UNIT - V

Greatest Integer Function:

For any real x, the symbol $[x]$ denotes the greatest integer $\leq x$.

$[7] = 7$, $[7.2] = 7$, $[7\frac{1}{3}] = 7$, $\left[\frac{2}{3}\right] = 0$, $[-2.5] = -3$

$[x]$ is the unique integer $\ni [x] \leq x < [x]+1$.

Defn:

$x = [x] + \{x\}$, where $[x]$ is the integer part and $\{x\}$ is the fractional part.

$\{7.5\} = 0.5$, $\{7\frac{2}{3}\} = .2/3$

THEOREM 4.1:

Let x and y be real no.'s, then

i) $[x] \leq x < [x]+1$, $x-1 < [x] \leq x$, $0 \leq x-[x] < 1$

ii) $[x] = \sum_{1 \leq i \leq x} 1$, if $x \geq 0$

iii) $[x+m] = [x] + m$, if m is an integer

iv) $[x]+[y] \leq [x+y] \leq [x]+[y]+1$

v) $[x]+[-x] = \begin{cases} 0 & \text{, if } x \text{ is an integer} \\ -1 & \text{, otherwise} \end{cases}$

vi) $\left[\frac{[x]}{m}\right] = \left[\frac{x}{m}\right]$, if m is a positive integer.

vii) $-[-x]$ is the least integer $\geq x$.

viii) $[x+\frac{1}{2}]$ is the nearest integer to x. If two integers are equally near to x, it is the largest of the

ix) $-\left[-x+\frac{1}{2}\right]$ is the nearest integer to x, if two integers are equally near to x, it is the smaller of the two.

x) If n and a are +ve integers, $\left[\frac{n}{a}\right]$ is the no. of integers among $1, 2, 3, \ldots n$ that are divisible by n.

Proof:

i) if x is an integer, $[x] = x$ —— (1)

If x is not an integer, $x = [x] + \{x\}$

$\therefore x > [x]$ or $[x] < x$ —— (2)

(1), (2) $\Rightarrow$

$[x] \leq x$ —— (3)

again $x = [x] + \{x\}$, where $0 \leq \{x\} < 1$

$\therefore x < [x] + 1$ —— (4)

(3), (4) $\Rightarrow$

$[x] \leq x < [x] + 1$

$x < [x] + 1 \Rightarrow x - 1 < [x]$ —— (5)

(3), (5) $\Rightarrow$ $x - 1 < [x] \leq x$

$x = [x] + \{x\}$

$x - [x] = \{x\}$.

if x is an integer, $\{x\} = 0$

i.e., $x - [x] = 0$ —— (6)

if x is not an integer $\{x\} > 0$

(6).(4) $\Rightarrow$ $x-[x] \geq 0$ —— (8)

but $x-[x] = \{x\} < 1$ —— (9)

(8).(9) $\Rightarrow$ $0 \leq x-[x] < 1$

ii) $[x] = \sum_{1 \leq i \leq x} i^0 = \sum_{1 \leq i \leq x} 1$

eg:

$[3.5] = \sum_{1 \leq i \leq 3.5} i^0 = 1^0+2^0+3^0 = 1+1+1 = 3$

iii) Since m is an integer,

$[x+m] = [x]+m$

iv) Let $x = n+\alpha$, $n = [x]$, $\alpha = \{x\}$

$y = m+\beta$, $m = [y]$, $\beta = \{y\}$

$[x]+[y] = n+m \leq [n+\alpha+m+\beta] = [x+y]$

$\therefore [x]+[y] \leq [x+y]$ —— (1)

$[x+y] = [n+m+\alpha+\beta] = n+m+[\alpha+\beta]$

$\alpha \leq 1$, $\beta \leq 1$, $[\alpha+\beta] \leq 1$

$\therefore [x+y] = n+m+[\alpha+\beta]$

$\leq n+m+1$

i.e., $[x+y] \leq [x]+[y]+1$ —— (2)

(1).(2) $\rightarrow$

$[x]+[y] \leq [x+y] \leq [x]+[y]+1$

v) Let $x = n+\alpha$, $n = [x]$, $\alpha = \{x\}$, $0 \leq \alpha < 1$

$-x = -n-\alpha$,

$[x] + [-x] = n + [-n-\alpha]$;

$[x] + [-x] = n + [-n-1+1-\alpha]$

$= n + (-n-1) + (1-\alpha)$

$= \begin{cases} -1+1 & , \text{ if } \alpha = 0 \\ -1+0 & , \text{ if } \alpha > 0 \end{cases}$ i.e., $-1 \le \alpha < 1$

$= \begin{cases} 0 & , \text{ if } x \text{ is an integer} \\ -1 & , \text{ otherwise.} \end{cases}$

vi) Let $x = n + \alpha$, $n = [x]$, $\alpha = \{x\}$, $0 \le \alpha < 1$

$\left[\frac{[x]}{m}\right] = \left[\frac{n}{m}\right]$ $n = qm + r$

$= \left[\frac{qm+r}{m}\right] = \left[\frac{qm}{m}\right] + \left[\frac{r}{m}\right]$

$= [q] + 0$ ——— (1)

$\left[\frac{x}{m}\right] = \left[\frac{n+\alpha}{m}\right] = \left[\frac{qm+r+\alpha}{m}\right] = \left[\frac{qm}{m}\right] + \left[\frac{r+\alpha}{m}\right]$

$= [q] + 0$ ——— (2)

$\therefore \left[\frac{[x]}{m}\right] = \left[\frac{x}{m}\right]$

vii) We have $x - 1 < [x] \le x$;

Replace x by $-x$

$-x - 1 < [-x] \le -x$

1st part $\Rightarrow -x - 1 < [-x]$

$\Rightarrow -[-x] < x + 1$ ——— (1)

2nd part $\Rightarrow [-x] \le -x$

$x \le -[-x]$ ——— (2)

(1), (2) $x \le -[-x] < x + 1$

$\therefore -[-x]$ is the least integer $\ge x$

$$[x]+[-x] = n+[-n-\alpha]$$

$$[x]+[-x] = n+[-n-1+1-\alpha]$$

$$= n+(-n-1)+(1-\alpha)$$

$$= \begin{cases} -1+1 & \text{, if } \alpha=0 \\ -1+0 & \text{, if } \alpha>0 \end{cases} \quad \text{i.e., } \alpha=1 \text{ if } 0\le\alpha<1$$

$$= \begin{cases} 0 & \text{, if } x \text{ is an integer} \\ -1 & \text{, otherwise.} \end{cases}$$

vi) Let $x = n+\alpha$, $n=[x]$, $\alpha=\{x\}$, $0\le\alpha<1$

$n = qm+r$ (by div. alg.)

$$\left[\frac{[x]}{m}\right] = \left[\frac{n}{m}\right] = \left[\frac{qm+r}{m}\right] = \left[\frac{qm}{m}\right] + \left[\frac{r}{m}\right]$$

$\because 0\le r<m$, $\therefore \frac{r}{m}=1$

$$= [q]+0 \quad \text{——— (1)}$$

$$\left[\frac{x}{m}\right] = \left[\frac{n+\alpha}{m}\right] = \left[\frac{qm+r+\alpha}{m}\right] = \left[\frac{qm}{m}\right] + \left[\frac{r+\alpha}{m}\right]$$

$$= [q]+0 \quad \text{——— (2)}$$

$\because 0\le r<m$, $0\le\alpha<1$

(1), (2) $\therefore \left[\frac{[x]}{m}\right] = \left[\frac{x}{m}\right]$

vii) We have $x-1 < [x] \le x$

Replace x by $-x$

$$-x-1 < [-x] \le -x$$

1st part $\Rightarrow$ $-x-1 < [-x]$

$$\Rightarrow -[-x] < x+1 \quad \text{——— (1)}$$

2nd part $\Rightarrow$ $[-x] \le -x$

$$x \le -[-x] \quad \text{——— (2)}$$

(1), (2) $x \le -[-x] < x+1$

$\therefore -[-x]$ is the least integer $\ge x$

viii) Let n be the nearest integer to x, taking the larger one if two are equally distinct.

Then $n = x + \theta$, $-\frac{1}{2} < \theta \leq \frac{1}{2}$ and

$x = n - \theta$

$[x + 1/2] = n + [-\theta + 1/2] = n$, since $0 \leq -\theta + 1/2 < 1$

$$\left[x + \tfrac{1}{2}\right] = \begin{cases} [x], & \text{if } x \text{ is an integer} \\ x, & \text{if } \{x\} < 1/2 \\ [x]+1, & \text{if } \{x\} > 1/2 \end{cases}$$

ix) Similar to (viii)

x) If $a, 2a, 3a, \ldots\ldots ja$ are all the +ve integers $\leq n$, that are divisible by a, we have to prove that $\left[\frac{n}{a}\right] = j$

$(j+1)a > n$

$ja \leq n < (j+1)a$

$j \leq n/a < j+1$ $\therefore \left[\frac{n}{a}\right] = j$

Eg:

Take the no's 1 to 15

No's divisible by 2 : 2, 4, 6, 8, 10, 12, 14

" " " 3 : 3, 6, 9, 12, 15

" " " 4 : 4, 8, 12

" " " 5 : 5, 10, 15

" " " 6 : 6, 12

$7 = \left[\frac{15}{2}\right]$

$5 = \left[\frac{15}{3}\right]$

$3 = \left[\frac{15}{4}\right]$

$2 = \left[\frac{15}{6}\right]$

$\left[\frac{n}{a}\right]$ means the no. of no's divisible by a

THEOREM - 4.2 (DE POLIGNAC'S FORMULA)

Let p denote a prime, then the largest exponent e such that $p^e | n!$ is $e = \sum_{i=1}^{\infty} \left[\frac{n}{p^i}\right]$

Proof:

If $\underline{p^i > n}$, $\left[\frac{n}{p^i}\right] = 0$

$\therefore$ the sum $e = \sum_{i=1}^{\infty} \left[\frac{n}{p^i}\right] = 0$

i.e., there is no factor in $n!$ which is divisible by p^i.

Let $p^i \leq n$

We prove the theorem by induction on n.

take $n=1$, then $1! = 1$, clearly $1 | 1$ and $e=0, i=1$

The divisor is 1 only

The theorem is true for $n=1$

Assume that the theorem is true for $n-1$.

i.e., the largest exponent e, $\ni p^e | (n-1)!$ is

$$e = \sum_{i=1}^{\infty} \left[\frac{n-1}{p^i}\right]$$

i.e., $\sum_{i=1}^{\infty} \left[\frac{n-1}{p^i}\right] \Big| (n-1)!$ ——— (1)

Take $n!$, $n! = n(n-1)!$

Let j be the largest integer $\ni p^j | n!$ ——— (2)

now, if $p^i | n$

$$\left[\frac{n}{p^i}\right] - \left[\frac{n-1}{p^i}\right] = \begin{cases} 1, & \text{if } p^i | n \\ 0, & \text{if } p^i \nmid n \end{cases} \quad \text{——— (3)}$$

$$\sum_{i=1}^{\infty} \left[\frac{n}{p^i}\right] - \sum_{i=1}^{\infty} \left[\frac{n-1}{p^i}\right] = \sum_{i=1}^{\infty} \left\{\left[\frac{n}{p^i}\right] - \left[\frac{n-1}{p^i}\right]\right\}$$

Since, j is the largest integer $\ni p^j | n$.

$$\sum_{i=1}^{\infty}\left[\frac{n}{p^i}\right]-\sum_{i=1}^{\infty}\left[\frac{n-1}{p^i}\right]=1+\cdots+1+0+\cdots$$

$= j$ times

$\Rightarrow p^j \mid n!$ by (3) (5)

(1) (2) $\Rightarrow$

$$p^{\sum_{i=1}^{\infty}\left[\frac{n-1}{p^i}\right]} > p^j \mid (n-1)!\,n \qquad p^j \mid (n)(n-1)!$$

i.e., $p^{\sum_{i=1}^{\infty}\left[\frac{n-1}{p_i}\right]} \cdot j \mid n! \longrightarrow$ i.e., $p^{\sum_{i=1}^{\infty}\left[\frac{n}{p^i}\right]} \mid n!$ from (1)

The theorem is true for n.

P.T. $\dfrac{n!}{a_1!\,a_2!\cdots a_r!}$ is an integer, $a_i \geq 0$, $a_1+a_2+\cdots a_r=n$.

It is enough to prove that the power of any prime divisor of $n!$ is greater than the power of the same prime divisor of $a_1!\,a_2!\cdots a_r!$

Proof:

Let p be any prime divisor of both Nr. and Dr.

The highest power of p in $a_1!$ is $\left[\frac{a_1}{p}\right]+\left[\frac{a_1}{p^2}\right]+\cdots$

The highest power of p in $a_2!$ is $\left[\frac{a_2}{p}\right]+\left[\frac{a_2}{p^2}\right]+\cdots$

. . . . . .

The highest power of p in $a_r!$ is $\left[\frac{a_r}{p}\right]+\left[\frac{a_r}{p^2}\right]+\cdots$

The sum of all these no's is the highest power of p in the product $a_1!\,a_2!\cdots a_r!$

Thus, the highest power of p in the Dr. is

$$\left[\frac{a_1}{p}\right]+\left[\frac{a_2}{p}\right]+\cdots+\left[\frac{a_r}{p}\right]+\left[\frac{a_1}{p^2}\right]+\left[\frac{a_2}{p^2}\right]+\cdots+\left[\frac{a_r}{p^r}\right]+\cdots$$

W.K.T. $[x]+[y] \leq [x+y]$

$$\left[\frac{a_1}{p}\right]+\left[\frac{a_2}{p}\right]+\cdots+\left[\frac{a_r}{p}\right] \leq \left[\frac{a_1}{p}+\frac{a_2}{p}+\cdots+\frac{a_r}{p}\right]$$

$[x]+[y] \leq [x+y]$

$\leq \left[\frac{n}{p}\right]$

$\left[\frac{a_1}{p^2}\right]+\left[\frac{a_2}{p^2}\right]+\cdots+\left[\frac{a_r}{p^2}\right] \leq \left[\frac{a_1}{p^2}+\frac{a_2}{p^2}+\cdots+\frac{a_r}{p^2}\right]$

$\leq \left[\frac{n}{p^2}\right]$

and so on.

Summing up these inequalities, we get the highest power of p in the Dr.

the highest power of p in the Dr. $\leq \left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\cdots$

$\leq$ the highest power of p in $n!$ Nr.

Thus, the highest power of p in the Dr. is less than or equal to the highest power of p in the Nr.

$\therefore \frac{n!}{a_1!\, a_2! \cdots a_r!}$ is an integer.

4.2 Arithmetic functions:

An arithmetic function is one whose domain is the set of positive integers and range is a subset of complex numbers.

Definitions:

For positive integer n,

i) $d(n)$ is the number of positive divisors of n.

ii) $\sigma(n)$ is the Sum of positive divisors of n.

iii) $\sigma_k(n)$ is the Sum of the k^{th} powers of the divisors of n

iv) $\omega(n)$ is the number of distinct primes dividing n

v) $\Omega(n)$ is the number of primes dividing n containing multiplicity.

Eg:

Let $n = 12$,

Positive divisor of 12: 1, 2, 3, 4, 6, 12

Prime divisor of 12: 2, 3

$d(n) = 6$, $\sigma(n) = 28$; $\sigma_2(n) = 1^2 + 2^2 + 3^2 + 4^2 + 6^2 + 12^2$

$= 210$

$\omega(12) = 2$; $\Omega(12) = 3$

Note:

$d(n)$ and $\omega(n)$ are special cases of $\sigma_k(n)$

i.e., $d(n) = \sigma_0(n)$

$\sigma(n) = \sigma_1(n)$

i.e., $d(n) = \sum_{d|n} d^0 = \sum_{d|n} 1$

$\sigma(n) = \sum_{d|n} d$, $\sigma_k(n) = \sum_{d|n} d^k$

$\omega(n) = \sum_{e|n} 1$, $\Omega(n) = \sum_{p^\alpha | n} \alpha$

THEOREM (4.3):

For each positive integer n, $d(n) = \prod_{p^\alpha | n} (\alpha + 1)$

(or)

If $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$, then

$d(n) = (e_1+1)(e_2+1)\cdots(e_r+1)$. Also $d(1) = 1$

Proof:

$d(n)$ is the no. of +ve divisors of n.

30

$n=1 \Rightarrow d(1)=1$

31

Let $n = p_1^{e_1} \cdot p_2^{e_2} \cdots p_r^{e_r}$

Take $p_1^{e_1}$, the +ve divisors of $p_1^{e_1}$ are $1, p_1^1, p_1^2, \ldots p_1^{e_1}$

$$\therefore d(p_1^{e_1}) = e_1+1$$

Similarly,

$$d(p_2^{e_2}) = e_2+1, \ldots, d(p_r^{e_r}) = e_r+1$$

$\therefore n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ has $(e_1+1)(e_2+1)\cdots(e_r+1)$ positive divisors.

$$\therefore d(n) = (e_1+1)(e_2+1)\cdots(e_r+1)$$

$$= \prod_{p^\alpha \| n} (\alpha+1)$$

Corollary:

If $(m,n)=1$, then $d(mn) = d(m) \cdot d(n)$

Proof:

Given $(m,n)=1$

let $m = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$

$n = q_1^{s_1} q_2^{s_2} \cdots q_k^{s_k}$

$mn = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r} q_1^{s_1} q_2^{s_2} \cdots q_k^{s_k}$

then,

$d(m) = (e_1+1)(e_2+1)\cdots(e_r+1)$

$d(n) = (s_1+1)(s_2+1)\cdots(s_r+1)$

$d(mn) = (e_1+1)(e_2+1)\cdots(e_r+1)(s_1+1)(s_2+1)\cdots(s_r+1)$

$d(mn) = d(m) \cdot d(n)$

Multiplicative:

If $f(n)$ is an arithmetic function not identically

zero, such that $f(mn) = f(m) \cdot f(n)$, for every pair of positive integers m, n satisfying $(m,n) = 1$, then $f(n)$ is said to be multiplicative.

If $f(m,n) = f(m) \cdot f(n)$ whether m and n are relatively prime or not, then $f(n)$ is said to be totally multiplicative (or) completely multiplicative.

Note-1:

If f is a multiplicative function, then $f(1) = 1$.

Proof:

$$f(n) = f(n \cdot 1) = f(n) \cdot f(1)$$

Since $f(n)$ is not zero, $f(1) = 1$

Note-2:

If f and g are multiplicative functions such that $f(p^\alpha) = g(p^\alpha)$, for all primes p and all positive integers α, then $f(n) = g(n)$, for all positive integers n, so that $f = g$.

If f and g are totally multiplicative functions $\ni f(p) = g(p)$, for all primes p, then $f = g$.

THEOREM (4.4)

Let $f(n)$ be a multiplicative function and let $F(n) = \sum_{d|n} f(d)$. Then $F(n)$ is multiplicative.

Proof:

Given $f(n)$ is multiplicative.

i.e., $f(mn) = f(m) \cdot f(n)$ ——— (1)

For every positive m, n ∋ $(m,n)=1$

Also given, $F(n) = \sum_{d|n} f(d)$ ——— (2)

33

To prove: $F(n)$ is multiplicative

Let $(m,n)=1$, then $F(m) = \sum_{d|m} f(d)$

If $m=1$, $F(1) = \sum_{d|1} f(d) = f(1) = 1$

If $n=1$ $F(n) = \sum_{d|1} f(d) = f(1) = 1$

$F(mn) = F(1 \cdot n) = F(n) = 1$, $F(n) = F(m) \cdot F(n)$

F is multiplicative.

Thus, if m or $n = 1$, then F is multiplicative.

Suppose $m \neq 1$, $n \neq 1$, then let the canonical forms of m and n be

$$n = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \cdots p_r^{\alpha_r}$$

$$m = q_1^{\beta_1} q_2^{\beta_2} q_3^{\beta_3} \cdots q_s^{\beta_s}$$

with positive exponents α_i and β_i and $p_1 p_2 \cdots p_r, q_1, q_2 \cdots q_s$ are distinct primes.

The positive divisors d_1 of n are just the numbers $d_1 = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_r^{\gamma_r}$ for all possible choices of γ's ∋

$0 \leq \gamma_i \leq \alpha$

The +ve divisors d_2 of m are given by

$d_2 = q_1^{\delta_1} q_2^{\delta_2} \cdots q_s^{\delta_s}$, $0 \leq \delta_i \leq \beta_i$

$$nm = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r} \cdot q_1^{\beta_1} q_2^{\beta_2} \cdots q_s^{\beta_s}$$

The +ve divisors of mn are

$d = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_r^{\gamma_r} q_1^{\delta_1} q_2^{\delta_2} \cdots q_s^{\delta_s} \Rightarrow d = (d_1 \cdot d_2)$

Also $(d_1, d_2) = 1$

Now, $F(nm) = \sum_{d \mid nm} f(d)$ $\because$ by (2)

$$= \sum_{d_1 d_2 \mid nm} f(d_1 d_2)$$

$$= \sum_{d_1 d_2 \mid nm} f(d_1) \cdot f(d_2) \quad \because \text{by (1)}$$

$$= \sum_{d_1 \mid n} \sum_{d_2 \mid m} f(d_1) f(d_2)$$

$$= \sum_{d_1 \mid n} f(d_1) \sum_{d_2 \mid m} f(d_2)$$

$$= F(n) \cdot F(m)$$

$\therefore$ F is multiplicative.

Note:

We have $d(mn) = d(m)\, d(n)$

$\therefore d$ is multiplicative.

Prove the above condition

THEOREM (4-5)

For every positive integer n, $\sigma(n) = \prod_{p \mid n} \frac{(p^{a+1} - 1)}{p - 1}$

Proof:

By defn, $\sigma(n) = \sum_{d \mid n} d$

$$\sigma(1) = \sum_{d \mid 1} d = 1$$

Let $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$

$$\sigma(n) = \sum_{d \mid n} d \quad \text{——(1)}$$

$$F(n) = \sum_{d \mid n} f(d) \quad \text{——(2)}$$

(1), (2) $\Rightarrow$ $d = f(d)$ $d = f(d)$, $n = f(n)$ $\sigma(n) = F(n)$

Also $(d_1, d_2) = 1$

now, $F(nm) = \sum_{d \mid nm} f(d)$ $\because$ by (2)

$$= \sum_{d_1 d_2 \mid nm} f(d_1 d_2)$$

$$= \sum_{d_1 d_2 \mid nm} f(d_1) \cdot f(d_2) \quad \because \text{by } (1)$$

$$= \sum_{d_1 \mid n} \sum_{d_2 \mid m} f(d_1) f(d_2)$$

$$= \sum_{d_1 \mid n} f(d_1) \sum_{d_2 \mid m} f(d_2)$$

$$= F(n) \cdot F(m)$$

$\therefore$ F is multiplicative.

Note:

We have $d(mn) = d(m)\, d(n)$

$\therefore$ d is multiplicative.

THEOREM (4.5)

For every positive integer n, $\sigma(n) = \prod_{p \mid n} \frac{(p^{a+1} - 1)}{p - 1}$

Proof:

By defn, $\sigma(n) = \sum_{d \mid n} d$

$$\sigma(1) = \sum_{d \mid 1} d = 1$$

Let $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$

$$\sigma(n) = \sum_{d \mid n} d \quad \text{---(1)}$$

$$F(n) = \sum_{d \mid n} f(d) \quad \text{---(2)}$$

(1), (2) $\Rightarrow$ $d' = f(d)$ $\quad d = f(d_1)$

$n = f(n)$ $\quad \sigma(n) = F(n)$

by thrm 4.4,

With $f(n)=n$, we have $F(n)=\sigma(n)$ is multiplicative.

(X) [$f(n)$ is multiplicative, since $p_1^{e_1}, p_2^{e_2} \cdots p_r^{e_r}$ are distinct]

The divisors of $p_1^{e_1}$ are $1, p_1, p_1^2 \cdots p_1^{e_1}$

Obvious Prime number >1 so $r>1$

$$\sigma(p_1^{e_1}) = 1 + p_1 + p_1^2 + \cdots + p_1^{e_1} \Rightarrow = \frac{p_1^{e_1+1}-1}{p_1-1}$$

($a=1$, $r=p_1$; $a\left(\frac{r^n-1}{r-1}\right)$)

$\therefore \sigma(p_1^{e_1}) = \frac{1(1-p_1^{e_1+1})}{1-p_1} = \frac{p_1^{e_1+1}-1}{p_1-1}$

III[ly],

$$\sigma(p_2^{e_2}) = \frac{p_2^{e_2+1}-1}{p_2-1}$$ and so on.

Since $\sigma(n)$ is multiplicative

$$\sigma(n) = \sigma(p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r})$$

$$= \sigma(p_1^{e_1}) \cdot \sigma(p_2^{e_2}) \cdots \sigma(p_r^{e_r})$$

$$= \frac{p_1^{e_1+1}-1}{p_1-1} \cdot \frac{p_2^{e_2+1}-1}{p_2-1} \cdots \frac{p_r^{e_r+1}-1}{p_r-1}$$

$$= \prod_{i=1}^{r} \left(\frac{p_i^{e_i+1}-1}{p_i-1}\right)$$

2m 2 marks frequent

Mobius Inversion formula:

Mobius μ function:

For positive integer n, (No. of distinct prime numbers)

$$\mu(n) = \begin{cases} (-1)^{\omega(n)}, & \text{if } n \text{ is square free} \\ 0, & \text{otherwise} \end{cases}$$

10, 1, 2×5 → square free nums

a number which is not divisible by perfect square

(or)

$$\mu(n) = \begin{cases} +1, & \text{if } n=1 \\ -1, & \text{if } n=p \text{ prime} \\ (-1)^r, & \text{if } n=p_1p_2\cdots p_r,\ p_i\text{'s are distinct primes} \\ 0, & \text{if } a^2 \mid n,\ a>1 \text{ (or) otherwise} \end{cases}$$

write $\mu(n)$ for $n=1,2,\cdots 20$

(4) THEOREM_4.7:

The function $\mu(n)$ is multiplicative and $\sum_{d|n} \mu(d) = \begin{cases} 1, & \text{if } n=1 \\ 0, & \text{if } n>1 \end{cases}$

Proof:

Let $m = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$

$n = q_1^{s_1} q_2^{s_2} \cdots q_k^{s_k}$, $(m,n)=1$

$\mu(m) = \mu(p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}) = 0$

$\mu(n) = \mu(q_1^{s_1} q_2^{s_2} \cdots q_k^{s_k}) = 0$

$\mu(mn) = \mu(p_1^{e_1} \cdots p_r^{e_r} \cdot q_1^{s_1} \cdots q_k^{s_k}) = 0$

$\therefore \mu(mn) = \mu(m) \cdot \mu(n)$, if $(m,n)=1$

If $m=1=n$, $\mu(m) = \mu(1) = 1$

$\mu(n) = \mu(1) = 1$

$\mu(mn) = \mu(1) = 1$

$\therefore \mu(mn) = \mu(m) \cdot \mu(n)$

If $m=p$, $n=q$, where p, q are primes

$\mu(mn) = \mu(pq) = (-1)^2 = (-1)(-1)$

$= \mu(p) \cdot \mu(q)$

$= \mu(m) \cdot \mu(n)$

Thus in all cases,

$\mu(mn) = \mu(m) \cdot \mu(n)$

$\therefore \mu(n)$ is multiplicative

To show that $\sum_{d|n} \mu(d) = \begin{cases} 1, & \text{if } n=1 \\ 0, & \text{if } n>1 \end{cases}$

case (i): $n=1$,

$\sum_{d|1} \mu(d) = \mu(1) = 1$

case(ii): $n>1$

$n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$

The divisors of n are $1, p_1, p_1^2, \ldots p_1^{e_1}, p_2, p_2^2, \ldots p_2^{e_2}$

$p_3\ p_3^2 \cdots p_3^{e_3} \cdot p_r\ p_r^2 \cdots p_r^{e_r} \cdots p_1p_2, p_1p_2^2, \ldots p_1p_2^{e_r}, \ldots$

$p_1p_2p_3, p_1p_2p_3^2, p_1p_2p_3^{e_3}$

37

$$\sum_{d|n} \mu(d) = \mu(1) + \mu(p_1) + \mu(p_2) + \cdots + \mu(p_r)$$

$$+ \mu(p_1p_2) + \mu(p_1p_3) + \cdots + \mu(p_1p_r) + \mu(p_2p_3) + \cdots + \mu(p_2p_r)$$

$$+ \cdots + \mu(p_1p_2p_3) + \cdots + \mu(p_1p_2\cdots p_r)$$

$$= 1 + {}^rC_1(-1)^1 + {}^rC_2(-1)^2 + \cdots + {}^rC_r(-1)^r$$

$$= [1 + (-1)]^r \qquad 1 + {}^nC_r(a) + {}^nC_r(a)^2 + \cdots {}^nC_r(a)^r = [1+a]^n$$

$$= 0$$

Thus, $\sum_{d|n} \mu(d) = 0$, if $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$

$$\therefore \sum_{d|n} \mu(d) = \begin{cases} 1, & \text{if } n = 1 \\ 0, & \text{if } n > 1 \end{cases}$$

$$\sum_{d|n} \mu(d) = \left[\frac{1}{n}\right]$$

State & prove

THEOREM - 4.8 (MOBIUS INVERSION FORMULA)

If $F(n) = \sum_{d|n} f(d)$ for every positive integer n, then

$$f(n) = \sum_{d|n} \mu(d)\, F\left(\frac{n}{d}\right). \quad \text{---} \ (1)$$

Proof.

Given $F(n) = \sum_{d|n} f(d)$, $\forall$ +ve integers n

put $n = \frac{n}{d}$, $d = \delta$

$$\therefore F\left(\frac{n}{d}\right) = \sum_{\delta | \frac{n}{d}} f(\delta)$$

$$\sum_{d|n} \mu(d)\, F\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d) \sum_{\delta | \frac{n}{d}} f(\delta) \quad \text{---} \ (2)$$

now, $\frac{n}{d}$ is a divisor of n and $\delta \left| \frac{n}{d} \right.$

$\therefore \delta$ runs through the divisors of n only

i.e., $d|n$, $\delta|\frac{n}{d} \Rightarrow \frac{\delta}{n}$, $d|\frac{n}{\delta}$ — (3)

(3) in (2) $\Rightarrow$

$$\sum_{d|n} \mu(d) F\left(\frac{n}{d}\right) = \sum_{\delta|n} f(\delta) \sum_{d|\frac{n}{\delta}} \mu(d)$$

by thm 4.7,

$$\sum_{d|\frac{n}{\delta}} \mu(d) = \begin{cases} +1, & \text{if } \frac{n}{\delta}=1 \\ 0, & \text{if } \frac{n}{\delta}>1 \end{cases}$$

also, $\mu(d) = \begin{cases} 1, & \text{if } d=1 \\ 0, & \text{otherwise} \end{cases}$

If $\frac{n}{\delta}=1$, then $n=\delta$

$$\sum_{d|n} \mu(d) F\left(\frac{n}{d}\right) = \sum_{\delta|n} f(\delta) \sum_{d|n|1} \mu(d)$$

$$= \sum_{n|n} f(n) \sum_{d|1} \mu(d)$$

$$= f(n) \cdot 1$$

$$= f(n)$$

Note:

Relation b/w Euler function & mobius function

W.K.T.

$$\sum_{d|n} \phi(d) = n \quad \text{—— (1)}$$

Let $F(n) = n$ —— (2)

(1) $\Rightarrow$ $\sum_{d|n} \phi(d) = F(n)$

by Mobius Inversion formula,

$$\phi(n) = \sum_{d|n} \mu(d) \cdot F\left(\frac{n}{d}\right)$$

$$= \sum_{d|n} \mu(d) \cdot \frac{n}{d} \quad [\text{by } (2)$$

$$\frac{\phi(n)}{n} = \sum_{d|n} \frac{\mu(d)}{d}$$

39

THEOREM - 4.9:

CONVERSE OF MOBIUS INVERSION FORMULA:

If $f(n) = \sum_{d|n} \mu(d)\, F\left(\frac{n}{d}\right)$ for every positive integer n,

then $F(n) = \sum_{d|n} f(d)$

Proof:

Given

$$f(n) = \sum_{d|n} \mu(d)\, F\left(\frac{n}{d}\right) \quad \text{---} (1)$$

$$f(d) = \sum_{\delta|d} \mu(\delta)\, F\left(\frac{d}{\delta}\right) \quad \text{---} (2)$$

now,

$$\sum_{d|n} f(d) = \sum_{d|n} \sum_{\delta|d} \mu(\delta) \cdot F\left(\frac{d}{\delta}\right) \quad \text{---} (3)$$

Put $\frac{d}{\delta} = \nu \Rightarrow \frac{d}{\nu} = \delta$ — (4)

(4) in (3) $\Rightarrow$

$$\sum_{d|n} f(d) = \sum_{d|n} \sum_{\nu|d} \mu\left(\frac{d}{\nu}\right) F(\nu) \quad \text{---} (5)$$

$$= \sum_{\nu|n} \sum_{\beta\nu|n} \mu(\beta)\, F(\nu)$$

$$= \sum_{\nu|n} F(\nu) \sum_{\beta\nu|n} \mu(\beta) \quad \text{---} (6)$$

by thm 4.7,

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n > 1 \end{cases}$$

$$\text{i.e., } \mu(\beta) = \begin{cases} 1 & \text{if } \beta = 1 \\ 0 & \text{if } \beta > 1 \end{cases}$$

put $\beta = 1$, $\nu = n$ — (7)

(6) $\Rightarrow$ $\sum_{d|n} f(d) = \sum_{\nu=n} F(\nu) \cdot 1 = F(n)$

The multiplication of arithmatic functions:

Dirichlet product or convolution:

If f and g are arithmatic functions, then the Dirichlet product of f and g is defined as $f * g$ and

$$(f*g)n = \sum_{d|n} f(d) \cdot g(n/d)$$

(or)

$$(f*g)n = \sum_{d|n} f\left(\frac{n}{d}\right) \cdot g(d)$$

for all positive integers n. Also,

$$(f*g)\, n = \sum_{d_1 d_2 = n} f(d_1) \cdot g(d_2)$$

Note:

1. Multiplication is commutative

$$f*g = g*f$$

2. Multiplication is associative

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

where, $$[(f*g)*h](n) = \sum_{d_1 d_2 d_3 = n} f(d_1)\, g(d_2)\, h(d_3)$$

3. Identity function

$$I(n) = \begin{cases} 1, & \text{if } n=1 \\ 0, & \text{if } n>1 \end{cases}$$

4. Unit function

$$U(n) = 1, \quad \forall \text{ +ve integer}$$

$$I(1) = U(1)$$
$$= E(1)$$
$$= 1$$

The function I is s.t $f * I = I * f = f$ for every arithmetic function f and so I is called a multiplicative identity for Dirichlet multiplication of arithmetic functions.

If two arithmetic functions f and g are multiplicative inverse of each other we write $f = g^{-1}$ and $g = f^{-1}$

THEOREM (1)

P.T

If an arithmetic function f has a multiplicative inverse iff $f(1) \neq 0$, If an inverse exists it is unique.

Proof:

Suppose f has a multiplicative inverse f^{-1}, then

$$(f * f^{-1})(1) = \sum_{d|1} f(d) f^{-1}\left(\frac{1}{d}\right) = f(1) f^{-1}(1) \quad \text{---} \quad (1)$$

but

$$(f * f^{-1})(1) = I(1) = 1 \quad \text{---} \quad (2)$$

$$f(1) f^{-1}(1) = 1 \quad \text{---} \quad (3), \quad f(1) \neq 0$$

now Suppose, $f(1) \neq 0$

$(3) \Rightarrow \quad f(1) f^{-1}(1) = 1$

Since, $f(1) \neq 0$, $f^{-1}(1) = \frac{1}{f(1)}$ --- (4)

now,

$$(f * f^{-1})(2) = \sum_{d|2} f(d) f^{-1}\left(\frac{2}{d}\right)$$

$$= f(1) f^{-1}\left(\frac{2}{1}\right) + f(2) f^{-1}\left(\frac{2}{2}\right)$$

$$= f(1) f^{-1}(2) + f(2) f^{-1}(1) \quad \text{---} \quad (5)$$

but, $(f * f^{-1})(2) = I(2) = 0$ — (6)

(5), (6) $\Rightarrow$ $f(1) f^{-1}(2) + f(2) f^{-1}(1) = 0$

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

continuing by induction, assume $f^{-1}(j)$ has been evaluated for $j = 2, 3, \ldots n-1$.

now we find $f^{-1}(n)$.

now, $n > 1$, $0 = I(n)$

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

$$= \sum_{d|n} f(d) f^{-1}\left(\frac{n}{d}\right)$$

$$= f(1) f^{-1}\left(\frac{n}{1}\right) + \sum_{d|n} f(d) f^{-1}\left(\frac{n}{d}\right), \quad d > 0$$

$$f(1) f^{-1}(n) = -\sum_{d|n} f(d) f^{-1}\left(\frac{n}{d}\right)$$

$$f^{-1}(n) = -\frac{\sum_{d|n} f(d) f^{-1}\left(\frac{n}{d}\right)}{f(1)}$$

This is the formula for $f^{-1}(n)$ and it is unique.

Thus f has a multiplicative inverse iff $f(1) \neq 0$ and the inverse if it exists is unique.

THEOREM-2:

The functions μ and ϕ are multiplicative.

i.e., $\mu * U = U * \mu = I$, i.e., $\mu = U^{-1}$ & $U = \mu^{-1}$

Proof:

By defn, $(f * g)(n) = \sum_{d|n} f(d) g\left(\frac{n}{d}\right)$

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

THEOREM 5:

The following relations hold among the functions

27. $I, U, E, \mu, \tau, \phi, \sigma$

i) $\mu = U^{-1}$ ii) $\tau = U * U$ iii) $\phi = \mu * E$ iv) $\sigma = U * E$

v) $\sigma = \phi * \tau$ vi) $\sigma * \phi = E * E$

Proof:

i) $\mu = \mu^{U^{-1}}$ (already proved)

ii) $\tau(n)$ = no. of +ve divisors of n; $\forall n$

Also, $U(n) = 1$,

Since all the f_n's are multiplicative, we prove the results for prime powers only

$$(U * U)(p^k) = \sum_{d|p^k} U(d)\, U\left(\frac{p^k}{d}\right)$$

$$= \sum_{d|p^k} 1 \cdot 1$$

$$= \tau(p^k) \cdot \sum_{d|n} 1$$

$$= d(n)$$

$$= \tau(p^k)$$

$$\therefore U * U = \tau$$

iii) $(\mu * E)(n) = \sum_{d|n} \mu(d)\, E\left(\frac{n}{d}\right)$

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

$$= \sum_{d|n} \frac{\mu(d)}{d} \cdot n \quad \text{——— (1)}$$

W.K.T. the relation between Eulers and mobius function.

$$\frac{\phi(n)}{n} = \sum_{d|n} \frac{\mu(d)}{d} \quad \text{---} (2)$$

$$(\mu * \varepsilon)(n) = \frac{\phi(n)}{n} \cdot n$$

$$= \phi(n)$$

$$\therefore \mu * \varepsilon = \phi$$

(ii) $(U * \varepsilon)(n) = \sum_{d|n} U(d)\, \varepsilon\left(\frac{n}{d}\right)$

$$= \sum_{d|n} 1 \cdot \frac{n}{d}$$

$$= \sum_{d|n} d$$

$$= \sigma(n)$$

$$\therefore (U * \varepsilon) = \sigma$$

(iii) $\phi * \tau = (\mu * \varepsilon) * (U * U)$

$$= (\mu * U) * (\varepsilon * U)$$

$$= I * (\varepsilon * U)$$

$$= I * I * U$$

$$= \varepsilon * U$$

$$\therefore \phi * \tau = \sigma$$

(iv) $\sigma * \phi = (U * \varepsilon) * (\mu * \varepsilon)$

$$= (\varepsilon * U) * (\mu * \varepsilon)$$

$$= \varepsilon * (U * \mu) * \varepsilon$$

$$= \varepsilon * I * \varepsilon$$

$$= \varepsilon * \varepsilon$$

$$\therefore \sigma * \phi = \varepsilon * \varepsilon$$

Thm 3.6 ∴

$\therefore (f*g)*h = f*(g*h)$

Identity:

W.K.T. $I(n) = \begin{cases} 1, & \text{if } n=1 \\ 0, & \text{if } n>1 \end{cases}$

$(f*I)(n) = \sum_{d|n} f(d) \cdot I\left(\frac{n}{d}\right)$

$= \sum_{\substack{d|n \\ d=n}} f(d) \cdot I\left(\frac{n}{d}\right) + \sum_{\substack{d|n \\ d<n}} f(d) I\left(\frac{n}{d}\right)$

$= f(n) \cdot I(1) + 0$

$= f(n)$

$\therefore f*I = f$

$(I*f)(n) = \sum_{d|n} I(d) \cdot f\left(\frac{n}{d}\right)$

$= \sum_{\substack{d|n \\ d=1}} I(d) f\left(\frac{n}{d}\right) + \sum_{\substack{d|n \\ d<1}} I(d) f\left(\frac{1}{d}\right)$

$= I(1) * f(n) + 0$

$= f(n) + 0$

$\therefore I*f = f$

$\therefore I$ is the identity element

ii) Inverse:

W.K.T. an arithmetic function f has a multiplicative inverse iff $f(1) \neq 0$ forms a group under Dirichlet multiplication

Now, we prove that the set of all multiplicative arithmetic functions is a group.

i) closure:

Let $(m,n) = 1$

consider 2 multiplicative functions f and g

$(f*g)(nm) = \sum_{d|nm} f(d)\, g\left(\frac{nm}{d}\right)$

$= \sum_{d_1|n} \sum_{d_2|m} f(d_1 d_2)\, g\left(\frac{nm}{d_1 d_2}\right)$

$$= \sum_{d_1 \mid n} \sum_{d_2 \mid m} f(d_1) f(d_2) \cdot g\left(\frac{n}{d_1}\right) g\left(\frac{m}{d_2}\right)$$

$$= \sum_{d_1 \mid n} f(d_1)\, g\left(\frac{n}{d_1}\right) \cdot \sum_{d_2 \mid m} f(d_2)\, g\left(\frac{m}{d_2}\right)$$

$$(f*g)(nm) = (f*g)(n) \cdot (f*g)(m)$$

$\therefore$ $f*g$ is a multiplicative function

ii) Associativity:

as in the previous proof

iii) Identity:

as in the previous proof

iv) Inverse:

Let f be a multiplicative function.

define a function g as $g(p^j) = f^{-1}(p^j)$

for every prime p and every integer $j \geq 0$

we prove that g is multiplicative:

For any integer $n = \prod_{i=1}^{r} p_i^{\alpha_i}$, we define

$g(n) = \prod_{i=1}^{r} g(p_i^{\alpha_i})$, where the primes p_i are distinct

$$g(nm) = \prod_{i=1}^{r} \prod_{j=1}^{s} g(p_i^{\alpha_i})\, g(q_j)^{\beta_j}$$

$$= \prod_{i=1}^{r} g(p_i^{\alpha_i}) \prod_{j=1}^{s} g(q_j)^{\beta_j}$$

$$= g(n) \cdot g(m)$$

$\therefore$ g is multiplicative

consider any prime power p^k

$$(f*g)(p^k) = \sum_{d_1 d_2 = p^k} f(d_1) g(d_2)$$

$$= \sum_{d_1 d_2 = p^k} f(d_1) f^{-1}(d_2)$$

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

$$= I(p^k)$$

$\therefore$ $f*g = I$

$\therefore$ $f^{-1} = g$ and it is unique

now assume $f = \mu * F$

$$u*f = u*(\mu*F)$$
$$= (u*\mu)*F$$
$$= I*F$$
$$= F$$
$$\therefore F = u*f$$

THEOREM-4:

The set of all arithmetic functions f with $f(1) \neq 0$ forms a group under Dirichlet multiplication. Similarly the set of all multiplicative arithmetic functions is a group.

Proof:

i) closure:

Consider the arithmetic functions f and g with $g(1) \neq 0$ and $f(1) \neq 0$

now, $(f*g)(1) = \sum_{d|1} f(d)\, g\left(\frac{1}{d}\right) = f(1) \cdot g(1) \neq 0$

$\therefore (f*g)$ belongs to the set (or) the set is closed under Dirichlet multiplication.

ii) Associativity:

Let h be another arithmetic function $\ni h(1) \neq 0$

$$[(f*g)*h](n) = \sum_{d_1 d_2 d_3 = n} f(d_1) \cdot g(d_2) \cdot h(d_3)$$

for any positive integer n.

where the sum is over all the d_1, d_2, d_3 of +ve integers such that $d_1 d_2 d_3 = n$

$$[f*(g*h)](n) = \sum_{d_1 d_2 d_3 = n} f(d_1) \cdot g(d_2) \cdot h(d_3)$$

$$= \sum_{d|n} \mu(d) \cdot 1 \quad \text{—— (1)} \quad , \quad U(n) = 1 \; \forall n$$

213

W.k.T.

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & , \text{ if } n = 1 \\ 0 & , \text{ if } n > 1 \end{cases}$$

but $$I(n) = \begin{cases} 1 & , \text{ if } n = 1 \\ 0 & , \text{ if } n > 1 \end{cases}$$

$$\therefore \sum_{d|n} \mu(d) = I(n) \quad \text{—— (2)}$$

(1) $\Rightarrow$ $$(\mu * U)(n) = I(n) \quad \text{—— (3)}$$

$$(U * \mu)(n) = \sum_{d|n} U(d)\, \mu\left(\frac{n}{d}\right)$$

$$= \sum_{d|n} 1 \cdot \mu\left(\frac{n}{d}\right)$$

put $\frac{n}{d} = r \Rightarrow \frac{n}{r} = d$ $\therefore$ if $d|n$, r also divides n

$$= \sum_{r|n} \mu(r)$$

$$\therefore (U * \mu)(n) = I(n) \quad \text{[by (2)} \quad \text{—— (4)}$$

(3), (4) $\Rightarrow$

$$\mu * U = U * \mu = I$$

$$\mu = U^{-1} \quad \& \quad U = \mu^{-1}$$

$\neq 0$

THEOREM-3:

If f and F are any arithmetic functions such that $F = U * f$, then $f = \mu * F$ and conversely.

Proof:

Let $F = U * f$

then, $\mu * F = \mu * (U * f)$

$= (\mu * U) * f$

$= I * f$

Recurrence Functions:

If a, b, x_0, x_1 are arbitrary numbers (even complex). let $f(0) = x_0$, $f(1) = x_1$ and $f(n+1) = a f(n) + b f(n-1)$ for $n \geq 1$. This determines $f(n)$ uniquely depending only on a, b, x_0, x_1.

Writing x_n for $f(n)$, $x_{n+1} = a x_n + b x_{n-1}$.

This relation is called recurrence relation. (or) recurrence formula.

Formula to find x_n of recurrence relation.

Let the recurrence relation be

$$x_{n+1} = a x_n + b x_{n-1} \quad \text{---} (1)$$

$$\begin{aligned} x_{n+1} - k x_n &= a x_n + b x_{n-1} - k x_n \\ &= (a-k) x_n + b x_{n-1} \\ &= (a-k) x_n + b x_{n-1} + ak x_{n-1} - k^2 x_{n-1} \\ &\quad - ak x_{n-1} + k^2 x_{n-1} \\ &= (a-k) x_n + b x_{n-1} + ak x_{n-1} - k^2 x_{n-1} \\ &\quad - (a-k) k x_{n-1} \\ &= (a-k)[x_n - k x_{n-1}] + [b + ak - k^2] x_{n-1} \quad \text{---} (2) \end{aligned}$$

Let k_1, k_2 be the roots of $k^2 - ak - b = 0$ —(3)

Then $k_1 + k_2 = a$ — (4)

Put $k = k_1$ in (2) and using (3), we get

$$\begin{aligned} x_{n+1} - k_1 x_n &= (a-k_1)(x_n - k_1 x_{n-1}) + 0 \\ &= (k_1 + k_2 - k_1)(x_n - k_1 x_{n-1}) \end{aligned}$$

(5)

III^{ly}, put $k = k_2$ in (2) and using (3) and (4)

$$x_{n+1} - k_2 x_n = (k_1 + k_2 - k_2)(x_n - k_2 x_{n-1}) + 0$$

$$= k_1 (x_n - k_2 x_{n-1}) \quad \text{—— (6)}$$

(5) $\Rightarrow$ $x_{n+1} - k_1 x_n = k_2 (x_n - k_1 x_{n-1})$

$$= k_2 k_2 (x_{n-1} - k_1 x_{n-2})$$

$$= k_2 k_2 k_2 (x_{n-2} - k_1 x_{n-3})$$

$$\cdots\cdots\cdots$$

$$= k_2^n (x_1 - k_1 x_0) \quad \text{—— (7)}$$

III^{ly},

$$x_{n+1} - k_2 x_n = k_1^n (x_1 - k_2 x_0) \quad \text{—— (8)}$$

(7) $-$ (8) $\Rightarrow$

$$(k_2 - k_1) x_n = k_2^n (x_1 - k_1 x_0) - k_1^n (x_1 - k_2 x_0)$$

$$x_n = \frac{k_2^n (x_1 - k_1 x_0) - k_1^n (x_1 - k_2 x_0)}{(k_2 - k_1)}$$

This is the formula for finding the values of x_n if $k_1 \neq k_2$.

Find the n^{th} term of the Fibonacci sequence (or) P.T. $F_n = \frac{1}{\sqrt{5}} \left[\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right]$ of the Fibonacci sequence.

Proof:

The Fibonacci sequence is

0, 1, 1, 2, 3, 5, 8, 13, ...

$F_0 = 0$, $F_1 = 1$, $F_{n+1} = F_n + F_{n-1}$ —— (1)

The recurrence formula is $x_{n+1} = a x_n + b x_{n-1}$

Here $a = 1$, $b = 1$