Unit-II III BSC - VI Sem mathematics. (S.V.R)

Paper - 6.2a. (Number theory)

Fermat's Little theorem: If 'p' is a prime and a is any integer such that (p is not a divisor of 'a') ie $p \nmid a$ and $(a, p) = 1$, then $a^{p-1} \equiv 1 \pmod p$

OR

$a^p \equiv a \pmod p$

Pseudo primes: If 'p' is a composite positive integer and 'a' is any integer and $a^p \equiv a \pmod p$ then 'p' is called a pseudo prime to the bas a.

If $(a, p) = 1$ then $a^p \equiv a \pmod p$ is equivalent to the $a^{p-1} \equiv 1 \pmod p$.

For Examples: Integers 341, 561, 645 are pseudo primes.

I) Show that the integer 341 is a pseudo prime.

Sol: Wehave $P = 341 = 11 \times 31$

By Fermat's Little theorem wehave

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

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

$2^{340} \equiv 1 \pmod{11}$ — (1)

$11 \,|\, \underline{341}$, 31; 11, 31 are primes

Let $(2, 31) = 1$, By Fermat's little theorem

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

$2^{30} \equiv 1 \pmod{31}$

$(2^{30})^{11} \equiv 1^{11} \pmod{31}$ ②

$2^{330} \equiv 1 \pmod{31}$ — ②.

But $2^5 = 32 \equiv 1 \pmod{31}$

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

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

$2^{10} \equiv 1 \pmod{31}$ — ③

$$31 \overline{)32} \quad \begin{array}{r} 1 \\ 32 \\ 31 \\ \hline 1 \end{array}$$

from ② & ③ we get

$2^{330} \times 2^{10} \equiv 1 \pmod{31}$

$\therefore 2^{340} \equiv 1 \pmod{31}$ — ④

From eqs ① & ④ we get

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

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

$\therefore$ 341 is a pseudo prime to the base 2.

2) S.T. 561 is a pseudo prime.

Sol: Let $P = 561 = 3 \cdot 11 \cdot 17$.

By Fermat's little theorem

$(a, p) = 1, \quad a^{p-1} \equiv 1 \pmod{p}$

Let $(2, 3) = 1, \quad 2^{3-1} \equiv 1 \pmod{3}$

$2^2 \equiv 1 \pmod{3}$

$(2^2)^{280} \equiv 1^{280} \pmod{3}$

$2^{560} \equiv 1 \pmod{3}$ — ①

$$\begin{array}{r|l} 3 & 561 \\ \hline 11 & 187 \\ \hline & 17 \end{array}$$

$561 = 3 \times 11 \times 17$

3, 11, 17 are prime nos.

Let $(2, 11) = 1$, $2^{11-1} \equiv 1 \pmod{11}$ ③ *

$2^{10} \equiv 1 \pmod{11}$ $(10 \times 56 = 560)$

$(2^{10})^{56} \equiv 1^{56} \pmod{11}$

$2^{560} \equiv 1 \pmod{11}$ — ②

Let $(2, 17) = 1$, $2^{17-1} \equiv 1 \pmod{17}$

$2^{16} \equiv 1 \pmod{17}$ $16 \times 35 = 560$

$(2^{16})^{35} \equiv 1^{35} \pmod{17}$

$2^{560} \equiv 1 \pmod{17}$ — ③

From eqs ①, ② & ③ we get

$2^{560} \equiv 1 \pmod{3 \times 11 \times 17}$

$2^{561-1} \equiv 1 \pmod{561}$

$\therefore$ 561 is a pseudo prime to the base 2

3) S.T. 645 is a pseudo prime.

Sol: let $P = 645 = 3 \times 5 \times 43$

By Fermat's little theorem,

$(a, p) = 1$, $a^{p-1} \equiv 1 \pmod{p}$

$$\begin{array}{r|l} 3 & 645 \\ \hline 5 & 215 \\ \hline & 43 \end{array}$$

$645 = 3 \times 5 \times 43$

Let $(2, 3) = 1$, $2^{3-1} \equiv 1 \pmod{3}$

$2^2 \equiv 1 \pmod{3}$

$(2^2)^{322} \equiv 1^{322} \pmod{3}$ $2 \times 322 = 644$

$2^{644} \equiv 1 \pmod{3}$ — ①

$(2,5)=1$, ④ $2^{5-1} \equiv 1 \pmod 5$

$2^4 \equiv 1 \pmod 5$

$(2^4)^{161} \equiv 1^{161} \pmod 5$

$2^{644} \equiv 1 \pmod 5$ — ②

$$4 \overline{)644} = 161, \quad 644 = 4 \times 161$$

Let $2^7 = 128 \equiv (-1) \pmod{43}$ $\quad 2^7 = 128$

$2^7 \equiv -1 \pmod{43}$

$(2^7)^{92} \equiv (-1)^{92} \pmod{43}$

$\therefore 2^{644} \equiv 1 \pmod{43}$ — ③

$$7 \overline{)644} = 92, \quad 644 = 7 \times 92$$

from eqn ①, ② & ③ we get

$$2^{644} \equiv 1 \pmod{3 \times 5 \times 43}$$

$$2^{644} \equiv 1 \pmod{645}$$

$$2^{645-1} \equiv 1 \pmod{645}$$

$\therefore$ 645 is a pseudo prime to the base 2

Wilson's theorem:

Statement: If p is a prime then $(p-1)! \equiv -1 \pmod p$

proof: When $p=2$ then $(2-1)! \equiv -1 \pmod 2$

$1! \equiv -1 \pmod 2$

$1 \equiv -1 \pmod 2$ is true

When $p=3$, then $(3-1)! \equiv -1 \pmod 3$

$2! \equiv -1 \pmod 3$

$2 \equiv -1 \pmod 3$ (or) $3 \equiv 0 \pmod 3$ is true

When $P>3$ Choose 'a' is any one of $(P-1)$ positive integers $1 \cdot 2 \cdot 3 \cdots (P-1)$.

Consider $ax \equiv 1 \pmod{p}$ — ① & $(a,p)=1$

$\therefore$ Eqn ① has a unique sol^n.

then there exists a unique integer a' such that $aa' \equiv 1 \pmod{p}$, $1 \le a' \le (P-1)$.

If $a=a'$ iff $a=1$ & $a=P-1$.

then $a^2 \equiv 1 \pmod{p}$ $\therefore$

$$(a^2-1) \equiv 0 \pmod{p} \Rightarrow p/(a^2-1) = p/(a-1)(a+1)$$

$\therefore$ ($p/ab \Rightarrow p/a$ or p/b)

$\therefore$ $p/a-1$ or $p/(a+1)$ ie $(a-1) \equiv 0 \pmod{p}$

$(a+1) \equiv 0 \pmod{p}$

$\therefore \Rightarrow a = (P-1)$.

If we omit the nos 1 & $(P-1)$.

$\therefore$ Remaining integers $2, 3, \cdots (P-2)$ into pairs a, a' where $a \neq a'$. $\therefore$ $aa' \equiv 1 \pmod{p}$

$$\therefore \quad 2 \cdot 3 \cdots (P-2) \equiv 1 \pmod{p}$$

$$\therefore \quad (P-2)! \equiv 1 \pmod{p}$$

$$(P-2)!\,(P-1) \equiv (P-1) \pmod{p}$$

$$(P-1)! \equiv 1 \pmod{p}$$

Problems: ① If 7 is prime then S.T $(7-1)! \equiv -1 \pmod 7$

Sol: By wilson's theorem If p is prime then $(p-1)! \equiv -1 \pmod p$

Let $p = 7$ is a prime.

To show that, $(7-1)! \equiv -1 \pmod 7$

$6! \equiv -1 \pmod 7$

let $6! = 1\cdot2\cdot3\cdot4\cdot5\cdot6$.

But $(1\cdot6) = 6 \equiv (-1) \pmod 7$

$(2\cdot4) = 8 \equiv 1 \pmod 7$

$(3\cdot5) = 15 \equiv 1 \pmod 7$

$7 - 6 = 7$, remainder -1

$\therefore (1\cdot6)(2\cdot4)(3\cdot5) \equiv (-1)(1)(1) \pmod 7$

$1\cdot2\cdot3\cdot4\cdot5\cdot6 \equiv -1 \pmod 7$

$6! \equiv -1 \pmod 7$ Hence wilson's theorem

② If 13 is a prime then S.T. $(13-1)! \equiv -1 \pmod{13}$

Sol: By wilson's theorem

$P = 13$ is a prime then To show that $(13-1)! \equiv -1 \pmod{13}$

$(12)! \equiv -1 \pmod{13}$

ie $12! = 1\cdot2\cdot3\cdot4\cdot5\cdot6\cdot7\cdot8\cdot9\cdot10\cdot11\cdot12 \equiv (-1) \pmod{13}$

Let $1\cdot12 = 12 \equiv -1 \pmod{13}$

$2\times7 = 14 \equiv 1 \pmod{13}$

$3\times9 = 27 \equiv 1 \pmod{13}$

$4\times10 = 40 \equiv 1 \bmod (13)$

$5\times8 = 40 \equiv 1 \bmod (13)$

$6\times11 = 66 \equiv 1 \pmod{13}$

$\therefore (1\cdot12)(2\cdot7)(3\cdot9)(4\cdot10)(5\cdot8)(6\cdot11) \equiv (-1)(1)(1)(1)(1)(1) \pmod{13}$

$1\cdot2\cdot3\cdot4\cdot5\cdot6\cdot7\cdot8\cdot9\cdot10\cdot11\cdot12 \equiv -1 \pmod{13}$ (7)

$$12! \equiv -1 \pmod{13}$$

$$(13-1)! \equiv -1 \pmod{13}$$

2) If 17 is prime then S.T. $(17-1)! \equiv -1 \pmod{17}$

OR

$$16! \equiv -1 \pmod{17}$$

Sol: By wilson's theorem

If p is prime then $(p-1)! \equiv -1 \pmod{p}$

If $p=17$ then to show that $(17-1)! \equiv -1 \pmod{17}$

$$16! \equiv -1 \pmod{17}$$

Let $16! = 1\cdot2\cdot3\cdot4\cdot5\cdot6\cdot7\cdot8\cdot9\cdot10\cdot11\cdot12\cdot13\cdot14\cdot15\cdot16 \equiv -1 \pmod{17}$

Let $(1\cdot16) = 16 \equiv -1 \pmod{17}$

$(2\cdot9) = 18 \equiv 1 \pmod{17}$

$(3\cdot6) = 18 \equiv 1 \pmod{17}$

$(4\cdot13) = 52 \equiv 1 \pmod{17}$

$(5\cdot7) \equiv 35 \equiv 1 \pmod{17}$

$(10\cdot12) = 120 \equiv 1 \pmod{17}$

$(11\cdot14) = 154 \equiv 1 \pmod{17}$

$(8\cdot15) = 120 \equiv 1 \pmod{17}$

$\therefore (1\cdot16)(2\cdot9)(3\cdot6)(4\cdot13)(5\cdot7)(10\cdot12)(11\cdot14)(8\cdot15) \equiv (-1)(1)(1)(1)(1)(1)(1)(1) \pmod{17}$

$1\cdot2\cdot3\cdot4\cdot5\cdot6\cdot7\cdot8\cdot9\cdot10\cdot11\cdot12\cdot13\cdot14\cdot15\cdot16 \equiv -1 \pmod{17}$

$$16! \equiv -1 \pmod{17}$$

$\therefore (17-1)! \equiv -1 \pmod{17}$ Hence wilson's theorem

(8)

(4) S.T. $(6!+1)$ is divisible by 7.

Sol: By Wilson's theorem

If p is prime, then $(p-1)! \equiv -1 \pmod{p}$

i.e. $(p-1)!+1 \equiv 0 \pmod{p}$

Let 7 is prime then $(7-1)! \equiv -1 \pmod{7}$

$6! \equiv -1 \pmod{7}$

$6!+1 \equiv 0 \pmod{7}$

$\therefore (6!+1)$ is divisible by 7

(5) P.T. $(12!+1)$ is divisible by 13.

(6) If p is prime number then S.T.

$2(p-3)!+1$ is a multiple of p.

Sol: By Wilson's theorem we have

If p is prime then $(p-1)! \equiv -1 \pmod{p}$

$(p-1)!+1 \equiv 0 \pmod{p}$

$\therefore (p-3)!\,(p-2)(p-1)+1 \equiv 0 \pmod{p}$

$\left(\because (p-1)! = (p-1)(p-2)(p-3)\cdots 3\cdot 2 \right.$

$\left. = (p-1)(p-2)\,(p-3)! \right)$

$\therefore (p-2)(p-1)\,(p-3)!+1 \equiv 0 \pmod{p}$

$(p^2-3p+2)(p-3)!+1 \equiv 0 \pmod{p}$

$(p^2-3p)(p-3)!+2\,(p-3)!+1 \equiv 0 \pmod{p}$

But $(p^2-3p)(p-3) \equiv 0 \pmod{p}$

$\therefore 2(p-3)!+1 \equiv 0 \pmod{p}$

$\therefore 2(p-3)!+1$ is a multiple of p

Fermat's number

Defn: An integers in the form $F_n = 2^{2^n}+1$ are called Fermat's numbers. Where $n \geq 0$
$n = 0, 1, 2, 3 \ldots$

Examples: Fermat's numbers.

$$F_n = 2^{2^n}+1$$

For $n=0$, $F_0 = 2^{2^0}+1 = 2+1 = 3$.

$n=1$, $F_1 = 2^{2^1}+1 = 2^2+1 = 4+1 = 5$

$n=2$, $F_2 = 2^{2^2}+1 = 2^4+1 = 16+1 = 17$

$n=3$, $F_3 = 2^{2^3}+1 = 2^8+1 = 256+1 = 257$

$n=4$, $F_4 = 2^{2^4}+1 = 65537$.

proposition: prove that the Fermat's number $F_5 = 2^{2^5}+1$ is divisible by 641

Sol: We wish to show that $641 / F_5$

ie 641 is a divisor of F_5 or F_5 is a divisible by 641

Let $641 = 5 \times 2^7 + 1$ or $641 = 2^4 + 5^4$

$(641-1) = 5 \times 2^7$ or $(641 - 5^4) = 2^4$.

Let $F_5 = 2^{2^5}+1 = 2^{32}+1 = 2^4 \cdot 2^{28}+1$

But $2^4 = (641-5^4)$

$F_5 = (641-5^4)\, 2^{28}+1$

$F_5 = 641 \cdot 2^{28} - 5^4 \cdot 2^{28}+1$

$F_5 = 641 \cdot 2^{28} - (5 \cdot 2^7)^4 + 1$

But $5 \times 2^7 = (641-1)$

$$F_5 = 641 \cdot 2^{28} - (5 \cdot 2^7)^4 + 1$$

$$F_5 = 641 \cdot 2^{28} - (641-1)^4 + 1$$

But $(a+b)^4 = a^4 + 4a^3b + \frac{4(4-1)}{2!}a^2b^2 + \frac{4(4-1)(4-2)}{3!}ab^3 + b^4$

$$(a-b)^4 = a^4 - 4a^3b + 6a^2b^2 - 4ab^3 + b^4$$

$$(641-1)^4 = (641)^4 - 4(641)^3 + 6(641)^2 - 4(641) + 1$$

$$(641-1)^4 = (641)^4 - 4(641)^3 + 6(641)^2 - 4(641) + 1$$

$$F_5 = 641 \cdot 2^{28} - (641-1)^4 + 1$$

$$F_5 = 641 \times 2^{28} - \left[(641)^4 - 4(641)^3 + 6(641)^2 - 4(641) + 1\right] + 1$$

$$F_5 = 641 \times 2^{28} - (641)^4 + 4(641)^3 - 6(641)^2 + 4(641) - 1 + 1$$

$$F_5 = 641 \times 2^{28} - (641)^4 + 4(641)^3 - 6(641)^2 + 4(641)$$

$$F_5 = 641\left[2^{28} - (641)^3 + 4(641)^2 - 6(641) + 4\right]$$

$F_5 = 641K \quad \forall K \in \mathbb{Z}$

where $K = (2^{28} - (641)^3 + 4(641)^2 - 6(641) + 4)$

$\Rightarrow 641 / F_5$

$\therefore F_5$ is divisible by 641

III BSC VI Semester

Mathematics paper - 6.2a

Number Theory

Unit:- 3 Mobius and Greatest integer function

Unit:- 3

The Mobius inversion formula

Mobius function

The Mobius function 'μ' is an Arithematic function (or) Number theoritic function. its domain is N and its range is $\{-1, 0, 1\}$.

i.e $\mu : N \longrightarrow \{-1, 0, 1\}$ is defined as

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1 \\ 0, & \text{if } p^2/n \text{ for some prime } p \text{ (n is not square free)} \\ (-1)^r & \text{if } n = p_1 p_2 \ldots p_r \text{ where } p_i \text{ are distinct prime (or } n \text{ is square free)} \end{cases}$$

Note: $\mu(p^k) = \begin{cases} 1, & \text{if } k = 0 \\ -1 & \text{if } k = 1 \\ 0 & \text{if } k \geq 2 \end{cases}$.

Examples:

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

$n = 2$, $\mu(2) = -1$ $(2 = 2^1, r = 1. \ \mu(2) = (-1)^r = -1)$

$n = 3$ $\mu(3) = -1$ $(3 = 3^1)$

$n = 4$ $\mu(4) = 0$ $(\because 4 = 2^2, 2^2/4)$

$n = 5$ $\mu(5) = -1$

$n = 6$ $\mu(6) = 1$ $(\because 6 = 2^1 \times 3^1, r = 2) \therefore \mu(6) = 1$

$n = 7$ $\mu(7) = -1$

$n = 18$ $\mu(18) = 0$ $(18 = 9 \times 2 = 3^2 \times 2, 3^2/18)$

$n = 20$ $\mu(20) = 0$ $(4 \times 5 = 20, 2^2/20)$

$n = 30$ $\mu(30) = (-1)^3$ $(30 = 2 \times 3 \times 5)$

$= -1$

Theorem: 01 Prove that the function μ is a Multiplicative function.

Proof: Let μ is a Mobius function

i.e. $\mu(n) = \begin{cases} 1 & \text{if } n=1 \\ 0 & \text{if } p^2/n \text{ for some prime } p \\ (-1)^r & \text{if } n = p_1 . p_2 \ldots p_r, \; p_i \text{ are distinct prime} \end{cases}$

we have to prove that

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

whenever m & n are relatively prime

Case: i If $m=1$ $n=1$

$\mu(m) = \mu(1) = 1$

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

then $\mu(m).\mu(n) = 1.1 = 1$

$mn = 1.1 = 1$

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

thus $\mu(mn) = \mu(m).\mu(n)$.

Case ii

if p^2/mn then p^2/m (or) p^2/n

since p^2/mn $\mu(mn) = 0$

if p^2/m then $\mu(m) = 0$ and also

$\mu(m).\mu(n) = 0$.

if p^2/n then $\mu(n) = 0$ and also

$\mu(m).\mu(n) = 0$

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

Case iii

Let us assume m and n are Square free Integers

say

Say $m = p_1 p_2 \dots p_r$ $\mu(m) = (-1)^r$ $\mu(n) = (-1)^s$

$n = q_1 q_2 \dots q_s$ with all the primes p_i and q_j being distinct then

$\mu(mn) = \mu(p_1 p_2 \dots p_r . q_1 q_2 \dots q_s)$

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

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

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

Hence μ is a Multiplicative function

Note For each +ve integer $n \geq 1$

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n > 1 \end{cases}$$ when d runs through +ve divisors of n

① Illustrate the value $\sum_{d|n} \mu(d)$ for $n = 10$.

Sol^n $n = 10$

The all positive divisors of 10 are

1, 2, 5, 10

∴ the desired sum is

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

$= 1 - 1 - 1 + 1$

$= 0$

Note. For each +ve integer $n \geq 1$

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if } n=1 \\ 0 & \text{if } n>1 \end{cases}$$ when d runs through +ve divisors of n

(1). Illustrate the value $\sum_{d|n} \mu(d)$ for $n=10$

Soln $n=10$

The all positive divisors of 10 are

1, 2, 5, 10

$\therefore$ The desired sum is

$$\sum_{d|10} \mu(d) = \mu(1)+\mu(2)+\mu(5)+\mu(10)$$
$$= 1-1-1+1 = \underline{\underline{0}}$$

Theorem

If $n \geq 1$ then $\mu(d) = \left[\frac{1}{n}\right] = \begin{cases} 1 & \text{if } n=1 \\ 0 & \text{if } n>1 \end{cases}$

Proof: The formula is clearly true for $n=1$.
Assume, then that $n>1$ and written
$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$.
In the sum $\sum_{d|n} \mu(d)$ the only non zero terms come from $d=1$ and from those divisors of n which are product of distinct primes. thus

$$\sum_{d|n} \mu(d) = \mu(1)+\mu(p_1)+\mu(p_2)+\dots \mu(p_k)+\mu(p_1 p_2)+ \dots + \mu(p_{k-1} p_k)+ \dots +\mu(p_1 p_2 \dots p_k)$$

$$= \dots = 1+\binom{k}{1}(-1)+\binom{k}{2}(-1)^2+\dots+\binom{k}{k}(-1)^k$$

$$= (1-1)^k = \underline{\underline{0}}$$

Mobius Inversion formula:

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

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

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

Proof

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

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

$$= \sum_{d|n}\left(\sum_{c|(n/d)} \mu(d) . f(c)\right) \rightarrow (1)$$

It is verified that

$d|n$ and $c|(n/d)$ iff $c|n$ and $d|(n/c)$

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

$$= \sum_{c|n}\left(f(c) . \sum_{d|(n/c)} \mu(d)\right) \rightarrow (2)$$

We know that for the +ve integer $n \geq 1$

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

the sum $\sum_{d|(n/c)} \mu(d)$ must vanish

Except when $n/c = 1$

Thus from (2)

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

Q Show that $\sum_{d|n}\left(\sum_{c|(n/d)} \mu(d).f(c)\right) = \sum_{c|10}\left(\sum_{d|(10/c)} f(c).\mu(d)\right)$

for $n=10$

Soln

$n = 10$

The all positive divisors of 10 are

$d = 1, 2, 5, 10.$

Now

if $d=1$ then $c|(10/d)$ ie. $c = 1, 2, 5, 10$

if $d=2$ then $c|(10/d)$ ie $c = 1, 5.$

if $d=5$ then $c|(10/d)$ ie $c = 1, 2$

if $d=10$ then $c|(10/d)$ ie $c = 1$

$$\therefore \sum_{d|10}\left(\sum_{c|(10/d)} \mu(d).f(c)\right)$$

$$= \mu(1)\left[f(1)+f(2)+f(5)+f(10)\right] + \mu(2)\left[f(1)+f(5)\right] + \mu(5)\left[f(1)+f(2)\right] + \mu(10)\left[f(1)\right]$$

$$= f(1)\left[\mu(1)+\mu(2)+\mu(5)+\mu(10)\right] + f(2)\left[\mu(1)+\mu(5)\right] + f(5)\left[\mu(1)+\mu(2)\right] + f(10)\left[\mu(1)\right].$$

$$= \sum_{c|10}\left(\sum_{d|(10/c)} f(c).\mu(d)\right)$$

Q For each +ve integer n S.T
$\mu(n)\,\mu(n+1)\,\mu(n+2)\,\mu(n+3)=0$.

proof

Let $\mu(n)\,\mu(n+1)\,\mu(n+2)\,\mu(n+3)$
$= \mu(n(n+1)(n+2)(n+3))$ ($\because \mu$ is Multiplicative function)

Now for each value of 'n' there will be 2 even and 2 odd no in the factors of rhs.

$\therefore$ There will be a one factor of 2^2 in the product $\therefore \mu(2^2)=0$.

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

Hence the proof.

Q If 'n' is a +ve integer $\ni n\geq 3$ then
$\sum\limits_{K=1} \mu(K!)=1$

Proof :- Let $n=3$

then $\sum\limits_{K=1}^{3} \mu(K) = \mu(1!)+\mu(2!)+\mu(3!)$
$= 1+(-1)+(-1)^2$
$= \underline{1}$

The result is true for $n=m$, then
$\sum\limits_{K=1}^{m} \mu(K!)=1$

The result is also true for $n=m+1$
$\sum\limits_{K=1}^{m+1} \mu(K!) = \sum\limits_{K=1}^{m} \mu(K!) + \mu((m+1)!)$
$= 1+0$
$= 1$

$\therefore \sum\limits_{K=1}^{n} \mu(K) = 1$ Hence the proof.

Scanned by CamScanner

Note: Let $n = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}$ be the prime factorization of 'n'. If f is a multiplicative function and is not identity indintically equal to zero then

$$\sum_{d|n} \mu(d) f(d) = (1-f(p_1))(1-f(p_2)) \ldots (1-f(p_r)).$$

(11) If $n = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}$ then

$$\sum_{d|n} \frac{\mu(d)}{d} = \left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right) \ldots \left(1-\frac{1}{p_r}\right)$$

Proof Let $f(n) = \frac{1}{n}$

then we have

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

Since 'f' is a Multiplicative function

i.e $\frac{1}{mn} = \frac{1}{m} \cdot \frac{1}{n}$

$$f(mn) = f(m).f(n)$$

$$\sum_{d|n} \mu(d) f(d) = (1-f(p_1))(1-f(p_2)) \ldots (1-f(p_r))$$

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

$$\sum_{d|n} \mu(d) \cdot \frac{1}{d} = \left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right) \ldots \left(1-\frac{1}{p_r}\right) \quad \left(\because f(p_r) = \frac{1}{p_r}\right)$$

$$\left(\because f(d) = 1/d\right)$$

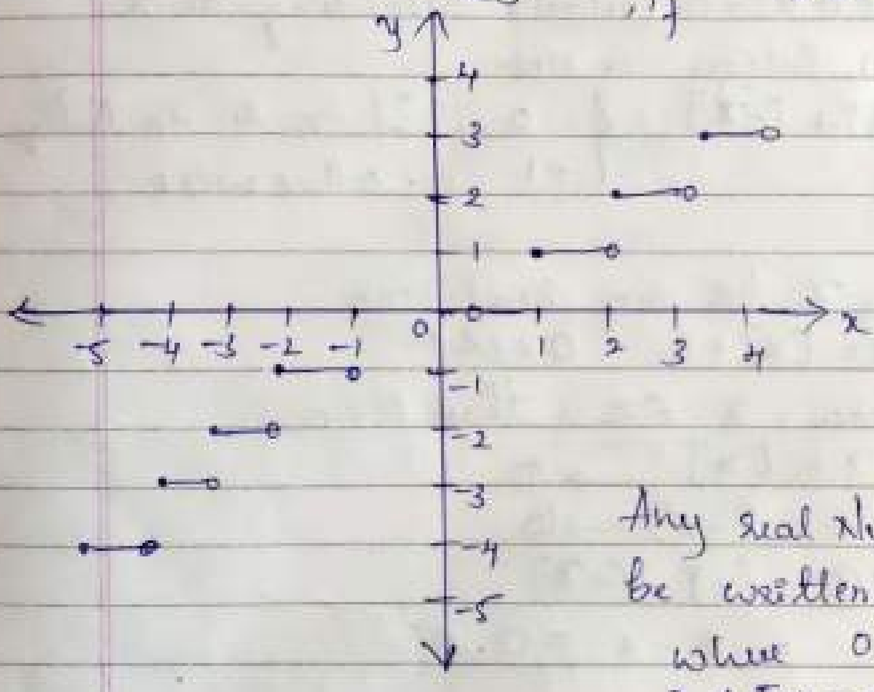
$$\therefore \sum_{d|n} \frac{\mu(d)}{d} = \left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right) \ldots \left(1-\frac{1}{p_r}\right)$$

Hence the proof.

Greatest integer function (or) step function (or) floor function

$[x] : \mathbb{R} \longrightarrow \mathbb{Z}$

If: $x = \begin{cases} -3 & , \text{if } -3 \le x < -2 \\ -2 & , \text{if } -2 \le x < -1 \\ -1 & , \text{if } -1 \le x < 0 \\ 0 & , \text{if } 0 \le x < 1 \\ 1 & , \text{if } 1 \le x < 2 \\ 2 & , \text{if } 2 \le x < 3 \\ 3 & , \text{if } 3 \le x < 4 \end{cases}$



Any real Number 'x' can be written as $x = [x] + \theta$,
where $0 \le \theta < 1$.

$x \neq [x + \theta]$

$3.2 = [3.2] + \theta$

$3.2 = 3 + \theta \; , (\theta = 0$

Defn

For an arbitrary real number x, then the largest integer less than (or) equal to x is called the integral part of x (or Greatest integer function (or Bracket function. It will be denoted by $[x]$

Example: $[3] = 3$, $[-4] = -4$, $[3.7] = 3$.
$[-4.2] = -5$, $[-3/2] = -2$, $[\sqrt{2}] = 1$

Note 1) $[x]$ is the largest integer $\le x$

2) If a and b are positive integer such that $a = bq + r$ where $0 \le r < b$ then

$\frac{a}{b} = q + \frac{r}{b}$ where $0 \le \frac{r}{b} < 1$.

$\therefore \left[\frac{a}{b}\right] = q$ is the quotient in the division of a by b.

Theorem Prove that the greatest integer function satisfies the properties $[x] + [-x] = 0$ (or) -1, according as x is an integer or not.

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

Proof.

a) Let x be any real no.

$x = [x] + \theta$; $0 \le \theta < 1$

Suppose $x \in Z$ then $\theta = 0$

$x = [x] \rightarrow ①$

$-x = [-x] \rightarrow ②$

$① + ② = [x] + [-x]$

$= x - x = 0$

b) If x is not an integer.

$x = [x] + \theta$; $0 < \theta < 1$

$-x = [-x] + \theta'$; $0 < \theta' < 1$

Adding $x + (-x) = [x] + \theta + [-x] + \theta'$

$0 = [x] + [-x] + (\theta + \theta')$

But $0 < (\theta + \theta') < 2$ and $\theta + \theta' = -\{[x] + [-x]\}$

$\therefore 0 < -\{[x] + [-x]\} < 2$ (or)

$-2 < \{[x] + [x]\} < 0$

$\therefore [x] + [-x]$ is an integer so

$[x] + [-x] = -1$

Theorem: ~~Prove that~~ Prove that. $\left[\frac{[x]}{n}\right] = \left[\frac{x}{n}\right]$ where n is a +ve Integer

Proof: Let $x \in R$

$x = [x] + \theta \quad , \quad 0 \le \theta < 1$

by division algorithm

$[x] = nq + r$ where, $0 \le r < n$

Consider

$$\left[\frac{x}{n}\right] = \left[\frac{[x] + \theta}{n}\right]$$

$$= \left[\frac{nq + r + \theta}{n}\right]$$

$$= \left[\frac{nq + r + \theta}{n}\right] = \left[q + \frac{r + \theta}{n}\right]$$

Since $r < n$

$$\left[\frac{x}{n}\right] = q \longrightarrow (1)$$

Also $\left[\frac{[x]}{n}\right] = \left[\frac{nq + r}{n}\right]$

$$= \left[q + \frac{r}{n}\right]$$

$$\left[\frac{[x]}{n}\right] = q \longrightarrow (2)$$

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

$$\left[\frac{[x]}{n}\right] = \left[\frac{x}{n}\right].$$

Note:

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 because $\left[\frac{n}{p^k}\right]=0$ for $p^k > n$.

Proof.

Among the first n positive integers, those divisible by p are $p, 2p, 3p \ldots tp$, where t is the largest integer such that $tp \leq n$.

Thus there are exactly $[n/p]$ multiples of p occurring in the product that defines n namely $p, 2p, 3p, \ldots \left[\frac{n}{p}\right].p$

(Since $\left[\frac{n}{p}\right]$ is the quotient in the division of n by p)

$$\therefore\ k(n!) = \frac{n}{p} + k\left(\left[\frac{n}{p}\right]!\right) \rightarrow (1)$$

Changing n to $\frac{n}{p}$ in (1) we get

$$k\left(\left[\frac{n}{p}\right]!\right) = \left[\frac{n}{p^2}\right] + k\left(\left[\frac{n}{p^2}\right]!\right) \rightarrow (2)$$

Substitute (2) in (1) we get

$$k(n!) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + k\left(\left[\frac{n}{p^2}\right]!\right)$$

Continuing this process, we can prove that

$$k(n!) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \cdots$$

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

Altanate proof:

1. Find the highest Power of a prime number P Contained in $n!$

Sol^n

Let $K(n!)$ denote the highest power of P Contained in $n!$

$n!$ is the Product of the factors $1, 2, 3 \ldots n$

The factors in $n!$ which will be divisible by p are $P, 2P, 3P \ldots \left[\frac{n}{P}\right]P$

[Since $\left[\frac{n}{P}\right]$ is the quotient in the divison of n by p]

Therefore $K(n!) = \left[\frac{n}{P}\right] + K\left(\left[\frac{n}{P}\right]!\right) \rightarrow (1)$

Changing n to $\frac{n}{P}$ in (1)

$$K\left(\left[\frac{n}{P}\right]!\right) = \frac{n}{P^2} + K\left(\left[\frac{n}{P^2}\right]!\right) \rightarrow (2)$$

Putting the value from 2 in 1, we get

$$K(n!) = \left[\frac{n}{P}\right] + \left[\frac{n}{P^2}\right] + K\left(\left[\frac{n}{P^2}\right]!\right)$$

Continuing this process we can prove that

$$K(n!) = \left[\frac{n}{P}\right] + \left[\frac{n}{P^2}\right] + \left[\frac{n}{P^3}\right] + \ldots$$

This process must end after a finite number of steps.

Q. Find the highest power of 3 which is contained in 100!

Sol^n $\sum_{k=1}^{\infty}\left[\frac{n}{p^k}\right] = \left[\frac{100}{3^1}\right]+\left[\frac{100}{3^2}\right]+\left[\frac{100}{3^3}\right]+\left[\frac{100}{3^4}\right]+\left[\frac{100}{3^5}\right]$

$= [33.33]+[11.11]+[3.7]+[1.2]+[0.4]$

$= 33+11+3+1+0$

$= \underline{\underline{48}}$

Q. Find the highest power of 5 dividing 1000!

(or) find the highest power of 5 which is contained 1000!

Sol^n $\sum_{k=1}^{\infty}\left[\frac{n}{p^k}\right] = \left[\frac{1000}{5}\right]+\left[\frac{1000}{5^2}\right]+\left[\frac{1000}{5^3}\right]+\left[\frac{1000}{5^4}\right]+\left[\cancel{\frac{1000}{5^5}}\right]$

$= 200+40+8+1 = 249$

$\therefore 5^{249}$ divides 1000!

Q. Find the highest power of 7 dividing 2000!

Sol^n $\sum_{k=1}^{\infty}\left[\frac{n}{p^k}\right] = \left[\frac{2000}{7}\right]+\left[\frac{2000}{7^2}\right]+\left[\frac{2000}{7^3}\right]+\left[\frac{2000}{7^4}\right]$

$= 285+40+5+0$

$= 330$

7^{330} divides 2000!

Try yourself

1. Find the highest power of 7 which is contained in 50! Ans:- 8.
2. Find the highest power of 3 dividing 500!
   Ans: 247

Scanned by CamScanner

Euler's phi function or Indicator (or) Totient function

Let m be any positive integer. The set of all positive integers less than m and relatively prime to m is denoted by $\phi(m)$ i.e, it is called as Euler's function or Euler's phi function.

Example: 1. Consider $m = 12$. The positive integers less than 12 and relatively prime to 12 are 1, 5, 7, and 11

$\therefore \phi(12) = 4$.

2. If $m = 7$ (a prime number) then the positive integer less than 7 and relatively prime to 7 are 1, 2, 3, 4, 5, 6, therefore $\phi(7) = 6$.

3. In General if p is prime number then $\phi(p) = p-1$, since if p is prime number then $1, 2, 3 \ldots (p-1)$ are less than p and co-prime to p and are $p-1$ in total

Theorem: If n is any integer, then $\phi(n) = n-1$ iff n is prime number.

Proof: Let n is a prime, $\phi(n)$ is the no of integer $< n$ and $(m, n) = 1$, where $m < n$. Since 'n' is a prime, then $\phi(n) = n-1$

Conversely, Let $\phi(n) = n-1$, then n is a prime number. Contrary, 'n' is a composite number. Since 'n' is a composite no. then $\exists$ a divisor 'd' $\ni$: $1 < d < n$, then $\phi(n) \leq (n-2)$

but $\phi(n) = n-1$, $\therefore$ n is a prime

Hence the proof.

Theorem: If p is a prime and $k>0$, then
$\phi(p^k) = p^k - p^{k-1} = p^k(1 - 1/p)$

Proof: The number of integers from 1 to p^k which are not co-prime to p^k are $p, 2p, 3p \dots (p^{k-1})p$

$\therefore$ Total number of such integers which are not co-prime to p^k are p^{k-1}.

$\therefore$ $\phi(p^k)$ = number of integers co-primes to p^k.

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

Note:

If a and b are co-prime to each other then $\phi(ab) = \phi(a).\phi(b)$ ($\because \phi$ is MF)

Eg: $\phi(12) = \phi(4 \times 3) = \phi(4).\phi(3)$
$\phi(12) \neq \phi(6) \times \phi(2)$
Because 6 and 2 are not co-primes.

Lemma: Given integers a, b, c $\gcd(a, b, c) = 1$ iff $\gcd(a, b) = 1$ and $\gcd(a, c) = 1$

Theorem: If the integer $n \geq 1$ has the prime factorization $n = p_1^{k_1} p_2^{k_2} p_3^{k_3} \dots p_r^{k_r}$ then

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

(or)

$\phi(n) = n(1 - 1/p_1)(1 - 1/p_2) \dots (1 - 1/p_r)$

Scanned by CamScanner

Proof: Let $n = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}$

Let $\phi(n) = \phi(p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r})$

$= \phi(p_1^{k_1}) \phi(p_2^{k_2}) \ldots \phi(p_r^{k_r})$

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

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

$= \left(p_1^{k_1} \cdot p_2^{k_2} \ldots p_r^{k_r}\right)\left[\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right) \ldots \left(1-\frac{1}{p_r}\right)\right]$

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

(1) Calculate $\phi(360)$, $\phi(5040)$ and $\phi(72000)$

Soln: $360 = 2^3 3^2 5^1 = p_1^{k_1} p_2^{k_2} \cdot p_3^{k_3}$

$\phi(n) = \phi(360) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\left(1-\frac{1}{p_3}\right)$

$= 360\left(\frac{1}{2}\right)\left(\frac{2}{3}\right)\left(\frac{4}{5}\right)$

$\phi(360) = 96$

Similarly $\phi(5040)$ & $\phi(72000)$ Try yourself.

(2) Verify that the equality of $\phi(n) = \phi(n+1) = \phi(n+2)$ holds where $n = 5186$

Soln: $n = 5186 = 2^1 \cdot 2593^1$

$\therefore \phi(5186) = 5186\left(1-\frac{1}{2}\right)\left(1-\frac{1}{2593}\right) = 5186\left(\frac{1}{2}\right)\left(\frac{2592}{2593}\right)$

$= 2592 \to (1)$

$n+1 = 5186+1 = 5187 = 3^1 \cdot 7^1 \cdot 13^1 \cdot 19^1$

$\phi(5187) = 5187\left(\frac{2}{3}\right)\left(\frac{6}{7}\right)\left(\frac{12}{13}\right)\left(\frac{18}{19}\right) = 2592 \to (2)$

$n+2 = 5186+2 = 5188 = 2^2 \cdot 1297$

$\therefore \phi(5188) = 5188\left(\frac{1}{2}\right)\left(\frac{1296}{1297}\right) = 2592 \to (3)$

from (1), (2) & (3)

$\therefore \phi(n) = \phi(n+1) = \phi(n+2)$ for $n = 5186$.

(3) Establish the assertions below
If n is an even integer then
$\phi(2n) = 2\phi(n)$

Proof: n is ... n is even

$$n = 2^{k_1} \cdot p_2^{k_2} \cdots p_r^{k_r}$$

$$2n = 2^{k_1+1} \cdot p_2^{k_2} \cdots p_r^{k_r+1}$$

$$\therefore \phi(2n) = 2n\left(1-\frac{1}{2}\right)\left(1-\frac{1}{p_2}\right)\left(1-\frac{1}{p_3}\right)\cdots\left(1-\frac{1}{p_r}\right)$$

$$\phi(2n) = n\left(1-\frac{1}{p_2}\right)\left(1-\frac{1}{p_3}\right)\cdots\left(1-\frac{1}{p_r}\right) \longrightarrow (1)$$

And

$$2\phi(n) = 2.n\left(1-\frac{1}{2}\right)\left(1-\frac{1}{p_2}\right)\left(1-\frac{1}{p_3}\right)\cdots\left(1-\frac{1}{p_r}\right)$$

$$2\phi(n) = n\left(1-\frac{1}{p_2}\right)\left(1-\frac{1}{p_3}\right)\cdots\left(1-\frac{1}{p_r}\right) \longrightarrow (2)$$

from (1) & (2) we get

$$\phi(2n) = 2\phi(n)$$

(4) If every prime that divides n also divides m, establish that $\phi(nm) = n.\phi(m)$

Proof

Let $p_1, p_2, \ldots, p_r$ be all the primes of n that divide m.

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

$m = (p_1^{j_1} \cdot p_2^{j_2} \cdots p_r^{j_r}) \cdot (q_1^{m_1} q_2^{m_2} \cdots q_s^{m_s})$

So that $q_i \neq p_j$

$$\therefore nm = (p_1^{k_1+j_1} \cdot p_2^{k_2+j_2} \cdots p_r^{k_r+j_r}) \cdot (q_1^{m_1} q_2^{m_2} \cdots q_s^{m_s})$$

$$\phi(nm) = (p_1^{k_1+j_1} \cdot p_2^{k_2+j_2} \cdots p_r^{k_r+j_r} \cdot q_1^{m_1} \cdots q_s^{m_s}) \cdot \left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_r}\right)\left(1-\frac{1}{q_1}\right)\cdots\left(1-\frac{1}{q_s}\right)$$

$$= p_1^{j_1} p_2^{j_2} \cdots p_r^{j_r}\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_r}\right)$$

$$\left(1-\frac{1}{q_1}\right)\cdots\left(1-\frac{1}{q_r}\right) p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}.$$

$$= \phi(m)\, p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$$

$$\phi(nm) = \phi(m).n$$

$$\therefore \quad \underline{\phi(nm) = n\,\phi(m)}$$

<u>Definition</u>

Let m be a positive integer.
A set of r integers $c_1, c_2, c_3 \ldots c_r$ is called a reduced set of residues modulo m if.

(i) No two c_i's are congruent modulo m

(ii) Each c_i is relatively prime to m

(iii) $r = \phi(m)$

Thus,

If $m=12$, then $1, 5, 7, 11$ forms (are relatively prime to m) form a reduced set of residues (mod 12).

Then we have $\phi(12) = \underline{4}$

Eulers theorem

If $n \geq 1$ and $\gcd(a,n) = 1$ then $a^{\phi(n)} \equiv 1 \pmod{n}$

Proof:

Let $\{r_1, r_2, r_3 \ldots r_{\phi(n)}\}$ be a reduced set of residues modulo n.

Since $(a,n) = 1$

$\therefore \{ar_1, ar_2, ar_3 \ldots ar_{\phi(n)}\}$ is also a reduced set of residues modulo n and consequently each ar_i is congruent modulo n to one and only r_j

Let

$$ar_1 \equiv x_1 \pmod{n}$$
$$ar_2 \equiv x_2 \pmod{n}$$
$$\vdots$$
$$ar_{\phi(n)} \equiv x_{\phi(n)} \pmod{n}.$$

then $x_1, x_2, x_3 \ldots x_{\phi(n)}$ are precisely $\{r_1, r_2 \ldots r_{\phi(n)}\}$ place in some order so that the product $x_1 x_2 \ldots x_{\phi(n)} = r_1 . r_2 . r_3 \ldots r_{\phi(n)} \longrightarrow ①$

then we have ($\because$ by multiplying above congruents)

$$ar_1 . ar_2 . ar_3 \ldots ar_{\phi(n)} \equiv x_1 . x_2 . x_3 \ldots x_{\phi(n)} \pmod{n}$$

$$r_1 . r_2 . r_3 \ldots r_{\phi(n)} a^{\phi(n)} \equiv r_1 . r_2 \ldots r_{\phi(n)} \pmod{n} \quad ②$$

($\because$ from 1)

from ① & ② by cancelling the term on both side we get

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

[Since each r_i where $i = 1, 2 \ldots \phi(m)$) is relatively prime to m, therefore their product $r_1 r_2 r_3 \ldots r_{\phi(m)}$ is also relatively prime to m. So cancelling $r_1 r_2 \ldots r_{\phi(m)}$ from both side of eqn we get
$a^{\phi(m)} \equiv 1 \pmod{n}$]

<u>Corollary</u>. Fermat's theorem as a corollary of Euler's theorem. If in Euler's theorem we take $m = p$, where p is prime, then $\phi(m) = \phi(p) = p-1$

$\therefore$ The result $a^{\phi(p)} \equiv 1 \pmod{p}$ takes the form $a^{p-1} \equiv 1 \pmod{p}$ which is Fermat's theorem

(Q) Find the unit digit of 3^{100} by means of Euler's theorem

<u>Soln</u> The gcd $(10, 3) = 1$
by Euler's theorem
$$3^{\phi(10)} \equiv 1 \pmod{10}$$
$\phi(10) = 4$
$$3^4 \equiv 1 \pmod{10}$$
$$(3^4)^{25} \equiv 1 \pmod{10}$$
$$3^{100} \equiv 1 \pmod{10}$$

$\therefore$ The unit digit of 3^{100} is <u>1</u>

(1) use Euler's theorem to establish the for any integer a, $a^{37} \equiv a \pmod{1729}$

Proof. $1729 = 7^1 . 13^1 . 19^1$

$\phi(7) = 7-1 = 6 \quad \phi(13) = 12 \quad \phi(19) = 18$

$\therefore a^6 \equiv 1 \pmod 7 \Rightarrow a^{36} \equiv 1 \pmod 7$

$a^{12} \equiv 1 \pmod{13} \Rightarrow a^{36} \equiv 1 \pmod{13}$

$a^{18} \equiv 1 \pmod{19} \Rightarrow a^{36} \equiv 1 \pmod{19}$

$\therefore a^{36} \equiv 1 \pmod{7.13.19}$

$\Rightarrow a^{37} \equiv a \pmod{7.13.19}$ ($\because$ by multiplying 'a' on BS)

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

2. use Euler theorem to establish for any integer a,

(i) $a^{33} \equiv a \pmod{4080}$ ($\because 4080 = 15^1 . 16^1 . 17^1$

(ii) $a^{13} \equiv a \pmod{2730}$ ($\because 2730 = 2.3.5.7.13$

Some properties of the phi 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.

Problem

① Illustrate the value of $\sum_{d|n} \phi(d)$ for $n = 10$

Soln

For $n = 10$, there are 1, 2, 5 and 10 positive divisors of 10.

$$\therefore \sum_{d|n} \phi(d) = \sum_{d|10} \phi(d) = \phi(1) + \phi(2) + \phi(5) + \phi(10)$$
$$= 1 + 1 + 4 + 4$$
$$= 10.$$

$$\sum_{d|n} \phi(d) = 10 = n.$$

② Find the number of positive integer ≤ 3600 that are coprime to 3600.

Soln

$$n = 36000 = 2^4 . 3^2 . 5^2$$
$$\phi(n) = \phi(3600) = \phi(2^4 . 3^2 . 5^2)$$

We have $\phi(n) = n\left(1 - \frac{1}{P_1}\right)\left(1 - \frac{1}{P_2}\right)\left(1 - \frac{1}{P_3}\right)$

$$\phi(3600) = 3600\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right)$$
$$= 3600\left(\frac{1}{2}\right)\left(\frac{2}{3}\right)\left(\frac{4}{5}\right)$$
$$= 960$$

Q. Prove that $\phi(m^2) = m\phi(m)$ for every positive m.

Proof:
m is a positive integer, therefore

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

where $p_1, p_2, p_3, \ldots p_r$ are distinct primes

$\therefore m^2 = p_1^{2k_1} \cdot p_2^{2k_2} \cdots p_r^{2k_r}$

Hence

$$\phi(m^2) = m^2\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_r}\right)$$

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

$\phi(m^2) = m\,\phi(m)$

Q. For $n>1$, the sum of the positive integers less than n and relatively prime to n is $\frac{1}{2} n\phi(n)$.

Let $a_1, a_2, a_3, \ldots a_{\phi(n)}$ be the positive integers less than n and relatively prime to n.

Now because

$\gcd(a, n) = 1$ iff $\gcd(n-a, n) = 1$

~~the numbers gcd (a,n)=1~~

The numbers $n-a_1, n-a_2 \ldots n-a_{\phi(n)}$ are equal in some order to $a_1, a_2, \ldots a_{\phi(n)}$.

then,

~~$a_1 + a_2 + \ldots a_{\phi(n)}$~~

$a_1 + a_2 + \cdots a_{\phi(n)} = (n-a_1) + (n-a_2) + \cdots$

$\cdots + (n - a_{\phi(n)})$

$a_1 + a_2 + \cdots + a_{\phi(n)} = (n-a_1) + (n-a_2) + \cdots (n - a_{\phi(n)})$

$= \phi(n).n - (a_1 + a_2 \cdots a_{\phi(n)})$

Hence $2(a_1 + a_2 \cdots a_{\phi(n)}) = n.\phi(n)$

$= \frac{1}{2} n \phi(n)$

(or).

Q. If $n > 1$, Prove that the Sum of $\phi(n)$ $\phi(n)$ Positive integers which are less than n and Relatively Prime to n is $\frac{n\phi(n)}{2}$

Sol^n

Let $a_1, a_2, a_3 \ldots a_{\phi(n)}$ be the Positive integers less than and Relatively prime to n we know that if a is an integer less than n and prime to n. then $(n-a)$ is also an integer $< n$ and prime to n.

therefore $\phi(n)$ integers less than n & prime to n are of type $a_1, a_2, a_3 \ldots$

$a_1, a_2\, a_3 \ldots \ldots (n-a_3)\, (n-a_2), (n-a_1)$

Let the sum of these $\phi(n)$ integers be denoted by S.

then $S = a_1 + a_2 + a_3 + \cdots + (n-a_3) + (n-a_2) + (n-a_1)$ $\longrightarrow (1)$

Writing the terms in reverse order

$S = (n-a_1) + (n-a_2) + (n-a_3) \cdots + a_3 + a_2 + 1$ $\longrightarrow (2)$

Adding (1) & (2) we have

$2S = n + n + n + \cdots + \phi(n)$

$\Rightarrow 2S = n\phi(n)$

$S = \frac{1}{2} n \phi(n)$

** All the Best **