Thursday
10/10/2019

Date
Page

* Unit III : Number Theoretic Function *

* **Def^n**-: Any function whose domain of def^n is the set of positive integers is said to be number theoretic function. It is also called as arithmatic function.

* **Definitions**-:

A given positive integer 'n', let $\tau(n)$ denotes the no. of positive divisors of 'n' and $\sigma(n)$ denotes the sum of these divisors.

$\tau(1) = 1$	and $\sigma(1) = 1$
$\tau(2) = 2$	$\sigma(2) = 1+2 = 3$
$\tau(3) = 2$	$\sigma(3) = 1+3 = 4$
$\tau(4) = 3$	$\sigma(4) = 1+2+4 = 7$
$\tau(5) = 2$	$\sigma(5) = 1+5 = 6$
$\tau(6) = 4$	$\sigma(6) = 1+2+3+6 = 12$
$\tau(7) = 2$	$\sigma(7) = 1+7 = 8$
$\tau(8) = 4$	$\sigma(8) = 1+2+4+8 = 15$
$\tau(9) = 3$	$\sigma(9) = 1+3+9 = 13$
$\tau(10) = 4$	$\sigma(10) = 1+2+5+10 = 18$

* **Note**-:

If 'n' is prime then,

i) $\tau(n) = 2$

ii) $\sigma(n) = n+1$

* **Theorem**-:

If $n = p_1^{k_1} \cdot p_2^{k_2} \cdots p_r^{k_r}$ is the prime factorisation of $n > 1$, then the possitive divisor of 'n' are precisely those integers 'd' of the form

$d = p_1^{a_1} \cdot p_2^{a_2} \cdot p_3^{a_3} \cdots p_r^{a_r}$; $0 \leq a_i \leq k_i$ and $0 \leq i \leq r$.

Proof:

The divisor '1' can be obtained for $a_1 = a_2 = a_3 = \cdots = a_r = 0$ and 'n' itself occurs when $a_1 = k_1, a_2 = k_2, a_3 = k_3, \cdots, a_r = k_r$.

Let 'd' be a proper divisor of 'n'.

$\therefore$ $n = dd'$ where $d, d' > 1$.

$\therefore$ By fundamental theorem of arithmatic,

$d = q_1 \cdot q_2 \cdot q_3 \cdots q_n$ and

$d' = t_1 \cdot t_2 \cdot t_3 \cdots t_m$.

Thus,

$n = p_1^{k_1} \cdot p_2^{k_2} \cdot \cdots p_r^{k_r}$

$= q_1 \cdot q_2 \cdot q_3 \cdots q_n \cdot t_1 t_2 \cdot t_3 \cdots t_n$.

By uniqueness of prime factorisation.

$\exists\ a_1 \cdot a_2 \cdot a_3 \cdots a_r$ such that $0 \leq a_i \leq k_i$, $0 \leq i \leq r$.

and $d = p_1^{a_1} \cdot p_2^{a_2} \cdot p_3^{a_3} \cdots p_r^{a_r}$

Conversely,

If $d = p_1^{a_1} \cdot p_2^{a_2} \cdot p_3^{a_3} \cdots p_r^{a_r}$ then there is $d' = p_1^{k_1 - a_1} \cdot p_2^{k_2 - a_2} \cdot \cdots p_r^{k_r - a_r}$ with

$dd' = p_1^{k_1} \cdot p_2^{k_2} \cdot p_3^{k_3} \cdots p_r^{k_r} = n$. ; $k_i - a_i \geq 0$

$\Rightarrow$ $d' > 1$

$\Rightarrow$ $d \mid n$.

* Theorem -:

If $n = p_1^{k_1} \cdot p_2^{k_2} \cdot p_3^{k_3} \cdots p_r^{k_r}$ is the prime factorisation of $n > 1$ then,

i) $\tau(n) = (k_1 + 1)(k_2 + 1)(k_3 + 1) \cdots (k_r + 1)$

ii) $\sigma(n) = \left(\frac{p_1^{k_1+1} - 1}{p_1 - 1}\right)\left(\frac{p_2^{k_2+1} - 1}{p_2 - 1}\right) \cdots \left(\frac{p_r^{k_r+1} - 1}{p_r - 1}\right)$

Proof:

We know that any divisor 'd' of 'n' is of the form,

$d = p_1^{a_1} \cdot p_2^{a_2} \cdot p_3^{a_3} \cdots p_r^{a_r}$; $0 \leq a_i \leq k_i$, $0 \leq i \leq r$.

Note that there are k_1+1 choices for a_1, k_2+1 choices for $a_2, \dots, k_r+1$ choices for a_r.

Hence $\tau(n) = (k_1+1)(k_2+1)(k_3+1)\cdots(k_r+1)$

and $\sigma(n) = (1+p_1+p_1^2+\cdots+p_1^{k_1})(1+p_2+p_2^2+\cdots+p_2^{k_2})$
$\cdots(1+p_r+p_r^2+\cdots+p_r^{k_r})$

$$= \left(\frac{p_1^{k_1+1}-1}{p_1-1}\right)\left(\frac{p_2^{k_2+1}-1}{p_2-2}\right)\cdots\left(\frac{p_r^{k_r+1}-1}{p_r-1}\right)$$

* Note -:

Using notation 'Π' for product $\tau(n)$, $\sigma(n)$ can be written as,

$$\tau(n) = \prod_{1\le i\le r}(k_i+1) \quad \text{and}$$

$$\sigma(n) = \prod_{1\le i\le r}\left(\frac{p_i^{k_i+1}-1}{p_i-1}\right)$$

Ex. Find $\tau(180)$ and $\sigma(180)$.

→ $180 = 2^2\times 3^2\times 5$

$\therefore \tau(180) = (2+1)(2+1)(1+1)$

$= 3\cdot 3\cdot 2$

$= 18$

and $\sigma(180) = \left(\frac{2^{2+1}-1}{2-1}\right)\left(\frac{3^{2+1}-1}{3-1}\right)\left(\frac{5^{1+1}-1}{5-1}\right)$

$= 7\cdot\frac{26}{2}\cdot\frac{24}{4}$

$= 7\cdot 13\cdot 6$

$= 546.$

Ex. Find $\tau(2019)$ and $\sigma(2019)$

→ $2019 = 3\times 673.$

$\therefore \tau(180) = (1+1)(1+1)$

$= 2\cdot 2 = 4.$

and $\sigma(2019) = \left(\frac{3^{1+1}-1}{3-1}\right)\left(\frac{673^{1+1}-1}{673-1}\right)$

$= \frac{8}{4} \cdot \frac{452928}{672}$

$= 2 \cdot (674 \cdot 0014)$

$= 2696.$

* Corollary -:

The product of possitive divisors of $n > 1$ is equal to $n^{\tau(n)/2}$.

Proof:

Let 'd' denote arbitary positive divisor of 'n' so that,

$n = dd'$ for some d'

As 'd' ranges over all $\tau(n)$, positive divisors of n, $\tau(n)$ equations of the type $n = dd'$, we occur and multiplying these equations together we get,

$\underbrace{n \cdot n \cdot n \cdots n}_{\tau(n) \text{ times}} = \underbrace{(dd') \cdot (dd') \cdots (dd')}_{\tau(n) \text{ times}}.$

$\therefore \quad n^{\tau(n)} = \left(\prod_{d|n} d\right)\left(\prod_{d'|n} d'\right)$

As 'd' runs through the divisor of 'n' so thus d'.

$\therefore$ We have,

$\prod_{d|n} d = \prod_{d'|n} d'$

$n^{\tau(n)} = \left(\prod_{d|n} d\right)^2$

$\therefore \quad n^{\tau(n)/2} = \prod_{d|n} d.$

Hence the proof.

Ex. Find product of all positive divisors of 16

→ Here $n = 16$

$\therefore \quad \tau(16) = 2^4$

$= (4+1)$

$= 5.$

Now,

$n^{\tau(n)} = (16)^{5/2}$

$= [(16)^{1/2}]^5$

$= (4)^5$

$= 1024$

Ex. $m = 2$, $n = 10$, $mn = 20$ then find $\tau(m)$, $\tau(n)$, $\tau(mn)$ and verify $\tau(m) \cdot \tau(n) = \tau(mn)$.

→ Here $m = 2$, $n = 10$, $mn = 20$.

$\tau(m) = \tau(2)$

$= 2^1$

$= (1+1)$

$= 2.$

$\tau(n) = \tau(10)$

$= \tau(2) \cdot \tau(5)$

$= (1+1)(1+1)$

$= 2 \cdot 2$

$= 4$

$\tau(mn) = \tau(2 \times 10)$

$= \tau(2^2 \times 5)$

$= \tau(2^2)\, \tau(5)$

$= (2+1)(1+1)$

$= 3 \cdot 2$

$= 6$

$\therefore \quad \tau(mn) \neq \tau(m) \cdot \tau(n)$

* Theorem -:

The functions 'τ' and 'σ' are multiplicative.

Proof:

Let 'm' and 'n' be relatively prime integers.

The result is trivially true if either 'm' or 'n' equals to 1.

Suppose $m = 1$ then,

$$\tau(mn) = \tau(1 \cdot n)$$
$$= \tau(n)$$
$$= 1 \cdot \tau(n)$$
$$= \tau(1) \cdot \tau(n) \quad ; \tau(1) = 1$$

Similarly,

$$\sigma(m,n) = \sigma(1 \cdot n)$$
$$= \sigma(n)$$
$$= 1 \cdot \sigma(n)$$
$$= \sigma(1) \cdot \sigma(n) \quad ; \sigma(1) = 1.$$

Thus 'σ' and 'τ' are multiplicative when either $m = 1$ or $n = 1$.

Suppose that $m, n > 1$ and $\gcd(m,n) = 1$

$\therefore m = p_1^{k_1} \cdot p_2^{k_2} \cdot p_3^{k_3} \cdots p_r^{k_r}$

and $n = q_1^{t_1} \cdot q_2^{t_2} \cdot q_3^{t_3} \cdots q_s^{t_s}$

be the prime factorisation of 'm' and 'n' respectively.

Since, $\gcd(m, n) = 1$.

$\therefore$ No 'p_i' can occure among th 'q_j'

It follows that the prime factorisation of 'mn' is given by,

$$mn = (p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r})(q_1^{t_1} q_2^{t_2} \cdots q_s^{t_s})$$

$$\therefore \tau(m,n) = (k_1+1)(k_2+1)(k_3+1)\cdots(k_r+1)(t_1+1)(t_2+1)(t_3+1)\cdots(t_s+1)$$

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

Similarly,

$$\sigma(mn) = \left[\frac{p_1^{k_1+1}-1}{p_1-1}\right]\left[\frac{p_2^{k_2+1}-1}{p_2-1}\right]\cdots\left[\frac{p_r^{k_r+1}-1}{p_r-1}\right]\left[\frac{q_1^{t_1+1}-1}{q_1-1}\right]$$
$$\left[\frac{q_2^{t_2+1}-1}{q_2-1}\right]\cdots\left[\frac{q_s^{t_s+1}-1}{q_s-1}\right]$$

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

∴ 'τ' and 'σ' are multiplicative.

Hence the proof.

* Multiplicative function-:

Let 'f' be a number theoretic function then 'f' is multiplicative if $f(mn) = f(m)f(n)$ whenever $\gcd(m,n) = 1$.

* Theorem-:

If 'f' is multiplicative function and 'F' is given by $F(n) = \sum_{d|n} f(d)$ then 'F' is also a multiplicative function.

Proof:

Let 'm' and 'n' be relatively prime positive integers then

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

$$= \sum_{d|mn} f(d_1 d_2) \quad ; \gcd(d_1, d_2) = 1$$

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

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

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

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

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

$\therefore$ F is multiplicative

Ex. Verify the result for $m = 8$ and $n = 3$

i.e. to verify $F(24) = F(8) \cdot F(3)$

i.e $\sum_{d|24} f(d) = \sum_{d|8} f(d) \cdot \sum_{d|3} f(d)$

→ Consider,

$$\sum_{d|24} f(d) = f(1)+f(2)+f(3)+f(4)+f(6)+f(8)+f(24)$$

$$= f(1\cdot1)+f(2\cdot1)+f(3\cdot1)+f(4\cdot1)+f(3\cdot2)+f(8\cdot1)+f(3\cdot8)$$

$$= f(1)\cdot f(1)+f(2)\cdot f(1)+f(3)\cdot f(1)+f(4)\cdot f(1)+f(3)\cdot f(2)+f(8)\cdot f(1)+f(3)\cdot f(8)$$

$$= f(1)[f(1)+f(2)+f(8)+f(4)] + f(3)[f(2)+f(4)+f(8)+f(1)]$$

$$= [f(1)+f(2)+f(4)+f(8)][f(1)+f(3)]$$

$$= \sum_{d|8} f(d) \cdot \sum_{d|3} f(d)$$

$F(24) = F(8) \cdot F(3)$

* Theorem -:

If $\gcd(m,n) = 1$ then the set of positive divisors 'mn' consist of all products d_1, d_2 where $d_1 | m$ and $d_2 | n$ and $\gcd(m,n) = 1$. Furthermore these products are distinct.

Proof:

We assume that $m > 1$ and $n > 1$.

Let $m = p_1^{k_1} \cdot p_2^{k_2} \cdot p_3^{k_3} \cdots p_r^{k_r}$ and

$n = q_1^{t_1} \cdot q_2^{t_2} \cdot q_3^{t_3} \cdots q_s^{t_s}$

be prime factorisation of 'm' and 'n' respectively

and also $p_i \neq q_j$ $(\because \gcd(m,n) = 1)$

Then the prime factorisation of 'mn' is

$mn = p_1^{k_1} \cdot p_2^{k_2} \cdot p_3^{k_3} \cdots p_r^{k_r} \cdot q_1^{t_1} \cdot q_2^{t_2} \cdot q_3^{t_3} \cdots q_s^{t_s}$

Hence any positive divisor 'd' is of the form,

$$d = p_1^{a_1} \cdot p_2^{a_2} \cdot p_3^{a_3} \cdots p_r^{a_r} q_1^{b_1} \cdot q_2^{b_2} \cdot q_3^{b_3} \cdots q_s^{b_s}$$

$\therefore d = d_1 \cdot d_2 \quad ; \quad 0 \leq a_i \leq k_i \,,\ 0 \leq b_j \leq t_j$

Where $d_1 = p_1^{a_1} \cdot p_2^{a_2} \cdot p_3^{a_3} \cdots p_r^{a_r}$.

$d_2 = q_1^{b_1} \cdot q_2^{b_2} \cdot q_3^{b_3} \cdots q_s^{b_s}$.

$\therefore d_1 \mid m$ and $d_2 \mid n$

since all p_i's and q_j's are distinct

i.e $p_i \neq q_j \quad (1 \leq i \leq r,\ 1 \leq j \leq s)$

$\therefore \gcd(d_1, d_2) = 1$

Hence the proof.

H.W.

Ex. Verify the resust for $m = 2$ and $n = 5$, i.e, to verify $F(10) = F(2) \cdot F(5)$

i.e $\sum_{d \mid 10} f(d) = \sum_{d \mid 2} f(d) \cdot \sum_{d \mid 5} f(5)$

→ Consider,

$$\sum_{d \mid 10} f(d) = f(1) + f(2) + f(5) + f(10)$$

$$= f(1)1) + f(2 \cdot 1) + f(5)1) + f(2 \cdot 5)$$

$$= f(1) \cdot f(1) + f(2) \cdot f(1) + f(5) \cdot f(1) + f(2) \cdot f(5)$$

$$= f(1)[f(1) + f(2)] + f(5)[f(1) + f(2)]$$

$$= [f(1) + f(2)] + [f(1) + f(5)]$$

$$= \sum_{d \mid 2} f(d) \cdot \sum_{d \mid 5} f(d)$$

$\therefore F(10) = F(2) \cdot F(5)$

Monday
14/10/2019

Date
Page

* Möbius Inversion Formula-1

For a positive integer 'n' define,

$$\mu(n) = \begin{cases} 1 & \text{if } n=1 \\ 0 & \text{if } p^2 \mid n \\ (-1)^r & \text{if } n = p_1 p_2 \cdots p_r, \text{ all } p_i \text{ are distinct.} \end{cases}$$

* Remark-:

Above definition state that $\mu(n)=0$ if 'n' is not square free integer and $\mu(n)=(-1)^r$ if 'n' is square free integer with 'r' prime factors.

e.g. (1) $\mu(30) = 5\times3\times2$

$r = 3$

$\therefore \mu(30) = (-1)^3 = -1.$

(2) $\mu(2019)$

$2019 = 3\times673$

$r = 2$

$\therefore \mu(2019) = (-1)^2 = 1$

$\therefore \mu(2019) = 1$

(3) $n = 251 = 1\cdot251 = (-1)^r = (-1)^1 = -1$

$\therefore \mu(251) = -1$

(4) $\mu(48) = 16\times3 = 2^2\cdot2^2\cdot3 \quad \because 2^2 \mid 48$

$\therefore \mu(48) = 0$

(5) $\mu(360) = 40\times9 = 80\times5\times9 = 2^3\times5\times3^2$

Here $3^2 \mid 360$

$\therefore \mu(360) = 0$

(6) $\mu(331) = 1 \cdot 331 = (-1)^r = (-1)^1 = -1$

(7) $\mu(1728) = 192 \times 9 = 192 \times 3^2$

Here $3^2 | 1728$

$\therefore \mu(1728) = 0$.

(8) $\mu(210) = 7 \times 3 \times 5 \times 2$

$\therefore r = 4$

$\therefore \mu(210) = (-1)^4 = 1$

(9) $\mu(2310) = 11 \times 210 = 11 \times 7 \times 3 \times 5 \times 2$

$\therefore r = 5$

$\therefore \mu(2310) = (-1)^5 = -1$.

* Note -:

If 'P' is prime number then,

$\mu(P) = -1$ and $\mu(P^K) = 0 \; ; K > 1$

* Theorem -:

The function 'μ' is multiplicative function.

Proof:

Take 'm' and 'n' are relatively prime integer.

Case 1 - Either $m = 1$ or $n = 1$

If $m = 1$ then $mn = n$

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

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

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

similarly, for $n = 1$,

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

Case 2 - Either 'm' and 'n' is not square free integers.

Let 'm' be a not square free integer.
i.e. $p^2 | m$, p is prime

$\therefore \mu(m) = 0$

But the product of 'mn' contains the factor p^2.

$\therefore \mu(mn) = 0$

In this case either $p^2 | m$ or $p^2 | n$ for some prime p. Then $\mu(m) = 0$ or $\mu(n) = 0$ and $p^2 | mn$.

Hence $\mu(mn) = 0 = \mu(m) \cdot \mu(n)$

Result holds trivially

case 3 - Both 'm' and 'n' are square free integers.

suppose that $m = p_1 p_2 p_3 \cdots p_r$; p_i's are distinct primes and $n = q_1 q_2 q_3 \cdots q_s$; q_j's are distinct prime

$\therefore \gcd(m, n) = 1$

Not $p_i = q_j$ then

$\mu(mn) = (-1)^{r+s}$

$= (-1)^r (-1)^s$

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

Hence result hold trivially.

$\therefore$ From case ①, ② and ③,
'μ' is multiplicative function.

* Theorem -:

For each positive integer $n \geq 1$,

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

Proof:

Assume that $n = 1$ then,

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

suppose $n > 1$ thus $n = p_1^{k_1} \cdot p_2^{k_2} \cdots p_r^{k_r}$

where p_i's are distinct prime

$$\gcd(p_i^{k_i}, p_j^{k_j}) = 1 \quad \text{for } i = 1, 2, \cdots, r$$
$$j = 1, 2, \cdots, r \text{ & } i \neq j$$

We know that 'u' is multiplicative function and $F(n) = \sum_{d|n} u(d)$.

It follows that 'F' is multiplicative function.

$$F(n) = F(p_1^{k_1} \cdot p_2^{k_2} \cdots p_r^{k_r})$$
$$= F(p_1^{k_1}) \cdot F(p_2^{k_2}) \cdots F(p_r^{k_r})$$
$$= 0 \cdot 0 \cdot 0 \cdots 0$$
$$F(n) = 0$$

for $n = p^k$ so it's positive divisors are $1, p, p^2, \cdots, p^k$

Thus, $F(p^k) = \sum_{d|p^k} u(d)$

$$= u(1) + u(p) + u(p^2) + \cdots + u(p^k)$$
$$= 1 - 1 + 0 + 0 + \cdots + 0$$
$$= 0$$

Therefore,

$$F(n) = \begin{cases} 1 & ; n = 1 \\ 0 & ; n > 1. \end{cases}$$

Que Prove that $\tau(n)$ is odd integer iff 'n' is perfect square

→ Suppose $\tau(n)$ is odd integer.

Claim - 'n' is perfect square.

On contrary assume that 'n' is not perfect square.

Let $n = p_1^{k_1} \cdot p_2^{k_2} \cdots p_r^{k_r}$; where at least one of the k_i is odd.

$\tau(n) = (k_1+1)(k_2+1)\cdots(k_r+1)$

since, k_i is odd.

$\therefore$ k_i+1 is even

Hence $\tau(n)$ is even integer.

$\therefore$ Contradiction to the fact that $\tau(n)$ is odd integer.

Hence 'n' is perfect square

Conversely,

'n' is perfect square then,

$n = p_1^{k_1} \cdot p_2^{k_2} \cdots p_r^{k_r}$; each k_i is even integer.

Then each factor k_i+1 is odd and product of odd integers is odd

$\therefore$ $\tau(n) = (k_1+1)(k_2+1)\cdots(k_r+1)$ is odd integer

Imp * Möbius Inversion formula -:

* Theorem:

Let 'F' and 'f' be two number theoretic function related by the formula

$F(n) = \sum_{d|n} f(d)$. Then $f(n) = \sum_{d|n} \mu(d) \cdot F(n/d)$

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

Proof:

Let 'F' and 'f' be two number theoretic functions related by the formula,

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

By given hypothesis,

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

$$\Rightarrow F(n/d) = \sum_{c|n/d} f(c) \quad \text{— ②}$$

consider,

$$f(n) = \sum_{d|n} \mu(d) F(n/d) = \sum_{d|n} \mu(d) \left[\sum_{c|n/d} f(c) \right]$$

$$= \sum_{d|n} \sum_{c|n/d} \left[\mu(d) f(c) \right] \quad -③$$

It can be verify that $d|n$ and $c|\frac{n}{d}$ iff. $c|n$ and $d|\frac{n}{c}$

since, $d|n$ and $c|\frac{n}{d}$

$\therefore \quad n = dk \quad \Rightarrow ck' = \frac{n}{d}$

$$\Rightarrow dk' = \frac{n}{c}$$

$$\Rightarrow d|\frac{n}{c}$$

Also $c|n$.

conversely, suppose that $c|n$ and $d|n/c$ this clearly implies that $c|n/d$ because of this expansion ③ becomes,

$$\sum_{d|n} \sum_{c|n/d} \mu(d) f(c) = \sum_{c|n} \sum_{d|n/c} f(c) \cdot \mu(d)$$

$$= \sum_{c|n} f(c) \cdot \sum_{d|n/c} \mu(d) \quad -④$$

(By using theorem,

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

$$\sum_{d|n/c} \mu(d) = \begin{cases} 1 & ; n=c \\ 0 & ; n>c \end{cases})$$

$$\sum_{d|n} \sum_{c|n/d} \mu(d) F(c) = \sum_{c|n} f(c) \cdot \sum_{d|1} \mu(d)$$

(∵ we consider $n>0$, $\sum_{d|n/c} \mu(d) = 0$)

$$= \sum_{n|n} f(n) \cdot \sum_{1|1} \mu(1) \qquad \left(\because d|1 \Rightarrow d=1 \Rightarrow \mu(d)=1\right)$$

$$= f(n)$$

$$\therefore \sum_{d|n} \sum_{c|n/d} \mu(d) f(c) = f(n)$$

Hence the proof.

Ex. Verify for $n=10$, $\sum_{d|10} \mu(d) \cdot F\left(\frac{10}{d}\right) = f(10)$

→ Here $n = 10$

$\Rightarrow$ $n = 1, 2, 5, 10$ are divisors of 10.

Now we know that,

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

$$\therefore \sum_{d|10} \mu(d) \cdot F\left(\frac{10}{d}\right) = \mu(1)\cdot F(10) + \mu(2)\cdot F(5) + \mu(5)\cdot F(2) + \mu(10)\cdot F(1)$$

$$= F(10) - F(5) - F(2) + F(1)$$

$$= f(1)+f(2)+f(5)+f(10) - f(1)-f(5) - f(1)-f(2)+f(1) \qquad \left(\because F(n)=\sum_{d|n} f(d)\right)$$

$$= f(10).$$

$$\therefore \sum_{d|10} \mu(d) \cdot F\left(\frac{10}{d}\right) = f(10)$$

* **Theorem –:**

If 'f' is multiplicative function and $F(n) = \sum_{d|n} f(d)$ then 'f' is multiplicative.

Proof:

Let 'm' and 'n' be relatively prime integers

We know that any divisors of mn can be uniquely written as $d = d_1 d_2$ where $d_1 | m$ and $d_2 | n$ and $\gcd(d_1, d_2) = 1$.

We also know that by mobius inversion theorem if 'F' and 'f' are related by,

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

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

Hence using the mobius inversion formula we have,

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

$$= \sum_{d_1 d_2 | mn} \mu(d_1 d_2) F\left(\frac{mn}{d_1 d_2}\right)$$

$$= \sum_{\substack{d_1|m \\ d_2|n}} \mu(d_1)\mu(d_2) F\left(\frac{m}{d_1}\right) \cdot F\left(\frac{n}{d_2}\right)$$

($\because$ 'F' and 'μ' are multipli.)

$$= \left[\sum_{d_1|m} \mu(d_1) F\left(\frac{m}{d_1}\right)\right]\left[\sum_{d_2|n} \mu(d_2) F\left(\frac{n}{d_2}\right)\right]$$

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

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

$\therefore$ f is multiplicative.

Hence the proof

* Note –:

For $n \geq 1$,

Define $M(n) = \sum_{k=1}^{n} \mu(k)$

e.g. For $n = 9$.

$$M(9) = \sum_{k=1}^{9} \mu(k)$$

$$= \mu(1) + \mu(2) + \mu(3) + \mu(4) + \mu(5) + \mu(6) + \mu(7) + \mu(8) + \mu(9)$$

$$= \mu(1) + \mu(2) + \mu(3) + \mu(2^2) + \mu(5) + \mu(2\cdot 3) + \mu(7) + \mu(2^3) + \mu(3^2)$$

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

$$= -2$$

Then $M(n)$ is difference between the number of square free integers $k \leq n$ with an even number of prime factor 'f' those with an odd number of prime factors.

Ex. For each positive integer 'n' prove that $\mu(n)\mu(n+1)\mu(n-2)\mu(n+3) = 0$

→ Case 1- If 'n' is even positive integer.

If 'n' is even then $n-2$ is also even.

$\therefore \mu(n)$ and $\mu(n-2)$ comes out to be zero.

(∵ product of any two successive even integers are divisible by 8 i.e. $2^3 \mid n(n-2)$)

$\therefore \mu(n)\mu(n-2) = 0$.

$\therefore \mu(n)\mu(n+1)\mu(n-2)\mu(n+3) = 0$.

Case 2- If 'n' odd integer.

If 'n' is odd integer then $n+1$ and $n+3$ are successive even integers.

$\therefore$ By case (1),

$\mu(n+1)\mu(n+3) = 0$

$\therefore \mu(n)\mu(n+1)\mu(n-2)\mu(n+3) = 0$.

* Greatest Integer function :-

For any real number 'x' the greatest integer function denoted by $[x]$ and it is defined as the largest integer $\leq x$ i.e. $[x]$ is the unique integer satisfying $x-1 < [x] \leq x$.

Note that any real number 'x' can be written as, $x = [x] + \theta \; ; \; 0 \leq \theta < 1$.

e.g. i) $x = 5.2$

$\Rightarrow x = [x] + \theta$

$\therefore 5.2 = [5.2] + \theta$

$= 5 + 0.2$

ii) $x = -5.2$

$\Rightarrow x = [x] + \theta$

$\therefore -5.2 = [-5.2] + \theta$

$= -6 + 0.8$

iii) $x = \frac{-3}{2} = -1.5$

$\Rightarrow x = [x] + \theta$

$\therefore -1.5 = [-1.5] + \theta$

$= -2 + 0.5$

iv) $x = \frac{10}{7} = 1.4$

$\Rightarrow x = [x] + \theta$

$\therefore 1.4 = [1.4] + \theta$

$= 1 + 0.4$

v) $x = -0.001$

$\Rightarrow x = [x] + \theta$

$\therefore -0.001 = [-0.001] + \theta$

$= 1 - 0.999$

vi) $x = -0.5$

$\Rightarrow x = [x] + \theta$

$\therefore -0.5 = [-0.5] + \theta$

$= 1 - 0.5$

Tuesday
15/10/2019

Date
Page

* **Theorem -:**

If 'n' is a positive integer and 'p' is a prime then the exponent of the highest power of 'p' that divides $n!$ is $\sum_{k=1}^{\infty} \left[\frac{n}{p^k}\right]$.

Where the series is finite $\left[\frac{n}{p^k}\right] = 0$; $p^k > n$.

Proof:

Among the first 'n' integers those divisible by prime 'p' are $p, 2p, 3p, 4p, \cdots, tp$. where 't' is the greatest integer such that,

$$tp \leq n$$

$$\Rightarrow t = \left[\frac{n}{p}\right]$$

Thus, there are $\left[\frac{n}{p}\right]$ multiples of 'p' occuring in $n!$

Further among the first 'n' integers those divisible by 'p^2' are $p^2, 2p^2, 3p^2, 4p^2, \cdots, tp^2$. where 't' is the largest positive integer such that,

$$tp^2 \leq n$$

$$\Rightarrow t = \left[\frac{n}{p^2}\right]$$

Thus, those integers which are divisible by 'p^q' are precisely $\left[\frac{n}{p^3}\right]$ in number.

Observe that highest power of 'p' that divides $n!$ is the sum of these integers namely

$$\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \cdots = \sum_{k=1}^{\infty} \left[\frac{n}{p^k}\right]$$

Hence the proof.

Ex: Determine the number of zero's with which the decimal representation of 50! terminates.

→ To determine the number of zero's, it is enough to observe how many 10 divides 50!.
i.e How many pairs of 5's and 2's divides 50!
For that we have to find exponent of 5 and 2 that divides 50!

The exponent of 2 $= \sum_{k=1}^{\infty} \left[\frac{50}{2^k}\right]$

$= \left[\frac{50}{2}\right] + \left[\frac{50}{2^2}\right] + \left[\frac{50}{2^3}\right] + \left[\frac{50}{2^4}\right] + \left[\frac{50}{2^5}\right]$

$= [25] + [12.5] + [6.45] + [3.125] + [1.5625]$

$= [25] + [12] + [6] + [3] + [1]$

$= 47$

and

The exponent of 5 $= \sum_{k=1}^{\infty} \left[\frac{50}{2^k}\right]$

$= \left[\frac{50}{5}\right] + \left[\frac{50}{5^2}\right]$

$= 10 + 2$

$= 12$

Thus there are 12 pairs and hence 12 zero's.

Ex. Show that 1000! ends up with 249 zero's.

→ $1000 = 10 \times 10 \times 10$

$= 5 \times 2 \times 5 \times 2 \times 5 \times 2$

$= 5^3 \cdot 2^3$

To determine the number of zero's, it is enough to observe how many 10 divides 1000!
i.e. How many pairs of 5's and 2's divides 1000!
For that we have to find exponent of 5 and 2 that divides 1000!

The exponent of 2 = $\sum_{k=1}^{\infty} \left[\frac{1000}{2^k}\right]$

$= \left[\frac{1000}{2}\right] + \left[\frac{1000}{2^2}\right] + \left[\frac{1000}{2^3}\right] + \left[\frac{1000}{2^4}\right] + \left[\frac{1000}{2^5}\right] + \left[\frac{1000}{2^6}\right] + \left[\frac{1000}{2^7}\right] + \left[\frac{1000}{2^8}\right] + \left[\frac{1000}{2^9}\right]$

$= [500] + [225] + [125] + [62.5] + [81.25] + [15.625] + [7.8125] + [3.90625] + [1.953125]$

$= 500 + 225 + 125 + 62 + 31 + 15 + 7 + 3 + 1$

$= 994$

and

The exponent of 5 = $\sum_{k=1}^{\infty} \left[\frac{1000}{5^k}\right]$

$= \left[\frac{1000}{5}\right] + \left[\frac{1000}{5^2}\right] + \left[\frac{1000}{5^3}\right] + \left[\frac{1000}{5^4}\right] +$

$= [200] + [40] + [8] + [1.6]$

$= 200 + 40 + 8 + 1$

$= 249$

Thus,

There are 249 pairs and hence 249 zero's.

* Theorem-:

If 'n' and 'r' are positive integers with $1 \le r \le n$ then then binomial coefficient $\binom{n}{r} = \frac{n!}{r!(n-r)!}$ is also an integer.

* Corollary-:

For a positive integer 'r' the product of any 'r' consecutive positive integers is divisible by r!

Proof:

Consider the product of 'r' consecutive positive integers, the largest of which is 'n' is $n.(n-1)(n-2)(n-3)\cdots(n-(r-2))(n-(r-1))$ we have,

$$n(n-1)(n-2)(n-3)\cdots(n-r+1) = n(n-1)(n-2)\cdots(n-r+1) \times \frac{(n-r)(n-(r+1))\cdots 3\cdot 2\cdot 1}{(n-r)(n-(r+1))\cdots 3\cdot 2\cdot 1}$$

$$= \frac{n!}{(n-r)!}$$

$$= \frac{n!}{(n-r)!\cdot r!} \times r!$$

since $\frac{n!}{(n-r)!\cdot r!}$ is an integer, the product of 'r' consecutive positive integers is divisible by r!.

Hence the proof.

* Theorem-:

Let 'f' and 'F' be number theoretic function such that $F(n) = \sum_{d|n} f(d)$ then for any positive

integer N.

$$\sum_{n=1}^{N} F(n) = \sum_{n=1}^{N} f(k)\left[\frac{N}{k}\right]$$

Proof:

Here given that,

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

$$\therefore \sum_{n=1}^{N} F(n) = \sum_{n=1}^{N} \sum_{d|n} f(d) \quad \text{—①}$$

We collect the terms with equal values of $f(d)$ in the double sum.

For a fixed positive integer $k \leq N$ the term $f(k)$ appears in $\sum_{d|n} f(d)$ iff 'k' is divisor of 'n'

Note that each integer has atleast itself as a divisor (and $1 \leq k \leq n$).

The R.H.S. of eqn ① includes $f(k)$ atleast once.

Now in oder to find the no. of times $f(k)$ occurs on R.H.S ①, it is sufficient to find the no. of integers among $1, 2, 3, \cdots, N$ which are divisible by 'k'.

There are exactly $\left[\frac{N}{k}\right]$ of them which are

$k; 2k, 3k, \cdots \left[\frac{N}{k}\right] k$.

Thus for each 'k' such that $1 \leq k \leq n$, $f(k)$ is a term of the sum $\sum_{d|n} f(d)$ for $\left[\frac{N}{k}\right]$ different positive integers $\leq n$.

Hence $\sum_{n=1}^{N} \sum_{d|n} f(d) = \sum_{k=1}^{n} f(k) \left[\frac{N}{k}\right]$ — (2)

∴ From (1) and (2) we have,

$$\sum_{n=1}^{N} f(n) = \sum_{k=1}^{N} f(k) \left[\frac{N}{k}\right]$$

* Corollary -:

For $N > 0$,

i) $\sum_{n=1}^{N} \tau(n) = \sum_{n=1}^{N} \left[\frac{N}{n}\right]$

ii) $\sum_{n=1}^{N} \sigma(n) = \sum_{n=1}^{N} n \cdot \left[\frac{N}{n}\right]$

Ex: Using the corollary find $\sum_{n=1}^{6} \tau(n)$ and $\sum_{n=1}^{6} \sigma(n)$ and verify the results.

→ i) $\sum_{n=1}^{N} \tau(n) = \tau(1) + \tau(2) + \tau(3) + \tau(4) + \tau(5) + \tau(6)$

$= 1 + 2 + 2 + 3 + 2 + 4$

$= 14.$

and

$$\sum_{n=1}^{6} \sigma(n) = \sum_{n=1}^{6} \left[\frac{6}{n}\right]$$

$$= \left[\frac{6}{1}\right] + \left[\frac{6}{2}\right] + \left[\frac{6}{3}\right] + \left[\frac{6}{4}\right] + \left[\frac{6}{5}\right] + \left[\frac{6}{6}\right]$$

$$= [6] + [3] + [2] + [1.5] + [1.2] + [1]$$

$$= 6 + 3 + 2 + 1 + 1 + 1$$

$$= 14$$

∴ L.H.S = R.H.S.

∴ $\sum_{n=1}^{N} \tau(n) = \sum_{n=1}^{N} \left[\frac{N}{n}\right]$

ii)

* Theorem -:

If 'p' is prime and $k > 0$ then

$$\phi(p^k) = p^k - p^{k-1} = p^k\left(1 - \frac{1}{p}\right)$$

Proof:

Amongest the integers $1, 2, 3, \ldots, p^k$ that are divisible by 'p' are $1 \cdot p, 2p, 3p, \ldots, p^{k-1} \cdot p$.

Thus the no. of positive integers less than 'n' or equal to p^k that are divisible by 'p' are p^{k-1}

$\therefore$ no. of positive integers $< p^k$ that are relatively prime to p^k is,

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

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

Hence the proof.

* Lemma-:

Given integers a, b, c ; gcd(a, bc) = 1 iff gcd(a, b) = 1 and gcd(a, c) = 1.

Proof:

Suppose gcd(a, bc) = 1.

∴ ∃ an integers 'x' and 'y' such that,

$ax + bcy = 1$

$\therefore a x + b(cy) = 1$

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

similarly,

$ax + cby = 1$

$\therefore ax + c(by) = 1$

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

Conversely,

suppose that $\gcd(a, b) = 1 = \gcd(a, c)$

∴ ∃ an integers 'x' and 'y' such that,

$ax + by = 1$

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

Then ∃ an integers 'x_1' and 'y_1' such that

$ax_1 + by_1 = 1$

Claim- $\gcd(a, bc) = 1$

Assume $\gcd(a, bc) = d$

$\Rightarrow d \mid a$ and $d \mid bc$

$\Rightarrow d \mid acx$ and $d \mid bcy$

$\Rightarrow d \mid acx + bcy$

$\Rightarrow d \mid c(ax + by)$

$\Rightarrow d \mid c$ $\quad (\because ax + by = 1)$

Here,

$d \mid a$ and $d \mid c$

$\Rightarrow d \mid \gcd(a, c)$

$\Rightarrow d \mid 1 \Rightarrow d = 1$

$\therefore \gcd(a, bc) = 1$

Hence the proof.

Imp

* **Theorem -:**

The function 'ϕ' is a multiplicative function.

Proof:

Let m, n be relatively prime integers. since, $\phi(1) = 1$ the result holds trivially when either $m = 1$ or $n = 1$.

Let $m > 1$ and $n > 1$.

Let us arrange m, n integers from 1 to mn as follows:

$$\begin{array}{cccccccc} 1 & 2 & 3 & \cdots & r & \cdots & m \\ m+1 & m+2 & m+3 & \cdots & m+r & \cdots & 2m \\ 2m+1 & 2m+2 & 2m+3 & \cdots & 2m+r & \cdots & 3m \\ \vdots & & & & & & \\ (n-1)m+1 & (n-1)m+2 & (n-1)m+3 & \cdots & (n-1)m+r & \cdots & nm \end{array}$$

Now $\phi(mn)$ is equal to the number of entries in the array which are relatively prime to 'mn'. We know that a number is relatively prime to 'mn' iff it is relatively prime each of 'm' and 'n'. We know that

$$\gcd(qm+r, n) = \gcd(m, r)$$

Thus if an element in the first row is relatively prime to 'm', then the whole column corresponding to that element is relatively prime to 'm'.

Therefore as many as $\phi(m)$ column contains integers relatively prime to 'm'.

Now it remains to show that each of these $\phi(m)$ column of contains $\phi(n)$ integers relatively prime to 'n'.

Consider the entries in the r^{th} column $r, m+r, 2m+r, \cdots, (n-1)m+r$.

since $km+r \equiv jm+r \pmod{n}$; $0 \le j < k < m$

$\Rightarrow km \equiv jm \pmod{n}$

$\Rightarrow k \equiv j \pmod{n}$ (as $\gcd(m,n)=1$)

$\Rightarrow n \mid k-j$

which is absurd.

Thus no two entries in the rth column are congruent to one another modulo 'n'. Therefore $r, m+r, 2m+r, \dots, (n-1)m+r$ are congruent to $0, 1, 2, \dots, n-1$ modulo 'n'. Therefore the rth column contains exactly as many integers relatively prime to 'n' as the number of integers $0, 1, 2, 3, \dots, n-1$ which are relatively prime to 'n'.

Thus this column contains $\phi(n)$ integers which is relatively prime to 'n'. Therefore each of $\phi(m)$ column contains $\phi(n)$ integers which are relatively prime to 'n'.

Hence, $\phi(mn) = \phi(m) \cdot \phi(n)$

Hence the proof.

* Theorem-:

If the integer $n>1$ has the prime factorisation $n = p_1^{k_1} \cdot p_2^{k_2} \cdots p_r^{k_r}$ then

$$\phi(n) = (p_1^{k_1} - p_1^{k_1-1})(p_2^{k_2} - p_2^{k_2-1}) \cdots (p_r^{k_r} - p_r^{k_r-1})$$

$$= n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right) \cdots \left(1-\frac{1}{p_r}\right)$$

Proof:

We shall prove this theorem by induction on 'r'.

For $r=1$ we have,

$n = p_1^{k_1}$ and

$$\phi(n) = \phi(p_1^{k_1})$$
$$= p_1^{k_1} - p_1^{k_1-1}$$
$$= p_1^{k_1}\left(1 - \frac{1}{p_1}\right)$$
$$= n\left(1 - \frac{1}{p_1}\right)$$

consider,
$$n = p_1^{k_1} \cdot p_2^{k_2} \cdots p_s^{k_s} \cdot p_{s+1}^{k_{s+1}}$$
and
$$\phi(n) = \phi(p_1^{k_1} \cdot p_2^{k_2} \cdots p_s^{k_s} \cdot p_{s+1}^{k_{s+1}})$$
$$= \phi(p_1^{k_1} \cdot p_2^{k_2} \cdots p_s^{k_s}) \cdot \phi(p_{s+1}^{k_{s+1}}) \quad (\because \phi \text{ is multiplicative})$$
$$= (p_1^{k_1} - p_1^{k_1-1})(p_2^{k_2} - p_2^{k_2-1}) \cdots (p_s^{k_s} - p_s^{k_s-1}) \cdots (p_{s+1}^{k_{s+1}} - p_{s+1}^{k_{s+1}-1})$$
$$= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_s}\right)\left(1 - \frac{1}{p_{s+1}}\right)$$

Hence the result holds for $r = s+1$ whenever it holds for $r = s$. Therefore, by principle of induction the results holds for any 'r'.

Ex. Let $n = 360$ then $\phi(360) = ?$

→ Let $n = 360$ then $n = 2^3 \cdot 3^2 \cdot 5$

$$\therefore \phi(360) = 360\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right)$$
$$= 360 \times \frac{1}{2} \times \frac{2}{3} \times \frac{4}{5}$$
$$= 360 \times \frac{4}{15}$$
$$= 96.$$

* Theorem -:

For $n>2$, $\phi(n)$ is an even integer.

Proof:

Suppose 'n' is a power of 2.

Let $n = 2^k$ for some positive integer $k>1$

then, $\phi(n) = \phi(2^k)$

$= 2^k \cdot \left(1-\frac{1}{2}\right)$

$= 2^{k-1}$; $k>1$

Which is even.

$\therefore 2^{k-1}$ is even for any positive integer $k>1$.

Suppose 'n' is not power 2 then there is odd prime 'p' that divides 'n'.

Let $n = p^k \cdot m$ where $p \nmid m$.

since $p \nmid m$, $\gcd(p^k, m) = 1$ and since ϕ is multiplicative,

$\phi(n) = \phi(p^k m)$

$= \phi(p^k) \cdot \phi(m)$

$= p^{k-1}(p-1) \cdot \phi(m)$.

since 'p' is odd prime, $p-1$ is even so $\phi(n)$ is even integer.

* Some properties of ϕ-function -:

* Theorem [Gauss]:

For each positive integer $n \geq 1$,

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

The sum being extended over all positive divisors of 'n'.

Proof:

The integers between '1' and 'n' can be separated into classes as follows.

If 'd' is divisor of 'n', we put integer 'm' in the class 'S_d' provided $\gcd(m,n) = d$.

In symbol, $S_d = \{m : \gcd(m,n) = d, 1 \le m \le n\}$

since $\gcd(m,n) = d$ we have,

$$\gcd\left(\frac{m}{d}, \frac{n}{d}\right) = 1$$

is relatively prime to $\frac{n}{d}$, i.e $\phi\left(\frac{n}{d}\right)$

Therefore, number of positive integer in 'S_d' is precisely $\left(\frac{n}{d}\right)$. further, each integer between '1' and 'n' belongs to precisely one 'sd'.

$$\therefore \quad n = \sum_{d|n} |S_d| = \sum_{d|n} \phi\left(\frac{n}{d}\right)$$

since 'd' runs over all the divisors 'd' of 'n' we can write,

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

Ex. Let $n = 10$, the integers relatively prime to 10 are 1, 3, 7, 9 and divisors of 10 are 1, 2, 5, 10

$S_1 = \{1, 3, 7, 9\}$, $|S_1| = \phi(10) = 4$

$S_2 = \{2, 4, 6, 8\}$, $|S_2| = \phi(5) = 4$

$S_5 = \{5\}$, $|S_5| = \phi(2) = 1$

$S_{10} = \{10\}$, $|S_{10}| = \phi(1) = 1$

$$\sum_{d|10} \phi(d) = \phi(1) + \phi(2) + \phi(5) + \phi(10)$$

$$= 1 + 1 + 4 + 4$$

$$= 10$$

* Theorem -:

For any positive integer n,

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

Proof:

We know,

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

By inversion formula we obtain,

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

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

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

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

* Lemma -:

Let $n > 1$ and $\gcd(a, n) = 1$. If $a_1, a_2, \dots, a_{\phi(n)}$ are positive integers less than 'n' and relatively prime to 'n' then $aa_1, aa_2, \dots, aa_{\phi(n)}$ are congruent modulo 'n' to $a_1, a_2, \dots, a_{\phi(n)}$ in some order.

Proof:

Claim - No two integers $aa_1, aa_2, \dots, aa_{\phi(n)}$ are congruent modulo 'n'.

Let if possible $aa_i \equiv aa_j \pmod{n}$; $1 \le i < j \le \phi(n)$ then as $\gcd(a, n) = 1$ we have,

$$a_i \equiv a_j \pmod{n}$$

$$\Rightarrow n \mid a_i - a_j$$

which is absurd

Now $\gcd(a_i, n) = 1$ and $\gcd(a, n) = 1$ where $1 \leq i < n$ implies that $\gcd(aa_i, n) = 1$ for each $i = 1, 2, \ldots, \phi(n)$

Thus for any fixed 'i', aa_i is congruent to unique 'b', $1 \leq b < n$

Hence $\gcd(b, n) = \gcd(aa_i, n) = 1$

Therefore 'b' must be one of $a_1, a_2, \ldots, a_{\phi(n)}$

since $aa_1, aa_2, \ldots, aa_{\phi(n)}$ are incongruent modulo 'n', they must be congruent modulo 'n' to $a_1, a_2, \ldots, a_{\phi(n)}$ in some order.

* Euler's Theorem :-

Let $n \geq 1$ and $\gcd(a, n) = 1$ then

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

Proof:

With no loss of generality we can take $n > 1$.

Let $a_1, a_2, \ldots, a_{\phi(n)}$ be possitive integers less than 'n' and relatively prime to 'n'. Then as $\gcd(a, n) = 1$, $aa_1, aa_2, \ldots, aa_{\phi(n)}$ are congruent to $a_1, a_2, \ldots, a_{\phi(n)}$ in some order.

Let $a_1', a_2', \ldots, a_{\phi(n)}'$ be a rearrangement of $a_1, a_2, \ldots, a_{\phi(n)}$ such that,

$$aa_i \equiv a_i' \pmod{n} \quad ; \quad 1 \leq i \leq \phi(n)$$

Thus,

$$aa_1 \equiv a_1' \pmod{n}$$
$$aa_2 \equiv a_2' \pmod{n}$$
$$\vdots$$
$$aa_{\phi(n)} \equiv a_{\phi(n)}' \pmod{n}$$

Therefore,

$$aa_1 \cdot aa_2 \cdots aa_{\phi(n)} \equiv a_1' a_2' \cdots a_{\phi(n)}' \pmod{n}$$

$\Rightarrow a^{\phi(n)} a_1 a_2 \cdots a_{\phi(n)} \equiv a_1 a_2 \cdots a_{\phi(n)} \pmod{n}$

since each a_i is relatively prime to n
$a_1 a_2 \cdots a_{\phi(n)}$ is relatively prime to n

Hence $a^{\phi(n)} \equiv 1 \pmod{n}$.

* **Remark -:**

Note that Euler's theorem is Euler's generalisation of Fermat's theorem.

* **Corollary -:**

For any prime 'p' and $p \nmid a$,

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

Ex Find the last two digits in the decimal expansion of 3^{256}.

→ We have to find smallest positive integer to which,

$$3^{256} \equiv 1 \pmod{100}$$

Note that $\gcd(3, 100) = 1$ so that

$$3^{\phi(100)} \equiv 1 \pmod{100}$$

$$\Rightarrow 3^{40} \equiv 1 \pmod{100}$$

Thus, $3^{240} = (3^{40})^6 \equiv 1 \pmod{100}$

Now, $3^4 \equiv 81 \pmod{100}$

$$\Rightarrow 3^4 \equiv (-19) \pmod{100}$$

$$\Rightarrow (3^4)^2 \equiv (-19)^2 \pmod{100}$$

$$\Rightarrow 3^8 \equiv (-39) \pmod{100}$$

$$\Rightarrow (3^8)^2 \equiv (-39)^2 \pmod{100}$$

$$\Rightarrow 3^{16} \equiv 21 \pmod{100}$$

Thus,

$$3^{256} = 3^{240} \cdot 3^{16} \equiv 1 \cdot 21 \equiv 21 \pmod{100}$$

Ex. Use Euler's theorem to establish the following

(a) For any integer a, $a^{37} \equiv a \pmod{1729}$

(b) For any integer a, $a^{13} \equiv a \pmod{2730}$

(c) For any integer a, $a^{33} \equiv a \pmod{4080}$

→ (a) $1729 = 7 \times 247$

$= 7 \times 13 \times 19$

By Euler's theorem,

$a^6 \equiv 1 \pmod{7}$ —①

$a^{12} \equiv 1 \pmod{13}$ —②

$a^{18} \equiv 1 \pmod{19}$ —③

∴ By ①, ② and ③,

$a^{36} \equiv 1 \pmod{1729}$

$a^{37} \equiv a \pmod{1729}$

(b) $2730 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 13$.

By Euler's theorem,

$a \equiv 1 \pmod{2}$ —①

$a^2 \equiv 1 \pmod{3}$ —②

$a^4 \equiv 1 \pmod{5}$ —③

$a^6 \equiv 1 \pmod{7}$ —④

$a^{12} \equiv 1 \pmod{13}$ —⑤

∴ By ①, ②, ③, ④ and ⑤,

$a^{25} \equiv 1 \pmod{2730}$

$a^{26} \equiv a \pmod{2730}$

$(a^{13})^2 \equiv a \pmod{2730}$

$\Rightarrow a^{13} \equiv a \pmod{2730}$

(c) $4080 = 2^4 \times 3 \times 5 \times 17 = 16 \times 15 \times 17$

$a^{\phi(n)} \equiv 1 \pmod{n}$

∴ $a^{\phi(16)} \equiv 1 \pmod{16} \Rightarrow a^8 \equiv 1 \pmod{16}$ —①

$a^{\phi(15)} \equiv 1 \pmod{15} \Rightarrow a^8 \equiv 1 \pmod{15}$ —②

$a^{\phi(17)} \equiv 1 \pmod{17} \Rightarrow a^{16} \equiv 1 \pmod{17}$ —③

$\therefore$ By ①, ② and ③

$a^{92} \equiv 1 \pmod{4080}$

$a^{93} \equiv a \pmod{4080}$.