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

Number Theory

Primitive roots and Indices

The order of an integer mod n ($n>1$)

Let a be any integer such that $(a, n) = 1$

i.e greatest common divisor (g.c.d) of a and n be 1 then by an order of an integer a we mean the least positive integer k such that $a^k \equiv 1 \pmod n$

Ex. Take $a = 2$. $n = 5$

i.e Find order of $2 \bmod 5$

Here gcd of 2 and 5 i.e $(2,5) = 1$

Now we have to find least positive integer k s.t.

Now,

$$2^1 \equiv 2 \pmod 5$$
$$2^2 \equiv 4 \pmod 5$$
$$2^3 \equiv 3 \pmod 5$$
$$2^4 \equiv 1 \pmod 5$$

Similarly $2^8 \equiv 1 \pmod 5$

Also we observe, $2^{12} \equiv 1 \pmod 5$

$\vdots$

least among $(4, 8, 12, \cdots) = 4$

i order of $2 \bmod 5$ is 4 as 4 is least positive integer such that

$$2^4 \equiv 1 \pmod 5.$$

CH-07 (02) Number Theory

Excercise Dr Satish Kumar Gupta

(1) Find order of $2 \bmod 7$ Ans. 03

(2) Find order of $2 \bmod 11$ Ans. 10

(3) Find order of $2 \bmod 13$ Ans. 12

(4) Find order of $3 \bmod 8$ Ans 02

Some theorems on order of an integer mod n.

Theorem 1. Let order of a mod n is k then prove

(i) if $a^h \equiv 1 \pmod n$ for some integer h then $k \mid h$.

(ii) if $a \equiv b \pmod n$ then b has order k modulo n

(iii) if $a^i \equiv b^j \pmod n \iff i \equiv j \pmod k$

Proof. (i) Given $a^k \equiv 1 \pmod n$

Let h be an integer

It is given that k, least positive integer

So by division algorithm there exists $q \in I$, $r \in I$ such that

$h = kq + r$ where $0 \le r < k$ — (1), I means set of integers

$\because a^h \equiv 1 \pmod n$

$\Rightarrow a^{kq+r} \equiv (a^k)^q \cdot a^r \pmod n$

$\equiv (1)^q \cdot a^r \pmod n$

$\Rightarrow a^h \equiv a^r \pmod n$

$\Rightarrow a^r \equiv 1 \pmod n$

[$\because a^h \equiv 1 \pmod n$ and $a \equiv b \pmod n \iff b \equiv a \pmod n$.]

But $r < k$ & k is least so r must be zero

$\because$ (1) $\Rightarrow h = kq \Rightarrow k \mid h$, proved.

Number Theory

(ii) Given order of $a \bmod n$ is k

$a \equiv b \pmod n$

To prove order of b is also k.

Soln. order of $a \bmod n$ is $k \Rightarrow a^k \equiv 1 \pmod n$ — (1)

it is given $a \equiv b \pmod n$

$\Rightarrow a^k \equiv b^k \pmod n$

$\Rightarrow 1 \equiv b^k \pmod n$, from (1)

$\Rightarrow b^k \equiv 1 \pmod n$,

ii order of $b \bmod n$ is also k.

(iii) Given order of $a \bmod n$ is k

$a^i \equiv a^j \pmod n$

To prove $a^i \equiv a^j \pmod n \Leftrightarrow i \equiv j \pmod k$

Proof. Given $a^i \equiv a^j \pmod n$

$\Leftrightarrow a^{i-j} \equiv 1 \pmod n$

$\Leftrightarrow k \mid (i-j)$ [$\because a^h \equiv 1 \pmod n \Rightarrow k \mid h$ as order of $a \bmod n$ is k]

$\Leftrightarrow i \equiv j \pmod k$

Theorem. (2) If $o(a) = k \pmod n$ then a^h has order $\frac{k}{(h,k)} = d$

Proof Let $(a,n) = 1$

$o(a) \bmod n = k$

$\Rightarrow a^k \equiv 1 \pmod n$ ——— (1)

To prove order of $a^h = \frac{k}{(k,h)} = d$, d = g.cd of h & k

Let $o(a^h) = t$

$\Rightarrow (a^h)^t \equiv 1 \pmod n$

$\Rightarrow a^{ht} \equiv 1 \pmod n$

$\Rightarrow k \mid ht$ as $o(a) = k$

Since $(h,k) = d \Rightarrow d \mid h$, $d \mid k$

$\Rightarrow h = k_1 d$

$k = k_2 d$

$\Rightarrow k_2 d \mid k_1 d t$

$\Rightarrow k_2 \mid k_1 t$ as $(k_1, k_2) = 1$

$\Rightarrow \frac{k}{d} \mid t$ ——— (2)

Now $(a^h)^{\frac{k}{d}} = (a^h)^{k_2} \pmod n$

$\equiv a^{k_1 d k_2} \pmod n$

$\equiv a^{k_1 k}$ $[dk_2 = k]$

$\equiv (1)^{k_1} \pmod n$

$\equiv 1 \pmod n$ $[\because a^h$ has order $t]$

$\Rightarrow t \mid \frac{k}{d}$ ——— (3)

(2) & (3) $\Rightarrow t = \frac{k}{d}$

$\therefore o(a^h) = t = \frac{k}{d} = \frac{k}{(h,k)}$ $[\because d = (h,k)]$

Theory 03. If the order of $a_1 \bmod n$ is k_1, order of $a_2 \bmod n$ is k_2, $(k_1, k_2) = 1$. Then prove that order of $a_1 a_2 \pmod n$ is $k_1 k_2$.

Proof. Given

order of $a_1 \bmod n$ is $k_1 \Rightarrow a_1^{k_1} \equiv 1 \pmod n$

order of $a_2 \bmod n$ is $k_2 \Rightarrow a_2^{k_2} \equiv 1 \pmod n$

To prove order of $a_1 a_2 \pmod n$ is $k_1 k_2$

Let order of $a_1 a_2 \bmod n$ is k

$\Rightarrow (a_1 a_2)^k \equiv 1 \pmod n$

$\Rightarrow \{[a_1 a_2]^k\}^{k_2} \equiv 1 \pmod n$

$\Rightarrow (a_1 a_2)^{k k_2} \equiv 1 \pmod n$

$\Rightarrow a_1^{k k_2} \cdot a_2^{k k_2} \equiv 1 \pmod n$

$\Rightarrow a_1^{k k_2} \cdot 1 \equiv 1 \pmod n$ $\quad [\because a_2^{k k_2} \equiv (a_2^{k_2})^k \pmod n \equiv 1^k \pmod n \equiv 1 \pmod n]$

$\Rightarrow a_1^{k k_2} \equiv 1 \pmod n$

$\Rightarrow k_1 \mid k k_2$ $\quad [\because a^h \equiv 1 \pmod n \Rightarrow k \mid h$ if order of $a \bmod n$ is $k]$

$\Rightarrow k_1 \mid k$ $\quad [\because (k_1, k_2) = 1]$ $\quad \text{---} (1)$

Again,

$(a_1 a_2)^k \equiv 1 \pmod n$

$\Rightarrow [(a_1 a_2)^k]^{k_1} \equiv 1 \pmod n$

$\Rightarrow (a_1 a_2)^{k k_1} \equiv 1 \pmod n$

$\Rightarrow a_1^{k k_1} a_2^{k k_1} \equiv 1 \pmod n$

$\Rightarrow 1 \cdot a_2^{k k_1} \equiv 1 \pmod n$ $\quad [\because a_1^{k k_1} \equiv (a_1^{k_1})^k \pmod n \equiv 1 \pmod n]$

$\Rightarrow k_2 \mid k k_1$ $\quad [\because$ order of $a_2 \bmod n$ is $k_2]$

$\Rightarrow k_2 | k$ as $(k_1, k_2) = 1$

——— (2)

Equation (1) and (2) implies that

$k_1 | k$

$k_2 | k$

$\Rightarrow k_1 k_2 | k$ ($\because (k_1, k_2) = 1$)

ex $2|6 \Rightarrow 2*3|6$ as $(2,3)=1$
$3|6$

ii $k = k_1 k_2$

ii order of $a_1 a_2 \bmod n$ is $k_1 k_2$.

Ex. (1) Take $a_1 = 2, n = 7$

$a_2 = 13, n = 7$

order of $2 \bmod 7$ is 3 i.e $k_1 = 3$

order of $13 \bmod 7$ is 2 i.e $k_2 = 2$

ii order of $26 (\bmod 7)$ is 6.

i.e order of $a_1 \bmod n$ is k_1

$a_2 \bmod n$ is k_2

$\Rightarrow$ order of $a_1 a_2 \bmod n$ is $k_1 k_2$.

(2) Do form another problem keeping in mind that

order of $a_1 \bmod n$ is k_1

$a_2 \bmod n$ is k_2

such that gcd of k_1, k_2 is 1.

and do your self.

Number Theory

Primitive root mod n

Let $(a,n)=1$

then a is a primitive root of n if it satisfies two properties:

(1) $a^{\phi(n)} \equiv 1 \pmod{n}$, $\phi(n)$ denotes Euler function of n.

(2) $a^k \not\equiv 1 \pmod{n}$, $\forall\ k < \phi(n)$.

Ex. Let $n=7$

Take $a=2$

clearly $(2,7)=1$ (Here $a=2$, $n=7$)

Note. Here 2 will be a primitive root of 7 if it will satisfy the above two conditions.

Here $\phi(n) = \phi(7) = 6$ ($n=7$, Here)

[$\phi(n)$ = no of integers less than n, prime to n.

$\phi(p) = p-1$, p is prime]

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

$2^2 \equiv 4 \pmod{7}$

$2^3 \equiv 1 \pmod{7}$

Here k's are 1, 2, 3, 4, 5 as $k < \phi(n)$ and $\phi(n)=6$

so all natural numbers less than 6 ($\phi(n)$) will be possible k's.

$\therefore$ for $a^k \equiv 1 \pmod{n}$, $a=2$, $k=3<6$, $n=7$

$\Rightarrow$ 2 is not primitive root of 7.

Take $a=3$

Clearly $(3,7)=1$ [i.e g.c.d of 3 & 7 is 1]

$n=7 \quad \phi(7)=6$

k's are 1, 2, 3, 4, 5 ($k < \phi(n)$, $\phi(n)=6$ Here)

$3^1 \equiv 3 \pmod 7$

$3^2 \equiv 2 \pmod 7$

$3^3 \equiv 6 \pmod 7$

$3^4 \equiv 4 \pmod 7$

$3^5 \equiv 5 \pmod 7$

$3^6 \equiv 1 \pmod 7$

[$3^k \not\equiv 1 \pmod 7$ $\forall\ k = 1, 2, 3, 4, 5 < 6$.]

$\therefore \quad 3^{\phi(n)} \equiv 1 \pmod 7$, $\phi(n)=6$

$3^k \not\equiv 1 \pmod 7$, $\forall\ k < 6$.

Here both conditions are satisfied

$\therefore$ 3 is a primitive root of 7.

Similarly Take $a=4$ so that $(4,7)=1$

$a=5$ so that $(5,7)=1$

$a=6$ So that $(6,7)=1$

and check whether 4 is p.r of 7

5 is p.r. of 7

6 is p.r of 7.

and Take $n = 11, 13, 15, 17, 19 \cdots$ etc

and Take a such that $(a,n)=1$

then find the values of a such that

a is a p.r of 11, 13, 15, 17, 19, - - -

i.e Take $a = 2, 3, 4, 5, 6, 7, 8, 9, 10$ s.t $(2,11)=1$

$(3,11)=1, (4,11)=1, (5,11)=1, (6,11)=1, (7,11)=1, \cdots$

and check whether a is a p.r of 11. for various values of a.

Number Theory

Excercise

(1) Find primitive root of 10 Take $(a,10)=1$ choose $a=?$

(2) Find primitive root of 15 Take $(a,15)=1$, choose $a=?$

Reduced residue mod n

A set $\{a_1, a_2, \cdots a_k\}$ is called reduced residue system mod n if

(1) $(a_1, n)=1$, $(a_2, n)=1$, $\cdots$, $(a_k, 1)=1$

i.e. each $(a_i, n)=1$, $\forall\ i=1,2,3,\cdots k$.

(2) $a_i \not\equiv a_j \pmod n$ for $i \neq j$

(3) there exist Integer k such that for each k, $k \equiv a_i \pmod n$ such that $(k, n)=1$.

Theorem 04. If a is a primitive root mod n then $a, a^2, a^3, \cdots, a^{\phi(n)}$ is a reduced residue system mod n

Proof. Recall a set $\{a_1, a_2, \cdots, a_k\}$ is called reduced residue system mod n if

(1) $(a_i, n)=1$, $\forall\ i=1,2,3,\cdots, k$.

(2) $a_i \not\equiv a_j \pmod n$, for $i \neq j$

(3) there exist positive Integer m such that for each m, $m \equiv a_i \pmod n$ where $(m, n)=1$.

Given a is a primitive root of n it means

(1) $(a, n)=1$ (2) $a^{\phi(n)} \equiv 1 \pmod n$

(3) $a^k \not\equiv 1 \pmod n$, $\forall\ k < \phi(n)$.

here we observe that

$(a, n) = 1$
$(a^2, n) = 1$
$(a^3, n) = 1$
$\vdots$
$(a^{\phi(n)}, n) = 1$

i.e $(a^h, n) = 1$, where $1 \leq h \leq \phi(n)$.

Also

$$a^i \not\equiv a^j \pmod{n} \text{ for } i \neq j$$

and

$$a^h \equiv k \pmod{n} \text{ for some } k < \phi(n),$$
$$, h = 1, 2, 3, \ldots \phi(n).$$

∴ all the conditions of reduced residue system are satisfied

∴ $(a, a^2, a^3, \ldots, a^{\phi(n)})$ is a reduced residue system mod n.

Number Theory

Theorem. 1. Lagrange's Theorem.

Statement. If p is a prime and

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0, \quad a_n \not\equiv 0 \pmod{p}$$

is a polynomial of degree n $(n \geq 1)$ with integral coefficients, then

$$f(x) \equiv 0 \pmod{p}$$ has at most n incongruent solutions mod p.

Proof. Let

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0, \quad a_n \not\equiv 0 \pmod{p}, \ p \text{ is a prime} \quad \text{— (1)}$$

To prove $f(x) \equiv 0 \pmod{p}$ has at most n incongruent solutions mod p. — (2)

We shall prove the Theorem by mathematical induction on the degree of $f(x)$.

If $n = 1$ then equation (1) implies

$$f(x) = a_1 x + a_0$$

$$\therefore f(x) \equiv 0 \pmod{p} \Rightarrow a_1 x + a_0 \equiv 0 \pmod{p}$$

$$\Rightarrow a_1 x \equiv -a_0 \pmod{p}$$

which has a unique solution mod p

$\therefore$ The given theorem is true for $n = 1$.

Now, assume that the theorem is true for a polynomial of degree $(k-1)$. And consider the case in which $f(x)$ has degree k.

Now, two cases arise

(1) $f(x)$ has no solution

(2) $f(x)$ has atleast one solution

(1) Suppose $f(x)$ has no solution so we are nothing to prove.

(2) Suppose $f(x)$ has atleast one solution say $x=a$

It means $(x-a)$ will divide $f(x)$, so we have

$$f(x) = (x-a)g(x) + r \quad \text{where } \deg g(x) = (k-1), \; r \in I, \text{ Integer} \quad \longleftarrow (3)$$

put $x=a$

$$\Rightarrow f(a) = 0 \cdot g(a) + r$$

$$\Rightarrow f(a) = r$$

$$\Rightarrow 0 \equiv r \pmod{p}$$

ii $f(x) \equiv [(x-a)g(x) + r] \pmod{p}$

$$\Rightarrow f(x) \equiv [(x-a)g(x) + 0] \pmod{p}$$

$$\Rightarrow f(x) \equiv (x-a)g(x) \pmod{p} \quad \longrightarrow (4)$$

If b is another one of the incongruent solution of $f(x) \equiv 0 \pmod{p}$, then $\longrightarrow (5)$

(4) and (5) $\Rightarrow$

$$0 \equiv (b-a)g(b) \pmod{p}$$

$$\Rightarrow 0 \equiv g(b) \pmod{p} \quad [\because b-a \not\equiv 0 \pmod{p}]$$

$\Rightarrow b$ satisfies $g(x) \equiv 0 \pmod{p}$

But by our assumption $g(x)$ has at most $(k-1)$ incongruent solutions [$\because x=b$ is one of among $(k-1)$ solutions]

So, $f(x) \equiv 0 \pmod{p}$ has no more than k incongruent solutions.

Take $k=n \Rightarrow f(x) \equiv 0 \pmod{p}$ has no more than n congruent solutions. Proved

Theorem. 2. If p is a prime number and $d|(p-1)$ Then the congruence $(x^d-1) \equiv 0 \pmod p$ has exactly d solutions.

Proof. Let $d|(p-1) \Rightarrow \exists\ k \in I$ such That

$$(p-1) = dk \quad \text{——— (1)}$$

for some integer k

∴ Now, consider

$$(x^{p-1}-1) = x^{dk}-1$$

$$= (x^d)^k - 1$$

$$= (x^d-1)\left[(x^d)^{k-1} + (x^d)^{k-2} + \cdots + x^d + 1\right]$$

$$\left[\because x^n-1 = x^{n-1}+x^{n-2}+\cdots+x+1\right], \text{ Here } x = x^d$$

$$(x^{p-1}-1) = (x^d-1)\,f(x)$$

where

$$f(x) = (x^d)^{k-1} + (x^d)^{k-2} + \cdots + x^d + 1\ ]$$

$$f(x) = [x^{dk-d} + x^{dk-2d} + x^{dk-3d} + \cdots + x^d + 1] \quad \text{——— (1)}$$

whose degree i.e $\deg f(x) = x^{dk-d}$

$$= x^{p-1-d} \quad (\because p-1 = dk)$$

By Lagrange's Theorem

$f(x) \equiv 0 \pmod p$ has at most $(p-1-d)$ solutions

We also know by fermat's theorem

$x^{p-1}-1 \equiv 0 \pmod p$ has exactly $(p-1)$ incongruent solutions namely $1, 2, 3, \cdots, (p-1)$.

Now, any solution $x \equiv a \pmod p$ of $x^{p-1}-1 \equiv 0 \pmod p$ that is not a solution of $f(x) \equiv 0 \pmod p$ must satisfy $x^d-1 \equiv 0 \pmod p$ $[\because d|p-1]$

For,

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

$$0 \equiv (a^d - 1) f(a) \bmod p$$

Since $p \nmid f(a)$ [$\because x \equiv a \pmod{p}$ is not a solution of $f(x) \equiv 0 \pmod{p}$]

$\Rightarrow p \mid a^d - 1$ [$mn \bmod p \equiv 0 \Rightarrow p \mid m$ or $p \mid n$]

$\Rightarrow a^d \equiv 1 \pmod{p}$

It means $a^d - 1 \equiv 0 \pmod{p}$

must have atmost $p-1-(p-1-d) = d$

incongruent solutions.

Theorem 03. If p is a prime and $d|(p-1)$ then there are exactly $\phi(d)$ incongruent integers having $d \bmod p$.

Proof. Let $d|(p-1)$ (p is a prime)

then we know

$(x^d - 1) \equiv 0 \pmod p$ has exactly d incongruent solutions

Let $\phi_1(d)$ = numbers of integers m such that $1 \le m \le (p-1)$, having each of order $d \bmod p$

i.e order of $1 \bmod p$ is d
$2 \bmod p$ is d
$3 \bmod p$ is d
$\vdots$
$(p-1) \bmod p$ is d [$a^h \equiv 1 \pmod p$ if $d|h$ & $o(a) = d$]

Now, we have

$$p-1 = \sum_{d|p-1} \phi_1(d) \quad \text{---(1)}$$

Also by Gauss theorem

$$p-1 = \sum_{d|p-1} \phi(d) \quad \text{---(2)}$$

$\therefore$ (1) and (2) implies

$$\sum_{d|p-1} \phi_1(d) = \sum_{d|p-1} \phi(d) \quad \text{---(3)}$$

[$\because \phi_1(d) \neq 0$]

If $\phi_1(d) > 0$

$\Rightarrow \exists$ an integer a of order d

$\Rightarrow \exists \exists$ d - incongruent solutions namely $a, a^2, a^3, a^3, \ldots a^d \bmod p$ that will satisfy $(x^d - 1) \equiv 0 \pmod p$. — (4)

$\therefore$ Any integer that has order $d \bmod p$ should be congruent to $a, a^2, \ldots a^d$.

Hence, the number of integers having order d mod p must be equal to $\phi(d)$.

Ex (1) Take $p = 17$

$p-1 = 16$

Now, Take $d = 2$

$2 | (p-1)$

$\phi(d) = \phi(2) = 1$

∴ There is only 1 solution having 2 (mod 17).
Each solution will have order 2 (mod 17).

(2) $p = 17$

$p-1 = 16$

$d = 4$

$d | p-1$ i.e $4 | 16 \Rightarrow \phi(d) = \phi(4)$

$= 2^2 - 2$

$= 2$

There are two incongruent solutions of 4 (mod 17). Each solution will have order 4 (mod 17)

(3) $p = 17$, $p-1 = 16$

$d = 8$

$\phi(d) = \phi(8)$

$= 8 \times (1 - \frac{1}{2}) = 4$

There are 4 incongruent solutions 8 (mod 17). Each solution will have order 8 (mod 17).

Theorem 07 If $(a,m)=1$ then a is a primitive root of m iff $a^{\frac{\phi(m)}{p}} \not\equiv 1 \pmod m$ for every prime divisor of $\phi(m)$.

Proof. Let a be an positive integer such that $(a,m)=1$

Let p be a prime divisor of $\phi(m)$

"if part" Suppose $a^{\frac{\phi(m)}{p}} \not\equiv 1 \pmod m$, $\forall$ prime divisor p of $\phi(m)$

to show a is primitive root of m

Suppose if possible a is not primitive root of m

$\Rightarrow \exists\, r \in N$ s.t $a^r \equiv 1 \pmod m$ where $r < \phi(m)$.

$\Rightarrow r \mid \phi(m)$ $\quad [\because a^{\phi(m)} \equiv 1 \pmod m]$

$\Rightarrow \frac{\phi(m)}{r}$ is an integer

$\Rightarrow \exists$ some prime number p such that

$p \mid \frac{\phi(m)}{r} \Rightarrow \frac{\phi(m)}{rp}$ is also an integer

We have $a^{\frac{\phi(m)}{p}} \equiv \left(a^r\right)^{\times \frac{\phi(m)}{rp}} \pmod m$

$\Rightarrow a^{\frac{\phi(m)}{p}} \equiv 1 \pmod m$ $\quad [\because a^r \equiv 1 \pmod m]$

which is a contradiction $\Rightarrow a$ is a p. root of m.

"only if part" Let a is a p. root of m

To show $a^{\frac{\phi(m)}{p}} \not\equiv 1 \pmod m$

a is a p. r of m

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

and $a^k \not\equiv 1 \pmod m$, $\forall\, k < \phi(m)$

$\Rightarrow a^{\frac{\phi(m)}{p}} \not\equiv 1 \pmod m$ $\quad [\because \frac{\phi(m)}{p} < \phi(m)]$

Hence the theorem.

Example based on Theorem 04

If $(a,m)=1$ then a is p.r. of m iff $a^{\frac{1}{p}\phi(m)} \not\equiv 1 \pmod m$, $\forall$ prime divisor p of $\phi(m)$

Ex Show 2 is a primitive root of 11

Here $a=2$, $m=11$

$(2,11)=1$ [i.e. g.c.d of 2 & 11 is 1]

Now $\phi(11)=10$

Choose those primes those divide 10

Here 2 and 5 are only two primes those divides $\phi(11)$.

So we shall show

$a^{\frac{\phi(m)}{p}} \not\equiv 1 \pmod m$ for $p=2$ and $p=5$

$a=2$, $\frac{\phi(m)}{p} = \frac{10}{2}, \frac{10}{5} \Rightarrow 5, 2$ respectively

$2^2 \equiv 4 \pmod{11} \Rightarrow 2^{\frac{\phi(11)}{5}} \not\equiv 1 \pmod{11}$ for $p=2$

$\left[\frac{\phi(11)}{5}=2\right]$

$2^3 \equiv 8 \pmod{11}$

$2^4 \equiv 5 \pmod{11}$

$2^5 \equiv -1 \pmod{11} \Rightarrow 2^{\frac{\phi(11)}{2}} \not\equiv 1 \pmod{11}$

$\left[\frac{\phi(11)}{2}=5\right]$

(i) $2^{\frac{\phi(11)}{p}} \not\equiv 1 \pmod{11}$ for $p=2$ and $p=5$

(ii) 2 is p.r. of 11.

(2) Find p.r. of 15

Sol We must have $(a, 15) = 1$

a's are 2, 4, 7, 8, 11, 13, 14

So possible p.r of 15 are 2, 4, 7, 8, 11, 13, 14

Now,

$$\phi(15) = \phi(3\times5) = \phi(3)\phi(5)$$
$$= 2\cdot4$$
$$\phi(15) = 8$$

2 is only prime divisor of 8

i.e. $\frac{\phi(15)}{2} = \frac{8}{2} = 4$

So we shall prove

If 2 is p.r of 15 then $2^4 \not\equiv 1 \pmod{15}$ [$\because a^{\frac{\phi(m)}{p}} \not\equiv 1 \pmod m$]

If 4 is p.r of 15 then $4^4 \not\equiv 1 \pmod{15}$ "

If 7 is p.r. of 15 then $7^4 \not\equiv 1 \pmod{15}$ "

If 8 is p.r. of 15 then $8^4 \not\equiv 1 \pmod{15}$ "

If 11 is p.r. of 15 then $11^4 \not\equiv 1 \pmod{15}$ "

If 13 is p.r. of 15 then $13^4 \not\equiv 1 \pmod{15}$ "

If 14 is p.r. of 15 then $14^4 \not\equiv 1 \pmod{15}$ ["]

Here we have

$2^4 \equiv 1 \pmod{15} \Rightarrow 2$ is not p.r. of 15

$4^2 \equiv 1 \pmod{15}$

$\Rightarrow 4^4 \equiv 1 \pmod{15} \Rightarrow 4$ is not p.r of 15

$7^2 \equiv 4 \pmod{15}$

$\therefore 7^4 \equiv 1 \pmod{15} \Rightarrow 7$ is not p.r. of 15

$8^2 \equiv 4 \pmod{15}$

$8^4 \equiv 1 \pmod{15} \Rightarrow 8$ is not p.r of 15

$11^2 \equiv 1 \pmod{15} \Rightarrow 11^4 \equiv 1 \pmod{15} \Rightarrow 11$ is not p.r. of 15.

$13^2 \equiv 4 \pmod{15} \Rightarrow 13^4 \equiv 1 \pmod{15} \Rightarrow 13$ is not p.r of 15

$14^2 \equiv 1 \pmod{15} \Rightarrow 14^4 \equiv 1 \pmod{15} \Rightarrow 14$ is not a p.r of 15

Hence there is no primitive root of 15. Ans.

Find p.r. of 17

Choose $(a, 17) = 1$

Possible a's are 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16

$\phi(17) = 16$

To find $\frac{\phi(17)}{p} = \frac{16}{p}$, p is prime divisor of 16

$\Rightarrow$ 2 is only prime divisor 16.

$\frac{\phi(17)}{2} = \frac{16}{2} = 8$

Now, $2^8 \equiv 1 \pmod{17} \Rightarrow$ 2 is not p.r of 17

$\left[2^{\frac{\phi(17)}{p}} \not\equiv 1 \pmod{17}\right]$ must be

$3^4 \equiv -4 \pmod{17}$

$3^8 \equiv 16 \pmod{17} \Rightarrow 3^8 \not\equiv 1 \pmod{17} \Rightarrow$ 3 is p.r. of 17.

$4^2 \equiv -1 \pmod{17}$

$\Rightarrow 4^8 \equiv 1 \pmod{17} \Rightarrow$ 4 is not p.r. of 17.

$5^2 \equiv 8 \pmod{17} \Rightarrow 5^4 \equiv 13 \pmod{17} \Rightarrow 5^8 \not\equiv +1 \pmod{17}$

$\Rightarrow$ 5 is p.r. of 17.

We shall check

$a^8 \not\equiv 1 \pmod{17}$ for $a = 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16$

Do your self.

Ans is $a = 6, 7, 10, 11, 12, 14$ } all are p.r. of 17

ii Total p.r. of 17 are 3, 5, 6, 7, 10, 11, 12, 14.

Primitive root of Compositive numbers

Theorem 1. $n=2$, $n=4$ has one p.r. namely 1 & 3 respectively.

Soln (1) Take $a=1$, $(1,2)=1$

$\phi(n)=\phi(2)=1$

$a^{\phi(n)} \equiv 1 \pmod n$, $a^k \not\equiv 1 \pmod n$, $\forall\ k < \phi(n)$

$1^1 \equiv 1 \pmod 2$

$\Rightarrow$ 1 is p.r. of 2.

(2) $n=4$

$(1,4)=1$, $(3,4)=1$ $\quad \phi(4)=2^2-2=2$

$a=1$, $a=3$

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

$a^k \not\equiv 1 \pmod n$, $\forall\ k < \phi(n)$

$1^1 \equiv 1 \pmod 4$

$1^2 \equiv 1 \pmod n \Rightarrow$ 1 is not p.r. of 4.

$\begin{cases} 3^2 \equiv 1 \pmod{2^2} \\ 3^1 \not\equiv 1 \pmod{2^2} \end{cases}$

$\Rightarrow$ 3 is a p.r. of 4.

Theorem. The integer 2^n has no primitive root for $n \geq 3$.

Proof. Let a be an odd integers

$n = 2^n$

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

then $(a, 2^n) = 1$

$$\phi(2^n) = 2^n - 2^{n-1}$$
$$= 2^{n-1}.2 - 2^{n-1}$$
$$= 2^{n-1}$$

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

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

$= 2^{n-2}$

$a^{2^{n-2}} \equiv 1 \pmod{2^n}$

$\Rightarrow$ a is not p.r of 2^n.

If $a^{\frac{\phi(2^n)}{2}} \equiv 1 \pmod{2^n}$

then 2^n has p.r of 2^n for $n \geq 3$.

For $n=3$

$$a^{2^{n-2}} \equiv 1 \pmod{2^n}$$

$\Rightarrow a^2 \equiv 1 \pmod 8$ $\forall$ odd number a

We shall prove it by mathematical induction.

Suppose the statement is true for $n = m \geq 3$

i.e $a^{2^{m-2}} \equiv 1 \pmod{2^m}$

Now $a^{2^{(m+1)-2}} = a^{2^{m+1-2}} = a^{2^{m-1}}$

$$= a^{2^{m-2}} \cdot a^{2^{m-2}}$$
$$= \left(a^{2^{m-2}}\right)^2$$
$$= (1 + \lambda . 2^m)^2$$
$$= 1 + 2.\lambda 2^m + \lambda^2 . 2^{2m}$$
$$= 1 + \lambda 2^{m+1} + \lambda^2 . 2^{2m}$$

$$a^{2^{m+1-2}} = 1 + \lambda 2^{m+1} + \lambda^2 . 2^{m-1} . 2^{m+1}$$

$\left[a^{2^{m-2} + 2^{m-2}} = a^{2.2^{m-2}} = a^{2^{m-1}} \right]$

$a^{2^{m-2}} = 1 + \lambda 2^m$

$$a^{2^{(m+1)-2}} = 1 + \lambda \cdot 2^{m+1} + \lambda^2 2^{m-1} \cdot 2^{m+1}$$

$$\Rightarrow a^{2^{(m+1)-2}} \equiv 1 \pmod{2^{m+1}}$$

$\left[m > 3,\ m-1 > 2 \Rightarrow m-1 > 1 \right]$

$\left[\because \lambda 2^{m+1} + \lambda^2 2^{m-1} 2^{m+1} \equiv 0 \pmod{2^{m+1}} \right]$

This shows that result is true for $n = m+1$

Hence, $a^{\frac{\phi(2^n)}{2}} \equiv 1 \pmod{2^n}$

$\Rightarrow$ a is not a p.r of 2^n, for $n > 3$.

Ex (1) $n = 16$, $a = 3$

3 is not a p.r. of 16

as $3^{\frac{1}{2}\phi(2^4)} \equiv 1 \pmod{2^4}$

(2) $n = 32$, $a = 7$

7 is not a p.r. of 2^5 $\left[32 = 2^5 \right]$

as $(7)^{\frac{1}{2}\phi(2^5)} \equiv 1 \pmod{2^5}$.

(3) $n = 128$, $a = 15$

15 is not a p.r. of 128 $(128 = 2^7)$

as $(15)^{\frac{1}{2}\phi(2^7)} \equiv 1 \pmod{2^7}$.

Theorem 3. If $m, n > 2$ and $(m, n) = 1$
then there exists no primitive root mod (mn).

Proof. Suppose if possible
a is a primitive root of mn

$\Rightarrow a^{\phi(mn)} \equiv 1 \pmod{mn}$ and $(a, mn) = 1$

$(a, mn) = 1 \Rightarrow (a, m) = 1, (a, n) = 1$

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

$a^{\phi(n)} \equiv 1 \pmod{n}$ — (2)

Let $h = \dfrac{\phi(m)\,\phi(n)}{(\phi(m), \phi(n))}$, $(\phi(m), \phi(n))$ means g.c.d of $\phi(m)$ & $\phi(n)$

Since $m, n > 2$

$\Rightarrow (\phi(m), \phi(n)) \geq 2$ [$\because \phi(m)$ and $\phi(n)$ are both even if $m, n > 2$]

$\therefore h \leq \dfrac{\phi(m)\,\phi(n)}{2}$

$\Rightarrow h \leq \dfrac{\phi(mn)}{2} < \phi(mn)$

$\Rightarrow h < \phi(mn)$

Now, $a^h \equiv a^{\frac{\phi(m)\,\phi(n)}{(\phi(m), \phi(n))}} \pmod{mn}$

$\equiv \left[a^{\phi(m)}\right]^{\frac{\phi(n)}{(\phi(m), \phi(n))}} \pmod{mn}$

$a^h \equiv 1 \pmod{mn}$ [$\because a^{\phi(m)} \equiv 1 \pmod{mn}$]

But $h < \phi(mn)$

$\therefore$ $\phi(mn)$ can not be order of a

i.e. $\phi(mn)$ can not divide h for this $\phi(mn)$ must be least positive integer

$\therefore$ we get contradiction

$\therefore$ a can not be p.r. of mod mn

$\Rightarrow$ ∄ no p.r. of mod mn.

Ex (1) $m=3, n=5$ clearly $m>2, n>2$, $(3,5)=1$
$\Rightarrow \exists$ no primitive root of mod 15.

(2) $m=3, n=7$, $(3,7)=1$
$\Rightarrow \exists$ no primitive root of mod 21.

(3) $m=3, n=11$, $(3,11)=1$
$\Rightarrow \exists$ no primitive root of mod 21

(4) $m=5, n=7$, $(5,7)=1$
$\Rightarrow \exists$ no primitive root of mod 35.

This is application part of Theorem 3,

Theorem 4. If p is odd prime then $\exists$ a primitive root of p such that $r^{p-1} \not\equiv 1 \pmod{p^2}$

Proof. Let p is odd prime. Let r be a primitive root of p.

If $r^{p-1} \not\equiv 1 \pmod{p^2}$ we are nothing to prove

Suppose if possible
$r^{p-1} \equiv 1 \pmod{p^2}$

Replace r by $r_1 = r+p$ [$\because$ if r is p.r of p $\Rightarrow r+p$ is also a p.r of p]

$\therefore r_1^{p-1} \equiv (r+p)^{p-1} \pmod{p^2}$

$\equiv r^{p-1}\left[1+pr^{-1}\right]^{p-1} \pmod{p^2}$

$\equiv r^{p-1}\left\{1+p(p-1)r^{-1}+\frac{(p-1)(p-2)}{\lfloor 2}p^2r^{-2}+\cdots\right\} \pmod{p^2}$

$\equiv r^{p-1}\left[1+p(p-1)r^{-1}\right] \pmod{p^2}$ $\left[\because \frac{(p-1)(p-2)}{\lfloor 2}p^2r^{-2} \bmod p^2 = 0 \text{ etc}\right]$

$\equiv \left[r^{p-1}+p(p-1)r^{p-2}\right] \pmod{p^2}$

$\equiv \left[r^{p-1}-pr^{p-2}+p^2r^{p-2}\right] \pmod{p^2}$

$$r_1^{p-1} \equiv (r^{p-1} - p r^{p-2}) \bmod p^2$$

$$[\because p^2 r^{p-2} \equiv 0 \pmod{p^2}]$$

$$r_1^{p-1} \equiv (1 - p r^{p-2}) \bmod p^2 \quad [\because r^{p-1} \equiv 1 \pmod{p^2}]$$

$$\equiv 1 \pmod{p^2} - p r^{p-2} \pmod{p^2}$$

$$\equiv 1 \pmod{p^2} - r^{p-2} \pmod{p}$$

[since r is a p.r of p $\Rightarrow r^{p-1} \equiv 1 \pmod{p}$ & $r^{p-2} \not\equiv 1 \pmod{p}$]

$$\Rightarrow r_1^{p-1} \not\equiv 1 \pmod{p^2}$$

which is a contradiction

$\therefore r^{p-1} \not\equiv 1 \pmod{p^2}$.

ex. Find p.r. of 5^2.

Solu. Let $r = 2$, $p = 5$

Then r will be a p.r. of p^2 if

$$r^{p-1} \not\equiv 1 \pmod{p^2}$$

but $r = 2$, $p = 5$

$$2^4 \not\equiv 1 \pmod{5^2} \quad [\because 2^4 \equiv 16 \pmod{25}]$$

$\therefore$ 2 is a p.r of 5^2.

Also $3^4 \not\equiv 1 \pmod{5^2}$

$\Rightarrow$ 3 is a p.r. of $\pmod{5^2}$

Similarly we can find other p.roots

Total p.roots of $5^2 = \phi[\phi(5^2)]$

$= \phi[5^2 - 5] = \phi(20)$

$= \phi(4)\,\phi(5)$

$= (2^2 - 2) \times 4 = \underline{8}$

Remember if $d \mid p-1$ then $x^d - 1 \equiv 0 \pmod p$ has exactly d solution, where p is prime

Ex. (1) Show $x^{18} \equiv 5 \pmod{73}$ is not solvable

Here $p = 73$, p is prime

$\phi(p) = p-1 \Rightarrow \phi(73) = 72$

If we Take $d = 18$

then $d \mid p-1$ i.e $18 \mid 72$

$\therefore x^{18} - 1 \equiv 0 \pmod{73}$ must have 18 solutions

It means $a^{\frac{p-1}{d}} \equiv a^4 \pmod{73} \equiv 1 \pmod{73}$ [$x^d \equiv 1 \pmod p$ if $d \mid p$]

$\Rightarrow a^4 \pmod{73} \equiv 5^4 \pmod{73} \equiv 1 \pmod{73}$

But $5^4 \not\equiv 1 \pmod{73}$

$\Rightarrow x^{18} \equiv 5 \pmod{73}$ has no solution.

(2) Solve $x^{15} \equiv 7 \pmod{19}$ [$x^n \equiv a \pmod p$]

$p = 19$, $\phi(19) = 18$

$d = (15, 18) = 3$ (g.c.d of (15, 18))

i.e $a^{\frac{p-1}{d}} \equiv 7^{\frac{p-1}{d}} \pmod{19}$ [$x^{d_i} \equiv 1 \pmod p$ if $d \mid p$]

$\Rightarrow a^{\frac{18}{3}} \equiv 7^6 \pmod{19}$

$\equiv 1 \pmod{19}$

[$7^2 \equiv 11 \pmod{19}$, $7^3 \equiv 1 \pmod{19}$, $\Rightarrow 7^6 \equiv 1 \pmod{19}$]

$\Rightarrow x^{15} \equiv 7 \pmod{19}$ has solution

To solve this we must find its least p.r

i.e p.r. of 19

Clearly 2 is p.r. of 19

$\phi(19) = 18$

2 is prime divisor of $\phi(19)$

$2^2 \not\equiv 1 \pmod{19}$

$2^9 \not\equiv 1 \pmod{19}$

$\Rightarrow$ $\exists$ h such that $[2^h \equiv a \pmod p]$

$2^h \equiv 7 \pmod{19}$, $0 \le h < \phi(19)$

$0 \le h < 18$, $\phi(19) = 18$

$\Rightarrow h = 6$

Now We have the congruence $[2^6 \equiv 7 \pmod{19}]$

Remember $ny \equiv h \pmod{\phi(m)}$ $\quad d = \frac{\phi(19)}{d}$, $d = (15, 18) = 3$

$15y \equiv 6 \pmod{18}$ $\quad [x^{15} \equiv 7 \pmod{19}$ i.e $n = 15]$

$15y = 6 + 18k$

For $k = 3$, $y = 4$

$k = 8$, $y = 10$

$k = 13$, $y = 16$

Required solutions will be $x \equiv 2^y \pmod{19}$

$\Rightarrow x \equiv 2^4 \pmod{19} \equiv 16 \pmod{19}$

$x \equiv 2^{10} \pmod{19} \equiv 7 \pmod{19}$

$x \equiv 2^{16} \pmod{19} \equiv 5 \pmod{19}$

Ans.

Indices

Index of a mod n

Let r is a primitive root of n. If $(a, n) = 1$

then by index of a mod n we mean the least positive h such that

$$(\text{primitive root})^h \equiv a \pmod n$$

i.e $r^h \equiv a \pmod n$

Here h is called ind. a mod n

i.e $(\text{primitive root})^{\text{Ind. a}} \equiv a \pmod n$

$\Rightarrow r^h \equiv a \pmod n$

Example Find index of 9 mod 19

Here $a = 9$, $n = 19$

Find p. r. of 19

2 is p. r of 19

$\therefore$ Search least positive integer h such that

$$2^h \equiv 9 \pmod{19}$$

$2^1 \equiv 1 \pmod{19}$ — (1)

$2^2 \equiv 4 \pmod{19}$ — (2)

$2^3 \equiv 8 \pmod{19}$ — (3)

$2^4 \equiv 16 \pmod{19}$ — (4)

$2^5 \equiv 13 \pmod{19}$ — (5)

$2^6 \equiv 7 \pmod{19}$ — (6), $2^7 \equiv 14 \pmod{19}$ — (7), $2^8 \equiv 9 \pmod{19}$ — (8)

$\therefore$ Index 9 (mod 19) = 8

Note: {2 की Power mod 19 तब तक निकालनी है जबतक 9 नहीं आ जाता}

Similarly

Equation (2) shows Ind. 4 mod 19 is 2 ($\because h=2$)

(3) " Ind. 8 mod 19 is 3 ($\because h=3$)

(4) " Ind 16 Mod 19 is 4 ($\because h=4$)

(5) " Ind 13 mod 19 is 5 ($\because h=5$)

(6) " Ind 7 mod 19 is 6 ($\because h=6$)

(7) " Ind 14 mod 19 is 7

List. Modulo 19.

a	4	8	16	13	7	14	9
Ind.a	2	3	4	5	6	7	8

Theorem 1. Let a be a primitive root modulo n and b, c and k be any integers

(i) $b \equiv c \pmod n \Rightarrow \text{ind}\, b = \text{ind}\, c \pmod{\phi(n)}$

Solution. Let $\text{ind}_a b = r_1$, $\text{ind}_a c = r_2$

We have $\Rightarrow a^{r_1} \equiv b \pmod n$, $a^{r_2} \equiv c \pmod n$

$b \equiv c \pmod n$

$\Rightarrow a^{r_1} \equiv a^{r_2} \pmod n$

$\Rightarrow a^{r_1 - r_2} \equiv 1 \pmod n$

$\Rightarrow \phi(n) \mid (r_1 - r_2)$

$\Rightarrow r_1 \equiv r_2 \pmod{\phi(n)}$

$\Rightarrow \text{ind}_a b \equiv \text{ind}_a c \pmod{\phi(n)}$

(ii) $\text{ind}\, bc = \text{ind}\, b + \text{ind}\, c \pmod{\phi(n)}$

Let $\text{ind}_a b = r_1$, $\text{ind}_a c = r_2$

Let $\text{ind}_a bc = r$

$a^r = a^{r_1} + a^{r_2}$

$a^r = a^{r_1 + r_2} \pmod n$

$\Rightarrow a^{r - (r_1 + r_2)} \equiv 1 \pmod n$

$\Rightarrow \phi(n) \mid r - (r_1 + r_2)$

$\Rightarrow r \equiv (r_1 + r_2) \pmod{\phi(n)}$

$\Rightarrow \text{ind}_a bc = \text{ind}_a b + \text{ind}_a c \pmod{\phi(n)}$

(iii) $\text{ind}\, b^k \equiv k\, \text{ind}\, b \pmod{\phi(n)}$

Let $\text{ind}_a b = r_1 \Rightarrow a^{r_1} \equiv b \pmod n$

$LHS = \text{ind}\, b^k = \text{ind}\,(b.b.b.b \cdots \text{upto } k \text{ times}) \pmod n$

$\equiv \text{ind}\, b + \text{ind}\, b + \cdots + \text{ind}\, b \pmod{\phi(n)}$ [$\because \text{ind}\, bc \equiv \text{ind}\, b + \text{ind}\, c \pmod{\phi(n)}$]

$\equiv k\, \text{ind}\, b \pmod{\phi(n)}$

(iv) put $k = 0$ in (iii),

$\text{ind}\, b^0 \equiv 0\, \text{ind}\, b \pmod{\phi(n)}$

$\Rightarrow \boxed{\text{ind}\, 1 \equiv 0 \pmod{\phi(n)}}$

Th 2. If r is the smallest primitive root of n and $r^h \equiv a \pmod n$ then $h \equiv \text{ind}\, a \pmod{\phi(n)}$

Sol Given r is the smallest primitive root of n

$\Rightarrow r^h \equiv a \pmod n$

$\Rightarrow r^h \equiv r^{\text{ind.}a} \pmod n$ [$\because a \equiv r^{\text{ind}\,a} \pmod n$ by def of ind]

$\Rightarrow r^{h - \text{ind.}a} \equiv 1 \pmod n$

$\Rightarrow \phi(n) \mid h - \text{ind.}a$ [$\because o(r) = \phi(n)$ as $r^{\phi(n)} \equiv 1 \pmod n$]

$\Rightarrow h \equiv \text{ind}\, a \pmod{\phi(n)}$

Th.03 If $a_1, a_2, \cdots, a_k$ are all primes to $n \pmod{\phi(n)}$ then $\text{ind.}a_1 + \text{ind.}a_2 + \cdots + \text{ind}\, a_k \equiv \text{ind.}\, a_1 a_2 a_3 \cdots a_k$.

Proof If r is the smallest primitive root of n, we have

$r^{\text{ind.}a_1} \equiv a_1 \pmod n$

$r^{\text{ind.}a_2} \equiv a_2 \pmod n$

$\vdots$

$r^{\text{ind}\,a_k} \equiv a_k \pmod n$

$r^{\text{ind.}a_1 + \text{ind}\,a_2 + \cdots + \text{ind.}\,a_k} \equiv a_1 \cdot a_2 \cdots a_k \pmod n$

$\Rightarrow \text{ind.}a_1 + \text{ind.}a_2 + \cdots + \text{ind.}a_k \equiv \text{ind.}\, a_1 a_2 \cdots a_k \pmod{\phi(n)}$

[$r^h \equiv a \pmod n$
$\Rightarrow h \equiv \text{ind.}\, a \pmod{\phi(n)}$ Theorem 2]

① Solve the linear congruence : $7x \equiv 2 \pmod 9$ — (1)

$$\phi(9) = 3^2 - 3 = 6$$

We know if i) $(a, n) = 1$

ii) $a^k \not\equiv 1 \pmod n$, $\forall\ k < \phi(n)$

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

then a is called primitive root of n.

Let $a = 2$ then $(2, 9) = 1$

$2^1 \equiv 2 \pmod 9$ $\quad 2^3 \equiv 8 \pmod 9$

$2^2 \equiv 4 \pmod 9$ $\quad 2^4 \equiv 7 \pmod 9$

$2^5 \equiv 5 \pmod 9$

$2^6 \equiv 1 \pmod 9$

∴ 2 is primitive root of 9.

Now, Taking ind. of both sides of (1), we get

$\text{Ind}.7 + \text{Index}_2 x \equiv \text{Index}\, 2 \pmod{\phi(9)}$

$\text{Ind}\,7 + \text{Ind}_2 x \equiv \text{Ind}\, 2 \pmod 6$

$4 + \text{Ind}_2 x \equiv 1 \pmod 6$ $\quad [\because \text{Ind}.7 = 4,\ \text{Ind}\,2 = 1]$

$\text{Ind}_2 x \equiv -3 \pmod 6$

$\text{Ind}_2 x \equiv (-3 + 6k) \bmod 6$

$\Rightarrow \text{Ind}_2 x \equiv 3 \pmod 6$

$\therefore \quad x = 2^3 \pmod 9$

$x = 8 \pmod 9$ Ans..

① $\text{Ind}_2 x \equiv 5 \pmod{36}$

$\Rightarrow x \equiv 2^5 \pmod{37} \Rightarrow \boxed{x \equiv 32 \pmod{37}}$

② $\text{Ind}_2 x \equiv 14 \pmod{36}$

$\Rightarrow x \equiv 2^{14} \pmod{37}$

$\boxed{x \equiv 30 \pmod{37}}$

③ $\text{Ind}_2 x \equiv 23 \pmod{36}$

$\Rightarrow x \equiv 2^{23} \pmod{37}$

$\boxed{x \equiv 5 \pmod{37}}$

④ $\text{Ind}_2 x \equiv 32 \pmod{36}$

$\Rightarrow x \equiv 2^{32} \pmod{37}$

$\boxed{x \equiv 7 \pmod{37}}$

ii Required solutions of $17x^{20} \equiv 19 \pmod{37}$ are

$x \equiv 32, 30, 5, 7 \pmod{37}$.