ROHINI COLLEGE OF ENGINEERING & TECHNOLOGY
Near Anjugramam Junction, Kanyakumari Main Road, Palkulam, Variyoor P.O - 629401
Kanyakumari Dist, Tamilnadu., E-mail : admin@rcet.org.in, Website : www.rcet.org.in

DEPARTMENT OF MATHEMATICS

NAME OF THE SUBJECT: ALGEBRA AND NUMBER THEORY

SUBJECT CODE : MA8551

REGULATION : 2017

UNIT – V : CLASSICAL THEOREMS AND MULTIPLICATIVE FUNCTIONS

MA8551 – Algebra and Number Theory

UNIT – V CLASSICAL THEOREMS AND MULTIPLICATIVE FUNCTIONS

Wilson Theorem:

1. State and prove Wilson's Theorem

Statement:

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

Proof :

We have to prove $(p-1)! \equiv -1 \pmod{p}$

When $p = 2$, $(p-1)! = (2-1)! = 1 \equiv -1 \pmod{2}$.

So, the theorem is true when $p = 2$.

Now let $p > 2$ and let a be a positive integer such that $1 \le a \le p-1$.

Since p is a prime and $a < p$, $(a, p) = 1$.

Then the congruence $ax \equiv 1 \pmod{p}$ has a solution a' congruence modulo p.

$\therefore$ $aa' \equiv 1 \pmod{p}$, where $1 \le a' < p-1$

$\therefore$ a, a' are inverses of each other modulo p.

If $a' = a$, then $a \cdot a \equiv 1 \pmod{p}$

$\Rightarrow a^2 - 1 \equiv 0 \pmod{p}$

$\therefore$ $p \mid a^2 - 1 \Rightarrow p \mid (a-1)(a+1)$

$\Rightarrow p \mid a-1$ or $p \mid a+1$

Since $a < p$, if $p \mid a+1$ then $a = p-1$.

If $p \mid a-1$, then $a - 1 = 0 \Rightarrow a = 1$

$\Rightarrow a = 1$ or $p-1$ if $a = a'$

i.e., 1 and $p-1$ are their own inverses.

If $a' \neq a$, excluding 1 and $p-1$, the remaining $p-3$ residues 2, 3, 4, ..., $(p-3)$, $(p-2)$ can be grouped into $\frac{p-3}{2}$ pairs of the type a, a' such that $aa' \equiv 1 \pmod{p}$

Multiplying all these pairs together we get, $2 \cdot 3 \cdot 4 \ldots (p-3)(p-2) \equiv 1 \pmod{p}$

$\Rightarrow 1.2 \cdot 3 \cdot 4 \ldots (p-2)(p-1) \equiv p-1 \pmod{p}$

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

Hence the theorem.

This can be rewritten as $(p-1)! + 1 \equiv 0 \pmod{p}$

$\Rightarrow p \mid (p-1)! + 1$,

which is the result suggested by Wilson.

2. Let p be a prime and n any positive integer. Prove that $\frac{(np)!}{n!p^n} \equiv (-1)^n \pmod{p}$

Proof:

First, we can make an observation. Let a be any positive integer congruent to 1 modulo p. Then by Wilson's theorem , $a(a+1)\ldots(a+(p-2)) \equiv (p-1)! \equiv -1 \pmod{p}$

In other words, the product of the p-1 integers between any two consecutive multiples of p is congruent to -1 mod p.

Then $\frac{(np)!}{n!p^n} = \frac{(np)!}{p.2p.3p\ldots(np)}$

$$= \prod_{r=1}^{n} \left[(r-1)p+1\right]...\left[(r-1)p+(p-1)\right]$$

$$\equiv \prod_{r=1}^{n} (p-1)!(\text{mod } p)$$

$$\equiv \prod_{r=1}^{n} (-1)(\text{mod } p) \equiv (-1)^n (\text{mod } p)$$

Fermat's Little Theorem:

1. State and prove Fermat's little theorem.

If p is a prime and *a* is any integer not divisible by p, then $a^{p-1} \equiv 1(\text{mod } p)$

Proof:

Given p is a prime and *a* is any integer not divisible by p

When an integer is divided by p, the set of possible remainders are 0, 1, 2, 3, ...,$p-1$

Consider the set of integers $1\cdot a, 2\cdot a, 3\cdot a, ...(p-1)\cdot a$ ---------- (1)

Suppose $ia \equiv 0(\text{mod } p)$, then $p \mid ia$.

But $p \nmid a \therefore p \mid i$, which is impossible, since $i < p$.

$$ia \not\equiv 0(\text{mod } p) \text{ for } i = 1, 2, ..., p-1.$$

So, no term of (1) is zero.

Next we prove they are all distinct

Suppose $ia \equiv ja(\text{mod } p)$, where $1 \le i,j \le p-1$.

Then $(i-j)a \equiv 0(\text{mod } p) \Rightarrow p \mid (i-j)a$

Since $p \nmid a$, $p \mid i-j$ and $i, j < p \Rightarrow \mid i-j \mid < p$.

$$\therefore i - j = 0 \Rightarrow i \equiv j(\text{mod } p)$$

$$\therefore \quad i \neq j \Rightarrow ia \neq ja.$$

This means, no two of the integers in (1) are congruent modulo p.

$\therefore$ The least residues (or remainders) of the integers $a, 2a, 3a, ...,(p-l)a$ modulo p are the same as the integers $1, 2, 3, ..., p-1$ in some order.

So, their products are congruent modulo p.

$$a \cdot 2a \cdot 3a \cdots (p-l)a \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) (\text{mod } p)$$

$\Rightarrow$ $l \cdot 2 \cdot 3 \cdots (p-l) \cdot a^{P-1} \equiv (p-l)!(\text{mod } p)$

$\Rightarrow$ $(p-l)! a^{P-1} \equiv (p-l)!(\text{mod } p)$

$\Rightarrow$ $a^{P-1} \equiv l(\text{mod } p)$ (since $p \nmid (p-l)$)

The result $a^{p-1} \equiv l(\text{mod } p)$ is equivalent to $a^p \equiv a (\text{mod } p)$.

2. Find the remainder when 24^{1947} is divided by 17

Solution.

We have to find the remainder when 241947 is divided by 17.

Here a = 24, p = 17

We know 17 is a prime & 17|24

$\therefore$ By Fermats theorem, $24^{17-1} \equiv 1(\text{mod } 17)$

$\Rightarrow$ $2416 \equiv 1(\text{mod } 17)$

$\therefore$ $(2416)^{121} \equiv 1^{121}(\text{mod } 17)$

$\Rightarrow$ $241936 \equiv 1(\text{mod } 17)$

Now **241947 = 241936+11= 241936 .2411**

$242 = 576 \equiv -2 \pmod{17}$

$\therefore \quad (242)^2 \equiv (-2)^2 \pmod{17}$

$\Rightarrow \quad 244 \equiv 4 \pmod{17}$

$(244)^2 \equiv 4^2 \pmod{17}$

$\Rightarrow \quad 248 \equiv 16 \pmod{17}$

$\equiv -1 \pmod{17}$

$2411 = 248.242.24 \equiv (-1)(-2).7 \pmod{17}$

$\equiv 14 \pmod{17}$

$\therefore \quad 241947 \equiv 14 \pmod{17}$

$\equiv 14 \pmod{17}$

∴ The remainder is 14 when 241947 is divided by 17.

Euler's Theorem:

1. State and prove Euler's theorem.

Let m be a positive integer and a be any integer such that (a, m) = 1.

Then $a^{\Phi(m)} \equiv 1 \pmod{m}$.

Proof :

Given m is a positive integer and a is any integer such that (a, m) = 1.

Let $r_1, r_2, \ldots, r_{\Phi(m)}$ be all the positive integers < m and relatively prime to m.

Since $r_i - r_j < m$, clearly $r_i \neq r_j \pmod{m}$ if $i \neq j$

Consider the products $ar_1, ar_2, \ldots, ar_{\Phi(m)}$

Since (a, m) = 1, $ar_i \neq ar_j \pmod{m}$ if $i \neq j$

we find $ar_1, ar_2, \ldots, ar_{\Phi(m)}$ mod m are distinct.

We now prove $(ar_i, m) = 1$

For, suppose $(ar_i, m) > 1$, then let p be a prime factor of $(ar_i, m) = d$.

∴ $p \mid a$ and $p \mid m$

⇒ $p \mid a$ or $p \mid r_i$ and $p \mid m$.

If $p \mid r_i$ and $p \mid m$ then, $(r_i, m) \neq 1$, a contradiction.

If $p \mid a$ and $p \mid m$, then $p \mid (a, m) \Rightarrow (a, m) \neq 1$, which is again a contradiction.

∴ $(ar_i, m) = 1, i = 1, 2, 3, \ldots, \Phi(m)$

∴ the $\Phi(m)$ least residues $ar_1, ar_2, \ldots, ar_{\Phi(m)}$ modulo m are distinct and relatively prime to m.

So, they are the same as integers $r_1, r_2, \ldots, r_{\Phi(m)}$, in some order modulo m.

∴ their product $ar_1 \cdot ar_2 \cdot \ldots \cdot ar_{\Phi(m)} \equiv r_1 \cdot r_2 \cdot \ldots \cdot r_{\Phi(m)} \pmod{m}$

⇒ $a^{\Phi(m)} r_1 . r_2, , r_{\Phi(m)} \equiv r_1 r_2 .. r_{\Phi(m)} \pmod{m}$

Since each r_i is relatively prime to m, $(r_1 r_2 .. r_{\Phi(m)}, m) = 1$

We get $a^{\Phi(m)} \equiv 1 \pmod{m}$

2. Using Euler's theorem, find the remainder when 245^{1040} is divided by 18.

Solution.

We have to find the remainder when 2451040 is divided by 18.

Here $a = 245 = 5 \cdot 72$ and $m = 18 = 32 \cdot 2$, (a, m) = 1

Hence by Euler's theorem,

$a^{\varphi(m)} \equiv 1 \pmod{m} \Rightarrow 245^{\varphi(m)} \equiv 1 \pmod{m}$

$$\varphi(18) = \varphi(3^2 . 2) = \varphi(3^2).\varphi(2) = 3^2\left(1 - \frac{1}{3}\right).1 = 6$$

But

$\therefore \; 245^6 \equiv 1 \pmod{18}$

$\therefore (245^6)^{173} \equiv 1^{173} (\text{mod} 18)$

$245^{1038} \equiv 1 (\text{mod} 18)$

$245^{1040} = 245^{1038+2} = 245^{1038} 245^2$

But $245 \equiv 11 (\text{mod} 18)$

$2452 \equiv 11^2$ (mod 18)

$\equiv 121$ (mod 18)

$\equiv 13$ (mod 18)

$245^{1040} \equiv 1 \cdot 13$ (mod 18)

$\equiv 13$ (mod 18)

∴ The remainder is 13 when 2451040 is divided by 18.

If $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ is the canonical decomposition of a positive integer n then derive the formula for the phi function $\phi(n)$ and use it to find $\varphi(6860)$

Proof:

To prove : If p is prime and e any positive integer then prove that $\varphi(p^e) = p^e - p^{e-1} = p^e(1 - \frac{1}{p})$

$\varphi(p^e) =$ **number of positive integers** $\leq p^e$ **and relatively prime to it**

= {number of positive integers $\leq p^e$ **}-{ number of positive integers** $\leq p^e$ **and not relatively prime to it}**

The number of positive integers $\leq p^e$ **is** p^e **(because they are 1, 2, 3, ..., p^e)**

The number of positive integers $\leq p^e$ **and not prime to it are the various multiples of p.**

They are $p, 2p, 3p, \ldots\ldots, (p^{e-1})p$

The number of such numbers $= p^{e-1}$

Hence $\varphi(p^e) = p^e - p^{e-1} = p^e(1 - \frac{1}{p})$

Since $\varphi(p^e) = p^e - p^{e-1} = p^e(1 - \frac{1}{p})$ **is a multiplicative function,**

$$\varphi(n) = \varphi(p_1^e p_2^e \ldots p_k^e) = \varphi(p_1^e)\varphi(p_2^e) \ldots \varphi(p_k^e)$$
$$= p_1^e(1 - \tfrac{1}{p_1})\, p_2^e(1 - \tfrac{1}{p_2}) \ldots p_k^e(1 - \tfrac{1}{p_k})$$
$$= p_1^e p_2^e \ldots p_k^e (1 - \tfrac{1}{p_1})(1 - \tfrac{1}{p_2}) \ldots (1 - \tfrac{1}{p_k})$$
$$= n(1 - \tfrac{1}{p_1})(1 - \tfrac{1}{p_2}) \ldots (1 - \tfrac{1}{p_k})$$

To find $\varphi(6860)$:

$$\varphi(6860) = \varphi(2^2).\varphi(5).\varphi(7^3)$$
$$= 2^2\left(1 - \frac{1}{2}\right) 4.7^3\left(1 - \frac{1}{7}\right) = 252$$

<u>Euler phi function:</u>

Let $\varphi : N \to N$ be a function defined by

φ(1)= 1 and

for n>1 φ(n)=the number of positive integer ≤ n and relative prime to n.

1. Prove that Euler phi function is multiplicative:

Proof:

Let m and n be positive integers such that (m, n) = 1.

To prove φ(mn) = φ(m) φ(n)

Arrange the mn integers 1, 2, 3, ..., mn in m rows of n numbers each.

1	$m+1$	$2m+1$	$3m+1$	...	$(n-1)m+1$
2	$m+2$	$2m+2$	$3m+2$	...	$(n-1)m+2$
3	$m+3$	$2m+3$	$3m+3$	...	$(n-1)m+3$
:	:	:	:	:	:
:	:	:	:	:	:
r	$m+r$	$2m+r$	$3m+r$	...	$(n-1)m+r$
:	:	:	:	:	:
rth row m	$2m$	$3m$	$4m$	...	nm

Let r be a positive integer ≤ m such that (r, m) > 1.

We will now show that no element of the rth row in the array is relatively prime to mn.

Let d = (r, m). Then d ∣ r and d ∣ m⇒ d ∣km + r for any integer k

This means d is a factor of every element in the rth row.

Thus, no element in the rth row is relatively prime to m and hence to mn if (r, m) > 1.

In other words, the elements in the array relatively prime to mn come from the rth row only if (r, m) = 1.

Since r < m and relatively prime to m, we find there are φ(m) such integers r and have φ(m) such rows.

Now let us consider the rth row where (r, m) = 1.

The elements in the rth row are r, m + r, 2m + r, ..., (n-1)m + r.

When they are divided by n, the remainders are 0, 1, 2, ..., n - 1 in some order of which φ(n) arc relatively prime to n.

Therefore, exactly φ(n) elements in the rth row are relatively prime to n and hence to mn.

Thus there are φ(m) rows containing positive integers relatively prime to mn and each row contain φ(n) elements relatively prime to it.

Hence the array contains φ(m) φ(n) positive integers ≤ mn and relatively prime to mn.

That is φ(mn) = φ(m) φ(n).

Hence φ is multiplicative function.

2. If p is prime and e any positive integer then prove that $\varphi(p^e)=p^e-p^{e-1}$. Also show that $\varphi(n)=\frac{n}{2}$ when $n = 2^k$

Proof:

$\varphi(p^e)$ = **number of positive integers** $\le p^e$ **and relatively prime to it**

= **{number of positive integers** $\le p^e$ **}-{ number of positive integers** $\le p^e$ **and not relatively prime to it}**

The number of positive integers $\le p^e$ **is** p^e **(because they are 1, 2, 3, ...,** p^e **)**

The number of positive integers $\le p^e$ **and not prime to it are the various multiples of p.**

They are $p, 2p, 3p, ...,(p^{e-1})p$

The number of such numbers $= p^{e-1}$

Hence $\varphi\left(p^e\right)=p^e-p^{e-1}$

$\varphi(n) = \frac{n}{2}$ **when** $n = 2^k$

To prove that

$Given\ n = 2^k$

$$\therefore \varphi(n) = \varphi(2^k) = 2^k\left(1-\frac{1}{2}\right) = 2^k.\frac{1}{2} = \frac{n}{2}$$

3. Find the primes p for which $\frac{2^{p-1}-1}{p}$ **is a square.**

Solution:

Suppose $\frac{2^{p-1}-1}{p} = n^2$ **for some positive integer n. Then** $2^{p-1}-1 = pn^2$

Clearly both p and n must be odd.

Let p=2k+1 for some positive integer k.

Then $2^{2k}-1 = pn^2$

$\Rightarrow \quad (2^k-1)(2^k+1) = pn^2$

Suppose (2^k-1) **is a perfect square,** $(2^k-1) = r^2 \Rightarrow 2^k = r^2+1$

$$2^{p-1} = 2^{2k} = (2^k)^2 = \left(r^2+1\right)^2$$

Since r≥1 and is odd, r = 2i + 1 for some integer i ≥ 0.

Then r2 = (2i + 1)2 has to be an odd number.

But r2 + 1= 2k ⇒ r2 + 1 has to divide 2.

⇒ r2 + 1 = 1 or 2.

⇒ r =0 or 1

$r = 0,\ 2^{p-1} = (0^2+1)^2 = 1$ **⇒ p=0 which is not possible**

$r = 1,\ 2^{p-1} = (1^2+1)^2 = 4$ **⇒ p=3**

Suppose (2^k+1) **is a perfect square**

$$(2^k+1) = s^2 \Rightarrow 2^k = s^2-1$$

$$2^{p-1} = (s+1)^2(s-1)^2$$

Then both s -1 and s+1 both must be the factors of 2

$$s-1 = 1 \text{ or } 2, \quad \& \quad s+1 = 1 \text{ or } 2$$

$$\Rightarrow s = 0, 1, 2 \text{ or } 3$$

If $s = 0;\ 2^{p-1} = (0+1)^2(0-1)^2 = 1 \Rightarrow p = 1$ **which is not possible**

If $s = 1;\ 2^{p-1} = (1+1)^2(1-1)^2 = 0$ **which is not possible**

If $s = 2;\ 2^{p-1} = (2+1)^2(2-1)^2 = 9$ **which is not possible**

$If \quad s=3;\ 2^{p-1}=(3+1)^2(3-1)^2=2^6 \Rightarrow p=7$

Thus p must be 3 or 7

Tau function:

Let n be a positive integer then

$\tau(n)$ denotes the number of positive factors of n that is $\tau(n) = \sum_{d/n} 1$

Sigma function:

Let n be a positive integer then $\sigma(n)$ denotes the sum of the positive factors of n that is

$$\sigma(n) = \sum_{d/n} d$$

Problems:

1. Evaluate $\tau(18)$ and $\tau(23)$

Solution:

The positive divisors of 18 are 1,2,3,6,9,18 so that $\tau(18) = 6$

23 being a prime , has exactly two positive divisors so $\tau(23) = 2$

2. Evaluate $\sigma(12)$ and $\sigma(28)$

Solution:

The positive divisors of 12 are 1,2,3,4,6,12 so that $\sigma(12) = 1 + 2 + 3 + 4 + 6 + 12 = 28$

The positive divisors of 28 are 1,2,4,7,14,28 so that $\sigma(28) = 1 + 2 + 4 + 7 + 14 + 28 = 56$