.

14.4.9 Note: The eccentricities of vertices of a graph may be represented as in Fig-14.4.9.

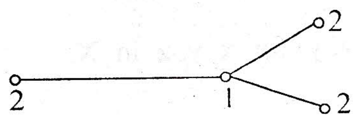


Fig-14.4.9

14.4.10 Example: Consider the tree given in Fig-14.4.10A.

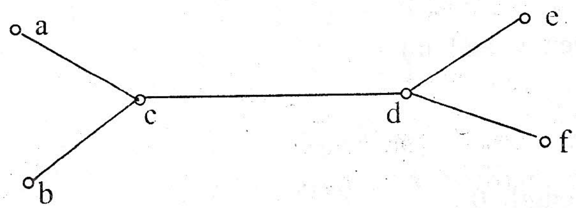


Fig-14.4.10 A

Here E (a) = 3, E (d) = 2; E (b) = 3, E (e) = 3; E(c) = 2, E (f) = 3.

The graph given in Fig-14.4.10A may be represented as the graph in Fig-14.4.10B:

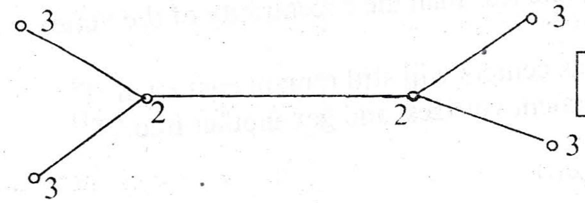


Fig-14.4.10 B

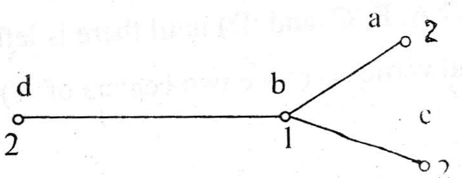
14.5 CENTERS IN A TREE

14.5.1 Definition: In a graph, a vertex with minimum eccentricity is called a **center** of the graph.

v is a center of a graph $\Leftrightarrow$ $E(v) = \min\{E(u) \,/\, u \in G\}$.

14.5.2 Example: (i) Consider the Graph-1 given in Fig-14.5.2A.

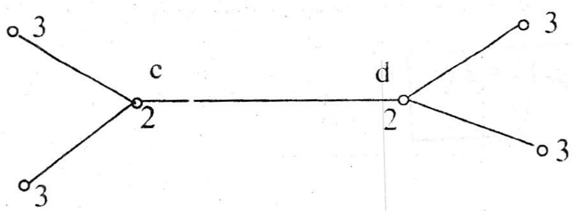
The center of this graph is b (since 'b' has the minimum eccentricity).



14.5.2 A
Graph-1

Consider the Graph-2 given Fig-14.5.2B. Here $E(c) = 2 = E(d)$.

So both c, d are centers.



14.5.2 B
Graph-2

Thus a tree may have two centers. Some authors refer to such centers as **'bicenters'**.

14.5.3 Note: In a circuit, every vertex has equal eccentricity.

14.5.4 Theorem: Every tree T has either one or two centers.

Proof: If T contains exactly one vertex, then that vertex is the center.
If T contains exactly two vertices, then these two vertices are centers.

Let T be any tree with more than two vertices.
Let $v \in V$. Now the maximum distance, $\max d(v, v_i)$ from the given vertex v to any other vertex v_i occurs only when v_i is a pendent vertex.
Then by the Theorem 14.3.1, T must have two or more pendent vertices.
Now by removing all pendent vertices from T, we get a tree T^1.

The eccentricity of a vertex v in T^1 is one less than the eccentricity of the vertex v in T. This is true for all vertices v.
Therefore all the vertices that T had as centers will still remain centers in T^1.
Now from T^1 we again remove all pendent vertices, and get another tree T^{11}.

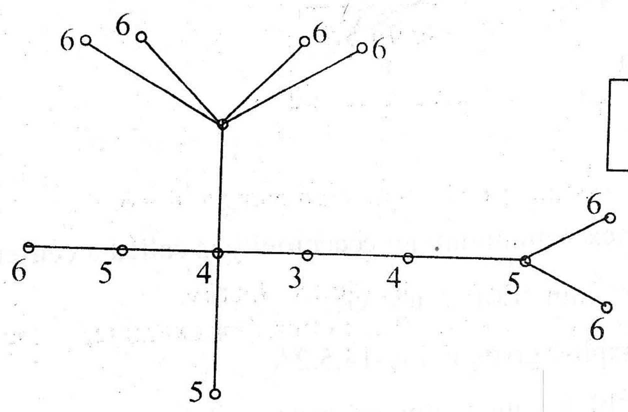


Fig-14.5.4 A
T

We continue this process (as shown in the Figures 14.5.4 A, B, C and D) until there is left either a vertex (which is the center of T) or an edge (whose end vertices are the two centers of T). Hence every tree has either one or two centers.

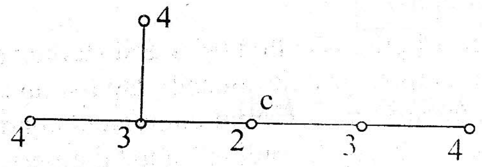


Fig-14.5.4 B
T^1

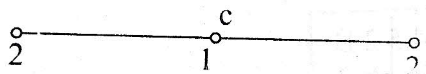


Fig-14.5.4 C
T^{11}

Center Fig-14.5.4 D

14.5.5 Corollary: From the above argument, we get that **if a tree has two centers, then the two centers must be adjacent.**

14.5.6 Definition: The eccentricity of a center in a graph (or in a tree) is called the **radius** of that graph.

14.5.7 Example: Consider the graphs T, T^1, T^{11} given in point 14.5.4. The radius of T is 3, the Radius of T^1 is 2; Radius of T^{11} is 1.

14.5.8 Definition: The length of the longest path in a tree is called **diameter** of a tree.

14.5.9 Example: (i) Consider the tree given in the Fig-14.5.9.
Clearly the diameter of T = 2, radius = 1.
The only largest paths in T are abc, abd, cbd,. (And their lengths are equal to 2).

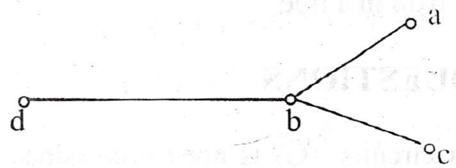


Fig-14.5.9
T

(ii) Consider the graph T given in point 14.5.9. The diameter of T = 6.

14.5.10 Problem: Is the diameter is equal to twice the radius? Justify.
Solution: The diameter is not always equal to twice the radius. For example, in the graph given in Fig-4.5.10, radius = 2, and diameter = 3

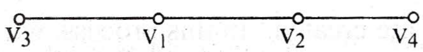


Fig-4.5.10

14.6 SUMMARY

In this lesson ,we dealt with a special type of graphs called trees and studied some properties. The concept of minimally connected graphs was introduced. By listing all the properties of tree, it was easy to observe that there are five different equivalent conditions for tree. The concepts : "distance", "center", "metric", "eccentricity", "radius", and "diameter" were discussed.

14.7 TECHNICAL TERMS

Tree:	A connected graph without circuits.
Null Tree:	A tree without any edges.
Pendant vertex:	A vertex of degree 1.
Minimally connected:	If the removal of any one edge from the graph results a disconnected graph.
Distance:	The distance between a pair of vertices is the length of the shortest path between them.
Eccentricity of a vertex (E(v)):	$E(v) = \max_{v_i \in G} d(v, v_i)$
Center of a graph:	A vertex with minimum eccentricity. [In other words, v is a center of a graph $\Leftrightarrow E(v) = \min \{E(u) / u \in G\}$].

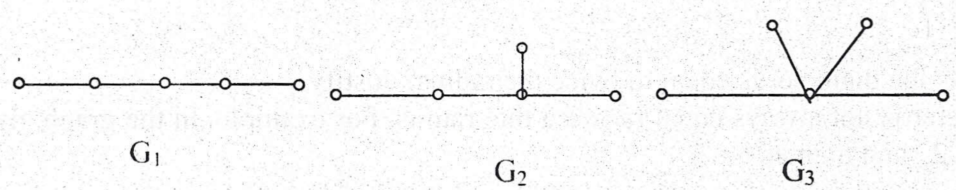
Radius of a graph: The eccentricity of a center in a graph (or in a tree).

Diameter of a tree: The length of the longest path in a tree.

14.8 ANSWERS TO SELF ASSESSMENT QUESTIONS

1: G_1 is a tree, since it is a connected graph without circuits. G_2 is not a tree (since it is not connected).

2:



First draw five vertices. Then connect them, so that no cycles are created. In this process, we must be careful that not to repeat trees since two trees which appear different may just be drawn differently. Here there are three trees with five vertices as shown above.

14.9 MODEL QUESTIONS

1. Define the terms: tree, minimally connected graph, pendent vertex, distance between two vertices in a connected graph, eccentricity of a vertex, centre of a graph and give an example of each.

2. Show that G is a tree ⇔ there is one and only one path between every pair of vertices.

3. (i). Show that a tree G with n vertices has n - 1 edges.
   (ii). Show that any connected graph G with n vertices and n - 1 edges is tree.

4. Show that a graph G is a tree ⇔ it is minimally connected.

5. Show that in a tree there exist at least two pendant vertices.

6. Show that every tree has either one or two centres.

14.10 REFERENCE BOOKS

1. Bondy J.A and Murty U.S.R, "Graph Theory with applications", North Holland, New York (1976).

2. Douglas B. West "Introduction to Graph Theory", Second Edition, Prentice Hall of India, New Delhi, 2002.

3. Harary Frank. "Graph Theory", Addison - Wesley Publishing Company, Inc., Reading, Mass., 1969.

4. John Clark and Derek Allan Holton, "A first look at Graph Theory" Allied Publishers, 1995

5. Narsingh Deo "Graph theory with applications to Engineering and Computer Science", Prentice Hall of India Pvt., Ltd., New Delhi, 1993.

6. Satyanarayana Bhavanari and Syam Prasad Kuncham "Graph Theory for Beginners", Satyasri Maths Study Centre, Guntur, AP, 2003.

Name of the Author of this Lesson: **Mr. J. L. Ram Prasad**

14

LESSON - 15

SOME TYPES OF TREES

Objectives

The objectives of this lesson are to:

- know different types of trees such as rooted, unrooted, labeled, unlabelled , binary trees, together with their properties.
- discuss about few applications of trees.
- understand those trees which are subgraphs of a given connected graph G containing all the vertices. (ie., spanning trees)
- compute rank and Nullity of a graph

Structure

15.0 Introduction
15.1 Rooted Trees
15.2 Binary Trees
15.3 On Counting Trees
15.4 Spanning Trees
15.5 Rank and Nullity
15.6 Summary
15.7 Technical terms
15.8 Answers to Self Assessment Questions
15.9 Model Questions
15.10 Reference Books

15.0 INTRODUCTION

In lesson 14, we introduced the concept of a tree, pendant vertices distance and centers in a tree. We studied some basic properties of trees. In this lesson, we present more results on trees, Binary rooted trees which are extensively used in the study of computer search methods, binary identification problems, and variable - length binary codes. The method of counting how many spanning trees and non - isomorphic spanning trees are there for a given graph was initiated by Cayley. He used trees to count the number of saturated hydrocarbons $C_n H_{2n+2}$ containing a given number of carbon items. He proved that, given n vertices, labelled 1, 2, ……..,n, there are n^{n-2} different ways of joining them to form a tree. Spanning trees are important in data networking. Spanning trees play a vital role in multicasting over Internet protocol (I.P) networks.

15.1 ROOTED TREES

15.1.1 Definition: A tree in which one vertex (called the **root**) is distinguished from all the other vertices, is called a **rooted tree**. In a rooted tree, the root is generally marked in a small triangle.

15.1.2 Example: Distinct rooted trees with four vertices, were given in Fig-15.1.2.

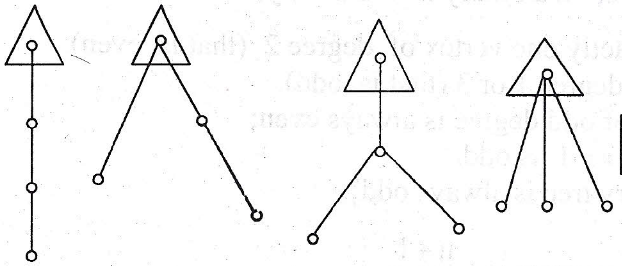


Fig-15.1.2

15.1.3 Note: Generally, the term 'tree' means trees without any root. However they are sometimes called **free trees** (or) **non-rooted trees**.

15.2 BINARY TREES

A variety of rooted trees (called the **Binary rooted trees**) is of particular interest (since they are extensively used in the computer search methods, binary identification problems, and variable length binary codes).

15.2.1 Definition: A tree in which there is exactly one vertex of degree 2, and all other remaining vertices are of degree one or three, is called a binary tree.

15.2.2 Note: (i) Clearly the Fig-15.2.2 represents a binary tree (because the only vertex 'v_1' is of degree 2, and all other vertices are of degree either 1 or 3).

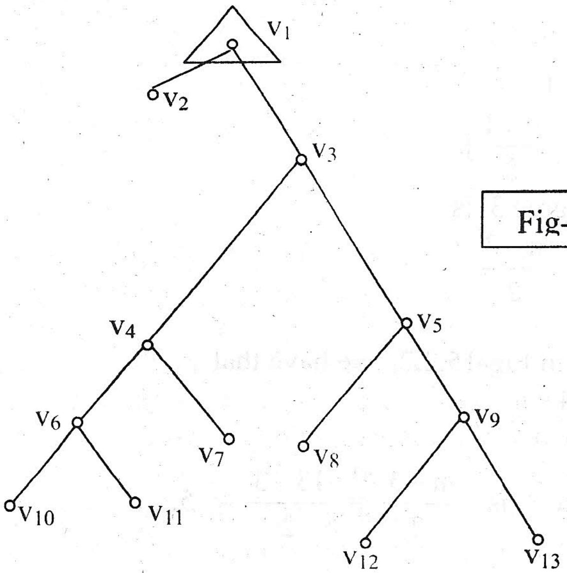


Fig-15.2.2

(ii) Since the vertex of degree 2 (that is, v_1) is distinct from all other vertices, this vertex v_1 is the root.

(iii) In a binary tree, the vertex with degree 2 serves as a root. So every binary tree is a rooted tree.

15.2.3 Properties of Binary trees:

Property (i): The number of vertices n, in a binary tree is always odd.

[**Reason:** In a Binary tree, there is exactly one vertex of degree 2 (that is, even).
The remaining (n - 1) vertices are of degree 1 or 3 (that is, odd).
We know that the number of vertices of odd degree is always even;
So n -1 is even. Hence n = (n - 1) + 1 is odd.
Thus, the number of vertices in a binary tree is always odd].

Property (ii): The number of pendent vertices is $\frac{n+1}{2}$.

[**Verification:** Consider a Binary tree T with n vertices. Write p = the number of pendent vertices.
Also there is a vertex of degree 2.
Now there exists a vertex of degree 2, and there are p vertices of degree 1.
The remaining (n - p - 1) vertices are of degree 3.
So number of vertices of degree 3 is (n - p -1).
We know that $2\,|E(T)| =$ sum of degree of the vertices,

$$= \sum \delta(v) \text{ (sum taken over all pendent vertices v)}$$

$$+ \sum \delta(v) \text{ (sum taken over all vertices v of degree 3)} + 2$$

$$= (p \times 1) + ((n - p - 1) \times 3) + 2 = 3n - 2p - 1.$$

$$\Rightarrow |E(T)| = \frac{1}{2}[3n - 2p - 1].$$

We know that in a tree, $|E(T)| = n - 1$

So $n - 1 = \frac{1}{2}(3n - 2p - 1) \Rightarrow p = \frac{n+1}{2}$].

Property 3: Number of vertices of degree 3 is

$$= n - p - 1 = n - \left(\frac{n+1}{2}\right) - 1 = \frac{n-3}{2}$$

15.2.4 Example: In the graph given in Fig-15.2.2, we have that

$n = 13$, $p = \frac{n+1}{2} = \frac{13+1}{2} = \frac{14}{2} = 7.$

Therefore number of vertices of degree 3 is $\frac{n-3}{2} = \frac{13-3}{2} = 5.$

15.2.5 Definition: A non-pendent vertex in a tree is called an **internal** vertex.

15.2.6 Note: The number of internal vertices in a Binary tree is

$\frac{n-1}{2}$ = (p - 1) where p = the number of pendent vertices.

[**Verification**: Number of internal vertices = n - p

$= n - (\frac{n+1}{2}) = \frac{n-1}{2} = \frac{n+1}{2} - 1 = p - 1$]

15.2.7 Example: In the **binary** tree given in Fig-15.2.2, the internal vertices are $v_1, v_3, v_4, v_5, v_6, v_9$. These are 6 (= 7 - 1 = p - 1) in number.

15.2.8 Definition: Let v be a vertex in a binary tree. Then v is said to be at **level** i if v is at a distance of i from the root.

15.2.9 Example: (i) A 13-vertex, 4-level binary tree was given in Fig-15.2.9.

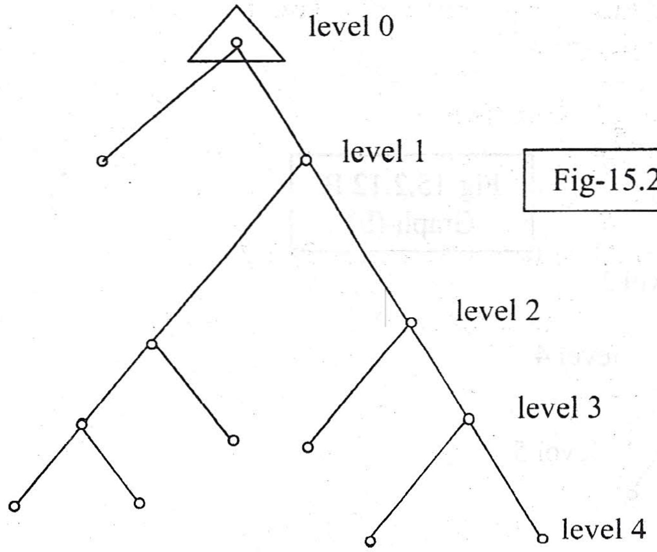


Fig-15.2.9

Here the number of vertices at levels 0, 1, 2, 3, 4 are 1, 2, 2, 4 and 4 respectively.

15.2.10 Definition: The sum of path lengths from the root to all pendent vertices is called the **path length** (or) **external path length** of a tree.

15.2.11 Example: The path length of the binary tree given in Fig-15.2.9 is:

1 + 3 + 3 + 4 + 4 + 4+ 4 = 23.

15.2.12 Example: In the Figures 15.2.12 A and B, there are two 11-vertex binary trees.

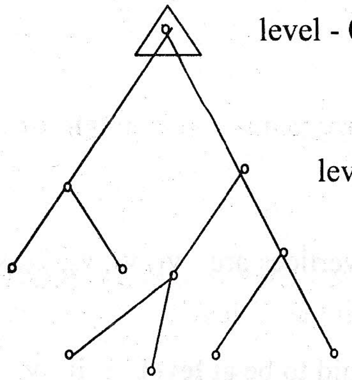


Fig-15.2.12 A
Graph-(a)

The path length of Graph-(a) : 2 + 2 + 3 + 3 + 3 + 3 = 16.

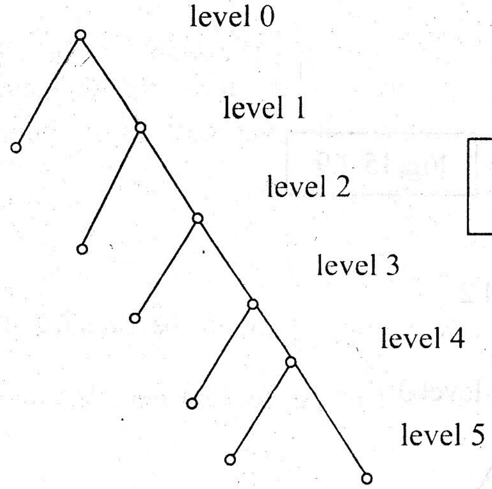


Fig-15.2.12 B
Graph-(b)

The path length of Graph-(b): 1 + 2 + 3 + 4 + 5 + 5 = 20.

15.2.13 Search procedures (An application)

Each vertex of a binary tree represents a test with two possible outcomes. We start at the root The outcome of the test at the root sends us to one of the two vertices at the next level, where further tests are made and so on.

Reaching a specified pendent vertex (that vertex which represents the goal of the search), terminates the search.

For such search procedures, it is often important to construct a binary tree in which, for a given number of vertices n, the vertex frothiest from the root in as close to the root as possible.

(i) There can be only one vertex (the root) at level 0. Number of vertices at level one is at most 2. Number of vertices at level two is at most 2^2 and so on.

So the maximum number of vertices possible in a k -level binary tree is
$2^0 + 2^1 + 2^2 + \ldots + 2^k$
So $n \leq 2^0 + 2^1 + 2^2 + \ldots + 2^k$

(ii) The maximum number among the levels of the vertices in a binary tree is called **height** of the tree.
So height = max { level of a vertex v / $v \in V$}.
This height is denoted by l_{max}.

(iii) To construct a binary tree for a given n such that the farthest vertex is as far as possible from the root, we must have exactly two vertices at each level, except at the 0 level.

So $\max l_{max} = \frac{n-1}{2}$.

15.2.14 Weighted path length: Suppose that every pendent vertex v of a **binary** **was** associated with a positive real number $w = f(v)$.
[It was illustrated in the Example 5.2.15].
Suppose m positive numbers $w_1, w_2, \ldots, w_m$ are given. The problem is to construct a **binary** tree with m vertices $v_1, v_2, \ldots, v_m$ (assume that $w_i = f(v_i)$, the associated real number) such that the sum $\sum w_i \cdot l(v_i)$ (sum taken over all pendent vertices) is minimum, where l(v) denotes the level of v.

15.2.15 Example: Suppose that there is a **Coke Machine**.

The machine is to have a sequence of tests (for example, it should be capable of identifying the coin that is put into the machine).
We suppose that five rupees coin, two rupees coin, one rupee coin and fifty paise coin can go through the slot.
So the machine can identify only these four coins.
Every coin put in, is to be tested by the machine.
Each test got the effect of partitioning the coins into two complementary sets.
[Suppose a coin is put into the machine. It should test whether the coin is "five rupee coin". If it is not a five rupees coin, then it should test whether it is a two rupees coin and so on].
We suppose the time taken for each test is.
Test type-1: One type of testing pattern was shown in Graph-(a) which was given in Fig-15.2.15 A.
Suppose the statistical data tells that
w_1 = probability of putting a Rs 5 coin = 0.5
w_2 = probability of putting a Rs 2 coin = 0.2
w_3 = probability of putting a Rs 1 coin = 0.2
w_4 = probability of putting a Rs 0.5 coin = 0.1

Now $\sum w_i \cdot l(v_i) = w_1 \cdot l(v_1) + w_2 \cdot l(v_2) + w_3 \cdot l(v_3) + w_4 \cdot l(v_4)$

$= (0.5)(1) + (0.2)(2) + (0.2)(3) + (0.1)(4) = 1.9$

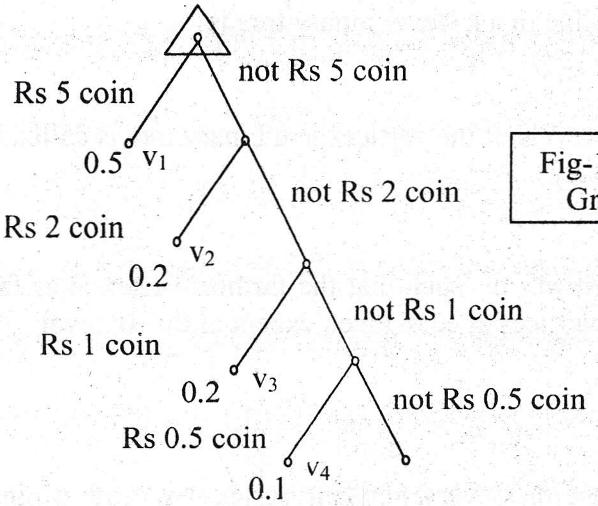


Fig-15.2.15 A
Graph-(a)

So expected time to be taken by the machine for testing one coin is 1.9t.

Thus if the machine follows (for its testing pattern) the binary tree given in Graph-(a), then the expected time for testing one coin is equal to 1.9t.

Test type-2: Another type of testing pattern was given in the Graph-(b) which was given in Fig-15.2.15 B. For Graph-(b),

$\sum w_i \cdot l(v_i)$

$= w_1 \cdot l(v_1) + w_2 \cdot l(v_2) + w_3 \cdot l(v_3) + w_4 \cdot l(v_4)$

$= (0.5)(2) + (0.2)(2) + (0.2)(2) + (0.1)(2)$

$= 2.0$

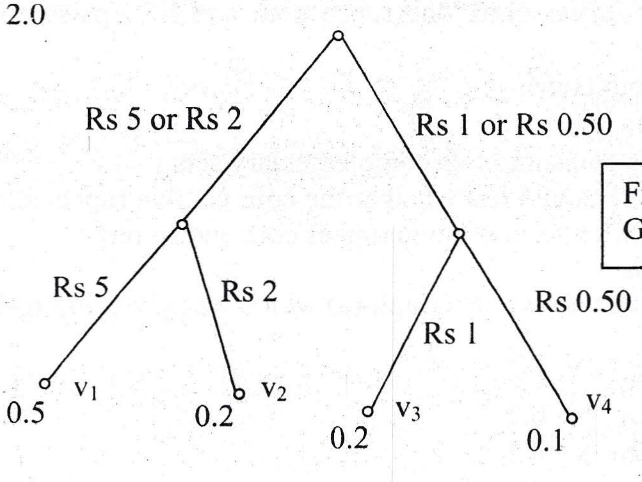


Fig-15.2.15B
Graph-(b)

So here, the expected time to be taken by the machine for testing one coin is 2t.

Thus if the machine follows (for its testing pattern the binary tree given in Graph-(b), then the expected time for testing one coin is 2t.

Conclusion: Now it can be understood that if there are two machines, machine-1 (follows the binary tree in Graph-(a)), and machine-2 (follows the binary tree in Graph-(b)), then machine-1 is more effective because it took less time for testing.

15.3 ON COUNTING TREES

15.3.1 Note: In 1857, Arthur Cayley discovered trees while he was trying to count the number of structural isomers of saturated hydrocarbons C_kH_{2k+2}. He used a connected graph to represent the C_kH_{2k+2} molecule. Corresponding to their chemical valances, a carbon atom was represented by a vertex of degree 4 and a hydrogen atom by a vertex of degree 1 (that is, a pendent vertex).

In C_kH_{2k+2}, there are $(k) + (2k + 2) = 3k + 2$ atoms.

So the number of vertices $= 3k + 2$.

The total number of edges: $e = \frac{1}{2}(\text{sum of degrees})$

$$= \frac{1}{2}[(4k) + (2k + 2)]$$

$$= 3k + 1.$$

Observe that $|E| = |V| - 1$.

Since the graph is connected and $|E| = |V| - 1$, we have that the graph is a tree.

Thus the problem of counting structural isomers of a given hydrocarbon becomes the problem of counting trees.

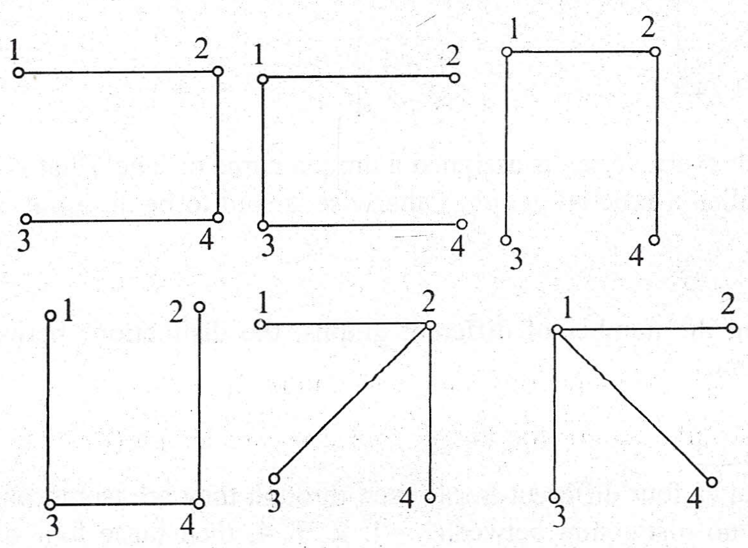
Now the Cayley posed a question:

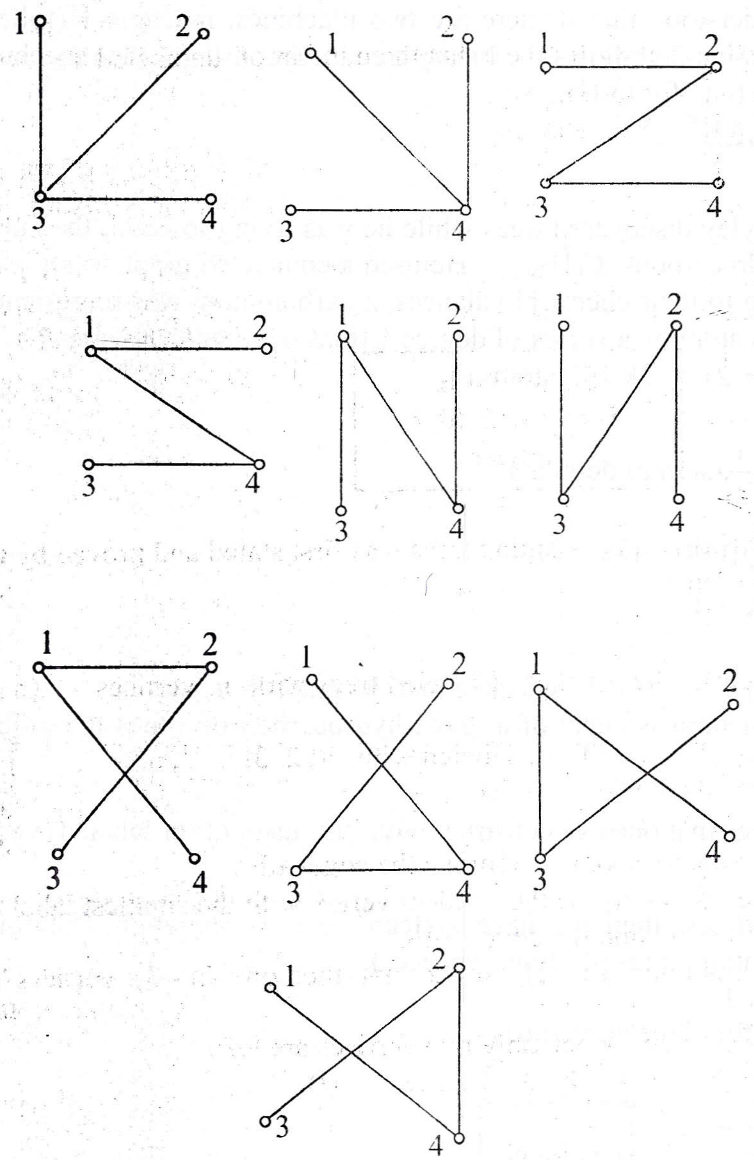
What is the number of different trees that one can construct with 'n' distinct (or labeled) vertices ?

15.3.2 Example: If G has 4 vertices, then we have sixteen trees as shown in the following figures.(Observe that there are no more trees of four vertices).

Here the vertex set $V = \{1, 2, 3, 4\}$.

The following are the 16 trees of four labeled vertices





15.3.3 Definition: A graph G in which every vertex is assigned a unique name or label (that is, no two vertices have the same label) is called a **labeled graph**. Otherwise is said to be an **unlabeled graph.**

15.3.4 Note: (i) when we are counting the number of different graphs, the distinction between labeled and unlabeled graphs is important.

(ii) Consider the graphs in Example 15.3.2.
The 5^{th}, 6^{th}, 7^{th} and 8^{th}, are counted as four different trees (even through they are isomorphic), because they **are labeled.** If there is no distinction between 1, 2, 3, 4, then these four trees counted as one.

(iii) A careful inspection of the 16 graphs will reveal that the number of unlabeled trees with four vertices (no distinction made between 1, 2, 3, 4), is two.
These two graphs were given in Fig-15.3.4 A and B.

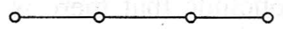


Fig-15.3.4 A
Tree-1 with four vertices

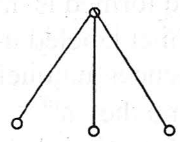


Fig-15.3.4 B
Tree-2 with four vertices

The following well-known theorem for counting trees was first stated and proved by Cayley, and is therefore called Cayley's theorem.

15.3.5 Theorem (Cayley's Theorem): The number of labeled trees with n vertices $(n \geq 2)$ is $n^{(n-2)}$.

Proof: Part-(i) Let the n vertices of a tree T be labeled with 1, 2, 3, . . . , n.
Remove the pendent vertex (and the edge incident on it)
having the smallest label (say, that vertex is a_1).
Suppose that a_1 is adjacent to b_1. Note that we also remove the edge a_1b_1.
Among the remaining $(n - 1)$ vertices, let a_2 be the pendent vertex with the smallest label and b_2 be the vertex adjacent to a_2. Remove a_2 and the edge a_2b_2.
This operation is repeated on the remaining $(n - 2)$ vertices and then on $(n - 3)$ vertices, and so on.
The process is terminated after $(n - 2)$ steps, when only two vertices are left.
In this process, we got the sequence $(b_1, b_2 \ldots, b_{n-2})$ .... (i)
Also this sequence is unique for T.
So T defines the sequence $(b_1, b_2, \ldots, b_{n-2})$ uniquely.

Part-(ii): Suppose a sequence $(b_1, b_2, \ldots, b_{n-2})$ of $(n - 2)$ labels is given.
Then we can construct a n-vertex tree uniquely as follows:
Determine the first number in the sequence

1, 2, 3, 4, . . . , n .... (ii)

that does not appear in sequence (i).
Suppose that this number is a_1.
Now the edge (a_1, b_1) is defined.
Remove b_1 from the sequence (i), and a_1 from the sequence (ii).
In the remaining sequence of (ii), find the first number that does not appear in the remainder of (i).
This would be a_2, and so the edge (a_2, b_2) is defined. Remove a_2 from (ii) and b_2 from (i).
The construction is continued till the sequence (i) has no element left.

Finally, the last two vertices remaining in (ii) are joined.
Then we get T.

Part-(iii): From part (i) and part (ii) we conclude the following: for each (n - 2) elements in the sequence (i), we can choose any one of n numbers.
So the number of (n - 2)- tuples that can be formed is $n^{(n-2)}$.
Each of these (n - 2)- tuples defining a distinct labeled tree of n vertices.
Since each tree defines one of these sequences uniquely, we conclude that there is a one-to-one correspondence between the labeled trees and the $n^{(n-2)}$ sequences.
Thus there are $n^{(n-2)}$ labeled trees with n vertices.

15.3.6 Example: (Observe the procedure in the proof of Theorem 15.3.5)

Part-(i): Suppose the given tree is T_1 (observe Fig-15.3.6 A).
a_1 = the pendent vertex with smallest label.
So a_1 is the vertex 2. Now $b_1 = 1$.
After removing a_1 and the edge (a_1, b_1), in the remaining graph
a_2 = the pendent vertex with smallest index = 4.

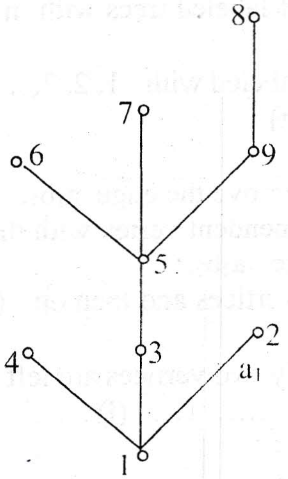


Fig-15.3.6 A

Now $b_2 = 1$.

$a_3 = 1$, $b_3 = 3$, $a_4 = 3$, $b_4 = 5$, $a_5 = 6$.
$b_5 = 5$, $a_6 = 7$, $b_6 = 5$, $a_7 = 5$, $b_7 = 9$.
Therefore we have the sequence
$(b_1, b_2, b_3, b_4, b_5, b_6, b_7) = (1, 1, 3, 5, 5, 5, 9)$.

Part (ii): (converse of above part (i)): we have to construct a tree with n = 9 vertices.
Consider 1, 2, 3, 4, 5, 6, 7, 8, 9 .... (i)
Given (n - 2)-tuple is (1, 1, 3, 5, 5, 5, 9) .... (ii)

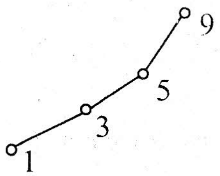


Fig-15.3.6 B

Observe the sequence in (ii).

First join 1 and 3 , 3 and 5, 5 and 9. Then we get the graph given in Fig-15.3.6 B.
Now the least number in (i) which is not in (ii), is 2. So we join 2 and 1.
Next least in (i) which is not in (ii) is 4. So we join 4 and 1.
Cancel 3 in (i) and 3 in (ii). Also cancel 5 in (i) and 5 in (ii) (in (ii), canceling of only one 5 is allowed).
The next least which is not in (ii) is 6. So we join 5 and 6.
The next least which is not in (ii) is 7. So we join 7 and 5.
The next least which is not in (ii) is 8.
The remaining number available in (ii) is 9.
So we join 8 and 9.

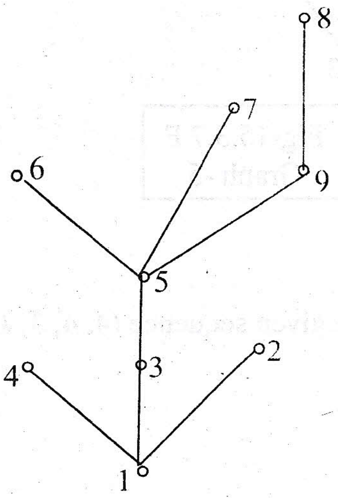


Fig-15.3.6 C

15.3.7 Example : (We provide only part (ii)).

Given (4, 4, 3, 1, 1) .... (ii)
So this is a $(n - 2) = 5$ tuple.
Since $n - 2 = 5$, we have that $n = 7$.
So we have to construct a tree with $n = 7$ vertices.
Consider 1, 2, 3, 4, 5, 6, 7 .... (i)
Construct a tree with 4, 3, 1 (entries in (ii)).
Observe Fig-15.3.7A. Join 4 and 3, join 3 and 1.

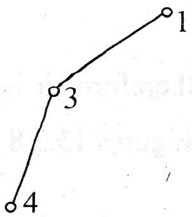


Fig-15.3.7 A
Graph-1

The least index which is in (i) and not in (ii) is 2.

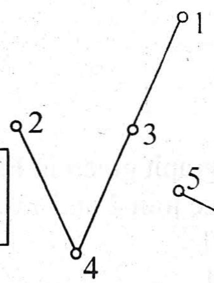


Fig-15.3.7 B
Graph-2

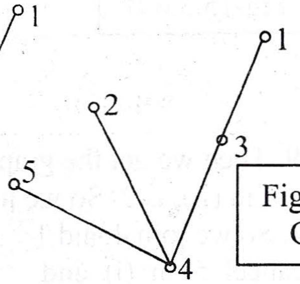


Fig-15.3.7 C
Graph-3

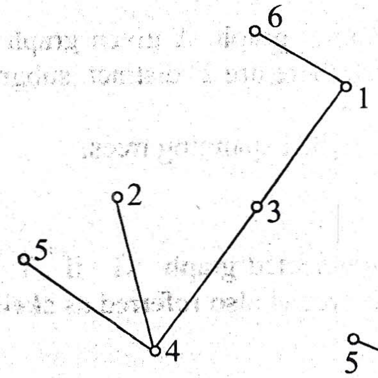


Fig-15.3.7 E
Graph -4

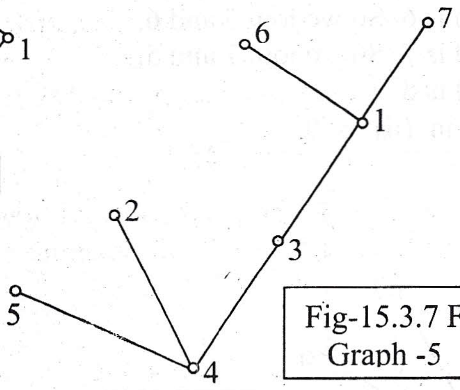


Fig-15.3.7 F
Graph -5

So we join 2 and 4 (since 4 is the first entry in the given sequence (4, 4, 3, 1, 1)).
Then we get graph 2.
The next least which is in (i) not in (ii) is 5.

So we join 5 and 4 and then we get graph-3.
Now we cancel 3 in (i) and 3 in (ii).
The next least in (i) not in (ii) is 6. So we join 6 and 1.
Next least which is in (i) and not in (ii) is 7.
So we join 7 and 1, and finally we get graph-5.

15.3.8 Unlabeled trees: (i) Since the vertices representing in hydrogen atom are pendant, they go with Carbon atoms only one way and hence make no contribution to isomerism.
Therefore, we need not show any hydrogen vertices.

(ii) Thus the tree representing C_kH_{2k+2} reduces to **one** with k vertices, each representing a carbon atom.

In this tree, no distinction can be made between vertices and therefore it is unlabeled. Thus for Butane (C_4H_{10}) there are only two distinct trees as given in the Figures 15.3.8 A and B.

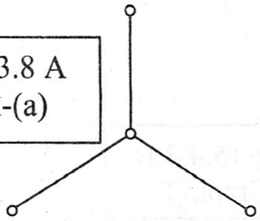


Fig-15.3.8 A
Graph-(a)

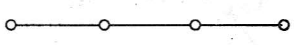


Fig-15.3.8 B
Graph -(b)

15.3 SPANNING TREES

In this section, we will study the tree as a subgraph of another **graph. A given graph may** have numerous subgraphs. If e is the number of edges in G, then there are 2^e **distinct subgraphs** are possible. Obviously some of these subgraphs will be trees.

Out of these trees we particularly interested in certain type of trees, called **spanning trees.**

15.4.1 Definition: A collection of trees is called a **forest**.

15.4.2 Definition: A tree T is said to be a **spanning tree** of a connected **graph** G if T is a subgraph of G and T contains all the vertices of G. Spanning tree **is also referred as skeleton** or **scaffolding.**

15.4.3 Example: Consider the graph G given in Fig-15.4.3 A.
Graph T (given in Fig-15.4.3 B) is a spanning tree of G.

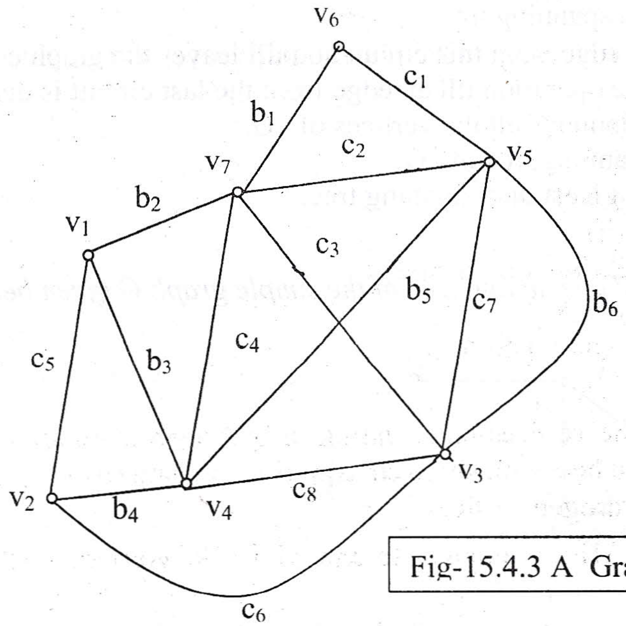


Fig-15.4.3 A Graph-G

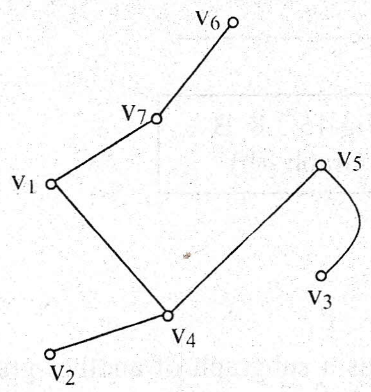


Fig-15.4.3 B
Graph-T

15.4.4 Note: (i) Since spanning trees are the largest (with the maximum number of edges) trees among all trees in G, we have that a spanning tree is also called a **maximal tree subgraph** or **maximal tree** of G.

(ii) Spanning is defined only for a connected graph. (because, a tree is always connected).

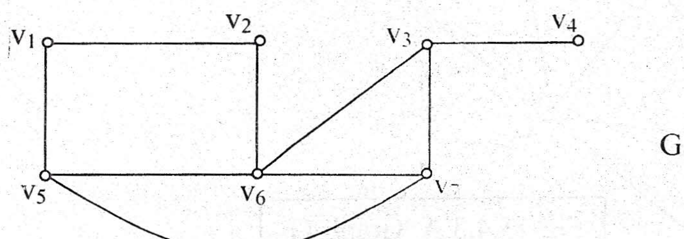
(iii) However, each component of a disconnected graph, does have a spanning tree.

Thus a disconnected graph with k components contains a spanning forest consisting of k spanning trees.

15.4.5 Theorem: Every connected graph has at least one spanning tree.

Proof: Let G be a connected graph.
If G has no circuit, then G is a spanning tree.
If G has a circuit, then delete an edge from this circuit and till leaves the graph connected.
If there are more circuits, repeat the operation till an edge from the last circuit is deleted, leaving the graph connected, circuitless, and contains all the vertices of G.
Thus the subgraph obtained is a spanning tree of G.
Hence every connected graph has at least one spanning tree.

Self Assessment Question 1: *Find a spanning tree of the simple graph G given below*:



15.4.6 Definition: (i) An edge in a spanning tree T is called a **branch** of T.

(ii) An edge of G that is not in a given spanning tree T is called a **chord**. In electrical engineering chord some times referred to as **tie** or a **link**.

15.4.7 Note: (i) Branches and chords are defined only with respect to a given spanning tree.

(ii) An edge that is a branch with respect to one spanning tree T_1 (of G) may be a chord with respect to another spanning tree T_2.

15.4.8 Definition: Let T be any spanning tree of a connected graph G, and T^1 is the complement of T in G. Then each edge in T is called a **branch** (with respect to T), and the set of all edges in T is called the **branch set.** Each edge in T^1 is called a **chord** (with respect to T), and the set of edges in T^1 is called the **chord set** (or) **Tie set.** T^1 is called as the **cotree.** We may write $\overline{T}$ instead of T^1.

15.4.9 Theorem: With respect to any of its spanning trees, a connected graph of 'n' vertices and 'e' edges has 'n-1' tree branches and $e - n + 1$ chords.

Proof: Let G be any connected graph on 'n' vertices and e edges.
Let T be any spanning tree in G.
Since every spanning tree of G contains all vertices of G, we have that $|V(T)| = n$ and so $|E(T)| = |V(T)| - 1 = n - 1$. Since every edge of a spanning tree T is called a branch of T, we have that G contains $n - 1$ branches.
Since the number of edges in G is e, we have that the number of chords of T is $e - (n - 1) = e - n + 1$.

15.4.10 Problem: There is a form consisting of six walled plots

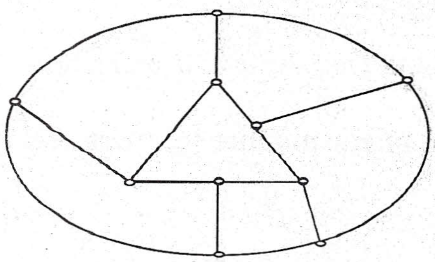


Fig-15.4.10

of land as shown in the Fig-15.4.10, and these plots are full of water. How many (minimum number of) walls are to be broken so that all the water can be drained out?

Solution: Consider the wall joints as vertices, and walls as edges. Then we can consider it as a graph. In this graph the number of vertices is $n = 10$, and the number of edges is $e = 15$.
If there exists a circuit, then the water inside the circuit cannot be drained out. So we have to remove minimum number of edges so that the graph do not contain circuits.
To have this, we should have a spanning tree with $(n - 1)$ edges. Hence we have to break $e - (n - 1) = e - n + 1 = 15 - 10 + 1 = 6$ edges (walls) so that all the water can be drained out.

Self Assessment Question 2: *How many edges must be removed from a connected graph with* n *vertices and* m *edges to produce a spanning tree?*

15)

15.5 RANK AND NULLITY

15.5.1 Note: Let G be a graph; n be the number of vertices in G; e be the number of edges in G; k be the number of components in G.

(i) If $k = 1$, then G is a connected graph.

(ii) Since every component of a graph must have at least one vertex, we have that $n \geq k$. (or $n - k \geq 0$).

(iii) Since a component is a connected subgraph, we have that in i^{th} component, the minimum number of edges = (number of vertices - 1)

$\Rightarrow \sum$ (minimum number of edges in the i^{th} component)

$\geq \sum$(number of vertices in the i^{th} component - 1)

$\Rightarrow e \geq \sum$ (minimum number of edges in the i^{th} component)

$\geq \sum$(number of vertices in the i^{th} component - 1)

$= [\sum$(number of vertices in the i^{th} component)] - $\sum 1$

$= n - k$.

Therefore we got that $e \geq (n - k) \Rightarrow e - n + k \geq 0$.

15.5.2 Note: Apart from the constraints $n - k \geq 0$;

$e - n + k \geq 0$, the three numbers n, e, and k are independent.

These are the fundamental and important numbers in graphs. [From these three numbers, we define two other important numbers called rank and nullity].

15.5.3 Definition: Let G be a graph. Then **rank** (r) of G is defined as $r = n - k$; and **nullity** of G is $\mu = e - n + k$.

The nullity of a graph is also referred to as its **cyclomatic number** (or) **first Betti number.**

15.5.4 Note: (a) Let G be a connected graph.

In a connected graph there is only one component, and so $k = 1$.

So rank of G = $r = n - 1$; and the nullity of G = $\mu = e - n + 1$.

(b) In a spanning tree we have

(i) $r = n - 1$ = number of branches.

(ii) $\mu = e - n + k = (n - 1) - n + 1 = 0$

= the number of chords.

(iii) $r + \mu = e$.

(c) Let G be a connected graph.

Then we can observe that

$r = n - 1$

= the number of branches in any spanning tree of G.

$\mu = e - (n - 1)$ = the number of chords in G

$r + \mu$ = the number of edges in G

15.6 SUMMARY

In this lesson, we learnt about rooted trees, binary trees, spanning trees and their properties. We discussed some important applications of trees. We also discussed the well-known theorem for counting trees which was first stated and proved by Caley. We learnt about the numbers Rank and Nullity in a graph and also proved some results on Rank and Nulllity.

15.7 TECHNICAL TERMS

Rooted tree: A tree in which one vertex (called the root) is distinguished from all the other vertices.

Binary tree: A tree in which there is exactly one vertex of degree 2, and all other remaining vertices are of degree one or three, is called a binary tree.

Internal vertex: A non-pendent vertex in a tree.

Level: Let v be a vertex in a binary tree. Then v is said to be at level i if v is at a distance of i from the root.

Path length: The sum of path lengths from the root to all pendent vertices.

Labeled graph and unlabeled graph: A graph in which every vertex is assigned a unique name or label (that is, no two vertices have the same label

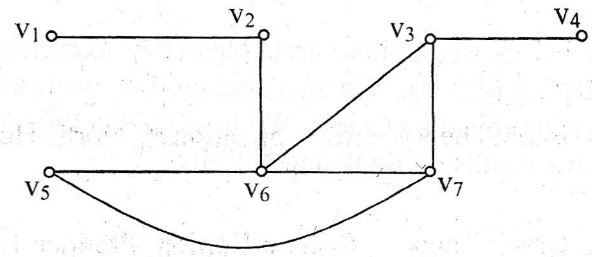
Forest: A collection of trees.

Spanning tree: A tree T is said to be a spanning tree of a connected graph G if T is a subgraph of G and T contains all the vertices of G. Spanning tree is also referred as skeleton or scaffolding.

Rank and Nullity: Let G be a graph. Then rank (r) of G is defined as $r = n - k$; and nullity of G is $\mu = e - n + k$.

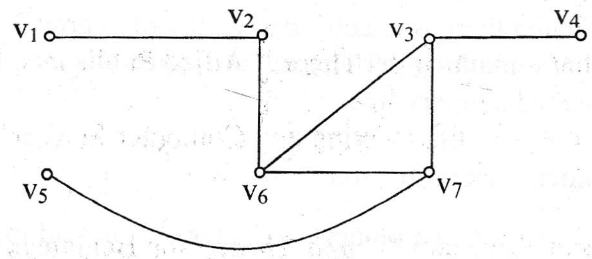
15.8 ANSWERS TO SELF ASSESSMENT QUESTIONS

1: Here the graph G is connected but it is not a tree since it contains simple circuits. First remove the edge v_1v_5. This eliminates one simple circuit and the resulting graph is still connected and contains every vertex of G. This is given in Fig G_1.



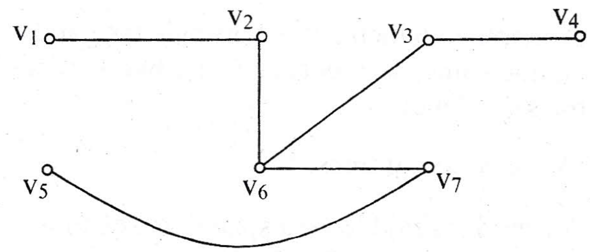
G_1

Next remove the edge v_5v_6 to eliminate a second simple circuit and the resulting graph is given in Fig G_2.



G_2

Finally remove the edge v_3v_7. Then the resulting graph G_3 is a connected simple graph without circuits. Moreover, it contains every vertex of G. So the graph G_3 is a spanning tree of G which is given in Fig G_3.



G_3

It is easy to see that the graph G_3 obtained above is not the only spanning tree of G.

2: m - n + 1 edges.

5.9 MODEL QUESTIONS

1. Show that number of vertices in a binary tree is always odd.
2. Show that the number of pendant vertices in a binary tree with n vertices is $\frac{n+1}{2}$.
3. Show that the number of labeled trees with n ($n \geq 2$) vertices is n^{n-2}.
4. Show that every connected graph has at least one spanning tree.

15.10 REFERENCE BOOKS

1. Bondy J.A and Murty U.S.R, "Graph Theory with applications", North Holland, New York (1976).

2. Douglas B. West "Introduction to Graph Theory", Second Edition, Prentice Hall of India, New Delhi, 2002.

3. Harary Frank. "Graph Theory", Addison - Wesley Publishing Company, Inc., Reading, Mass., 1969.

4. John Clark and Derek Allan Holton, "A first look at Graph Theory" Allied Publishers, 1995

5. Narsingh Deo "Graph theory with applications to Engineering and Computer Science", Prentice Hall of India Pvt., Ltd., New Delhi, 1993.

6. Satyanarayana Bhavanari and Syam Prasad Kuncham "Graph Theory for Beginners", Satyasri Maths Study Centre, Guntur, AP, 2003.

Name of the Author of this Lesson: **Mr. J. L. Ram Prasad**

LESSON - 16

CUT-SETS

Objectives

The objectives of this lesson are to:

- study about subgraphs of a connected graph G* whose removal from G separates some vertices from others in G.
- discuss some properties of cut sets.
- appreciate the great importance of cut-sets in studying the properties of communication and transportation networks.
- learn about fundamental cut-sets and fundamental circuits.

Structure

16.0 INTRODUCTION

In this lesson, we learn that a cut set of a graph is a set of edges such tht the removal of these edges produces a subgraph with more connected components than in the original graph, but no proper subset of this set of edges has this property. Cut sets are of great importance in studying properties of communication and transportation networks. These are used to identify weak spots in a communication nets and transportation network. We study the parallelism between circuit and cut sets. We further learn that a minimal set of cut sets from which we can obtain every cut set of a graph by taking ring sums, is the set of all fundamental cut-sets with respect to a given spanning tree. We alsostudy the relation between fundamental circuits and cut sets

16.1 CUT-SETS

16.1.1 Definition: Let G be a connected graph. A **cut-set** is a subset C of the set of all edges of G whose removal from the graph G leaves the graph G disconnected; and removal of any proper subset of C does not disconnect the graph G.
(Equivalently, cut-set can also be defined as a minimal set C of edges in a connected graph G whose removal reduces the rank of the graph by one).

16.1.2 Example: Observe Graph-(a) given in Fig-16.1.2A. If we remove {a, c, d, f} from Graph-(a), then we get the subgraph-(b) given in Fig-16.1.2B.
So in the Graph-(a), the subset {a, c, d, f} of edges, is a cut-set.
Also there are many other cut-sets such as {a, b, g}, {a, b, e, f}, {d, h, f}.
Also edge set {k} is also a cut-set.

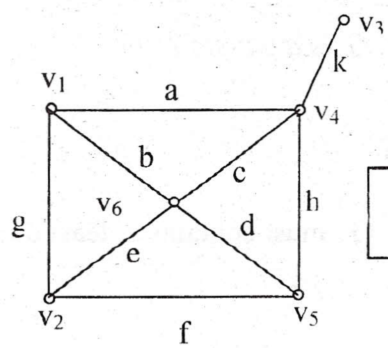


Fig-16.1.2 A
Graph-(a)

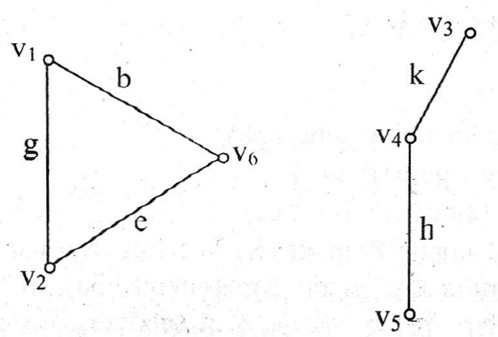


Fig-16.1.2 B Subgraph-(b)

Self Assessment Question 1: *Is the set of edges {a, c, h, d} in the graph 16.1.2 A, a cut set ?*

16.1.3 Note: (i) A cut-set is also some times called as **minimal cut-set** (or) a **proper cut-set** (or) a **simple cut-set** (or) a **co-cycle**.

(ii) A cut-set "cuts" the graph into two subgraphs.

(iii) Observe the graphs given in Example 16.1.2.

The rank of the graph-(a) is 5 $(n - k = 6 - 1)$.
The rank of the subgraph-(b) is 4 $(n - k = 6 - 2)$.

16.1.4 Note: "If we partition all the vertices of a connected graph G into two mutually exclusive subsets V_1 and V_2, then a cut-set is a set consists of minimal number of edges whose removal from G destroys all paths between the two sets V_1 and V_2 of vertices".

16.1.5 Example: Consider the graphs given in the Figures 16.1.2 A and B. In graph-(a), the cut-set {a, c, d, f} connects the vertex set $V_1 = \{v_1, v_2, v_6\}$ with $V_2 = \{v_3, v_4, v_5\}$.
Clearly, the removal of the cut-set $S = \{a, c, d, f\}$ from G, destroys all the paths between two vertex sets $V_1 = \{v_1, v_2, v_6\}$ and $V_2 = \{v_3, v_4, v_5\}$.

Self Assessment Question 2: *Is every edge of a tree G is a cut-set ?*

16.2 SOME PROPERTIES OF CUT-SETS

16.2.1 Theorem: Every cut-set in a connected graph G must contains at least one branch of every spanning tree of G.

Proof: Let T be any spanning tree of G, and let S be any cut-set in G.

Suppose $S \cap T = \phi$. Then $T \subseteq G \setminus S$.
Let v, u be two vertices in G

$\Rightarrow$ v, u are vertices in T
(since T is a spanning subgraph)

$\Rightarrow$ v, u are connected by a path P in T
(since T is a tree)

$\Rightarrow$ v, u are connected by a path P in $G \setminus S$
(since $T \subseteq G \setminus S$).

We proved that every two vertices in $G \setminus S$ are connected by a path, a contradiction. Here $S \cap T \neq \phi$.

16.2.2 Theorem: [Converse of the Theorem 16.2.1]

In a connected graph G, any minimal set Q of edges containing at least one branch of every spanning tree of G is a cut-set.
[In other words, if Q is minimal in $\zeta = \{S \mid S$ is a set of edges, $S \cap T \neq \phi$ for any spanning tree T of G$\}$, then Q is a cut-set.

Proof: Let G be a connected graph and Q be a minimal set of edges containing at least one branch of every spanning tree of G.
We have to show that Q is a cut-set.
Now consider the subgraph $G \setminus Q$
[the graph obtained by removing the edges of Q from G].
Since the subgraph $G \setminus Q$ contains no spanning tree of G, we have that $G \setminus Q$ is a disconnected graph [if $G \setminus Q$ is connected, then it contains a spanning tree].
Take any edge 'e' from Q and write $Q^1 = Q - \{e\}$.
Since Q is minimal in the set ζ, we have that Q^1 is not in the set ζ.

$\Rightarrow$ there exists a spanning T such that $Q^1 \cap T = \phi$.

$\Rightarrow$ $T \subseteq G \setminus Q^1$ $\Rightarrow$ $G - Q^1$ is connected.

Now we observed that the removal of any proper subset of Q does not disconnect the graph G.
Thus Q is a minimal set of edges whose removal from G disconnects G.
This shows that Q is a cut-set.
This completes the proof.

16.2.3 Theorem Every circuit has an even number of edges in common with any cut-set.

Proof: Let G be a connected graph, and S a cut-set in G.

Suppose that the removal of S partitions the set of vertices of G into two disjoint subsets V_1 and V_2.
Observe the graph given in the Figure-16.2.3.
Circuit Γ in G was represented by lines with arrows.
The arrows indicate the direction.

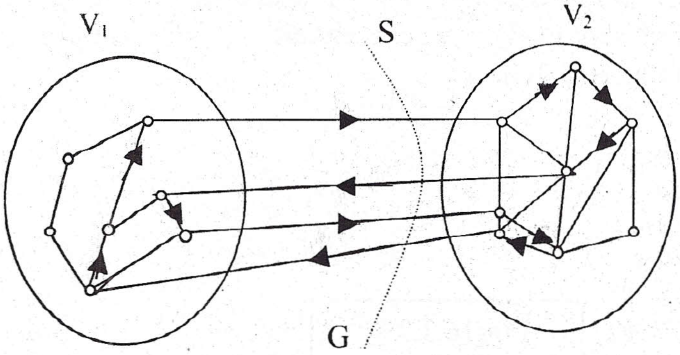


Fig-16.2.3

Case-(i): If all the vertices in Γ are with in the vertex set V_1 (or in V_2), then the number of edges common to both S and Γ is '0'.
That is, $n(S \cap \Gamma) = 0$, an even number
[Here n(g) stands for the number of edges in a subgraph g].
So in this case the theorem is true.

Case-(ii): Suppose that some of the vertices of Γ are in V_1, and some of them are in V_2.
Let us start with a vertex $v = v_0$ in Γ which is also in V_1.
We can write the circuit as $v_0 e_1 v_1 e_2 v_2 \ldots e_{n-1} v_{n-1} e_n v_0$.
Now $v_0 \in V_1$. By our supposition (of this case-(ii)), there exists i such that $v_i \in V_2$.

Let k be the least such that $v_k \in V_2$.

So $v_{(k-1)} \in V_1$ and $v_{(k-1)} v_k \in S$.
Now we are in V_2 and we have to traverse back to V_1.
Now m be the least such that $k \leq m$ and $v_m \in V_1$.
Clearly $v_{(m-1)} \in V_2$ and $v_m v_{(m-1)} \in S$.
Observe that if we traverse from V_1 to V_2 and back to V_1 once, we got two edges in $S \cap \Gamma$.
So by the closed nature of a circuit, whenever we traverse from V_1 to V_2, we have to traverse back.
Thus the number of edges we traverse between V_1 and V_2 must be even and also these edges are in S.
So the number of edges common to S and Γ is even.

16.3 FUNDAMENTAL CIRCUITS

16.3.1 Note: If we add an edge between any two vertices of a tree, then a circuit is created. This is because, there already exists one path between any two vertices of a tree, adding an edge in between, creates an additional path, and hence a circuit.

16.3.2 Definition: Let T be any spanning tree of a connected graph G. Adding any one chord to T will create exactly one circuit. Such a circuit formed by adding a chord to a spanning tree, is called a **fundamental circuit.**

16.3.3 Example: Consider the graph G (given in Fig-16.3.3A), and its spanning tree T (given in Fig-16.3.3B) of G. Now, if we add the chord c_1 to T, we get a circuit '$b_1 b_2 b_3 b_5 c_1$' which is called as fundamental circuit (given in Fig-16.3.3C).

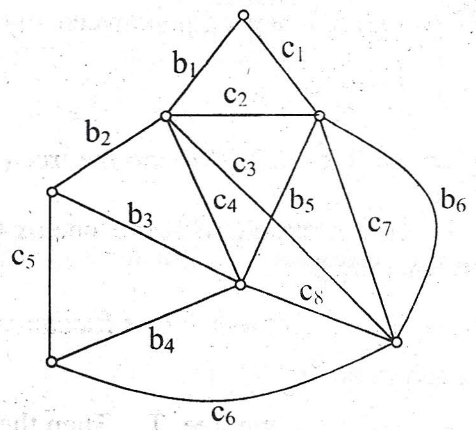


Fig-16.3.3 A
Graph-G

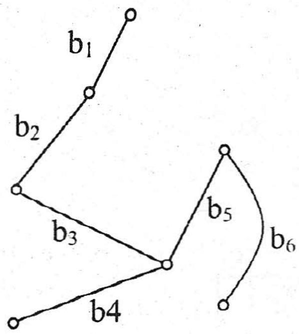


Fig-16.3.3 B
Spanning tree-T

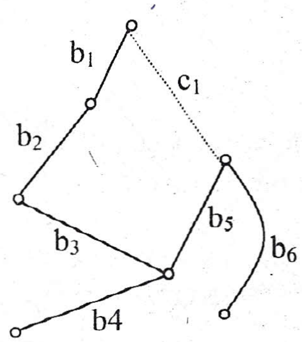


Fig-16.3.3 C
Fundamental circuit-F

16.3.4 Theorem: A connected graph G is a tree ⇔ adding an edge between any two vertices in G creates exactly one circuit.

Proof: Suppose G is a true. Suppose we add a new edge $\bar{e} = uv$ between two vertices u and v in G. Since G is a tree, G contains a path from u and v.
By joining this new edge, there creates exactly one circuit.

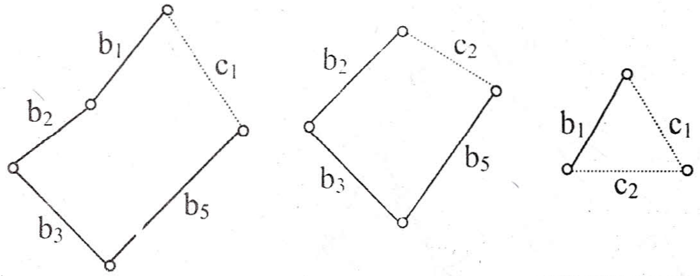
Converse: Suppose the converse hypothesis. Suppose G contains a circuit: $v_1e_1v_2e_2\ldots e_nv_1$. By adding new edge $e^1 = v_1v_2$, we get two circuits $v_1e^1 v_2e_1 v_1$ and $v_1e^1 v_2e_2v_3\ldots e_nv_1$, a contradiction. So G contains no circuits. Now we show that G is connected. Let u, v be two vertices in G. Add a new edge $e^* = uv$ to G.
Then by converse hypothesis, there creates a circuit.
Suppose the circuit is $u e^* e_1v_1e_2v_2\ldots.e_ku$. Now $ve_1v_1e_2v_2\ldots e_ku$ is a path in between v and u.
This shows that the graph G is connected. Hence G is a tree.

16.3.5 Corollary: Suppose G is a tree. Then by adding a new edge between any two vertices in G creates, exactly one fundamental circuit.

16.3.6 Note: (i) Let us observe the graph G (given in Fig-16.3.3A), and the tree (T) $\{b_1, b_2, b_3, b_4, b_5, b_6\}$ given in the Fig-16.3.3B. Add 'c_1' to T.
Then we get a subgraph $\{b_1, b_2, b_3, b_5, b_6, c_1\}$; which is a circuit (observe circuit (i) given in the following figures). This circuit is called a fundamental circuit.

(ii) Now if we add the chord c_2 (instead of c_1), we will get a different fundamental circuit $\{b_2, b_3, b_5, c_2\}$. (See Circuit-2)

(iii) Now suppose that we add both the chords c_1 and c_2 to the tree T. Then the subgraph $\{b_1, b_2, b_3, b_4, b_5, b_6, c_1, c_2\}$ contain not only the fundamental circuits we just mentioned, but it also a contains the circuit $\{b_1, c_1, c_2\}$, which is not a fundamental circuit (see circuit-3). There are 75 circuits in the graph given in the Fig-16.3.3A [by enumeration on computer], among which only 8 are fundamental circuits, each was formed by adding one chord..



Circuit-1 Circuit-2 Circuit-3

16.3.7 Note: (i) A circuit is called a fundamental circuit only with respect to a given spanning tree. A given circuit may be fundamental circuit with respect to a given spanning tree, but not with respect to a different spanning tree of the same graph. The number of fundamental circuits in a graph is fixed.

(ii) In the most of applications we are not interested in all the circuits of a graph but only in a set of fundamental circuits. The concept of a fundamental circuit introduced by 'Birchoff' is of enormous significance in electrical network analysis.

16.4 ALL CUT-SETS IN A GRAPH

16.4.1 Definition: Let T be a spanning tree of a connected graph G, and 'b' be a branch in T. Since {b} is a cut-set in T, the set {b} partitions all the vertices of T into two disjoint sets one at each end of b. Consider the same partition of vertices in G, and the cut-set S in G that corresponds to this partition. Now it is clear that this cut-set S will contain only one branch b of T, and the other edges (if any) in S are chords with respect to T. Such a cut-set S containing exactly one branch of the tree T is called a **fundamental cut-set** (or **basic cut-set**) with respect to T.

16.4.2 Example: Consider the graph G and one of its spanning subtrees T (given in the Figures 16.4.2 A and B).
All the fundamental cut-sets with respect to T were shown in the Fig-16.4.2A, by dotted lines/curves.

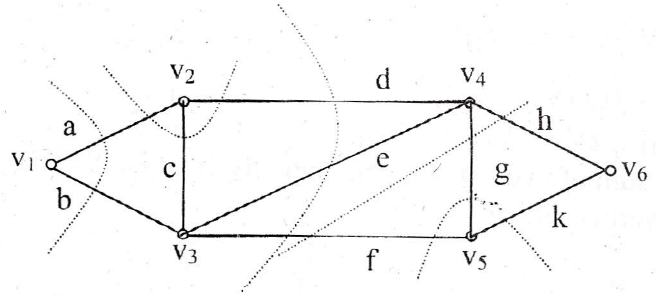


Fig-16.4.2 A
Fundamental cut-sets of the graph G

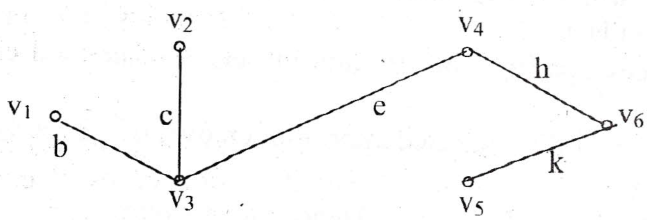


Fig-16.4.2 B
Spanning tree - T

16.4.3 Note: (i) We know that, every chord of a spanning tree defines a unique fundamental circuit. In the same manner, every branch of a spanning tree defines a unique fundamental cut-set.

(ii) The term fundamental cut-set (like the term fundamental circuit) has meaning only with respect to a given spanning tree.

16.4.4 Theorem: The ring sum of any two cut-sets in a graph is either a third cut-set (or) edge-disjoint union of cut-sets.

Proof: Let S_1 and S_2 be any two cut-sets in a given connected graph G.
Let V_1 and V_2 be the partition of the set V of vertices of G corresponding to S_1; where both V_1 and V_2 are unique and disjoint.
Let V_3 and V_4 be the partition of the set V of vertices of G corresponding to S_2; where both V_3 and V_4 are unique and disjoint.
Clearly $V_1 \cup V_2 = V$ and $V_1 \cap V_2 = \phi$
$V_3 \cup V_4 = V$ and $V_3 \cap V_4 = \phi$.
Write $V_5 = [V_1 \cap V_4] \cup [V_2 \cap V_3]$.
It is clear that $V_5 = V_1 \oplus V_3$.
[Verification: $V_1 \cap V_4 = V_1 \cap (V \setminus V_3) = V_1 \setminus V_3$;

$V_2 \cap V_3 = (V \setminus V_1) \cap V_3 = (V_3 \setminus V_1)$.
So $(V_1 \cap V_4) \cup (V_2 \cap V_3) = V_1 \oplus V_3$].
Write $V_6 = (V_1 \cap V_3) \cup (V_2 \cap V_4)$.
Now $V_6 = V_2 \oplus V_3$.

[**Verification**: $V_2 \oplus V_3 = (V_2 \setminus V_3) \cup (V_3 \setminus V_2)$

$$= (V_2 \cap V_3^1) \cup (V_3 \cap V_2^1)$$
$$= (V_2 \cap V_4) \cup (V_3 \cap V_1) = V_6].$$

Now we can observe that the ring sum of two cut-sets S_1 and S_2 (that is, $S_1 \oplus S_2$) consists of the edges that join vertices in V_5 to vertices in V_6.

[**Observation**: Let $\overline{vu} = e \in S_1 \setminus S_2$.
With out loss of generality, we assume that $v \in V_1$ and $u \in V_2$.
Since $\overline{vu} \notin S_2$, we have that either $v, u \in V_3$ or $v, u \in V_4$.
If $v, u \in V_3$, then $v \in V_1 \cap V_3$ and $u \in V_2 \cap V_3$ and so $\overline{vu}$ is from V_6 to V_5.
If $v, u \in V_4$, then $v \in V_1 \cap V_4$ and $u \in V_2 \cap V_4$, and so $\overline{vu}$ is from V_5 to V_6.
In the other cases, the observation is similar].
Thus the set of edges $S_1 \oplus S_2$ produces a partition of V into subsets V_5 and V_6 such that $V_5 \cup V_6 = V$ and $V_5 \cap V_6 = \phi$.
If the subgraphs containing V_5 and V_6 disconnected after the removal of $S_1 \oplus S_2$ (form G), then $S_1 \oplus S_2$ is a cut-set.
Otherwise $S_1 \oplus S_2$ is an edge-disjoint union of cut-sets. Hence the theorem.

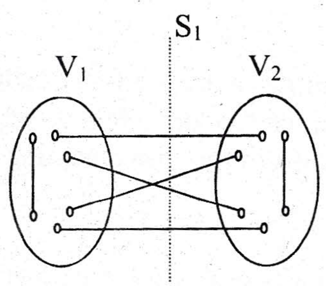


Fig-16.4.4 A

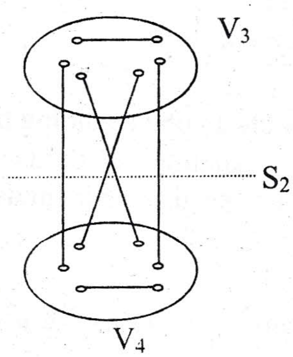


Fig-16.4.4 B

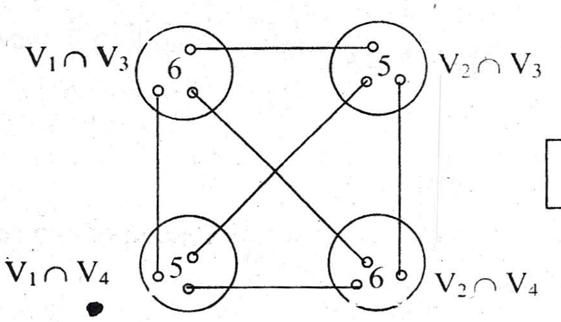


Fig-16.4.4 C

$V_5 = (V_1 \cap V_4) \cup (V_2 \cap V_3)$ and $V_6 = (V_1 \cap V_3) \cup (V_2 \cap V_4)$

16.4.5 Example: (i) Consider the graph given in Fig-16.4.5.

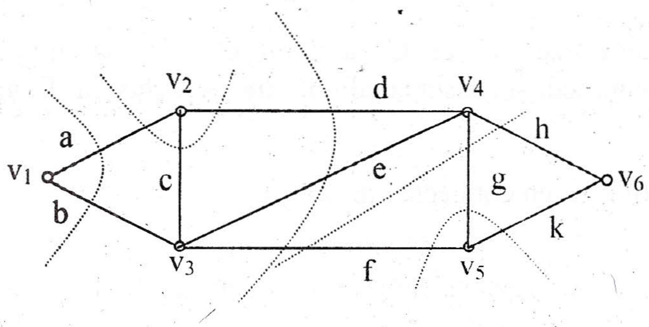


Fig-16.4.5

Take $S_1 = \{d, e, f\}$, $S_2 = \{f, g, h\}$.

So $V_1 = \{v_1, v_2, v_3\}$, $V_2 = \{v_4, v_5, v_6\}$ is the partition of V with respect to S_1.
Clearly $V_1 \cup V_2 = \{v_1, v_2, v_3, v_4, v_5, v_6\} = V$ and $V_1 \cap V_2 = \phi$.
Similarly $V_3 = \{v_1, v_2, v_3, v_4\}$, $V_4 = \{v_5, v_6\}$ is the partition of V with respect to S_2.
Clearly $V_3 \cup V_4 = V$ and $V_3 \cap V_4 = \phi$.
Let $V_5 = (V_1 \cap V_4) \cup (V_2 \cap V_3)$
$= \phi \cup \{v_4\} = \{v_4\}$.
[Also $V_1 \oplus V_3 = \{v_4\}$. So $V_1 \oplus V_3 = \{v_4\} = V_5$].
Similarly $V_6 = (V_1 \cap V_3) \cup (V_2 \cap V_4)$
$= \{v_1, v_2, v_3\} \cup \{v_5, v_6\} = \{v_1, v_2, v_3, v_5, v_6\}$.
[Also $V_2 \oplus V_3 = \{v_1, v_2, v_3, v_5, v_6\}$. So $V_2 \oplus V_3 = V_6$.]
Therefore $V_5 = \{v_4\}$ and $V_6 = \{v_1, v_2, v_3, v_5, v_6\}$.
Clearly $V_5 \cup V_6 = V$ and $V_5 \cap V_6 = \phi$.
Therefore $S_1 \oplus S_2 = \{d, e, g, h\}$ partitions V into V_5 and V_6.
Hence it is a cut-set.

(ii) Similarly, $\{a, b\} \oplus \{b, c, e, f\} = \{a, c, e, f\}$ is another cut-set.

(iii) $\{d, e, g, h\} \oplus \{f, g, k\} = \{d, e, f, h, k\}$ is not a cut-set [because, one of its proper subsets $\{d, e, f\}$ is a cut-set]
$= \{d, e, f\} \cup \{h, k\}$, an edge-disjoint union of cut-sets.

16.4.6 Problem: Consider the graph given in the Example 16.4.5.

(i) Find out the five fundamental cut-sets.

(ii) Find out the ring sum of each pair of fundamental cut-sets.

(iii) Find whether they (the ring sums obtained in (ii)) are cut-sets or disjoint union of two cut-sets.

16.5 FUNDAMENTAL CIRCUITS AND CUT-SETS

16.5.1 Theorem: With respect to a given spanning tree T of G, a chord c_i that determines a fundamental circuit Γ occurs in every fundamental cut-set associated with the branches in Γ and in no other.

Proof: Part-(i): Let T be any spanning tree of a given connected graph G.

Let c be a chord with respect to T.
Suppose Γ is the fundamental circuit made by c which consisting of 'k' branches $b_1, b_2, \ldots, b_k$ in addition to the chord c.
Note that $b_1, b_2, \ldots, b_k \in T$ and $c \notin T$.
So $\Gamma = \{c, b_1, b_2, \ldots, b_k\}$ is a fundamental circuit with respect to T.
We know that every branch of any spanning tree has a fundamental cut-set associated with it (by the Theorem 16.2.1).
So we can take a fundamental cut-set S_1 associated with b_1 (means $b_1 \in S_1$) consisting of q chords in addition to the branch b_1.
Suppose $S_1 = \{b_1, c_1, c_2, \ldots, c_q\}$ is that fundamental cut-set with respect to T.
Note that $c_1, c_2, \ldots, c_q$ are not in T and $b_1 \in T$.

Part-(ii): Now by the Theorem 16.2.3, there must be an even number of edges common to both S_1 and Γ.
Here the edge b_1 is in both Γ and S_1.
So $\{b_1\} \subseteq \Gamma \cap S_1$.
If $b_i \in \Gamma \cap S_1$ for some $2 \leq i \leq k$, then $b_i = c_j$ for some $1 \leq j \leq q$, a contradiction (since $b_i \in T$ and $c_j \notin T$).
So $c \in \Gamma \cap S_1$.
Hence $\Gamma \cap S_1 = \{b_1, c\}$

$\Rightarrow c \in S_1 = \{b_1, c_1, c_2, \ldots, c_q\}$

$\Rightarrow c = c_j$ for some $1 \leq j \leq q$ (since $c_i \neq b_1$).

Thus the chord c is one of the chords $c_1, c_2, \ldots, c_q$.
Therefore the chord c is contained in the fundamental cut-set associated with b_1.
Now exactly the same argument holds for all the fundamental cut-sets associated with the branches $b_2, \ldots, b_k$ (in Γ). Therefore by that argument, the chord c is contained in every fundamental cut-set associated with the branches in Γ.

Part-(iii): Now we show that c is not in any other fundamental cut-set.
If possible, suppose the chord c is in some other fundamental cut-set S^1, with respect to 'T' besides those associated with $b_1, b_2, \ldots, b_k$.
Then $b_1, b_2, \ldots, b_k \notin S^1$ and $c \in S^1$

$\Rightarrow S^1 \cap \Gamma = S^1 \cap \{b_1, b_2, \ldots, b_k, c\} = \{c\}$,

a contradiction (since the number of elements in the intersection of a cut-set and a circuit is even).
So the chord c is not in any fundamental cut-sets other than those associated with b_i, $1 \leq i \leq k$.
Hence the theorem.

16.5.2 Example: Consider the graph G given in the Fig-16.5.2A, and the spanning tree T = {b, c, e, h, k} given in Fig-16.5.2B.

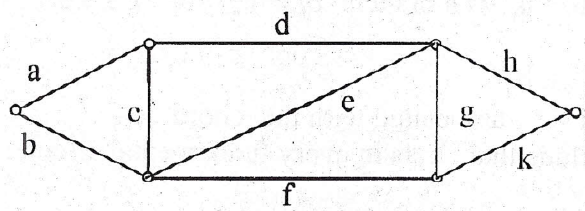


Fig-16.5.2 A
Graph - G

Observe that the fundamental circuit made by the chord f, is {f, e, h, k}.

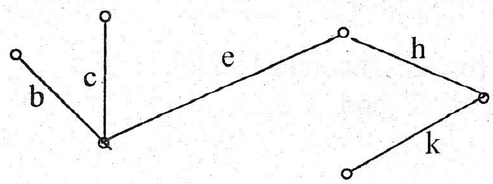


Fig-16.5.2 B
Spanning tree T

Clearly here e, h, k are branches.

The cut-set determined by branch e is: {d, e, f}
The cut-set determined by branch h is: {f, g, h}
The cut-set determined by branch k is: {f, g, k}

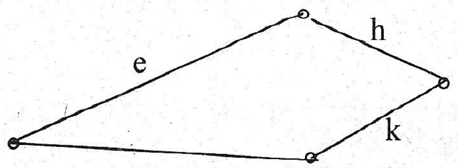


Fig-16.5.2 C
Fundamental circuit

Note that the chord f occurs in each of these three fundamental cut-sets associated with the branches e, h, k and there is no other fundamental cut-set containing f.

16.5.3 Theorem: (Converse of the Theorem 16.5.1)
With respect to a given spanning tree T of G, a branch b (that determines a fundamental cut-set S) is contained in every fundamental circuit associated with the chords in S, and in no others.
Proof: (The proof of this theorem consists of arguments similar to that of the Theorem 16.5.1).
Let G be a connected graph and T be a spanning tree.

Part-(i): Let S be a fundamental cut-set determined by branch b.
Suppose $S = \{b, c_1, c_2, \ldots, c_p\}$.

Now $b \in T$ and $c_1, c_2, \ldots, c_p \notin T$.
Let Γ_1 be a fundamental circuit determined by chord c_1.
Suppose $\Gamma_1 = \{c_1, b_1, b_2, \ldots, b_q\}$.

Now $c_1 \notin T$ and $b_1, b_2, \ldots, b_q \in T$.

Also $c_1 \in S \cap \Gamma_1$.

Part-(ii): Since the number of edges common to S and Γ_1 is even (by the Theorem 16.2.3) [some b_j for $1 \le j \le q$ is in S. Since this b_j is a branch $b_j \neq c_k$ for $1 \le k \le p \Rightarrow b_j = b$],

We have that b must be in one of the $b_1, b_2, \ldots, b_q$.

This shows that b is in the fundamental circuit Γ_1 associated with the chord c_1.

Now by using the same argument, we can conclude that b is in every fundamental circuit associated with the chords $c_2, \ldots, c_p$.

Thus b is contained in every fundamental circuit associated with the chords $c_1, c_2, \ldots, c_p$ in the cut-set S.

Part-(iii): Now we will show that b is not in any other fundamental circuit.

For this, suppose b occurs in a fundamental circuit Γ_{p+1} that associated with a chord other than $c_1, c_2, \ldots, c_p$.

Now Γ_{p+1} and S have even number of common elements (by the Theorem 16.2.3).

Since b is common there exists one more element common in S and Γ_{p+1}

$\Rightarrow c_i \in \Gamma_{p+1}$ for some i,

a contradiction for the selection of Γ_{p+1}.

So b is not in Γ_{p+1}.

Thus b is not in any other fundamental circuit.

This completes the proof of the theorem.

16.5.4 Example: Consider the graph G, and the spanning tree $T = \{b, c, e, h, k\}$ given in the Figures 16.5.2A and 16.5.2 B.

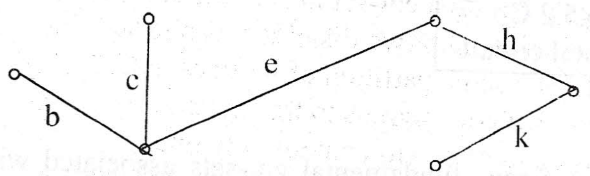


Fig-16.5.4 A

Consider the branch e of T.

Now $S = \{e, d, f\}$ is a fundamental cut-set associated with the branch e.

Note that d, f are chords.

Therefore the two fundamental circuits made by the chords d and f are:

Fundamental circuit associated with chord d is {d, c, e}, and the fundamental circuit associated with chord f is {f, e, h, k}.

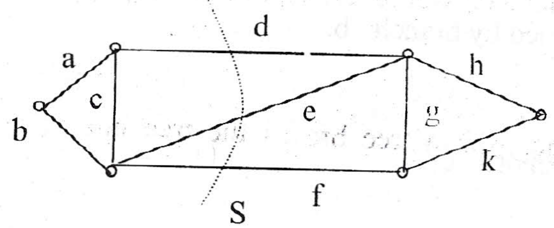


Fig-16.5.4 B

We may observe that the branch e is contained in both these fundamental circuits, and the branch e is not in the three remaining fundamental circuits
(which are {a, c, b}, {c, d, f, g}, {g, b, k}).

16.6 SUMMARY

In this lesson, we learnt about cutsets, properties of cutsets and their applications. Inparticular their use in to identifying the weak spots in a communication net. For a given graph we were able to find all cutsets, fundamental cutsets and their interrelations with circuits. We observed that every branch of spanning tree defines a unique fundamental cutset, just as every chord of a spanning tree defines a unique fundamental circuit. We came to know that the term fundamental cut set (like the term fundamental circuit) has meaning only with respect to a given spanning tree. We had shown in Theorem 16.4.4 how other cut sets of a graph can be obtained from given set of cut sets.

16.7 TECHNICAL TERMS

Cut set: A subset of the set of all edges of a connected graph whose removal from the graph leaves the graph disconnected; and the removal of any proper subset of it does not disconnect the graph.

fundamental circuit: A circuit formed by adding a chord to a spanning tree.

fundamental cut set: Let T be a spanning tree of a connected graph G, and 'b' be a branch in T. Since {b} is a cut-set in T, the set {b} partitions all the vertices of T into two disjoint sets one at each end of b. Consider the same partition of vertices in G, and the cut-set S in G that corresponds to this partition. Now it is clear that this cut-set S will contain only one branch b of T, and the other edges (if any) in S are chords with respect to T. Such a cut-set S containing exactly one branch of the tree T is called a fundamental cut-set (or basic cut-set) with respect to T.

16.8 ANSWERS TO SELF ASSESSMENT QUESTIONS

1: No. (Reason: the set of edges {a, c, h, d} is not a cut-set (because, one of its proper subsets {a, c, h} is a cut-set)).

2: Yes. (Reason: because removal of any edge from a tree breaks the tree into two disjoint connected components).)

16.9 MODEL QUESTIONS

1. Define the terms (i). cut set; (ii). fundamental cut set and give an example for each.

2. Show that every circuit has an even number of edges in common with any cut set.

3. Show that the ring sum of any two cutsets in a graph is either a third cut set or an edge disjoint union of cut sets.

4. Prove with respect to a given spanning tree T of G, a branch b (that determines a fundamental cut-set S) is contained in every fundamental circuit associated with the chords in S, and in no others.

16.10 REFERENCE BOOKS

1. Bondy J.A and Murty U.S.R, "Graph Theory with applications", North Holland, New York (1976).

2. Douglas B. West "Introduction to Graph Theory", Second Edition, Prentice Hall of India, New Delhi, 2002.

3. Harary Frank. "Graph Theory", Addison - Wesley Publishing Company, Inc., Reading, Mass., 1969.

4. John Clark and Derek Allan Holton, "A first look at Graph Theory" Allied Publishers, 1995

5. Narsingh Deo "Graph theory with applications to Engineering and Computer Science", Prentice Hall of India Pvt., Ltd., New Delhi, 1993.

6. Satyanarayana Bhavanari and Syam Prasad Kuncham "Graph Theory for Beginners", Satyasri Maths Study Centre, Guntur, AP, 2003.

Name of the Author of this Lesson: **Dr.Bhavanari Satyanarayana**

LESSON - 17

CONNECTIVITY AND SEPARABILITY

Objectives

The objectives of this lesson are to:

- discuss about edge connectivity and vertex connectivity of a counter graph G
- learn some concepts related to separable graphs.
- know the relationship between spanning trees and cutsets.
- discuss about few applications of the concepts like edge connectivity and vertex connectivity.
- know different version of Menger's Theorem.

Structure

17.0 INTRODUCTION

In this lesson, we define the other parameters of a graph namely edge connectivity and vertex connectivity. The that vertex connectivity is meaningful only for graphs that have three or more vertices and are not complete.

Menger, in 1927, showed that the vertex connectivity of a graph is related to the number of vertex - disjoint paths between two vertices in a graph. A variation of Menger's theorem, a very important and practical result in the maximum - flow, minimum - cut theorem.

The purpose of this lesson is to find the best way of connecting 'n' stations that are connected by 'e' lines.

17.1 CONNECTIVITY

17.1.1 Definition: The number of edges in the minimal cut-set (that is, cut-set with the fewest number of edges) is called the **edge connectivity** of G. [Equivalently, the edge connectivity of a connected graph G can be defined as the minimum number of edges whose removal (that is, deletion) reduces the rank of the graph by one]. Some authors use $\lambda(G)$ to denote the number 'edge connectivity of G'.

17.1.2 Example:(i)Consider the graph-(a) given in the Fig-17.1.2A.

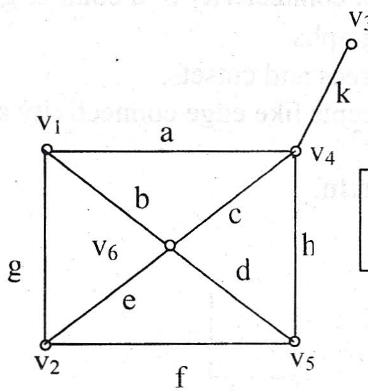


Fig-17.1.2 A
Graph-(a)

The edge-connectivity of this graph is 1 (because {k} is the only a smallest cut-set with fewest number of edges).

(ii) Consider the graph-(b) given in the Fig-17.1.2B.
The edge-connectivity of this graph is 2 (because {a, b} is the smallest cut-set with fewest number of edges).

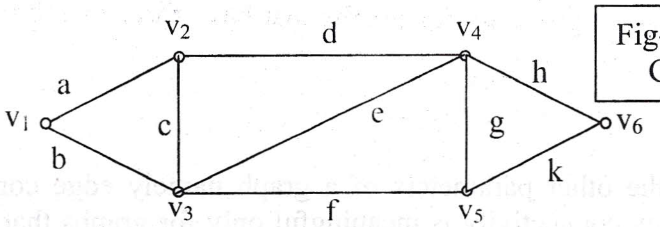
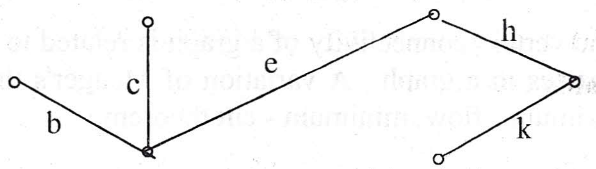


Fig-17.1.2 B
Graph-(b)



·Fig-17.1.2 C
T: is a tree

(iii) The edge-connectivity of a tree is 1 (because every branch in a tree is a cut-set and it is also smallest).

17.1.3 Definition: The **vertex connectivity** (or connectivity) of a (connected) graph G is defined as the minimum number of vertices, whose removal from G provides a disconnected graph. Some authors use k(G) to denote the 'vertex connectivity of G'.

17.1.4 Example: (i) The vertex connectivity of the graph-(a) given in the Fig-17.1.2A is 1 (because we get a disconnected graph if we remove the vertex v_4 from graph-(a)).

(ii) The vertex connectivity of the graph-(b) given in the Fig-17.1.2B is 2 (because the removal of two vertices only can disconnect the graph).

Self Assessment Question 1: *Consider the graph-(c) given in Fig-17.1.4. What is the vertex connectivity of this graph ?*

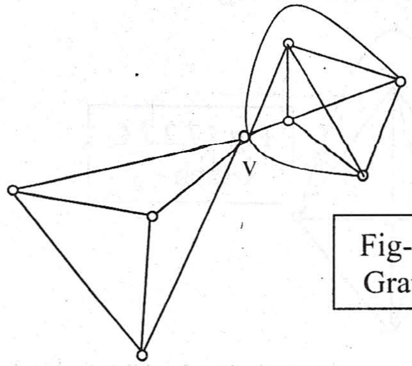


Fig-17.1.4
Graph-(c)

17.1.5 Note: (i) The vertex connectivity of a tree is one.

(ii) Vertex connectivity and edge connectivity defines only for the connected graphs. Some authors defines both the edge connectivity and vertex connectivity of a disconnected graph as 0.

(iii) Vertex connectivity is meaningful only for graphs that have three or more vertices and are not complete.

17.2 SEPARABILITY

17.2.1 Definition: A connected graph G is said to be **separable** if its vertex connectivity is one [equivalently, a connected graph G is said to be **separable** if there exists a subgraph g in G such that $\bar{g}$ (the complement of g) and g have only one vertex in common]. A graph which is not separable is called as **non-separable** graph.

17.2.2 Example: (i) Consider the graph-(c) given in Fig-17.2.2A.

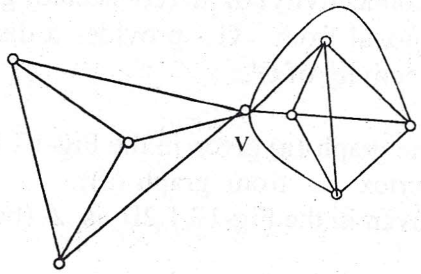


Fig-17.2.2 A
Graph-(c)

It is a separable graph (because the vertex connectivity of this graph is one).

[**Verification:** Consider the graphs g and $\bar{g}$ given in the Figures 17.2.2 B and C.

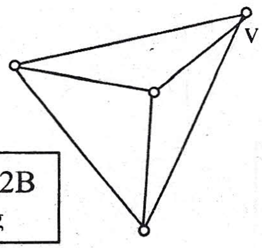


Fig-17.2.2B
Graph - g

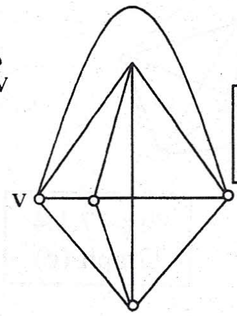


Fig-17.2.2 C
Graph - $\bar{g}$

The graphs g and $\bar{g}$ are subgraphs of the graph-(c). We observe that the graph $\bar{g}$ is the complement of g. Also g and $\bar{g}$ have only one vertex v in common.
So the graph-(c) is a separable graph.]

17.2.3 Definition: In a separable graph, a vertex whose removal disconnects the graph is called a **cut-vertex** or a **cut-node** or an **articulation point.**

17.2.4 Example: Consider the graph-(c) given in the Fig-17.2.2A. In this graph, v is a cut-vertex.

17.2.5 Note: In a tree, every vertex with degree > 1, is a cut-vertex.

17.2.6 Example: Consider the tree T given in the Fig-17.2.6

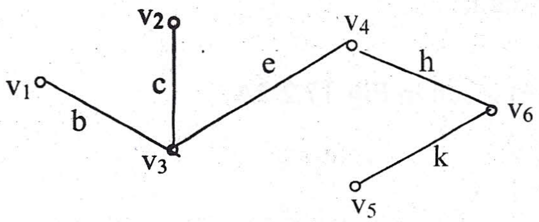


Fig-17.2.6

Here $d(v_3) = 3$, $d(v_4) = 2$, and $d(v_6) = 2$.

So the vertices v_3, v_4, and v_6 are cut-vertices.

[Observe that the removal of any one of these three vertices disconnects the graph].

17.3 MORE CONCEPTS ON CONNECTIVITY AND SEPARABILITY

17.3.1 Theorem: A vertex v in a connected graph G is a cut-vertex $\Leftrightarrow$ there exists two vertices x and y in G such that every path between x and y passes through v.

Proof: Let v be any vertex in a connected graph G.
Assume that v is a cut-vertex.
Then clearly the removal of v from G disconnects the graph G.
That is, $G - v$ is disconnected.
Hence $G - v$ has at least two components.
[Since every disconnected graph contains at least two components].
Since 'v' is a cut-vertex, we have that the removal of v from G partitions the vertex set V into two disjoint subsets V_1 and V_2 (say).
Since $G - v$ has two components, we have that V_1
consists of the points of one component, and V_2 consists of the points of the other component.
Then any two vertices $x \in V_1$ and $y \in V_2$ lie in different components of $G - v$.
Therefore every $x - y$ path in G contains v.
Thus every path between x and y passes through v.

Converse: Suppose that every path between x and y passes through v.

We show that this vertex v is a cut-vertex in G.
Since every path between two vertices x and y in G passes through v, we have that there can not be a path joining these two vertices x and y in $G - v$.
Thus $G - v$ is disconnected, and hence v is a cut-vertex in G.
This completes the proof.

17.3.2 Theorem: The edge connectivity of a graph G cannot exceed the degree of the vertex with the smallest degree.
In symbols, we can write as $\lambda(G) \leq \delta(G)$, where
$\lambda(G)$ = edge connectivity, and
$\delta(G) = \delta(v)$ where v is with minimum degree].
Proof: Let v be a vertex with the smallest degree in G.
Let $s = d(v)$ = degree of v.
Then there exist edges $e_1, e_2, \ldots, e_s$ with end point v.
Now the removal of the edges $e_1, e_2, \ldots, e_s$, will disconnect the graph.
So there exists a subset S of $\{e_1, e_2, \ldots, e_s\}$ which is a cut-set.
Now we got a cut-set S such that $|S| \leq s = d(v)$.
We know that edge connectivity $= \min\{|Y| \ / \ Y \text{ is a cut-set}\}$
$\leq |S| \leq d(v)$.

Hence the theorem.

17.3.3 Theorem: The vertex connectivity of a graph G can never exceed the edge connectivity of G. In symbols, we write $k(G) \leq \lambda(G)$, where $k(G)$ denotes the vertex connectivity, and $\lambda(G)$ denotes the edge connectivity.

Proof: Let the edge connectivity of G be α.

So there exists a cut-set S with $|S| = \alpha$.
Let 'S' partitions the set of vertices of G into subsets V_1 and V_2.
Now by removing at most α-vertices either from V_1 (or from V_2) on which the edges in S are incident, we can have the same effect as the removal of S.
So there exists vertices $v_1, v_2, \ldots v_\alpha$ whose removal from G creates a disconnection

$\Rightarrow$ vertex connectivity $\leq \alpha$

$\Rightarrow$ vertex connectivity $\leq$ edge connectivity.

Hence the vertex connectivity of any graph G can never exceed the edge connectivity of G.

Combining the statements of the two Theorems 17.3.2 and 17.3.3, we get the following Theorem 17.3.4.

17.3.4 Theorem: For any graph G, we have the following:

vertex connectivity $\leq$ edge connectivity $\leq$ d(v), where v is the vertex with smallest degree. [In symbols, we can write this as $k(G) \leq \lambda(G) \leq \delta(G)$].

Self Assessment Question 2: *Verify that in a non-separable graph with more than two vertices, every cut-set contains at least two edges.*

17.3.5 Theorem: Consider all the graphs with 'n' vertices and 'e' edges

(with $e \geq n - 1$).

The maximum vertex connectivity among all these graphs, is the integral part of the number $\frac{2e}{n}$

(that is, $\left[\frac{2e}{n}\right]$).

Proof: part-(i) Let G be a graph with n vertices and e edges.

Since every edge in G contributes two to the degrees of the vertices, we have that the total (2e degrees) is divided among n vertices.

If all the vertices are of equal (same) degree, then $d(v) = \frac{2e}{n}$ for all vertices v.

Otherwise, there must be at least one vertex in G whose degree is less than the number $\frac{2e}{n}$.

By the Theorem 17.3.4, we have that $k(G)$ = vertex connectivity $\leq$ d(v), where v is the vertex with smallest degree.

Since d(v) is the degree of a vertex with smallest degree, we have that $d(v) \leq \frac{2e}{n}$.

Therefore $k(G) \leq d(v) \leq \frac{2e}{n} \Rightarrow k(G) \leq \frac{2e}{n}$.

Part-(ii): Now we have to show that this value can be actually achieved.
That is, we have to construct a graph with n vertices, and e edges with vertex connectivity equal to $\left[\frac{2e}{n}\right]$.

For this, we construct an n-vertex regular graph G^* of degree $\left[\frac{2e}{n}\right]$ and then we add the remaining $e - \frac{n}{2}\left[\frac{2e}{n}\right]$ edges (arbitrarily) between any two pairs of vertices.

Now by removing $\left[\frac{2e}{n}\right]$ vertices only, one can get a disconnected graph form G^*.

Thus the vertex connectivity of G^* is equal to $\left[\frac{2e}{n}\right]$.

Thus maximum vertex connectivity $= \left[\frac{2e}{n}\right]$.

17.3.6 Note: The three theorems 17.3.2, 17.3.3 and 17.3.6 can be summarized as follows:

vertex connectivity $\leq$ edge connectivity
$\leq$ d(v) where v is with minimum degree
$\leq \frac{2e}{n}$

(because there exist vertex with degree $\leq \frac{2e}{n}$), and the maximum vertex connectivity is $\left[\frac{2e}{n}\right]$.

17.3.7 Example: Consider the graphs 1 and 2 (given in the Figures 17.3.7 A and B).

These are graphs with 8 vertices and 16 edges.

Here we can achieve a vertex connectivity (and therefore edge connectivity) as high as 4 $(= \frac{2 \times 16}{8} = \frac{32}{8} = 4)$.

(i) **In Graph-1**, we observe that the vertex connectivity = 1, and the edge connectivity = 3.

(ii) In Graph -2, we observe that the vertex connectivity = 4,

and the edge connectivity = 4.

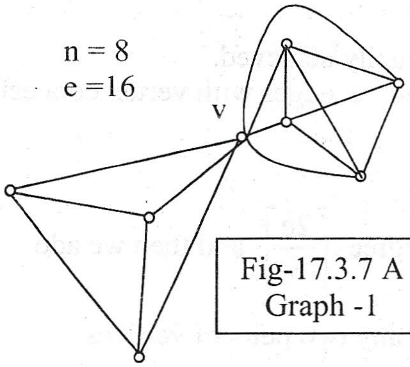


Fig-17.3.7 A
Graph -1

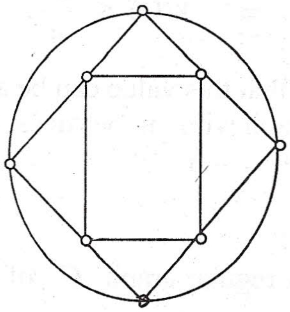


Fig-17.3.7 B
Graph -2

n = 8
e = 16

17.3.8 An application: Suppose we are given n stations that are to be connected by means of e lines (telephone lines/ bridges/ rail roads/ tunnels/ high ways) where $e \geq n - 1$.
What is the best way of connecting?
Here by "best" we mean that the network should be as invulnerable to the destruction of individual stations and individual lines as possible.
[In other words, construct a graph with n vertices and e edges that has the maximum possible edge connectivity and vertex connectivity].

17.3.9 Example: Consider the Graph-1 given in the Example 17.3.7.

Here if one vertex v is bombed, then the remaining stations can not communicate each other. If three lines destroyed, then the stations can not communicate each other.

17.3.10 Example: Consider the Graph-2 given in the Fig-17.3.7B.

For this graph, vertex connectivity = 4 = edge connectivity.
Consequently, even after any three stations are bombed, (or any three lines destroyed), the remaining stations can still communicate with each other.

17.4 MENGER'S THEOREM

17.4.1 Definition: A graph G is said to be **k-connected if the vertex** connectivity of G is k

[observe that 1-connected graphs are same as separable **graphs].**

17.4.2 Definition: Let u, v be two distinct points of a connected graph G.

(i) Two paths joining u and v are called **disjoint** (some times called **point-disjoint**) if they have no points other than u and v (and hence no lines) in common.

(ii) Two paths joining u and v are called **line-disjoint** if they have no lines in common.

17.4.3 Definition: A set S of points, lines or points and lines separates u and v if u and v are in different components of G - S. [Clearly, no set of points separates two adjacent points].

17.4.4 Theorem: (Menger's Theorem) The minimum number of points separating two non-adjacent points s and t is the maximum number of disjoint s-t paths.

Proof: part-(i): Suppose that k points separate s and t.

If (the number of disjoint paths joining s and t) $\geq$ k + 1, then we should remove at least k + 1 points to separate s and t, a contradiction.

Therefore there can not be more than k disjoint paths joining s and t.

Now it remains to show that there are k disjoint s - t paths in G.

This is obvious if k = 1.

Part-(ii): In a contrary way, suppose that the result is not tree for some k > 1.

[That is, there exists a graph G, two points s and t in G such that it takes k points to separate s and t, the number of disjoint s - t paths is less than k].

Let h be the smallest among such numbers k.

So there exists a graph F, two points s, t in F, it takes h points to separate s and t, the number of distinct s - t paths is less than h. .... (i)

We remove lines from F until we obtain a graph G such that h points are required to separate s and t in G but for any line x of G, only (h - 1) points are required to separate s and t in $G\backslash\{x\}$.

Part-(iii): Now we investigate some properties in G.

By the definition of G, for any line x of G, there exists a set S(x) of (h -1) points which separate s and t in G - {x}.

Now G - S(x) contains at least one s - t path, since it takes h points to separate s and t in G.

Also each such s - t path must contain the line $x = \overline{uv}$.

Now v, u $\notin$ S(x).

If u $\neq$ s and u $\neq$ t, then S(x) $\cup$ {x} separates s and t in G.

Now we verify that

"No point is adjacent to both s and t in G" ...... (ii)

In a contrary way, suppose ω is adjacent to both s and t in G.

Then G - ω requires (h - 1) points to separate s and t and so (by the minimality of h) the graph G - ω has (h - 1) disjoint s - t paths.

Replacing ω, we have h disjoint s - t paths in G, a contradiction to (i). Therefore (ii) is true.

Part-(iv): Let W be any collection of h points separating s and t in G.

We call "a path joining s with some $\omega_i \in W$ and containing no other point of W" as **s -W path**.

Write P_s = collection of s - W paths, and

P_t = collection of W - t paths.

So each $s - t$ path begins with a member of P_s and ends with a member of P_t (because every $s - t$ path contains a points of W).
Moreover, the paths in P_s, P_t have the points of W in common and no others in common.
Part-(v): Now we show that either $P_s - W = \{s\}$ or $P_t - W = \{t\}$.
If not, both P_s plus the lines $\{\omega_1 t, \omega_2 t, \ldots\}$, and P_t plus the lines $\{s\omega_1, s\omega_2, \ldots\}$ are graphs with fewer points than G in which s and t are non-adjacent and h-connected.
Therefore in each, there are h disjoint $s - t$ paths (we get these paths by combining $s - W$ and $W - t$ portions), a contradiction.
So $P_s - W = \{s\}$ or $P_t - W = \{t\}$
$\Rightarrow$ all the points in W are adjacent to s or all the points of W are adjacent to t.
Now we proved that any collection W of h points separating s and t is adjacent either to s or to t ..... (iii)

Part-(vi): Let $P = \{s, u_1, u_2, \ldots, t\}$ be a shortest $s - t$ path in G and let $\overline{u_1 u_2} = x$.
If $u_2 = t$, then we have the given diagram and so u_1 is adjacent to both s and t, a contradiction to (ii).

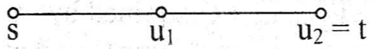


Fig-17.4.4

Hence $u_2 \neq t$.

Suppose $S(x) = \{v_1, v_2, \ldots, v_{h-1}\}$ where $S(x)$ is the separating set containing $(h - 1)$ points in $G \setminus \{x\}$. [Note that here $S(x)$ separates s and t].
If $\overline{u_1 t}$ is in G, then u_1 is adjacent to both s and t, a contradiction to (ii).
Therefore $\overline{u_1 t} \notin G$.
Write $W = S(x) \cup \{u_1\}$.
Then W is separates s and t in G.
Now by (iii), all the points of W are either adjacent to s or adjacent to t.
Since u_1 is adjacent to s, we have that all the points of W are adjacent to s.
Thus $sv_i \in G$ for $1 \leq i \leq (h-1)$.
So (by (ii)), $v_i t \notin G$ for all i.
Write $W^* = S(x) \cup \{u_2\}$.
Then W^* is separating s and t in G.
Now by (iii), all the points of W^* are adjacent to s or adjacent to t.
Since $v_1, \ldots, v_{h-1}$ are adjacent to s, we have that $\overline{su_2} \in G$.
Now $\{s, u_2, u_3, \ldots, t\}$ is a path from s to t shorter than P (see the beginning of Part-(vi)), a contradiction.
Hence the (contrary) assumption at the beginning of part-(ii), is not tree.
This completes the proof of the theorem.

17.4.5 Theorem: (Menger's Theorem - Part-ii)

A connected graph G is k-connected ⇔ every pair of vertices in G is joined by k or more paths that do not intersects (means vertex disjoint paths) and at least one pair of vertices is joined by k non-intersecting paths.

Proof: Suppose G is k-connected.

Then to separate any two points s and t, we should have at least k points in the separating set W

[and there exist two points s and t for which a separating set W for s and t contains exactly k points].

⇔ there exist at least k vertex disjoint paths between any two vertices s and t

[and there exist two points s and t such that there exist exactly k vertex disjoint paths between s and t]

⇔ every pair of vertices in G is joined by k or more paths that do not intersects and at least one pair of vertices is joined by k non-intersecting paths.

This completes the proof.

17.4.6 Theorem: (Edge version of Menger's theorem)

The edge connectivity of a graph G is k ⇔ every pair of vertices in G is joined by k or more edge-disjoint paths (that is, paths that may intersect, but have no edge in common), and at least one pair of vertices is joined by exactly k edge-disjoint paths.

Proof: Suppose that the edge connectivity of G is k.

Let u, v be two distinct vertices of G.

Then any u - v separating set of edges must have at least k edges.

So there must be at least k edge disjoint u - v paths, as required.

Also there exist a pair of vertices which are joined by k edge disjoint paths.

Converse: Suppose that given any pair of distinct vertices u and v of G, there are at least k edge disjoint paths from u to v (and at least one pair of vertices is joined by exactly k edge-disjoint paths).

So for each pair of vertices u and v, every u - v separating set of edges must have at least k edges.

Thus it requires the deletion of at least k edges from G in order to produce a disconnected graph.

17.5 SUMMARY

In this lesson we learnt the concepts of edge connectivity, vertex connectivity and separability. We studied some results based on these concepts. Then we switched over to prove an important theorem, namely Menger's Theorem in vertex version and the edge version. We constructed a graph with n vertices and e edges that has the maximum possible edge connectivity and vertex connectivity.

17.6 TECHNICAL TERMS

Edge Connectivity: The number of edges in the minimal cut-set (that is, cut-set with the fewest number of edges).

Vertex Connectivity: The vertex connectivity (or connectivity) of a (connected) graph is the minimum number of vertices, whose removal disconnects the graph.

Separability: A connected graph with vertex connectivity one.

Cut - Vertex: In a separable graph, a vertex whose removal disconnects the graph.

k- Connected: The vertex connectivity of a graph is k.

17.7 ANSWERS TO SELF ASSESSMENT QUESTIONS

1: Clearly the vertex connectivity of this graph is 1 (because the removal of v disconnects the graph).

2: Let S be a cut-set in a non-separable graph G.

Since G is non-separable, we have that vertex connectivity > 1.

Now 1 < vertex connectivity ≤ edge connectivity ≤ $|S|$

$\Rightarrow |S| > 1 \Rightarrow |S| \geq 2$.

$\Rightarrow$ S contains at least two elements.

$\Rightarrow$ S contains at least two edges.

17.8 MODEL QUESTIONS

1. Prove that a vertex v in a connected graph G is a cut-vertex $\Leftrightarrow$ there exists two vertices x and y in G such that every path between x and y passes through v.

2. Prove that the vertex connectivity of a graph G can never exceed the edge connectivity of G.

3. Prove that the minimum number of points separating two non-adjacent **points** s and t is the maximum number of disjoint s-t paths.

4. Show that a connected graph G is k-connected $\Leftrightarrow$ every pair of vertices in G is joined by k or more paths that do not intersects (means vertex disjoint paths) and at least one pair of vertices is joined by k non-intersecting paths.

17.9 REFERENCE BOOKS

1. Bondy J.A and Murty U.S.R, "Graph Theory with applications", North Holland, New York (1976).

2. Douglas B. West "Introduction to Graph Theory", Second Edition, Prentice Hall of India, New Delhi, 2002.

3. Harary Frank. "Graph Theory", Addison - Wesley Publishing Company, Inc., Reading, Mass., 1969.

4. John Clark and Derek Allan Holton, "A first look at Graph Theory" Allied Publishers, 1995

5. Narsingh Deo "Graph theory with applications to Engineering and Computer Science", Prentice Hall of India Pvt., Ltd., New Delhi, 1993.

6. Satyanarayana Bhavanari and Syam Prasad Kuncham "Graph Theory for Beginners", Satyasri Maths Study Centre, Guntur, AP, 2003.

Name of the Author of this Lesson: **Dr.Bhavanari Satyanarayana**

LESSON - 18

PLANAR GRAPHS

Objectives

The objectives of this lesson are to:

- know the notion of a planar graph.
- understand the characterization of planar graphs
- observe the Kuratowski's graph
- identify different representations of a planar graph.

Structure

18.0 INTRODUCTION

In this lesson we consider the embedding (drawing without crossings) of graphs on surfaces, especially on the plane. We study the planar graphs, which has great significance from a theoretical point of view i.e., whether it is possible to draw a graph G in a plane without its edges crossing over. Planarity and other related concepts are useful in many practical situations. In designing printed circuits, it is desirable to have as few lines cross as possible.

We also observed the non - planar graphs, called Kuratoski's graphs. We provided a useful characterization of Kuratoski's graphs. That is., a graph is non- planar if it contains either of the graphs K_5 or $K_{3,3}$ as subgraphs. We gave an illustration to cetrtain results in this lesson for better understanding.

18.1 PLANAR GRAPHS

18.1.1 Note: (i) Now we define an abstract graph $G_1 = (V, E, \varphi)$.

Suppose V consists the 5 objects named as a, b, c, d and e; and E consists of 7 objects (none of which is in V) named as 1, 2, 3, 4, 5, 6, 7.

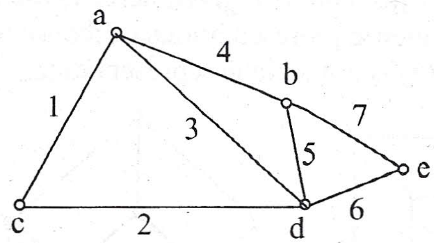
The relationship between the two sets V and E is defined by the mapping φ.

$$\varphi = \begin{bmatrix} 1 \to \{a, c\} & 5 \to \{b, d\} \\ 2 \to \{c, d\} & 6 \to \{d, e\} \\ 3 \to \{a, d\} & 7 \to \{b, e\} \\ 4 \to \{a, b\} & \end{bmatrix}$$

Here $1 \to \{a, c\}$ means that object 1 from E is mapped onto the pair (unordered) $\{a, c\}$ of objects from V.

(ii) Now this combinatorial abstract object $G_1 = (V, E, \varphi)$ can be represented by means of a geometric figure, which is given in Figure-18.1.1. Now the Figure-18.1.1 shows a geometric representation of G_1.

Fig-18.1.1



18.1.2 Definition: (i) A graph G is said to be a **planar graph** if there exists some geometric representation of G which can be drawn on a plane such that no two of its edges intersect.

(ii) A graph that can not be drawn on a plane without a cross over between its edges is called a **non-planar graph**.

(iii) A drawing of a geometric representation of a graph on any surface such that no edges intersect is called an **embedding**.

18.1.3 Note: A graph G is non-planar if all the possible geometric representations of G can not be embedded in a plane.

18.1.4 Note: We can define the planar graph as follows:

(i) A geometric graph G is **planar** if there exists a graph G^* which is isomorphic to G that can be embedded in a plane. Otherwise, G is **non-planar**.

(ii) An embedding of a planar graph G on a plane is called a **plane representation** of G.

18.1.5 Note: Consider the graph given in Figure-1.

Figure-1

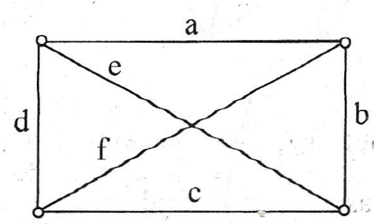
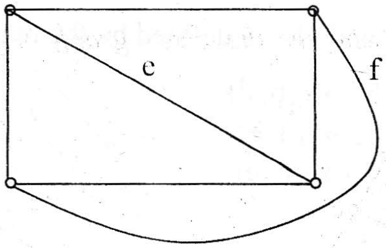
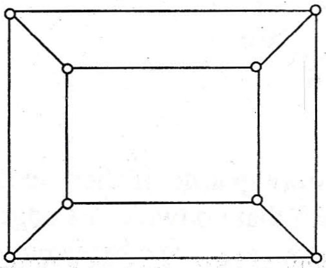


Figure - 2

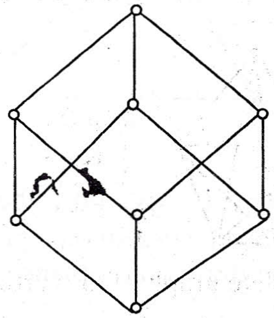


If we draw the edge f out side the quadrilateral while the other edges are unchanged, then we get the Figure-2.
The graph given in Figure-2 can be embedded in a plane.
So the graph given in Figure-2 is planar. Therefore the graph given in Figure-1 is a planar graph.

18.1.6 Example: Observe the graphs - (a) and (b) given here. These two graphs are isomorphic to each other. But they are different geometric representations of the same graph. Here Graph-(a) is a plane representation, and the Graph-(b) is not a plane representation.



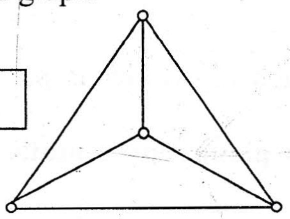
Graph - (a)

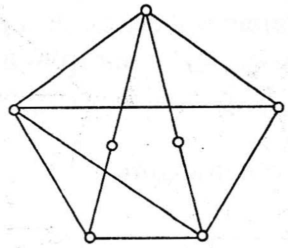


Graph- (b)

18.1.7 Example: Consider the following graphs G_1, G_2 and G_3. Clearly G_1 and G_3 are planar. G_3 is a geometric representation of G_2; and G_3 can be embedded in a plane. Therefore G_2 is also a planar graph.

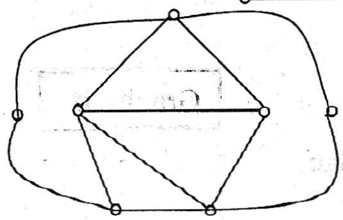
G_1



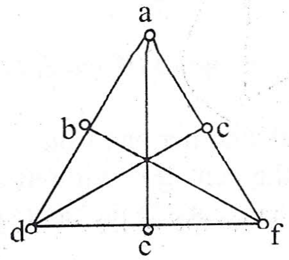


G_2

G_3



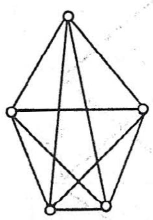
Self Assessment Question 1: *Check whether the given graph is planar. If so give its planar representation*



18.2 KURATOWSKI'S TWO GRAPHS

In this section, we discuss two non-planar graphs which are named as **Kuratowski's graphs** (after the Polish Mathematician Kasimir, Kuratowski, who discovered their unique property).

18.2.1 Note: Observe the graph K_5 (Kuratowski's first graph) given here. This is a complete graph on 5 vertices.



K_5

18.2.2 Theorem: The complete graph of 5 vertices (denoted by K_5) is a non-planar graph.

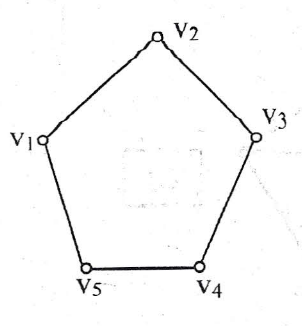
Proof: Suppose the five vertices of the complete graph are v_1, v_2, v_3, v_4, v_5.

Since the graph is complete, we get a circuit going from

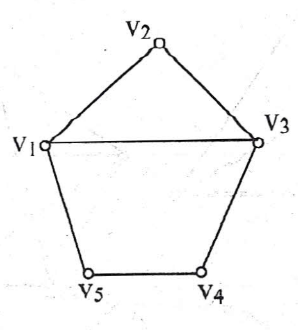
v_1 to v_2 to v_3 to v_4 to v_5 to v_1.

That is, we have a pentagon (given in Graph-A).

Now this pentagon must divide the plane of the paper into two regions, one inside and the other outside.



Graph - A

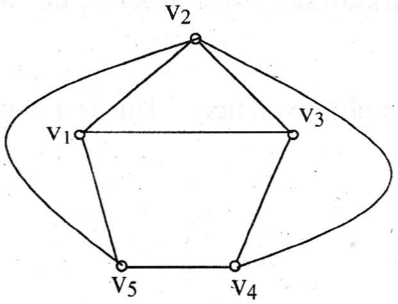


Graph - B

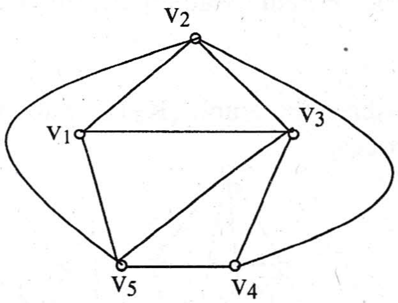
We have to connect v_1 and v_3 by an edge.

This edge may be drawn inside (or) outside the pentagon (without intersecting the 5 edges of Graph-A).

Let us select a line from v_1 to v_3 inside the pentagon. (if we choose outside, then we end up with a similar argument). Now we have Graph-B.
Now we have to draw an edge from v_2 to v_4, and another one from v_2 to v_5.
Since neither of these edges can be drawn inside the pentagon without crossing over the edges that have already drawn, we have to draw both these edges outside the pentagon.
Now we have Graph-C.
Now the edge connecting v_3 and v_5 can not be drawn outside the pentagon without crossing the edge between v_2 and v_4. So v_3 and v_5 have to be connected with an edge inside the pentagon. Now we have the Graph-D.



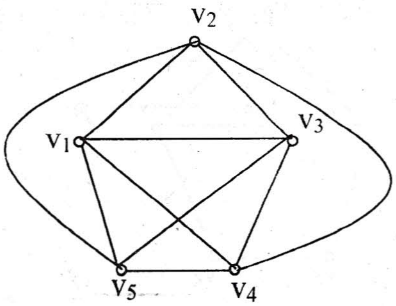
Graph - C



Graph - D

Now we have to draw an edge between v_1 and v_4.

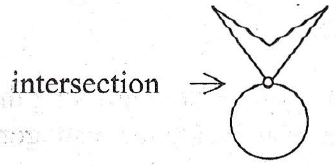
It is clear that this edge can not be drawn either inside (or) outside the pentagon without a cross-over (Observe Graph-E).
Thus this graph can not be embedded in a plane.
Hence the complete graph K_5 on 5 vertices is non-planar.

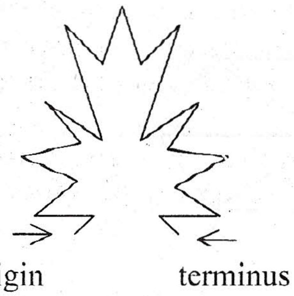


Graph - E

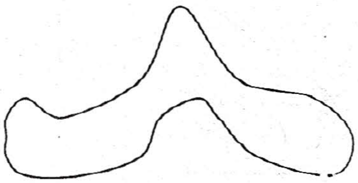
18.2.3 Note: A **Jordan curve** is the continuous non-self-intersecting curve whose origin and terminus coincide.

18.2.4 Example:





C_1 C_2



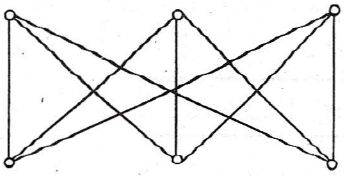
C_3

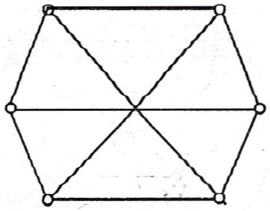
(i) C_1 is not a Jordan curve (because it intersects itself).

(ii) C_2 is not a Jordan curve (because origin and terminus are not coincide).

(iii) C_3 is a Jordan curve.

18.2.5 Definition: Consider the graphs (a) and (b) given here. These are regular connected graphs with 6 vertices and 9 edges. These two graphs are isomorphic and so they represent the same graph. This graph is called as the **Kuratowski's 2nd graph.** These two graphs show the two common geometric representations of the Kuratowski's second graph.





(a) (b)

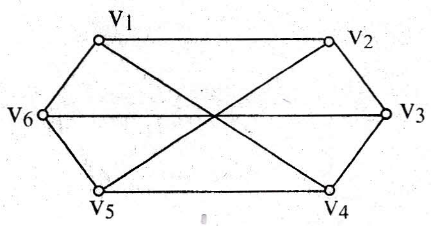
Fig. 18.2.5(a) Fig: 18.2.5.(b)

The Kuratowski's 2nd graph is denoted by $K_{3,3}$.

18.2.6 Theorem: Kuratowski's 2nd graph is a non-planar graph.

Proof: Observe the Kuratowski's 2nd graph $K_{3,3}$.

$K_{3,3}$



It is clear that the graph contains six vertices v_i, $1 \le i \le 6$ and there are edges

$\overline{v_1v_2}$, $\overline{v_2v_3}$, $\overline{v_3v_4}$, $\overline{v_4v_5}$, $\overline{v_5v_6}$, $\overline{v_6v_1}$.

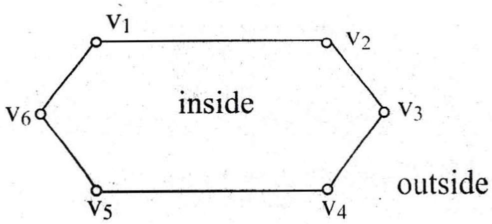


Fig- 18.2.6 (a)

Now we have a Jordan curve. So plane of the paper is divided into two regions, one inside and the other outside.

Since v_1 is connected to v_4, we can add the edge $\overline{v_1v_4}$ in either inside or outside (without intersecting the edges already drawn). Let us draw $\overline{v_1v_4}$ inside.

(If we choose outside, then we end up with the same argument Now we have the Fig- 18.3.6(b))

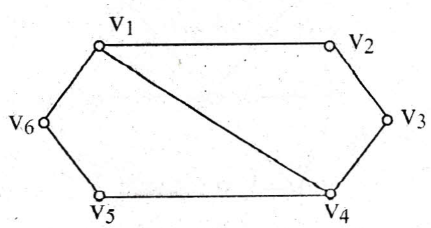


Fig- 18.2.6 (b)

Next we have to draw an edge $\overline{v_2v_5}$ and also another edge $\overline{v_3v_6}$.

First we draw $\overline{v_2v_5}$.

If we draw it inside, we get a cross over the edge $\overline{v_1v_4}$.

So we draw it outside. Then we get the Fig-18.2.6(c).

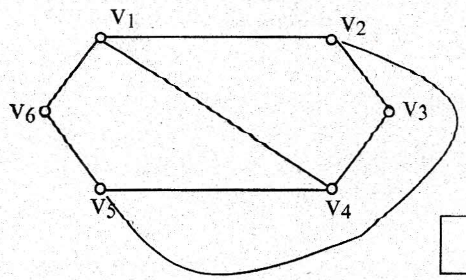


Fig-18.2.6(c)

Still we have to draw an edge from v_3 to v_6.

If $\overline{v_3v_6}$ drawn inside, it cross the edge $\overline{v_1v_4}$ (see the Fig-18.2.6(d)).

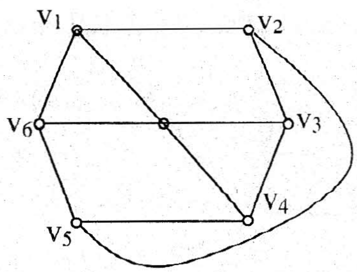


Fig-18.2.6(d)

So we can not draw it inside.

So we select the case of drawing $\overline{v_3v_6}$ cross the edge $\overline{v_2v_5}$ (see the Fig-18.2.6(e)).
Thus $\overline{v_3v_6}$ can not be drawn either inside or outside with out a cross over.
Hence the given graph is not a planar graph.

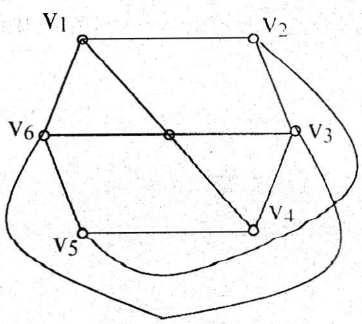


Fig-18.2.6(e)

18.2.7 Note : In the notations: K_5, $K_{3,3}$, the letter K represents the first letter in the name Kuratowski.

18.2.8 Common properties of Kuratowski's 1^{st} and 2^{nd} graphs:

(i) Both are regular graphs.

(ii) Both are non-planner.

(iii) Removal of one edge (or) vertex makes each a planar graph.

(iv) The two graphs are non-planar with the smallest number of edges.
Thus both are the **simplest** non-planar graphs.

Self Assessment Question 2: *Let G be a graph with a representation containing two intersecting edges. Can we conclude that "G is non planar".*

18.3 DIFFERENT REPRESENTATIONS OF A PLANAR GRAPH

18.3.1 Note: A plane graph G divides the plane into number of **regions** [also called **windows**, **faces**, or **meshes**] as shown in following Fig-18.3.1.

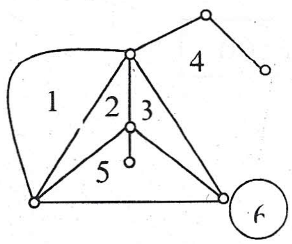


Fig-18.3.1

A region characterized by the set of edges or the set of vertices forming its boundary.

In the Fig-18.3.1, the numbers 1, 2, 3, 4, 5, 6 stand for the regions.

18.3.2 Note: (i) A region is not defined in a non-planar graph

(ii) For example, we can not define region in the graph by Fig-18.3.2.

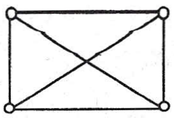
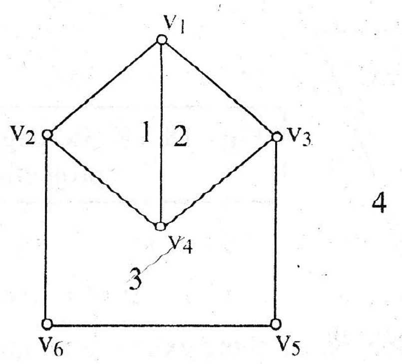


Fig-18.3.2

18.3.3 Note: The portion of the plane lying out side a graph embedded in plane (such as the region 4 in the graph given in the Fig-18.3.1) is called an **infinite** [or **unbounded** or **outer** or **exterior**] **region** for that particular plane representation.
In the Fig-18.3.1, the region 4 is an infinite Region.

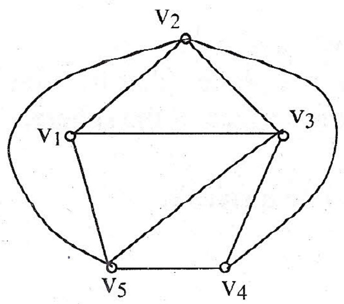
18.3.4 Example: Observe the graph given in the Fig-18.3.4. Clearly it has 4 regions. The region 4 is an infinite region.

Fig-18.3.4

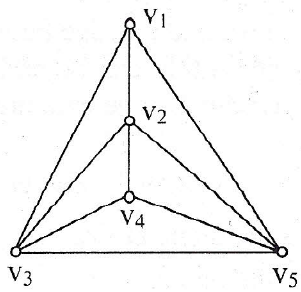


18.3.5 Note: If we consider two different embeddings of a given planar graph, then the infinite regions of these two representations may be different.

18.3.6 Example: Consider the graph G_1 and G_2 given here.



Graph - G_1



Graph - G_2

These two graphs are two different embeddings of the same graph. Here the finite region $v_1 v_3 v_5$ in G_1 becomes the infinite region in G_2.

18.3.7 Embedding on a sphere: To eliminate the distinction between finite and infinite regions, a planar graph is often embedded in the surface of a sphere.
It is accomplished by stereographic projection of a sphere on a plane.

18.3.8 Theorem: A graph can be embedded in the surface of a sphere $\Leftrightarrow$ it can be embedded on a plane.

Proof: Put the sphere on the plane, and call the point of contact SP (South pole). Now draw a straight line perpendicular to the plane at SP. Let the point of intersection of this line with the surface of the sphere be called NP (North pole). Observe the Figure 3.8.8

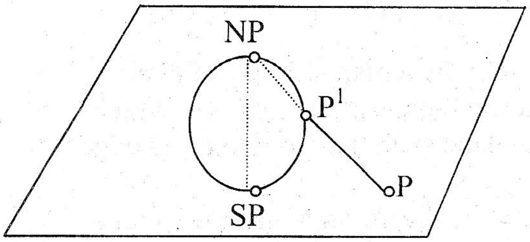


Fig - 18.3.8 Stereographic projection

Now corresponding to any point P on the plane, there exists a unique point P^1 on the sphere and vice versa; where P^1 is the point at which the straight line from P to NP intersects the surface of the sphere.

If graph contains vertices $v_1, v_2, \ldots, v_n$, and $v_1^1, v_2^1, \ldots, v_n^1$ are the corresponding points on the sphere, then there is a one-to-one correspondence between the set $\{v_1^1, v_2^1, \ldots, v_n^1\}$ of points of the sphere and the set $\{v_1, v_2, \ldots, v_n\}$ of finite points on the plane.

If there is an edge between v_i and v_j, then we add an edge between v_i^1 and v_j^1.

From this construction, it is clear that any graph that can be embedded in a plane (that is, drawn one plane such that its edges do not intersect) can also be embedded in the surface of the sphere.

Converse: Take a graph with vertices $v_1^1, v_2^1, \ldots, v_n^1$ that embedded on a sphere.

Draw line through NP and v_i^1. It meets the plane at v_i.

Now represent the points $v_1, v_2, \ldots, v_n$ on the plane.

If there is an edge between v_i^1 and v_j^1, then we draw an edge between v_i and v_j.

So we can conclude that any graph that can be embedded on sphere can be embedded on a plane.

18.3.9 Theorem: A planar graph may be embedded in a plane such that any specified region (that is, specified by the edges forming it) can be made the infinite region.

Proof: A planar graph embedded in the surface of a sphere divides the surface into different regions.

Each region in the sphere is finite.

The infinite region on the plane having been mapped onto the region containing the point NP.

Now it is clear that by suitably rotating the sphere we can make any specified region map onto the infinite region on the plane. From this we have the conclusion.

18.4 SUMMARY

In this lesson, we learnt the concepts of a planar graph, non - planar graph and embedding. We analyzed find whether a given graph is planar or non - planar, and discussed two specific and most important fundamental non - planar graphs: Kuratowski's 1st and 2nd graphs. We also presented few examples to understand these explicitly.

18.5 TECHNICAL TERMS

Planar graph: *A graph G is said to be a planar graph if there* exists some geometric representation of G which can be drawn on a plane such that no two of its edges intersect.

Non - planar graph: A graph that can not be drawn on a plane without a cross over between its edges.

Embedding: A drawing of a geometric representation of a graph on any surface such that no edges intersect.

Kuratowski's 1st graph: A complete graph with five vertices.

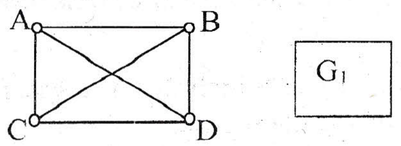
Kuratowski's 2nd graph: A regular connected graph with 6 vertices and 9 edges.

Infinite region: The portion of the plane lying out side a graph embedded in the plane is an infinite region for that particular plane representation.

18.6 ANSWERS TO SELF ASSESSMENT QUESTIONS

1: No

2: (i). Consider the graph



In G_1, AD and BC are intersecting edges, but it is a planar graph.

(ii). Consider the graph K_5. Here we have intersecting edges but it is non - planar.
Conclusion: We cannot say about the planarity of a graph having two intersecting edges.

18.7 MODEL QUESTIONS

1. Define the terms planar graph, Embedding, plane representations, Kuratowski's two graphs.
2. Show that the complete graph of 5 vertices (denoted by K_5) is a non-planar graph.
3. Prove that Kuratowski's 2nd graph is a non-planar graph.
4. Prove that a graph can be embedded in the surface of a sphere $\Leftrightarrow$ it can be embedded on a plane.

18.8 REFERENCE BOOKS

1. Bondy J.A and Murty U.S.R, "Graph Theory with applications", North Holland, New York (1976).

2. Douglas B. West "Introduction to Graph Theory", Second Edition, Prentice Hall of India, New Delhi, 2002.

3. Harary Frank. "Graph Theory", Addison - Wesley Publishing Company, Inc., Reading, Mass., 1969.

4. John Clark and Derek Allan Holton, "A first look at Graph Theory" Allied Publishers, 1995

5. Narsingh Deo "Graph theory with applications to Engineering and Computer Science", Prentice Hall of India Pvt., Ltd., New Delhi, 1993.

6. Satyanarayana Bhavanari and Syam Prasad Kuncham "Graph Theory for Beginners", Satyasri Maths Study Centre, Guntur, AP, 2003.

Name of the Author of this Lesson: **Dr. Bhavanari Satyanarayana**

LESSON : 19

EULER'S FORMULA AND DUAL GRAPHS

Objectives

After reading this lesson, the reader should able to:

(i) know the number of regions of a connected planar graph.
(ii) observe the plane representation of a graph.
(iii) know the step wise procedure to detect the planarity.
(iv) write the geometric dual of a planar graph.

Structure

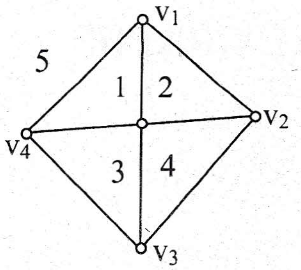
19.0 INTRODUCTION

In this lesson, we give a simple formula showing the relationship between the number of vertices, edges and faces in a connected plane graph. It is one of the best known formulae in Graph Theory and was proved by Euler in 1752. In this lesson we study a necessary and sufficient condition for a graph G to be planar namely Kuratowski's Theorem.

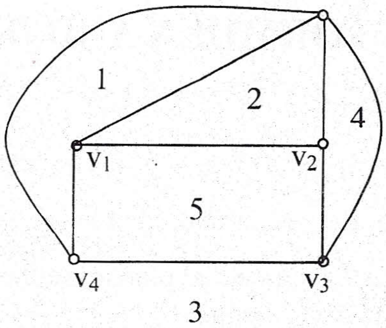
The existence of a dual graph gives another alternative characterization of a planar graph. Whitney gave a combinatorial definition of dual, which is an abstract formulation of the concept of geometric dual. He also proved that a graph is planar if and only if it has combinatorial dual. Geometric dual of a graph depends on the embedding of the graph in the plane. So the same graph may have different geometric duals for different embeddings.

19.1. EULER'S FORMULA

19.1.1 Example: Consider the 3-connected wheel given in Graph-(a). The Graph-(b) is another embedding into the plane (for the same graph). These Graph-(a) and Graph-(b) can be represented on the sphere.



Graph - (a)



Graph - (b)

Observe that the representation Graph-(a) divide the plane into 5 regions.

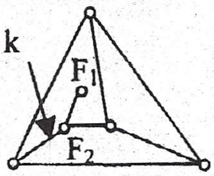
Here the region 5 in an infinite region.
Observe the Graph-(b). In this graph the region 3 in the infinite region.
The following Euler's formula provides an information about the number of regions in any planar graph.

19.1.2 **Theorem: (Euler's Formula)** A connected planar graph with n vertices and e edges has $e - n + 2$ regions.
[Let G be a connected plane graph and let n, e, and f denote the number of vertices, edges and faces (or regions) of G respectively.
Then $n - e + f = 2$ (or) $f = e - n + 2$].
Proof: We prove this theorem by Mathematical Induction on the number of faces f.
Part-(i): Suppose that $f = 1$.
Then G has only one region.
If G contains a cycle, then it will have at least two faces, a contradiction.
So G contains no cycles.
Since G is connected, we have that G is a tree.
We know that in a tree $n = e + 1$.
So $e - n + 2 = e - (e + 1) + 2 = 1 = f$.
So the statement is true for $f = 1$.
Part-(ii): Now suppose the Induction hypothesis that $f > 1$ and the theorem is true for all connected plane graphs with the number of faces less than f.
Since $f > 1$, we have that G is not a tree (since a tree contains only one infinite region).
Then by a known theorem [Statement: G is a tree $\Leftrightarrow$ every edge of G is a bridge], G has an edge k, which is not a bridge.
So the subgraph $G - k$ is still connected.
Since any subgraph of a plane graph is also a plane graph, we have that $G - k$ is also a plane graph.
Since k is not a bridge, we have that k is a part of a cycle.
[Since an edge e of G is a bridge $\Leftrightarrow$ e is not part of any cycle in G].

So it separates two faces F_1 and F_2 of G from each other.

Therefore in G - k, these two faces F_1 and F_2 combined to form one face of G - k.
We can observe this fact in the Figures-19.1.2A and B.

Fig-19.1.2 A
Graph G
4 faces



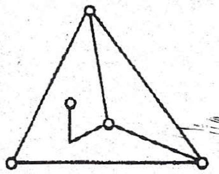


Fig-19.1.2 B
Graph G - k
3 faces

Let n(G - k), e(G - k), f(G - k) denote the number of vertices, edges and faces of G - k respectively.
Now we have n(G - k) = n, e(G - k) = e - 1 and
f(G - k) = f - 1.
By our induction hypothesis, we have that n(G - k) - e(G - k) + f(G - k) = 2

$\Rightarrow$ n - (e - 1) + (f - 1) = 2

$\Rightarrow$ n - e + f = 2 $\Rightarrow$ f = e - n + 2.

Hence by Mathematical Induction, we conclude that the statement is true for all connected planar graphs.

Self Assessment Question 1: *Suppose that a connected simple planar graph has 20 vertices each of degree 3. Into how many regions does a representation of this planar graph split the plane ?*

19.1.3 Definition: Let ϕ be a face of a plane graph G. We define the **degree of** ϕ (denoted by $d(\phi)$) to be the number of edges on the boundary of ϕ.

19.1.4 Note: For any interior face ϕ of a simple plane graph, we have that $d(\phi) \geq 3$.

19.1.5 Theorem: Let G be a simple planar graph with n vertices and e edges, where $n \geq 3$. Then (i) $2e \geq 3f$ (or $e \geq \frac{3}{2}f$) (ii) $e \leq (3n - 6)$

Proof: Case-(i) Suppose that G is connected.

Part-(i): If n = 3, then we have three vertices.

Since G is simple, there exist at most three edges.

So $e \leq 3$. If e = 3, then G is given by the Figure-19.1.5.

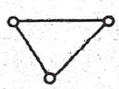


Fig-19.1.5

So f = 2 and e = 3 $\Rightarrow 2e \geq 3f$

If e < 3, then (since G is connected) e = 2 and f = 1

$\Rightarrow$ $2e \geq 3f$.

In this case, we proved (i).

Since $e \leq 3$, we have $3n - 6 = 3 \times 3 - 6 = 3 \geq e$.

In this case, we proved (ii).

Part-(ii): Now assume that $n \geq 4$.

If G is a tree, then $f = 1$ and $e = n - 1$

Now $e = n - 1 \geq 4 - 1 = 3$

$$\geq \frac{3}{2} = \frac{3}{2} \times 1 = \frac{3}{2} f.$$

Also $(3n - 6) - e = (3n - 6) - (n - 1)$

$$= 2n - 5 \geq 2 \times 4 - 5 \geq 0$$

$\Rightarrow$ $3n - 6 \geq e$.

Therefore (i) and (ii) are true if G is a tree and $n \geq 4$.

Part-(iii): Now suppose that $n \geq 4$ and G is not a tree. Since G is connected, G contains a cycle.

Since G is simple (there are no multiple edges), we have that each face has at least three edges on its boundary, and so $d(\phi) \geq 3$ for each face ϕ.

Write $b = \sum_{\phi \in \xi} d(\phi)$ ...... (i)

where ξ denotes the set of all faces of G.

There are f faces participated in the sum (i), and each face has at least three edges.

So each face contributes at least 3 in the sum (i).

So f faces contribute 3f. Now we get that $b \geq 3f$.

When we are summing up for b (in (i)), each edge of G (if it is counted) was counted either once or twice.

(Twice if it occurred as a boundary edge for two faces).

Even if all edges participate in the sum (i), then the number is 2e. So $b \leq 2e$.

Now $2e \geq b \geq 3f$ $\Rightarrow$ $e \geq (\frac{3}{2})f$ (or $\frac{2}{3}e \geq f$)

Part-(iv): Now by Euler's formula, we have that $e - n + 2 = f$ (or) $n = e - f + 2$.

Now $n = e - f + 2 \geq e - (\frac{2}{3}e) + 2 = \frac{e}{3} + 2$

$\Rightarrow$ $n \geq \frac{e}{3} + 2$ $\Rightarrow$ $3n \geq e + 6$ $\Rightarrow$ $e \leq 3n - 6$.

This proves (ii).

Case (ii): Now suppose that G is a non-connected graph.

Step-(i): Let $G_1, \ldots G_t$ be its connected components, and let n_i, e_i denote the number of vertices, number edges (respectively) in G_i for each i ($1 \le i \le t$).

Now $n = \sum_{i=1}^{t} n_i$ and $e = \sum_{i=1}^{t} e_i$.

Then each G_i is a planar connected simple graph (since G is planar simple graph).

So we have that $e_i \le 3n_i - 6$ (by case(i)) for $1 \le i \le t$.

Now $e = \sum_{i=1}^{t} e_i \le \sum_{i=1}^{t} (3n_i - 6)$

$= \sum_{i=1}^{t} 3n_i - \sum_{i=1}^{t} 6 = 3\sum_{i=1}^{t} n_i - 6t$

$= 3n - 6t \le 3n - 6$ (since $t \ge 1 \Rightarrow 6t \ge 6 \Rightarrow -6t \le -6$)

Hence $e \le 3n - 6$.

Step-(ii): Suppose that each G_i creates f_i regions.
Then $(f_i - 1)$ regions are internal regions of G_i.
Now f = (the number of internal regions of G) + 1 (related to external region)

$= [\sum_{1}^{t} (\text{number of internal regions of } G_i)] + 1$

$= [\sum_{1}^{t} (f_i - 1)] + 1 = \sum_{1}^{t} f_i - t + 1$

$= [\sum_{1}^{t} f_i] - (t - 1)$ [since G is disconnected and t = no. of components > 1

we have $t - 1 > 0$].

$\le [\sum_{i=1}^{t} \frac{2e_i}{3}] - (t - 1)$ [since $3f_i \le 2e_i$ by case (i)]

$= [\frac{2}{3} \sum_{1}^{t} e_i] - (t - 1)$

$= \frac{2}{3} e - (t - 1) \le \frac{2}{3} e$ (since $t - 1 > 1$)

$\Rightarrow f \leq \frac{2}{3} e \quad \Rightarrow \quad 3f \leq 2e$

This proves (i). This completes the proof.

19.1.6 **Note:** In some cases, the relation (given in the statement of the Theorem 19.1.5) $e \leq 3n - 6$ may be useful in finding out whether a given graph is planar or not.

19.1.7 **Corollary:** The Kuratowski's 1st graph K_5 (The complete graph on five vertices) is non-planar.

Proof: In a contrary way suppose that K_5 is planar.
Observe the diagram (given in Fig-19.1.7) for K_5.

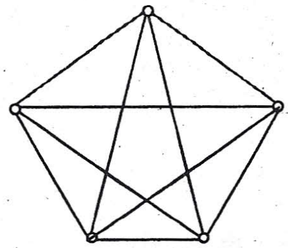


Fig-19.1.7
K_5

It is a simple graph with $n = 5 \geq 3$ and $e = 10$.
By the Theorem 4.5, we have that $3n - 6 \geq e$
$\Rightarrow 9 \geq e = 10$, a contradiction.
So we conclude that K_5 is a non-planar graph.

19.1.8 **Note:** (i) The Theorem 19.1.5, states that the **planar graphs** satisfy the condition $e \leq 3n - 6$.

(There exists some non-planar graphs which satisfy this condition).

(ii) From the following example we can understand that $K_{3,3}$ is a non-planar graph and satisfies the condition that $e \leq 3n - 6$.

19.1.9 **Example:** Consider the Kuratowski's 2nd graph $K_{3,3}$.

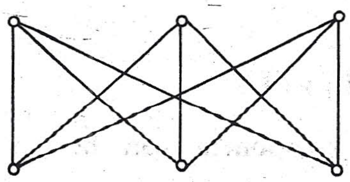


Fig-19.1.9 A

$K_{3,3}$

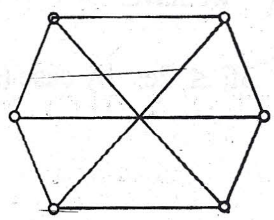


Fig-19.1.9 B

Clearly this graph $K_{3,3}$ satisfies the equation $e \leq 3n - 6$.

[Reason: In $K_{3,3}$, we have that $e = 9$ and $n = 6$.
Now $3n - 6 = 12 \Rightarrow e < 3n - 6$].
But we know that $K_{3,3}$ is a non-planar graph.

19.1.10 Problem: Show that $K_{3,3}$ is non-planar.

Solution: In a contrary way, we suppose that $K_{3,3}$ is planar.
Note that $n = 6$ and $e = 9$.
In $K_{3,3}$ every face has at least four edges on its boundary.
So $d(\phi) \geq 4$ for each face ϕ.
Write $b = \sum_{\phi \in \xi} d(\phi)$ ... (i)

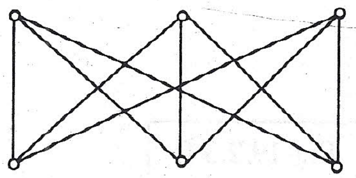


Fig-19.1.10 A

$K_{3,3}$

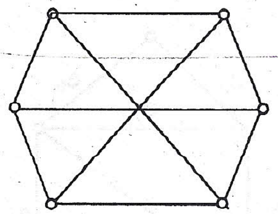


Fig-19.1.10 B

where ξ denotes the set of all faces of G.
The notation we use is $|\xi| = f$.
Now $b = \sum_{\phi \in \xi} d(\phi) \geq \sum_{\phi \in \xi} 4 = |\xi| \times 4 = 4f$.
Since each edge was counted either once or twice in (i) (if it is counted) (twice if it occurred as a boundary edge for two faces), we have that $b \leq 2e$.
Therefore $2e \geq b \geq 4f$
$\Rightarrow e \geq 2f$
$\Rightarrow e \geq 2(e - n + 2)$ (since $f = e - n + 2$)
$\Rightarrow 9 \geq 2(9 - 6 + 2) \Rightarrow 9 \geq 2(5)$
$\Rightarrow 9 \geq 10$, a contradiction.
Hence $K_{3,3}$ is a non-planar graph.

19.2. PLANE REPRESENTATION AND CONNECTIVITY

In a disconnected graph, the embedding of each component can be considered independently.
So it is clear that a disconnected graph is planar $\Leftrightarrow$ each of its components is planar.
Thus it is enough to study the planarity for connected graphs.
Similarly, in a separable graph, the embedding of each block can be considered independently.
So a separable graph is planar $\Leftrightarrow$ each of its block is planar.

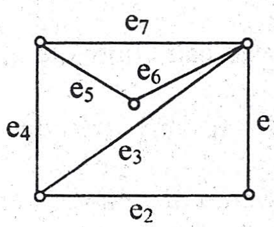
Thus it is enough to study the concepts embedding (or) planarity only for non-separable graphs.

19.2.1 Definition: Two embeddings of a planar graph on spheres are said to be **not distinct**, if the embeddings can be made to coincide by suitably rotating one sphere with respect to the other and possibly distorting (that is, either pulling or adjusting) the regions (without leaving a vertex cross an edge).

19.2.2 Definition: If every pair from the set of all possible embeddings of the given graph G on a sphere, are not distinct, then we say that the graph G have **unique embedding** on a sphere. In this case, we also say that G have a **unique plane representation**.

19.2.3 Example: Consider the two embeddings (of the same graph) given in Fig-19.2.3.In the embedding (b), the infinite region (with respect to plane) is bounded with 5 edges. In the embedding (a), the infinite region is bounded with 4 edges. Also it can be observed that in the embedding (a), there is no region which is bounded by 5 edges.

Fig-19.2.3 A



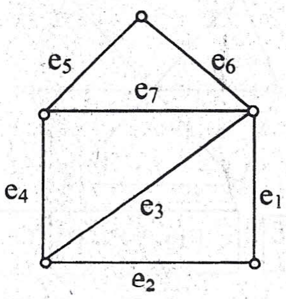


Fig-19.2.3 B

Thus by rotating two spheres on which (a) and (b) are embedded, we can not make them coincide. Hence the two embeddings are distinct. So we conclude that the graph has no unique plane representation.

Self Assessment Question 2 : *Check whether the two planar representation of a graph have the same regions ?*

19.2.4 Example: Observe the two graphs given in Figure-19.2.4A and B.

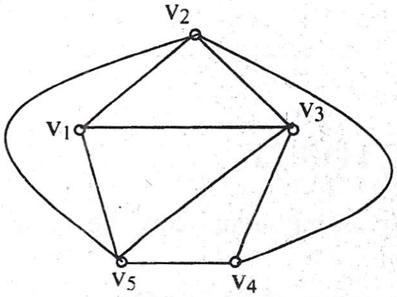


Fig-19.2.4 A

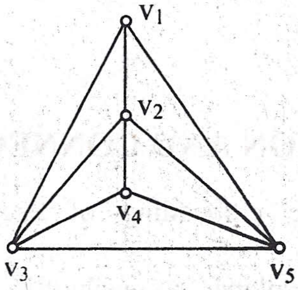


Fig-19.2.4 B

These two graphs are two embeddings of the same graph. If we consider their representations on a sphere, they can be made to coincide.
[Remember that edges can be bent, and in a spherical embedding there is no infinite region]. So the graph has a unique plane representation.

19.3. DETECTION OF PLANARITY

19.3.1 Elementary Reduction Procedure:

Step-(i): Since a disconnected graph is planar ⇔ each of its components is planar, it is enough to observe each component independently.
Also a separable graph is planar ⇔ each of its block is planar.
Therefore for the given arbitrary graph G, we determine the set $\{G_1, G_2, \ldots, G_k\}$ of all non-separable blocks of G.
Then it is enough to test planarity for each G_i.
Step-(ii): Since addition (or) removal of self-loops does not effect the planarity, we remove all self-loops.
Step-(iii): Since parallel edges do not affect the planarity, we can eliminate edges in parallel by removing all, but one edge between every pair of vertices.
Step-(iv): Elimination of a vertex of degree 2 by merging (or fusing) two edges in series does not effect the planarity.
[two edges are said to be in series if they have exactly one vertex in common and this vertex is of degree 2]
So eliminate all edges in series.
Repeated application of steps (iii) and (iv) will usually reduce the given graph drastically, and the reduced graph is very convenient for study.

19.3.2 Example: Consider the graph given in the Figure-19.3.2.

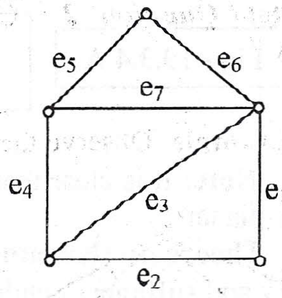


Fig-19.3.2

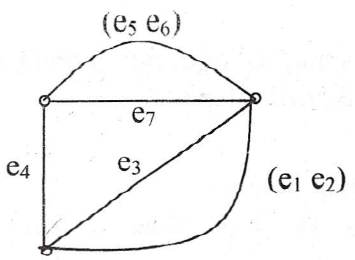


Fig - 19.3.2 (a)
Series Reduction

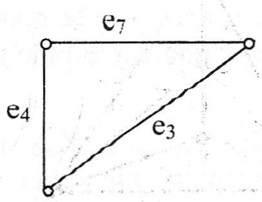


Fig - 19.3.2 (b)
Parallel Reduction

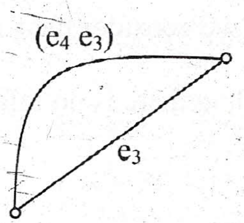


Fig - 19.3.2 (c)
Series Reduction

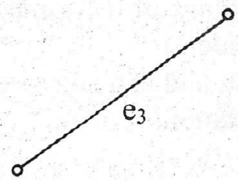


Fig - 19.3.2 (d)
Parallel Reduction

By the repeated applications of step (iii) and (iv) of the above procedure, we get the graph in Figure - 19.3.2 (d).

19.3.3 **Definition:** Two graphs G_1 and G_2 are said to be **homeomorphic** if the graph G_1 can be obtained from the graph G_2 by the creation of edges in series (that is, insertion of vertices of degree 2) (or) by the merge of edges in series.

19.3.4 **Example:** The three graphs given in the Figures-19.3.4A, B and C, are homeomorphic to each other.

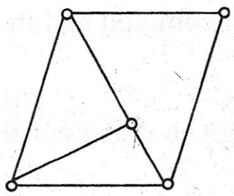


Fig - 19.3.4 A

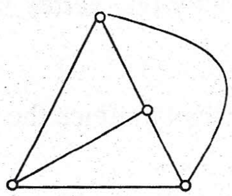


Fig - 19.3.4 B
(by merging)

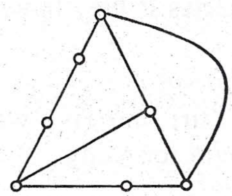


Fig - 19.3.4 C
(by creating)

19.3.5 **Note:** It is clear that if G_1 and G_2 are homomorphic, then G_1 is non-planar $\Leftrightarrow$ G_2 is non-planar.

19.3.6 **Theorem: (Kuratowski's Theorem (1930))**

A necessary and sufficient condition for a graph G to be planar is that G does not contain either of the Kuratowski's two graphs (or) any graph homeomorphic to either of them.

Proof: Let G be a planar graph.
We know that the Kuratowski's two graphs K_5 and $K_{3,3}$ are non-planar.
If the graph G contains a subgraph homeomorphic to either K_5 or $K_{3,3}$, then G is non-planar a contradiction to our assumption.
Thus there is no subgraph of G which is homeomorphic to either K_5 or $K_{3,3}$.

Converse: Suppose that G contains no subgraph which is homeomorphic to either K_5 or $K_{3,3}$. In a contrary way, suppose that G is non-planar.
Now let G be a non-planar graph having the minimum number of edges.
Then G must be a component.
Then $\delta(G) = \delta(v)$, the degree of v where v is of minimum degree ≥ 3.
Now we can obtain (for a complete proof, the reader may refer to (Harary "Graph Theory", Narosa Publishing House, New Delhi)) a subgraph of G^* of G which is homeomorphic to either of Kuratowski's two graphs, a contradiction.

19.3.7 **Note:** (i) Observe the graph given in the Figure - 19.3.7.

This graph is a non-planar graph and it contains no subgraph which is either isomorphic to K_5 or $K_{3,3}$.
From this example, we can understand that it is not necessary for a non-planar graph to have either of the Kuratowski's graphs as a subgraph.

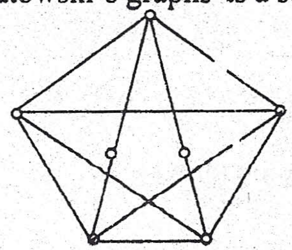


Fig-19.3.7

(ii) A non-planar graph contains a subgraph which is homeomorphic to one of the Kuratowski's graphs.

19.3.8 **Problem:** Find whether the given Graph 19.3.8 is planar?

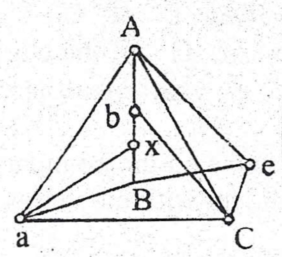


Fig- 19.3.8 A

Solution: Now we reduce the Graph-19.3.8, by removing edges (using the elementary reduction procedure) so that the remaining graph is still non-planar.
Let us remove the edges (a, x) and (A, C).

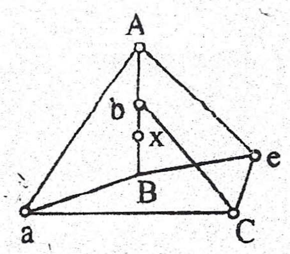


Fig-19.3.8 B

[Here we remove (A, C) to get a subgraph. This operation is not a part of elementary reduction procedure].
Then we get a subgraph which is Graph-(b).
Take Graph-(b) and merge the two edges (which are in series) at the vertex x. Then we get Graph-(c).
It is clear that Graph-(c) and Graph-(d) are homeomorphic.
Now it is easy to observe that Graph-(c) and Graph-(d) are two distinct representations of the same graph.
Graph-(d) is nothing but the Kuratowski's second graph.

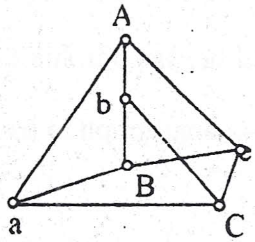


Fig-19.3.8 C

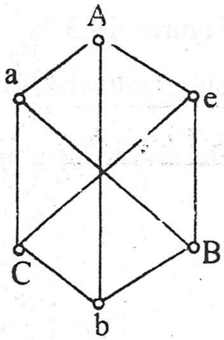


Fig-19.3.8 D

Therefore Graph-19.3.8A contains a subgraph which is homeomorphic to $K_{3,3}$.

Hence we conclude that the given graph is non-planar.

19.4. GEOMETRIC DUAL

19.4.1 Definition: Let G be a plane graph. We define the **dual** of G to be the graph G^* constructed as follows:

(i) To each face (or region) f of G there is a corresponding vertex f^* of G^*.

(ii) To each edge e of G, there is a corresponding edge e^* of G^* [if the edge e occurs on the boundary of the two faces f and g, then create an edge e^* that joins the corresponding vertices f^* and g^* in G^*].

[If the edge e is a bridge, then we treat it as an edge, it occurs twice on the boundary of the face f in which face it lies. So the corresponding edge e^* is a loop incident with the vertex f^* in G^*].

19.4.2 Procedure to construct a dual from a given graph:

Step-(i): Consider the given planar graph and identify the regions F_i, $1 \le i \le n$.
[Consider the plane representation of the graph given in Figure-19.4.2 A. In this graph there are 6 faces (or regions) F_1, F_2, F_3, F_4, F_5, and F_6].

Step-(ii): Place the points $p_1, p_2, \ldots, p_n$ on the plane one for each of the regions.
[In the example, place 6 points p_1, p_2, p_3, p_4, p_5, p_6.
Note that p_i is a point in the interior of the region F_i].
Observe the Fig-19.4.2 B.

Step-(iii): If two regions F_i and F_j are adjacent (that is, having a common edge), then draw a line joining the corresponding points p_i and p_j that intersects the common edge between F_i and F_j exactly once.
[If there is more than one edge common between F_i and F_j, then we draw one line between the points p_i and p_j for each of the common edges].
We perform this procedure for all $i, j \in \{1, 2, \ldots, n\}$ such that $i \neq j$.

Step-(iv): Suppose a region F_k contains an edge e lying

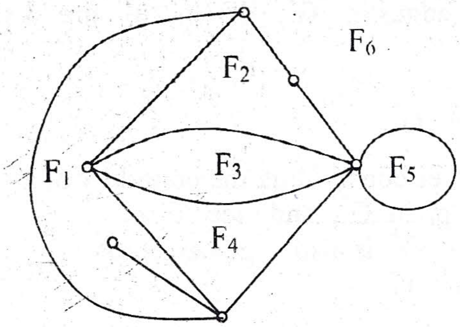


Fig-19.4.2 A

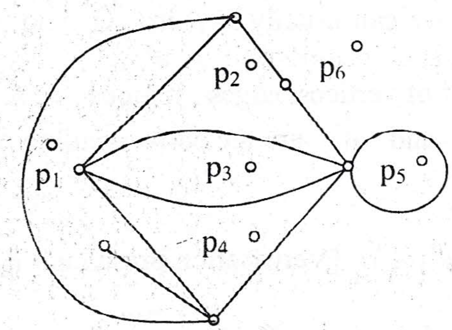


Fig-19.4.2 B

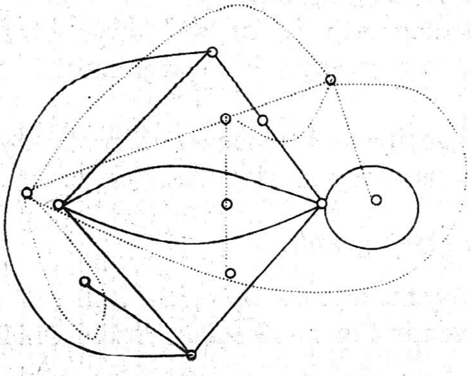


Fig-19.4.2 C

entirely in it, then we draw a self-loop at the point p_k intersecting e exactly once.

We perform this procedure for all such F_k.
By using this procedure we obtain a new graph G^*.
Such a graph G^* obtained here is called a **dual** (or **geometric dual**) of G.
[In this example, the dual G^* was shown with broken lines (observe Fig- 19.4.2 C). This dual G^* consist of 6 vertices p_1, p_2, p_3, p_4, p_5, and p_6 and the edges (broken) joining these vertices].

19.4.3 **Note:** From the construction of the dual G^* of G, it is clear that there is a one-to-one correspondence between the set of all edges of G and the set of all edges of G^*. Also note that one edge of G^* intersects one edge of G.

19.4.4 **Observations:** (i) An edge forming a self-loop in G yields a pendent edge in G^*.

(ii) A pendent edge in G yields a self-loop in G^*.

(iii) Edges that are in series in G produce parallel edges in G^*. [If e_1, e_2 are in series in G, then e^*_1, e^*_2 are parallel in G^*].

(iv) Parallel edges in G produce edges in series in G^*.

(v) It is a general observation that the number of edges constituting the boundary of a region F_i in G is equal to the degree of the corresponding vertex p_i in G^*, and vice versa.

(vi) The graph G^* is embedded in the plane, and so G^* is also a planar graph.

(vii) Consider the process of drawing a dual G^* from G.

It can be observed that G is a dual G^*.

Therefore instead of calling G^*, a dual of G, we can usually say that G and G^* are **dual graphs.**

(viii) If n, e, f, r and μ denotes the number of vertices, edges, regions, rank and nullity of a connected planar graph G, and if n^*, e^*, f^*, r^* and μ^* are the corresponding numbers in the dual graph G^*; then

$n^* = f$, $e^* = e$, $f^* = n$.

From these facts, we can get that $r^* = \mu$ and $\mu^* = r$ [Verification presented in the following problem].

Self Assessment Question 3: *If G^* is the dual of G, then verify that*

(i) rank of G = nullity of G^* [that is $r = \mu^*$]

(ii) rank of G^* = nullity of G [that is $r^* = \mu$]

19.4.5 **On the uniqueness of dual graphs:**

(i) Consider the graph G_1 and its dual G_1^*.

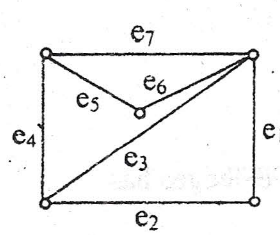


Fig-19.4.5A
Graph - G_1

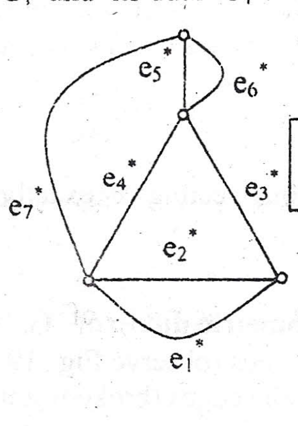


Fig-19.4.5 B
Graph - G_1^*

Also consider the Graph - G_2 and its dual Graph - G_2^*.

(ii) *Observe that Graph - G_1 and Graph - G_2 are two different* planar representations of a same graph (say, G).

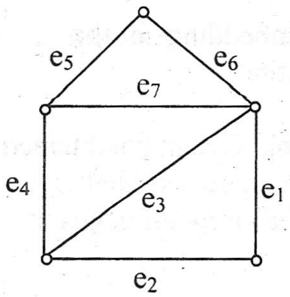


Fig-19.4.5 C
Graph - G_2

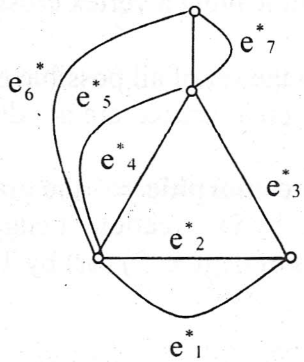


Fig-19.4.5 D
Graph - G_2^*

(iii) The Graph - G_2^* contains a vertex of degree 5, and the Graph - G_1^* contains no vertex of degree 5. Therefore G_1^* and G_2^* are non-isomorphic.
So we have that $G_1 \cong G_2$ but $G_1^* \quad G_2^*$.
(iv) From (iii), we may conclude that two isomorphic planar graphs may have distinct non-isomorphic duals.

19.5 SUMMARY

In this lesson, we revised that eventhough, a planar graph may have different plane representations, the number of regions resulting from each embedding is the same, which is precisely the Euler's formula, gives the number of regions in any planar graph. We studied that $e \leq 3n - 6$ is only a necessary but not a sufficient condition for the planarity of a graph. Kuratowski's 2nd graph stands as an example for this statement. Some simple and efficient criterion for detection of planarity was discussed.

It is observed that the geometric dual of a plane map is a plane graph. We deducted that two isomorphic planar graphs may have distinct non-isomorphic duals.

19.6 TECHNICAL TERMS

1. Euler's formula: A connected planar graph with n vertices and e edges has $e - n + 2$ regions.

2. Degree of ϕ, $(d(\phi))$: The number of edges on the boundary of a face ϕ of a plane graph G .

3. Not distinct embedding: (on sphere) The embeddings that can be made to coincide by suitably rotating one sphere with respect to the other and possibly distorting (that is, either pulling or adjusting) the regions (without leaving a vertex cross an edge).

4. Unique embedding: (on sphere) Every pair from the set of all possible embeddings of the given graph G on a sphere, are not distinct.

5. Homeomorphism: G_1 and G_2 are **homeomorphic** $\Leftrightarrow$ the graph G_1 can be obtained from the graph G_2 by the creation of edges in series (that is, insertion of vertices of degree 2) (or) by The merge of edges in series.

6. Kuratowski's theorem: A necessary and sufficient condition for a graph G to be planar is that G does not contain either of the Kuratowski's two graphs (or) any graph homeomorphic to either of them.

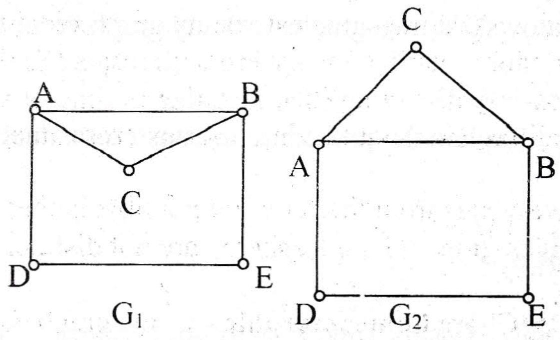
7. Dual: The **dual** of G to be the graph G^* constructed as follows:
(i) To each face (or region) f of G there is a corresponding vertex f^* of G^*.
(ii) To each edge e of G, there is a corresponding edge e^* of G^* [if the edge e occurs on the boundary of the two faces f and g, then create an edge e^* that joins the corresponding vertices f^* and g^* in G^*].
[If the edge e is a bridge, then we treat it as an edge, it occurs twice on the boundary of the face f in which face it lies. So the corresponding edge e^* is a loop incident with the vertex f^* in G^*].

19.7 ANSWERS TO SELF ASSESSMENT QUESTIONS

1: We know that $2|E| = \sum_{v} \deg(v) \Rightarrow 2|E| = 20 \times 3 = 60$

$\Rightarrow |E| = 30$. Now by Euler's formula, the number of regions is equal to $e - n + 2 = 30 - 20 + 2 = 12$.

2: Consider the following graphs:



In G_1, the infinite region is formed by the four edges AB, BE, DE and AD where as in G_2 there is no infinite region bounded by any four edges.

3: Suppose the graph G contains one component. Then $r = n - 1 = f^* - 1$

$= (\text{number of regions}) - 1$

$= (e^* - n^* + 2) - 1$

(since in general $f = e - n + 2$)

$= e^* - n^* + 1 = e^* - (n^* - 1)$

$=$ number of edges - rank

$=$ nullity $= \mu^*$

Now $r^* =$ rank of $G^* = n^* - 1$

$= (\text{number of vertices in } G^*) - 1$

$= (\text{number of regions in } G) - 1$

$= f - 1 = (e - n + 2) - 1 = e - (n - 1)$

$=$ number of edges in G - rank of G

$=$ nullity of G $= \mu$

19.8 MODEL QUESTIONS

1. Show that a connected planar graph with n vertices and e edges has $e - n + 2$ regions.

2. Let G be a simple planar graph with n vertices and e edges, where $n \geq 3$. Then Prove that (i) $2e \geq 3f$ (or $e \geq \frac{3}{2}f$) (ii) $e \leq (3n - 6)$.

3. Sh[illegible] hat the graphs $K_{3,3}$ and K_5 are non-planar.

4. Prove the necessary and sufficient condition for a graph G to be planar is that G does not contain either of the Kuratowski's two graphs (or) any graph homeomorphic to either of them.

5. Define Dual of a graph G and Explain the procedure to construct a dual from a given graph.

19.9 REFERENCE BOOKS

1. Bondy J.A and Murty U.S.R, "Graph Theory with applications", North Holland, New York (1976).

2. Douglas B. West "Introduction to Graph Theory", Second Edition, Prentice Hall of India, New Delhi, 2002.

3. Harary Frank. "Graph Theory", Addison - Wesley Publishing Company, Inc., Reading, Mass., 1969.

4. John Clark and Derek Allan Holton, "A first look at Graph Theory" Allied Publishers, 1995

5. Narsingh Deo "Graph theory with applications to Engineering and Computer Science", Prentice Hall of India Pvt., Ltd., New Delhi, 1993.

6. Satyanarayana Bhavanari and Syam Prasad Kuncham "Graph Theory for Beginners", Satyasri Maths Study Centre, Guntur, AP, 2003.

Name of the Author of this Lesson: **Dr. Bhavanari Satyanarayana**

LESSON – 20

VECTOR SPACES OF A GRAPH

Objectives

The objectives of this lesson are to:

- know some fundamental concepts in algebra, which are useful in the study of graphs
- represent graphs algebraically and to manipulate them algebraically
- understand that sets of certain subgraphs of a given graph satisfy some postulates, and thus form their groups.
- introduce the concepts: Modular Arithmetic, Galois field modulo m, k-dimensional vector space, and basis
- observe that, there is a vector space W_G associated with every graph G.

Structure

20.0 INTRODUCTION

The concept of vector space is an important tool in the theory and applications of graphs. Most of the digital computers do not allow to work on pictorial and design of graphs, so it is essential to represent a graph algebraically. In this lesson we brought out the structure of vector space associated with a graph; studied some of its properties in analogue of algebraic properties. We also obtained some simple results relating dimension, basis.

20.1 SETS WITH ONE OPERATION

20.1.1 Definition: A **set** is a collection of objects in which we can say whether a given object belongs to the collection or not. If A is a set and x is an object in A, then we say that a is an **element** of A. In this case we say that a **belongs** to A, and this fact is denoted by $a \in A$.

19

20.1.2 Definition: Let A, B be sets. If every element of A is an element of B, then we say that A is a **subset** of B.
If A is a subset of B and B has at least one element that is not in the set A, then A is called a **proper subset** of B.

20.1.3 Definition: Let S_1 and S_2 be any two sets.

(i) The set $\{x \,/\, x \in S_1 \text{ or } x \in S_2\}$ is said to be the **union** of S_1 and S_2. The union of S_1 and S_2 is denoted by $S_1 \cup S_2$.

(ii) The set $\{x \,/\, x \in S_1 \text{ and } x \in S_2\}$ is said to be the **intersection** of S_1 and S_2. The intersection of S_1 and S_2 is denoted by $S_1 \cap S_2$.

(iii) A set with operations defined on it is called an **algebraic system** (or) **Algebra.**

20.1.4 Definition: A system $(S, *)$ is said to be a group if it satisfies the following axioms:

(i) Closure axiom: $a, b \in S \Rightarrow a * b \in S$.
(ii) Associative axiom: $a, b, c \in S \Rightarrow (a*b)*c = a*(b*c)$
(iii) Identity axiom: there exists an element $e \in S$ such that $a*e = e*a$ for all $a \in S$.
(iv) Inverse axiom: $a \in S \Rightarrow$ there corresponds $b \in S$ such that $a * b = e = b* a$.

20.1.5 Definition: A group is said to be a **commutative (Abelian) group** if $a*b = b*a$ for all $a, b \in S$.

20.1.6 Theorem: (i) The ring sum of two circuits in a graph G is either a circuit (or) an edge-disjoint union of circuits.

(ii) The ring sum of any two edge disjoint union of circuits is also a circuit or another edge-disjoint union of circuits.

Proof: Let Γ_1 and Γ_2 be any two circuits in a graph G.
Case-(i): If the two circuits Γ_1 and Γ_2 have no edge (or) no vertex in common, then the ring sum of Γ_1 and Γ_2 (that is, $\Gamma_1 \oplus \Gamma_2$) is a disconnected subgraph of G.
Clearly it is an edge-disjoint union of circuits.
Case-(ii): If the two circuits Γ_1 and Γ_2 do have one or more edges (or) vertices in common, then we have the following situations:
Since the degree of every vertex in a circuit is 2, we have that every vertex v in the subgraph $\Gamma_1 \oplus \Gamma_2$ has degree d(v); where $d(v) = 2$, if v is in Γ_1 only (or) in Γ_2 only (or) if one of the edges formerly incident on v was both in Γ_1 and Γ_2.
(or) $d(v) = 4$ if Γ_1 and Γ_2 are just intersect at v (without a common edge).
Therefore in $\Gamma_1 \oplus \Gamma_2$ the degree of a vertex is either 2 or 4.
Thus $\Gamma_1 \oplus \Gamma_2$ is an Euler graph (by a known result).
Since $\Gamma_1 \oplus \Gamma_2$ is an Euler graph; we have $\Gamma_1 \oplus \Gamma_2$ consists either a circuit (or) an edge-disjoint union of circuits. (by a known result).

Hence the ring sum of two circuits is either a circuit (or) an edge-disjoint union of circuits.
This completes the proof of (i).
(ii) follows directly from (i).

20.1.7 Theorem: The set consisting of all the circuits and the edge-disjoint unions of circuits (including the null set ϕ) in a graph G is an Abelian group under the operation ring sum $\oplus$.

Proof: Let Γ be the set consisting of all circuits and edge-disjoint unions of circuits including ϕ.

Now we have to show that, $(\Gamma, \oplus)$ is an Abelian group.
Let $\Gamma_1, \Gamma_2 \in \Gamma$.
By the Theorem 20.1.6, $\Gamma_1 \oplus \Gamma_2$ is either a circuit (or) an edge-disjoint unions of circuits.
This shows that $\Gamma_1 \oplus \Gamma_2 \in \Gamma$.
So the operation " $\oplus$ " satisfies the closure property.
Clearly the associative and commutative laws hold good.
Here the null graph ϕ acts as the identify element.
(because $\phi \oplus g = g$ for any subgraph g of G).
It is clear that a circuit (or) an edge-disjoint union of circuits Γ_1 is its own inverse (because of $\Gamma_1 \oplus \Gamma_1 = \phi$ for any $\Gamma_1 \in \Gamma$).
Hence $(\Gamma, \oplus)$ is an Abelian group.

20.1.8 Theorem: The set consisting of all cut-sets and the edge-disjoint unions of cut-sets (including the null set ϕ) in a graph G is an Abelian group under the ring-sum operation $\oplus$.

Proof: By the Theorem 16.4.4 of lesson -16, the ring sum of two cut-sets is again a cut-set (or) an edge-disjoint union of cut-sets.
So the closure property hold good.
Clearly the associative and commutative axioms hold good.
The null graph ϕ acts as the identity element (because $S_1 \oplus \phi = S_1$ for any cut-set S_1).
Also a cut-set (or) an edge-disjoint union of cut-sets Γ_1 is its own inverse (because $\Gamma_1 \oplus \Gamma_1 = \phi$).
This completes the proof of the Theorem.

20.2 SETS WITH TWO OPERATIONS

20.2.1 Definition: A system (R, $*$) is said to be a **ring** if it satisfies the following:

(i) (R, $*$) is an Abelian group.
(ii) (R,) is a semi-group.
(iii) Distributive laws: $a(b * c) = (ab) * (ac)$; $(a * b)c = (ac) * (bc)$.

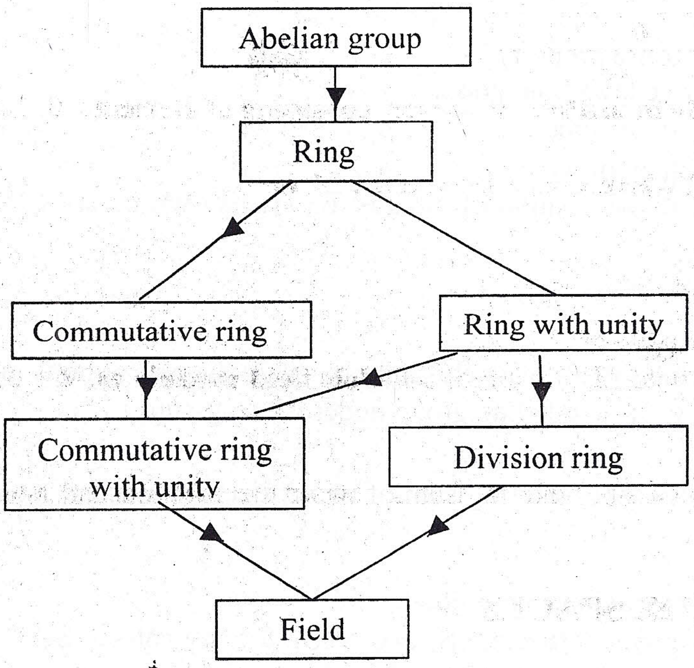
20.2.2 Definition: (i) A ring R is said to be a **commutativering,** if it satisfies the commutative property with respect to (that is, $ab = ba$ for all $a, b \in R$).

(ii) A commutative ring R that has an identity element $1 \in R$ is called a **commutative ring with unity**. Here the unity element 1 satisfies the property $a1 = 1a = a$ for all $a \in R$.

(iii) A ring with unity is said to be a **division ring** (or) **a skew-field** (or) **S-field** if every non-zero element of it has an inverse with respect to .
That is, $0 \neq x \in R \Rightarrow$ there exists $x^{-1} \in R$ such that $x\,x^{-1} = e = x\,x^{-1}$.

(iv) A commutative division ring is called a **field**.

20.2.3 Note: Diagrammatic representation showing the relationship of some algebraic systems with two internal operations:



20.2.4 Examples: (i) The set Z of all integers is not a field with respect to the usual operations + and • (multiplication). [Because there are non-zero elements of Z which have no multiplicative inverse, for example $2 \in Z$ has no multiplicative inverse in Z).

(ii) (R, +, •), (C, +, •) and (Q, +, •) are fields, where

R = The set of all Real numbers.

C = The set of all Complex numbers.

Q = The set of all Rational numbers.

20.3 MODULAR ARITHMETIC AND GALOIS FIELD

20.3.1 Definition: (i) Consider $Z_3 = \{0, 1, 2\}$ = the ring of integers modulo 3.

The addition and multiplication for Z_3 are called **addition modulo 3** and **multiplication modulo 3.** Both these two operations put together, we call it as **modulo 3 arithmetic.** Observe the addition and multiplication tables.

In modulo 3 arithmetic, $1 + 1 + 2 \bullet 2 + 1 + 2 + 1 = 1 \pmod 3$

$+_3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

(a)

$\bullet_3$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

(b)

(ii) In general, we can define **modulo m arithmetic** system consisting of elements 0, 1, 2, ..., m-1 and the following relationship:

for any $q > m - 1$, $q = r \pmod m$ where $q = m \cdot p + r$ and $r < m$.

20.3.2 Definition: Write $Z_m = \{0, 1, 2, \ldots, m-1\}$.

Now Z_m is a field $\Leftrightarrow$ m is a prime number.

If m is a prime number, then the field Z_m is called a **Galois field modulo m.** We denote it by GF(m).

20.3.3 Example: $Z_2 = \{0,1\}$ is a Galois field modulo 2 under the addition and multiplication modulo 2. It is denoted by GF(2).

20.4 VECTORS AND VECTOR SPACES

20.4.1 Note (i) In an ordinary two-dimensional (Euclidean) plane, a point is represented by an ordered pair of numbers $X = (x_1, x_2)$.

The point X may be regarded as a **vector**.

(ii) In a 3-dimensional Euclidean space, a point can be represented as a triplet (x_1, x_2, x_3).

Some times we may represent this element as the column vector $\begin{pmatrix} x_1 \\ x_2 \\ x3 \end{pmatrix}$

(iii) Consider GF(2).

Then every number in a triplet may be either equal to 0 or 1.

Thus there are 8 ($= 2^3$) vectors possible in a 3-dimsional space and these are (0,0,0) (0,0,1), (0,1,0), (0, 1, 1), (1, 0, 0), (1, 0, 1), (1, 1, 0), (1, 1, 1).

Extending this concept, a vector in a k-dimensional Euclidian space is an ordered k-tuple.

For example, the 7-tuple (0, 1, 1, 0, 1, 0, 1) represents a vector in a 7-dimensional vector space over the field GF(2).(iv) The numbers from a filed may be called as **scalars.** In GF(2), the scalars are 0 and 1.

20.4.2 Definition : A **k-dimensional vector space** (or a linear vector space) over the filed F is an object consisting of the following:

(i) A filed F [with its set of elements S and two operations $*$ and $\odot$]. (Note that $*$ is additive operation and $\odot$ is multiplicative operation).

(ii) A set W of k-tuples (all entries are taken from F).

(iii) A binary operation ◈ (called **vector sum**) between the elements of the set W, such that (W, ◈) is an Abelian group.

(iv) A binary operation $\boxdot$ (called **scalar multiplication**) which when applied between any scalar $c \in F$ and a vector $X = (x_1, x_2, \ldots, x_k) \in W$, produces a vector $p \in W$.

Then p is called the **scalar product** of c and X.

The scalar product is given by

$$p = c \boxdot X = c \boxdot (x_1, x_2, \ldots, x_k)$$
$$= (c \odot x_1, c \odot x_2, \ldots, c \odot x_k).$$

Furthermore, the scalar multiplication satisfies the following properties:

(i) $c_1 \boxdot (c_2 \boxdot X) = (c_1 \odot c_2) \boxdot X$, $c_1, c_2 \in F$.

(ii) $c_1 \boxdot (X$ ◈ $Y) = (c_1 \boxdot X)$ ◈ $(c_2 \boxdot Y)$

(iii) $(c_1 * c_2) \boxdot X = (c_1 \boxdot X)$ ◈ $(c_2 \boxdot X)$

(iv) $1 \boxdot X = X$, where 1 is the identity with respect to in F.

20.5 VECTOR SPACE ASSOCIATED WITH A GRAPH

20.5.1 Note: (i) Let us consider the graphs given in the Figures 20.5.1 A, B, C.

These graphs are with four vertices and five edges e_1, e_2, e_3, e_4, e_5.
Any subset of these five edges (that is, any subgraph g) of G can be represented by a 5-tuple:
$X = (x_1, x_2, x_3, x_4, x_5)$ where $x_i = 1$ if the edge e_i is in g.
$= 0$ if e_i is not in g.

(ii) The subgraph g_1 given in Fig - 20.5.1B, may be represented as (1, 0, 1, 0, 1).
The subgraph g_2 given in Fig - 20.5.1 C may be represented as (0, 1, 1, 1, 0).

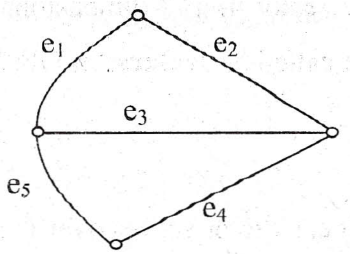


Fig - 20.5.1A

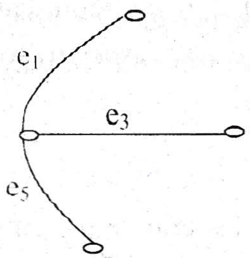


Fig - 20.5.1 B

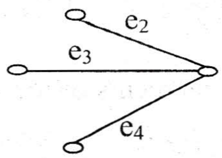


Fig - 20.5.1 C

It is clear that $2^5 = 32$ such 5-tuples are possible, including the zero vector

O = (0, 0, 0, 0, 0) which represents a null graph and (1, 1, 1, 1 ,1) represents the graph given in 20.5.1A

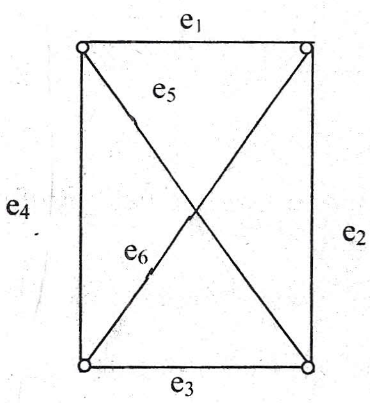
20.5.2 Note: Let G be a graph with n edges.

Suppose g_1, g_2 are two subgraphs and $(h_1, h_2, \ldots, h_n)$,
$(f_1, f_2, \ldots, f_n)$ are the n-tuple representations for g_1, g_2 respectively.
If an edge e_i is in both g_1 and g_2, then e_i is not in $g_1 \oplus g_2$.
Since e_i is in both g_1 and g_2, we have that $h_i = 1, f_i = 1$.
Now $h_i + f_i = 1 + 1 = 0 \pmod 2$.
So in the binary representation for $g_1 \oplus g_2$ the i^{th} component is 0.
The ring sum operation between two subgraphs corresponds to the modulo 2 addition between the two n-tuples
$(h_1, h_2, \ldots, h_n)$, $(f_1, f_2, \ldots, f_n)$ representing the two subgraphs.

20.5.3 Example: Consider the two subgraphs g_1 and g_2 (figure 20.5.1 B, C) of G (figure 20.5.1 A).

The sub graph $g_1 = \{e_1, e_3, e_5\}$ represented by (1, 0, 1, 0, 1), and $g_2 = \{e_2, e_3, e_4\}$ represented by (0, 1, 1, 1, 0).
Clearly $g_1 \oplus g_2 = \{e_1, e_2, e_3, e_4, e_5\}$ represented by (1, 1, 0, 1, 1) ...... (i)
Also, the modulo 2 addition between the two 5-tuples
(1, 0, 1, 0, 1) and (0, 1, 1, 1, 0) is given by (1, 0, 1, 0, 1) + (0, 1, 1, 1, 0)
= (1 + 1, 0 + 1, 1 + 1, 0 + 1, 1 + 0)
= (1, 1, 0, 1, 1) ..... (ii)
Observe that (i) and (ii) are same.

Self Assessment Question 1 : *Construct $g_1 \oplus g_2$ from G where g_1 and g_2 are sub graphs of G induced by $\{e_1, e_3, e_4, e_5\}$ and $\{e_1, e_2, e_3, e_6\}$ respectively.*



G

20.5.4 Definition: A **vector space** W_G **associated with a graph** G consists of

(i) Galois field modulo 2.
That is, the set {0, 1} with operation addition modulo 2 (written as '+').
The addition modulo 2 is given by

$$0 + 0 = 0,\ 1 + 0 = 1,\ 0 + 1 = 1,\ 1 + 1 = 0$$

and multiplication modulo 2 is given by

$$0 \cdot 0 = 0 = 0 \cdot 1 = 1 \cdot 0,\ 1 \cdot 1 = 1.$$

(ii) 2^e vectors (e-tuples), where e is the number of edges in G.

(iii) An addition operation between two vectors X, Y in this space, defined as the vector sum $X \oplus Y = (x_1 + y_1, x_2 + y_2, \ldots, x_e + y_e)$, where $X = (x_1, x_2, \ldots, x_e)$, $Y = (y_1, y_2, \ldots, y_e)$ and + being the addition modulo 2.

(iv) A scalar multiplication between a scalar $c \in Z_2$ and a vector X be defined as $c.X = (c \cdot x_1, c \cdot x_2, \ldots, c \cdot x_e)$.

20.6 BASIS VECTORS OF A GRAPH

20.6.1 Definition: A set of vectors $X_1, X_2, \ldots, X_r$ (over some field F) is said to be **linearly independent** (simply L.I) if for any scalars $c_1, c_2, \ldots, c_r$ in F we have that
$c_1X_1 + c_2X_2 + \ldots + c_rX_r = 0 \Rightarrow c_1 = 0 = c_2 = \ldots = c_r$.
Otherwise, the set of vectors is said to be **linearly dependent** (simply, L.D).

Self Assessment Question 2: *Verify whether the vectors* $X_1 = \begin{pmatrix}1\\4\\0\end{pmatrix}$, $X_2 = \begin{pmatrix}0\\1\\2\end{pmatrix}$,

$X_3 = \begin{pmatrix} 3 \\ 0 \\ 0 \end{pmatrix}$ *are linearly independent over the field* R *of real numbers.*

20.6.2 Problem: Find whether the vectors X_1, X_2 and X_3 given by $X_1 = \begin{pmatrix} 0 \\ 2 \\ -2 \end{pmatrix}$, $X_2 = \begin{pmatrix} 1 \\ 2 \\ 0 \end{pmatrix}$, $X_3 = \begin{pmatrix} 0.5 \\ 0 \\ 1 \end{pmatrix}$ are linearly independent over the field R of real numbers.

Solution: Suppose $c_1 \begin{pmatrix} 0 \\ 2 \\ -2 \end{pmatrix} + c_2 \begin{pmatrix} 1 \\ 2 \\ 0 \end{pmatrix} + C_3 \begin{pmatrix} 0.5 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$ for some scalars c_1, c_2, c_3

$\Rightarrow$ $c_2 + 0.5c_3 = 0$, $2c_1 + 2c_2 = 0$, $-2c_1 + c_3 = 0$

$\Rightarrow$ $-c_1 = c_2 = -0.5\, c_3$.

Now we can take $c_1 = 1$, $c_2 = -1$, $c_3 = 2$.

Then we get that $c_1 \begin{pmatrix} 0 \\ 2 \\ -2 \end{pmatrix} + c_2 \begin{pmatrix} 1 \\ 2 \\ 0 \end{pmatrix} + c_3 \begin{pmatrix} 0.5 \\ 0 \\ 1 \end{pmatrix} = 0$ for some non zero scalars c_1, c_2, c_3.

Therefore X_1, X_2, X_3 are linearly dependent.

20.6.3 Definition: If every vector in a vector space W can be expressed as the linear combination of vectors from a given set B of k linearly independent vectors, then the set of vectors B is called a **basis** (or) a **coordinate system** in the vector space.
[Equivalently: A given set B of a vector space W is said to be a **basis** if

(i) The given set B of vectors is a linearly independent set, and

(ii) every vector in W can be expressed as the linear combination of the vectors from B].

If B is a basis, then the vectors in B are called as basis vectors.

20.6.4 Definition: (i) If every vector in a vector space W can be expressed as a linear combination elements of a given set S of vectors, then we say that the set S **spans the vector space** W.

(ii) The minimum number of linearly independent vectors required to span W is called the **dimension** of the vector space W.

(iii) Any set of k linearly independent vectors that spans W (where W is a k dimensional vector space) is called a **basis** for the vector space W.

The vectors in a basis are put together called the **basis vectors**.

20.6.5 Example: (i) The **natural** (or) **standard basis** in a k-dimensional vector space is the following set of k unit vectors:

$$\begin{pmatrix}1\\0\\:\\:\\:\\0\end{pmatrix}, \begin{pmatrix}0\\1\\0\\:\\:\\0\end{pmatrix}, \ldots, \begin{pmatrix}0\\0\\:\\:\\0\\1\end{pmatrix}$$

(ii) Any vector in the k-dimensional vector space (over the field of real numbers) can be expressed as a linear combination of these k vectors.

20.6.6 Definition: Consider the vector space W_G associated with a given graph G. Corresponding to each subgraph of G, there was a vector in W_G represented by an e-tuple. The **natural basis for this vector space** W_G is a set of e linearly independent vectors, each representing a subgraph consisting of exactly one edge of G.

20.6.7 Example: Consider the graph given in Figures 20.5.1A

(i) Here the set of five vectors (1, 0, 0, 0, 0), (0, 1, 0, 0, 0), (0, 0, 1, 0, 0), (0, 0, 0, 1, 0), (0, 0, 0, 0, 1) serves as a basis for W_G.

(ii) For the graph given in Figure 20.5.1A, the possible subgraphs are $2^e = 2^5 = 32$. Any of these possible 32 subgraphs can be represented (uniquely) by a linear combination of these 5 vectors.

20.7 SUMMARY

In this lesson, we dealt with the algebraic concepts of a graph, particularly the vector space associated with a graph. The fundamentals such as sets with one operation, and sets with two operations were given. For a graph, the ring sum of two circuits were studied. Some results and examples concerning modular arithmetic and Galois fields (G.F 2) were provided.

20.8 TECHNICAL TERMS

Modulo m arithmetic : System consisting of elements 0, 1, 2, …, m-1 with the following relationship: for any $q > m - 1$, $q = r \pmod{m}$ where $q = m \cdot p + r$ and $r<m$

Skew field: A ring with unity and if every non-zero element of it has an inverse with respect to . That is, $0 \neq x \in R \Rightarrow$ there exists $x^{-1} \in R$ such that $x\, x^{-1} = e = x\, x^{-1}$.

Basis: If every vector in a vector space W can be expressed as the linear combination of vectors from a given set B of k linearly independent vectors, then the set of vectors B is called a basis (or) a coordinate system in the vector space.

Standard Basis: The natural (or) standard basis in a k-dimensional vector space is the following set of k unit vectors:

$$\begin{pmatrix}1\\0\\ \vdots\\ \vdots\\ \vdots\\0\end{pmatrix}, \begin{pmatrix}0\\1\\0\\ \vdots\\ \vdots\\0\end{pmatrix}, \ldots, \begin{pmatrix}0\\0\\ \vdots\\ \vdots\\0\\1\end{pmatrix}.$$

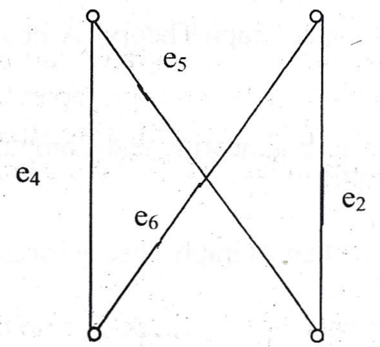
Natural Basis for W_G: The natural basis for this vector space W_G is a set of 'e' linearly independent vectors, each representing a subgraph consisting of exactly one edge of G.

20.9 ANSWERS TO SELF ASSESSMENT QUESTIONS

1: The subgraph $g_1 = \{e_1, e_3, e_4, e_5\}$ is represented by (1, 0, 1, 1, 1, 0)
The subgraph $g_2 = \{e_1, e_2, e_3, e_6\}$ is represented by (1, 1, 1, 0, 0, 1)

Then $g_1 \oplus g_2 = (1, 0, 1, 1, 1, 0) + (1, 1, 1, 0, 0, 1)$
$= (1 + 1, 0 + 1, 1 + 1, 1 + 0, 1 + 0, 0 + 1)$
$= (0, 1, 0, 1, 1, 1)$

Therefore $g_1 \oplus g_2$ is given by



2: Suppose $c_1X_1 + c_2X_2 + c_3X_3 = 0$ for some scalars c_1, c_2, c_3.

$$\Rightarrow c_1\begin{pmatrix}1\\4\\0\end{pmatrix} + c_2\begin{pmatrix}0\\1\\2\end{pmatrix} + c_3\begin{pmatrix}3\\0\\0\end{pmatrix} = \begin{pmatrix}0\\0\\0\end{pmatrix}$$

$\Rightarrow c_1 + 3c_3 = 0,\ 4c_1 + c_2 = 0,\ 2c_2 = 0$

Now $2c_2 = 0 \Rightarrow c_2 = 0$.
$4c_1 + c_2 = 0$ and $c_2 = 0 \Rightarrow c_1 = 0$.
Since $c_1 = 0$ and $c_1 + 3c_3 = 0$, we have $c_3 = 0$.
Therefore $c_1 = c_2 = c_3 = 0$.
This shows that $\{X_1, X_2, X_3\}$ is a linearly independent set.

20.10 MODEL QUESTIONS

1. Define the terms: modulo 'm' arithmetic, k-dimensional vector space.
2. Prove that (i).the ring sum of two circuits in a graph G is either a circuit (or) an edge-disjoint union of circuits; and
(ii) The ring sum of any two edge disjoint union of circuits is also a circuit or another edge-disjoint union of circuits.
3. Prove that the set consisting of all the circuits and the edge-disjoint unions of circuits (including the null set ϕ) in a graph G is an Abelian group under the operation ring sum $\oplus$.

20.11 REFERENCE BOOKS

1. Bondy J.A and Murty U.S.R, "Graph Theory with applications", North Holland, New York (1976).

2. Douglas B. West "Introduction to Graph Theory", Second Edition, Prentice Hall of India, New Delhi, 2002.

3. Harary Frank. "Graph Theory", Addison - Wesley Publishing Company, Inc., Reading, Mass., 1969.

4. John Clark and Derek Allan Holton, "A first look at Graph Theory" Allied Publishers, 1995

5. Narsingh Deo "Graph theory with applications to Engineering and Computer Science", Prentice Hall of India Pvt., Ltd., New Delhi, 1993.

6. Satyanarayana Bhavanari and Syam Prasad Kuncham "Graph Theory for Beginners", Satyasri Maths Study Centre, Guntur, AP, 2003.

Name of the Author of this Lesson: **Dr. Bhavanari Satyanarayana**