CLASS: Msc MATHEMATICS IV SEM

SUBJECT CODE: H-4049

SUBJECT NAME: NUMBER THEORY

TAUGHT BY:DR SATISH KUMAR

ASSOCIATE PROFESSOR

DEPARTMENT OF MATHEMATICS

DN PG COLLEGE MEERUT

Euler's function

let $n \in N$ then

$\phi(n)$ = total no of positive integers less than n and relative prime to n

Ex $\phi(1) = 1$ $\qquad$ $\phi(4) = 2$ $[(1,4)=1, (2,4)=2, (3,4)=1]$

$\phi(2) = 1$ $\qquad$ $\phi(5) = 4$

$\phi(3) = 2$ $\qquad$ $\phi(p) = p-1$, p is prime

General formula $\quad n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$

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

Note: $\phi(p^k) = p^k - p^{k-1}$, p is prime

Theorem 5. if $(m,n) = 1$ then prove $\phi(mn) = \phi(m)\phi(n)$.

Proof. ~~Since~~ let $(m,n) = 1$

~~Since~~ $\phi(1) = 1 \Rightarrow$ result is obvious

Let $m > 1, n > 1$

We arrange The integers $1, 2, 3, \ldots, mn$ in m column and n rows as follows:

$$\begin{array}{cccccccc}
0+1 & 2 & 3 & \cdots & r & (r+1) & \cdots & m \\
(m+1) & (m+2) & (m+3) & & m+r & (m+r+1) & \cdots & n+m \\
(2m+1) & (2m+2) & (2m+3) & & (2m+r) & (2m+r+1) & \cdots & 3m \\
 & & & & & & & \vdots \\
(n-1)m+1 & (n-1)m+2 & & - & (n-1)m+r & \cdots & & mn
\end{array}$$

Entries in r^{th} column is
$r, m+r, m+m+r, \cdots (n-1)m+r$ ——— (1)

This entry form an A.P. of n-terms with common difference m prime to n. Each column in the above array contains exactly $\phi(n)$ integers prime to n. Also it is obvious that each term of (i) is prime to m iff r is prime to m. But r is prime to m for $\phi(m)$ values of r. Thus, there are exactly $\phi(m)$ columns in which every integer is relatively prime to m. Therefore there are in all $\phi(m)\phi(n)$ integers less than mn and prime to both m and n.

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

<u>Th. 06</u> If p is a prime, $k>0$ then

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

Proof. We know if p is prime then

For $k=1$ $\phi(p) = p-1$ $[\because (1,p)=1, (2,p)=1, \cdots (p-1,p)=1]$

If $k>1$ then $p, p^2, p^3, \cdots, p^{k-1}, p^k$ are divisible by p among the integers $1, 2, \cdots, p^k$.

Thus the set $\{1, 2, \cdots p^k\}$ contains exactly $p^k - p^{k-1}$ integers which are relatively prime to p^k.

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

Ex (2) ~~let~~ To find $\phi(2^6)$

Here $(2, 2^6) \neq 1$, $(2^2, 2^6) \neq 1$, $(2^3, 2^6) \neq 1$
$(2^4, 2^6) \neq 1$, $(2^5, 2^6) \neq 1$

$$\Rightarrow \phi(2^6) = 2^6 - 2^5 = 2^5[2-1] = 32$$

(3) $\phi(p^{k+1}) = p^{k+1} - p^k = p \cdot p^k - p^k$
$= p[p^k - p^{k-1}] = p\,\phi(p^k)$

Th 67 if $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$

then
$$\phi(n) = \phi(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k})$$
$$= \phi(p_1^{\alpha_1})\,\phi(p_2^{\alpha_2}) \cdots \phi(p_k^{\alpha_k})$$
$$= (p_1^{\alpha_1} - p_1^{\alpha_1 - 1})(p_2^{\alpha_2} - p_2^{\alpha_2 - 1}) \cdots (p_k^{\alpha_k} - p_k^{\alpha_k - 1})$$
$$= p_1^{\alpha_1}\left(1 - \frac{1}{p_1}\right) p_2^{\alpha_2}\left(1 - \frac{1}{p_2}\right) \cdots p_k^{\alpha_k}\left(1 - \frac{1}{p_k}\right)$$
$$= \{p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}\}\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right)$$
$$\phi(n) = n \cdot \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right)$$
, proved.

Ex (3) Find $\phi(900)$

Soln $900 = 2^2 \times 3^2 \times 5^2$

$$\phi(900) = 900\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right)$$
$$= 900 \times \frac{1}{2} \times \frac{2}{3} \times \frac{4}{5} = 300 \times \frac{4}{5} = 240$$

Ex 04 $\phi(5040)$

Ans $5040 = 2^4 \times 3^2 \times 5 \times 7$

$$\phi(5040) = 5040\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right)\left(1 - \frac{1}{7}\right) = 1152$$

Example. 05. Show $\phi(n) = \phi(n+1) = \phi(n+2)$ for $n = 5186$

Solution. Let $n = 5186$

$\phi(n) = \phi(2 \times 2593)$, $n = 5186$

$= \phi(2)\, \phi(2593)$

$= (2-1)\,[2593^1 - 2593^0]$ $[\because \phi(p) = p-1$, p is prime$]$

$\phi(5186) = 2592$ — (1)

$\phi(n+1) = \phi(2593)$

$= \phi[3 \times 7 \times 13 \times 19]$

$= \phi(3)\,\phi(7)\,\phi(13)\,\phi(19)$

$= 2 \times 6 \times 12 \times 18$

$= 144 \times 18$

$\phi(n+1) = 2592$ — (2)

$\phi(n+2) = \phi(5186+2) = \phi(5188)$

$= \phi(2^2 \times 1297)$

$= (2^2 - 2^1)\, \phi(1297)$

$= 2 \times 1296$

$\phi(n+2) = 2592$ — (3)

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

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

Example.6. Prove $\phi(n) = \phi(n+2)$ is satisfied by $n = 2(2p-1)$ whenever p and $(2p-1)$ are both odd prime.

Sol. Given

$$n = 2(2p-1) \quad \text{—— (1)}$$

where p and $(2p-1)$ are both odd prime

To prove $\phi(n) = \phi(n+2)$.

$$\begin{aligned} LHS &= \phi(n) \\ &= \phi[2(2p-1)] \\ &= \phi(2)\cdot\phi(2p-1) = 1\cdot\phi(2p-1) \\ &= \phi(2p-1) = 2p-1-1 = 2(p-1) \end{aligned}$$

$$\Rightarrow \phi(n) = 2(p-1) \quad \text{—— (2)}$$

Again, $\phi(n+2) = \phi[2(2p-1)+2]$

$$\begin{aligned} &= \phi[4p\cancel{-2}\cancel{+2}] \\ &= \phi(4)\cdot\phi(p) \\ &= (2^2-2)(p-1) \end{aligned}$$

$$\phi(n+2) = 2(p-1) \quad \text{—— (3)}$$

from (2) and (3), we get

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

Ex.07 If p and $(p+2)$ are both primes
Show $\phi(p+2) = \phi(p)+2$

Solⁿ Given p and $(p+2)$ are both primes

To prove $\phi(p+2) = \phi(p)+2$

$LHS = \phi(p+2) = p+2-1 = p+1$ —— (1)

$RHS = \phi(p)+2 = p-1+2 = p+1$ —— (2)

(1) & (2) $\Rightarrow \phi(p+2) = \phi(p)+2$. proved.

CH-06
Pdf-02

06

Number Theory
Dr Satish Kr Gupta

Ex. 08. If p and $(2p+1)$ are both primes and $n = 4p$ then show $\phi(n+2) = \phi(n)+2$

Sol. Given p and $(2p+1)$ are both primes

$n = 4p$

To prove $\phi(n+2) = \phi(n)+2$

$LHS = \phi(n+2)$

$= \phi(4p+2)$

$= \phi(2)\,\phi(2p+1)$ $\quad [\phi(2p+1) = 2p\cancel{+1}\cancel{-1}]$

$= 1 \cdot 2p$

$\phi(n+2) = LHS = 2p$ ——— (1)

$RHS = \phi(n)+2$

$= \phi(4p)+2$

$= \phi(4)\,\phi(p) + 2$

$= (2^2-2)(p-1) + 2$

$= 2(p-1)+2$

$\phi(n)+2 = 2p$ ——— (2)

from (1) & (2)

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

Eg To show $\phi(2n) = \phi(n)$

Soln $LHS = \phi(2n) = \phi(2)\,\phi(n)$

$= \phi(n)$ $\quad [\because \phi(2) = 2-1]$

$= RHS.$ proved.

Scanned with CamScanner

CH-06 (07) Number Theory
Pdf-02 Dr Satish Kr Gupta.

Ex.10. If n is a composite number then

$$\phi(n) \le n - \sqrt{n}$$

Sol: Let $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots\dots p_k^{\alpha_k}$, p_1 is smallest prime

then

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

$$\le n\left(1-\frac{1}{p_1}\right)$$

$$\le n\left(1-\frac{1}{\sqrt{n}}\right) \quad [\because p_1 \le \sqrt{n}]$$

$$\le \left(n - \frac{n}{\sqrt{n}}\right)$$

$$\phi(n) \le n - \sqrt{n}$$, proved.

State and prove Euler's theorem

Euler's Theorem

Statement. Let $(a, n) = 1$, $a, n \in N$ then

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

Proof. Let $(a, n) = 1$, $a, n \in N$

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

If $n = 1$, $\phi(1) = 1$ $\Rightarrow$ $a \equiv 1 \pmod{1}$

$\Rightarrow$ Theorem is obvious

If $n > 1$

Let $a_1, a_2, a_3, \dots, a_{\phi(n)}$ be the positive integers less than n relative prime to n. i.e $(a_i, n) = 1$, $\forall i$.

Let $(a, n) = 1$ then [i.e $a_i \not\equiv a_j \pmod{n}$]

$aa_1, aa_2, aa_3, \dots, aa_{\phi(n)}$ be different congruent (mod n)

Suppose if possible

$$aa_i \equiv aa_j \pmod{n}$$

$$\Rightarrow a_i \equiv a_j \pmod{n} \quad [\because (a, n) = 1]$$

which is a contradiction

$\therefore$ $aa_i \not\equiv aa_j \pmod n$

Now we have

$$aa_1 \equiv a_1' \pmod n$$
$$aa_2 \equiv a_2' \pmod n$$
$$aa_3 \equiv a_3' \pmod n$$
$$\vdots$$
$$aa_{\phi(n)} \equiv a_{\phi(n)}' \pmod n$$

where $aa_1, aa_2, \dots aa_{\phi(n)}$ are in some order of $a_1', a_2', \dots a_{\phi(n)}'$

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

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

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

$$\left[\begin{array}{l} \because a_1 . a_2 \cdots a_{\phi(n)} \equiv a_1' a_2' \cdots a_{\phi(n)}' \\ (a_i, n) = 1 \end{array} \right]$$

, proved.

Theorem 2. The sum of positive integers less than n and relatively prime to n is equal to $\frac{n}{2} \cdot \phi(n)$

i.e $\sum_{(r,n)=1} r = \frac{1}{2} n \phi(n)$

Proof. Let $r_1, r_2, r_3, \dots r_{\phi(n)}$ be the positive integers less than n and relatively prime to n

Now $(r, n) = 1 \Leftrightarrow (n-r, n) = 1$

$$\Rightarrow r_1 + r_2 + \dots + r_{\phi(n)} = n - r_1 + n - r_2 + \dots n - r_{\phi(n)}$$

$$r_1 + r_2 + \dots + r_{\phi(n)} = n\,\phi(n) - (r_1 + r_2 + \dots + r_{\phi(n)})$$

$$\Rightarrow 2[r_1 + r_2 + \dots + r_{\phi(n)}] = n\phi(n)$$

$$\Rightarrow r_1 + r_2 + \dots + r_{\phi(n)} = \frac{1}{2} n \phi(n).$$ proved.