Monday
30/09/2019

Date
Page

* Unit II : Theory of Congruence *

* Congruent -:

Let N be fixed positive integer, two integers 'a' and 'b' are said to be congruent modulo 'n' written as $a \equiv b \pmod{n}$

e.g. i) $6 \equiv 4 \pmod{2}$

ii) $33 \equiv 3 \pmod{10}$

iii) $17 \equiv -3 \pmod{20}$

* Incongruent -:

'a' is incongruent to 'b' modulo n. If 'n' dose not divide a-b i.e $n \nmid a-b$ then we say that a is incongruent to b mod n.

In this case we write $a \not\equiv b \pmod{n}$.

e.g. i) $2 \not\equiv -5 \pmod{3}$

ii) $75 \not\equiv 8 \pmod{11}$

* Note -:

① Any two integers are congruent modulo n = 1.

② Any two numbers 'a' and 'b' congruent modulo n = 2 if 'a' and 'b' both are even or odd

* Theorem -:

For arbitory integers 'a' and 'b', $a \equiv b \pmod{n}$ iff 'a' and 'b' leaves the same non-negative remainder when divided by n.

Proof:

Firstly suppose that $a \equiv b \pmod{n}$

i.e $n \mid a-b$

i.e $a-b = nk$; $k \in \mathbb{Z}$.

$\Rightarrow \quad a = b + nk \quad \text{--- (1)}$

Let 'r' be the remainder obtained when 'n' is divided by 'b' i-e $n|b$.

Then by division algorithm,

$$b = nq + r \quad ; \quad 0 \le r < n \quad \text{--- (2)}$$

Which indicates that 'b' leaves the non-negative remainder 'r'.

Substituting eqⁿ (2) in eqⁿ (1),

$$a = (nq + r) + nk$$

$$a = nq + r + nk$$

$$a = (q + k)n + r$$

That means 'a' leaves the same remainder 'r' which is non-negative

conversely,

Suppose that 'a' and 'b' leaves the same remainder 'r' when divided by 'n'.

i.e $\quad a = nq_1 + r \quad ; \quad 0 \le r < n$

$\quad\quad b = nq_2 + r \quad ; \quad 0 \le r < n$

$\therefore \quad a - b = n(q_1 - q_2)$

$\Rightarrow \quad n | a - b$

$\Rightarrow \quad a \equiv b \pmod{n}$

Hence the proof.

Ex. Consider 5 and 9 on dividing by 4.

$\rightarrow \quad 5 \equiv 1 \pmod 4$

$\quad\quad 9 \equiv 1 \pmod 4$

$\Rightarrow \quad 5 \equiv 9 \pmod 4$.

Ex. Consider -56 and -11 on dividing by 9.

$\rightarrow \quad -56 \equiv -2 \pmod 9$

$\quad\quad -11 \equiv -2 \pmod 9$

$\Rightarrow \quad -56 \equiv -11 \pmod 9$.

Date
Page

* Theorem -:

Let $n>1$ be fixed and a, b, c, d be arbitary integers then the following properties hold:

a) $a \equiv a \pmod n$

b) If $a \equiv b \pmod n$ then $b \equiv a \pmod n$

c) If $a \equiv b \pmod n$ and $b \equiv c \pmod n$ then $a \equiv c \pmod n$.

d) If $a \equiv b \pmod n$ and $c \equiv d \pmod n$ then $a+c \equiv b+d \pmod n$ and $ac \equiv bd \pmod n$.

e) If $a \equiv b \pmod n$ then $a+c \equiv b+c \pmod n$ and $ac \equiv bc \pmod n$

f) If $a \equiv b \pmod n$ then $a^k \equiv b^k \pmod n$ for any integer k.

Proof:

a) $n \mid 0$; $n>1$

$\Rightarrow n \mid a-a$

$\Rightarrow a \equiv a \pmod n$.

b) $a \equiv b \pmod n$

$\Rightarrow n \mid a-b$

$\Rightarrow a-b = nk$; $k \in \mathbb{Z}$

$\Rightarrow b-a = -nk$

$\Rightarrow b-a = n(-k)$; $-k \in \mathbb{Z}$

$\Rightarrow n \mid b-a$

$\Rightarrow b \equiv a \pmod n$.

c) Here $a \equiv b \pmod n$ and $b \equiv c \pmod n$.

$\Rightarrow n \mid a-b$ and $n \mid b-c$

$\Rightarrow n \mid a-b+b-c$

$\Rightarrow n \mid a-c$

$\Rightarrow a \equiv c \pmod n$.

d) suppose $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$

$\Rightarrow n \mid a-b$ and $n \mid c-d$

Then $\exists$ integers 'r' and 's' such that.

$a-b = nr$ and $c-d = ns$.

consider,

$$(a+c)-(b+d) = a+c-b-d$$
$$= (a-b)+(c-d)$$
$$= nr+ns$$
$$= n(r+s)$$

$\Rightarrow n \mid (a+c)-(b+d)$

$\Rightarrow a+c \equiv b+d \pmod{n}$

and

suppose $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$

$\Rightarrow n \mid a-b$ and $n \mid c-d$

Then $\exists$ integers 'r' and 's' such that,

$a-b = nr$ and $c-d = ns$.

consider,

$$ac-bd = ac-bc+bc-bd$$
$$= c(a-b)+b(c-d)$$
$$= c \cdot nr + b \cdot ns$$
$$= n(cr+bs)$$
$$= n(rc+sb)$$

$\Rightarrow n \mid ac-bd$.

$\Rightarrow ac \equiv bd \pmod{n}$.

e) suppose $a \equiv b \pmod{n}$ and from case (a)

$c \equiv c \pmod{n}$ always hold.

& from (d),

$a+c \equiv b+d \pmod{n}$

and $ac = bd \pmod{n}$.

f) Here $a \equiv b \pmod{n}$

$\Rightarrow n \mid a-b$

If 'k' is any positive integer then we know that $a^k - b^k = (a-b)(a^{k-1} + a^{k-2}b + \cdots + b^{k-1})$

since $n \mid a-b$

we have $n \mid (a-b)(a^{k-1} + a^{k-2}b + \cdots + b^{k-1})$

Ex. Show that $41 \mid 2^{20} - 1$.

→ Here, We have to show that $2^{20} \equiv 1 \pmod{41}$

$\therefore 2^5 \equiv -9 \pmod{41}$

$(2^5)^4 \equiv (-9)^4 \pmod{41}$

$\Rightarrow 2^{20} \equiv (-9)^2 \times (-9)^2 \pmod{41}$

$2^{20} \equiv 81 \cdot 81 \pmod{41}$

$2^{20} \equiv (-1)(-1) \pmod{41}$

$2^{20} \equiv 1 \pmod{41}$

$\Rightarrow 41 \mid 2^{20} - 1$

Ex. Find the remainder obtained by dividing $1! + 2! + 3! + \cdots + 100!$ by 12.

→ We have, $1! \equiv 1 \pmod{12}$

$2! \equiv 2 \pmod{12}$

$3! \equiv 6 \pmod{12}$

$4! \equiv 0 \pmod{12}$

$\vdots$

$100! \equiv 0 \pmod{12}$

$\therefore 1! + 2! + 3! + \cdots + 100! \equiv (1+2+6+0+\cdots+0) \pmod{12}$

i.e. $1! + 2! + 3! + \cdots + 100! \equiv 9 \pmod{12}$

$\therefore$ 9 is the required remainder

Ex. What is the remainder when the following sum is divided by 4.

$1^5 + 2^5 + 3^5 + 4^5 + \cdots + 100^5$.

$1^5 \equiv 1 \pmod 4$
$2^5 \equiv 0 \pmod 4$
$3^5 \equiv 3 \pmod 4$
$4^5 \equiv 0 \pmod 4$
$5^5 \equiv 1 \pmod 4$
$6^5 \equiv 0 \pmod 4$
$7^5 \equiv 3 \pmod 4$
$8^5 \equiv 0 \pmod 4$
$\vdots$
$100^5 \equiv 0 \pmod 4$

$\therefore\ 1^5+2^5+3^5+4^5+5^5+6^5+7^5+8^5+\cdots+100^5 \equiv$
$1+0+3+0+1+0+3+0+\cdots+0 \pmod 4$

$\therefore\ 1^5+2^5+3^5+4^5+5^5+6^5+7^5+8^5+\cdots+100^5$
$\equiv 100 \pmod 4$

$\therefore\ 1^5+2^5+3^5+\cdots+100^5 \equiv 0 \pmod 4$

* Remark-:

If $a \equiv b \pmod n$ then $ac \equiv bc \pmod n$ for any $c \in \mathbb{Z}$.

e.g. i) $5\cdot 2 \equiv 6 \cdot 2 \pmod 2$
$\Rightarrow 5 \not\equiv 6 \pmod 2$

ii) $5 \cdot 3 \equiv 4 \cdot 3 \pmod 3$
$\Rightarrow 5 \not\equiv 4 \pmod 3$

* Theorem-:

If $ac \equiv bc \pmod n$ then $a \equiv b \pmod{n/d}$ where $d = \gcd(c, n)$.

Proof:

We have, $ac \equiv bc \pmod n$
$\Rightarrow n \mid ac - bc$
$\Rightarrow ac - bc = nk \quad \text{--- } k \in \mathbb{Z}$
$\text{———} \ (1)$

since $d = \gcd(c, n)$

$\Rightarrow d \mid c$ and $d \mid n$

$\exists$ relatively prime integers 'r' and 's' such that $c = dr$ and $n = ds$.

From ①,

$$c(a-b) = nk$$

$$dr(a-b) = ds \cdot k$$

$$r(a-b) = sk.$$

$\Rightarrow s \mid r(a-b)$

$\Rightarrow s \mid (a-b)$; $\gcd(r, s) = 1$

$\Rightarrow a \equiv b \pmod{s}$

$\Rightarrow a \equiv b \pmod{n/d}$

Hence the proof.

* Corollary -:

If $ac \equiv bc \pmod{n}$ and $\gcd(c, n) = 1$ then $a \equiv b \pmod{n}$.

Proof:

Here $ac \equiv bc \pmod{n}$

Then by previous theorem,

$$a \equiv b \pmod{n/d}$$

where $\gcd(c, n) = 1$.

i.e. $d = 1$.

$\Rightarrow a \equiv b \pmod{n/1}$

$\therefore a \equiv b \pmod{n}$

Hence the proof.

* Corollary -:

If $ac \equiv bc \pmod{p}$, where p is prime and $p \nmid c$ then $a \equiv b \pmod{p}$

Proof:

Here $ac \equiv bc \pmod{p}$, where p is prime with $p \nmid c$.

i.e. $ac \equiv bc \pmod{p}$ with $\gcd(p, c) = 1$

$\therefore$ By previous corollary,

$a \equiv b \pmod{p}$

Hence the proof.

e.g. i) $33 \equiv 15 \pmod{9}$

$\Rightarrow 3 \cdot 11 \equiv 3 \cdot 5 \pmod{9}$

$\Rightarrow 11 \equiv 5 \pmod{9/3}$

$\Rightarrow 11 \equiv 5 \pmod{3}$

ii) $-35 \equiv 45 \pmod{8}$

$\Rightarrow -7 \times 5 \equiv 9 \times 5 \pmod{8}$

Here $\gcd(5, 8) = 1$

$\Rightarrow -7 \equiv 9 \pmod{8/1}$

$\Rightarrow -7 \equiv 9 \pmod{8}$

* Note-:

① $\gcd(c, n) = n$ then $ac \equiv bc \pmod{n}$

$\Rightarrow a \equiv b \pmod{n}$

Which holds trivially.

② $ab \equiv 0 \pmod{n}$ and $\gcd(a, n) = 1$.

$\Rightarrow b \equiv 0 \pmod{n}$

$ab \equiv a \cdot 0 \pmod{n}$

$\therefore b \equiv 0 \pmod{n}$

③ $ab \equiv 0 \pmod{p}$, where p is prime then either $a \equiv 0 \pmod{p}$ or $b \equiv 0 \pmod{p}$.

Here $ab \equiv 0 \pmod p$

$\Rightarrow p \mid ab$

$\Rightarrow p \mid a$ or $p \mid b$

$\Rightarrow a \equiv 0 \pmod p$ or $b \equiv 0 \pmod p$

(4) Given integer $b > 1$, any positive integer N can be written uniquely in terms of powers of b as,

$$N = a_m b^m + a_{m-1} b^{m-1} + \cdots + a_2 b^2 + a_1 b + a_0$$

Where a_k can be $0, 1, 2, \ldots, b-1$

e.g. i) suppose $b = 3$, $N = 25$

$\therefore 25 = 2 \cdot 3^2 + 2 \cdot 3 + 1$

ii) suppose $b = 2$, $N = 30$

$\therefore 30 = 2^4 + 2^3 + 2 + 2^1$

* Theorem-:

Let $p(x) = \sum_{k=0}^{n} c_k x^k$ be a polynomial function of 'x' with integer coefficient c_k. If $a \equiv b \pmod n$ then $p(a) \equiv p(b) \pmod n$.

Proof:

since $a \equiv b \pmod n$ then

$a^k \equiv b^k \pmod n$ --- $k \in \mathbb{Z}^+$

$\therefore$ For $k = 0, 1, 2, \ldots, n$ we have,

$a^0 \equiv b^0 \pmod n$

i.e. $1 \equiv 1 \pmod n$

$a \equiv b \pmod n$

$a^2 \equiv b^2 \pmod n$

$a^3 \equiv b^3 \pmod n$

$\vdots$

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

$1 + a + a^2 + \cdots + a^n \equiv (1 + b + b^2 + \cdots + b^n) \pmod n$

$$\therefore \sum_{k=0}^{n} a^k \equiv \sum_{k=0}^{n} b^k \pmod n.$$

We know that,

$$a \equiv b \pmod{n}$$

$$\Rightarrow \quad ac \equiv bc \pmod{n}$$

$$\therefore \sum_{k=0}^{n} c_k a^k \equiv \sum_{k=0}^{n} c_k b^k \pmod{n}$$

$$\therefore \quad P(a) \equiv P(b) \pmod{n}$$

Hence the proof.

* Solution of congruence relation -:

If $P(x)$ is polynomial in 'x' with integer coefficient then we say that 'a' is solution of congruence relation.

$P(x) \equiv 0 \pmod{n}$ if $P(a) \equiv 0 \pmod{n}$.

* Corollary -:

If 'a' is solution of $P(x) \equiv 0 \pmod{n}$ and $a \equiv b \pmod{n}$ then $P(b) \equiv 0 \pmod{n}$.
(i.e. 'b' is also solution of $P(x) \equiv 0 \pmod{n}$.)

since, 'a' is solution of $P(x) \equiv 0 \pmod{n}$.

i.e. $P(a) \equiv 0 \pmod{n}$

also we have, $a \equiv b \pmod{n}$

$\therefore$ By using previous theorem,

$$P(a) \equiv P(b) \pmod{n}$$

i.e $P(b) \equiv P(a) \pmod{n}$

$\therefore$ By using transitivity of congruence relation we have,

$$P(b) \equiv 0 \pmod{n}$$

i.e 'b' is solution of $P(x) \equiv 0 \pmod{n}$

Que. If $a \equiv 1 \pmod{2^4}$ then
i) $\gcd(a, 2^4) = 16$
ii) $\gcd(a, 2^4) = 4$
iii) $\gcd(a, 2^4) = 2$
iv) $\gcd(a, 2^4) = 1$

→ We know that;

$$\gcd(a, n) = \gcd(b, n)$$

$\therefore \quad a = a, \ n = 2^4, \ b = 1$

$\therefore \quad \gcd(a, 2^4) = \gcd(1, 2^4)$

Here $\gcd(1, 2^4) = 1$

$\therefore \quad \gcd(a, 2^4) = 1.$

Ex: If $a \equiv b \pmod{n}$ then prove that $\gcd(a, n) = \gcd(b, n)$.

→ We have $a \equiv b \pmod{n}$

$\Rightarrow \quad n \mid a-b$

Let us suppose that,

$d_1 = \gcd(a, n)$

and $d_2 = \gcd(b, n)$

$\Rightarrow \quad d_1 \mid a, \ d_1 \mid n$ and $d_2 \mid b, \ d_2 \mid n$.

$\Rightarrow \quad d_1 \mid n$ and $n \mid a-b$

$\Rightarrow \quad d_1 \mid a-b$ and $d_1 \mid a$

$\Rightarrow \quad d_1 \mid a-(a-b)$

$\Rightarrow \quad d_1 \mid b$

$\Rightarrow \quad d_1 \mid b$ and $d_1 \mid n$.

$\Rightarrow \quad d_1 \leq d_2 \quad \text{---} ①$

Now,

$d_2 | a-b$ and $d_2 | b$

$\Rightarrow d_2 | a-b+b$

$\Rightarrow d_2 | a$

$\therefore d_2 | a$ and $d_2 | n$

$\Rightarrow d_2 \leq d_1 \quad \text{---} ②$

From ① and ②, we have,

$d_1 = d_2$

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

Hence the proof.

Ex. Give an example to show that $a^2 \equiv b^2 \pmod{n}$ need not imply $a \equiv b \pmod{n}$.

→ i) $3^2 \equiv 2^2 \pmod{5}$

$3 \not\equiv 2 \pmod{5}$

ii) $4^2 \equiv 5^2 \pmod{9}$

$4 \not\equiv 5 \pmod{9}$

Ex. Find the remainder when 2^{50} is divided by 7.

→ $2^3 \equiv 1 \pmod{7}$

$\Rightarrow (2^3)^{16} \equiv 1^{16} \pmod{7}$

$\Rightarrow 2^{48} \equiv 1 \pmod{7}$

$\Rightarrow 2^{48} \cdot 2^2 \equiv 1 \cdot 2^2 \pmod{7}$

$\Rightarrow 2^{50} \equiv 4 \pmod{7}$

$\therefore$ remainder $= 4$.

Ex. Find the remainder when 41^{65} is divided by 7.

→ $41 \equiv (-1) \pmod{7}$

$\Rightarrow (41)^{65} \equiv (-1)^{65} \pmod{7}$

$\Rightarrow 41^{65} \equiv (-1) \pmod{7}$

$\Rightarrow 41^{65} \equiv 6 \pmod{7}$

$\therefore$ remainder $= 6$.

Ex. Find the remainder when 4444^{4444} is divided by 9.

→ Now,

$$1111 \equiv 9\times 123 + 4 \pmod 9$$
$$1111 \equiv 4 \pmod 9$$
$$4444 \equiv 16 \pmod 9$$
$$4444 \equiv -2 \pmod 9$$
$$4444^{4444} \equiv (-2)^{4444} \pmod 9$$
$$\equiv 2^{4444} \pmod 9$$

$$1111 \equiv 9\times 123+4 \pmod 9$$
$$2^{1111} \equiv 2^{9\times 123+4} \pmod 9$$
$$\equiv 2^{9\times 123}\cdot 2^4 \pmod 9$$
$$\equiv (2^9)^{123}\cdot 2^4 \pmod 9$$
$$\equiv [(2^3)^3]^{123}\cdot 2^4 \pmod 9$$
$$\equiv [(-1)^3]^{123}\cdot 2^4 \pmod 9$$
$$\equiv -2^4 \pmod 9$$
$$2^{1111} \equiv 2 \pmod 9$$
$$2^{4444} \equiv 2^4 \pmod 9$$
$$\equiv -2 \pmod 9$$
$$2^{4444} \equiv 7 \pmod 9$$

∴ Remainder $= 7$

Ex. Find the last two digits of the number 9^{9^9}.

→ Here gcd $(9, 10) = 1$

∴ By using Euler's theorem,

$$9^{\phi(10)} \equiv 1 \pmod{10}$$
$$9^4 \equiv 1 \pmod{10}$$
$$(9^4)^2 \equiv 1^2 \pmod{10}$$
$$9^8 \equiv 1 \pmod{10}$$
$$9^8\cdot 9 \equiv 1\cdot 9 \pmod{10}$$
$$\Rightarrow 9^9 \equiv 9 \pmod{10} \Rightarrow 10 \mid 9^9 - 9$$
$$\Rightarrow 9^9 - 9 = 10\cdot k \quad ; k \in \mathbb{Z}.$$

$\Rightarrow \quad 9^9 = 10k + 9$

$\Rightarrow \quad 9^{9^9} = 9^{10k+9}$

We have,

$$9^3 \equiv 29 \pmod{100}$$
$$(9^3)^3 \equiv (29)^3 \pmod{100}$$
$$9^9 \equiv (29)^3 \pmod{100}$$
$$9^9 \equiv (29)^2 \cdot 29 \pmod{100}$$
$$9^9 \equiv 41 \cdot 29 \pmod{100}$$
$$\equiv 1189 \pmod{100}$$
$$9^9 \equiv 89 \pmod{100}$$
$$9^{10} \equiv 9(89) \pmod{100}$$
$$9^{10} \equiv 801 \pmod{100}$$
$$9^{10} \equiv 1 \pmod{100}$$
$$(9^{10})^k \equiv 1^k \pmod{100}$$
$$9^{10k} \equiv 1 \pmod{100}$$
$$9^{10k} \cdot 9^9 \equiv 9^9 \pmod{100}$$
$$9^{10k+9} \equiv 9^9 \pmod{100}$$

$$9^{9^9} \equiv 89 \pmod{100}$$

Hence last two digits are 89.

* Theorem :-

If $a_m 10^m + a_{m-1} 10^{m-1} + \cdots + a_1 10 + a_0$ be the decimal expansion of positive integer N. where $0 \le a_k < 10$. Let $s = a_0 + a_1 + \cdots + a_m$ then $9 \mid N$ if and only if $9 \mid s$

Proof:

Consider a polynomial, $p(x) = \sum_{k=0}^{n} a_k x$ with integer coefficient.

Let $10 \equiv 1 \pmod 9$

$$\therefore P(10) \equiv P(1) \pmod 9$$
$$\sum_{k=0}^{n} a_k 10^k \equiv \sum_{k=0}^{n} a_k 1^k \pmod 9$$
$$\therefore \sum_{k=0}^{n} a_k 10^k \equiv \sum_{k=0}^{n} a_k \pmod 9$$

$\therefore (a_0 + a_1 10 + a_2 10^2 + \cdots + a_n 10^n) \equiv (a_0 + a_1 + a_2 + \cdots + a_n) \pmod 9$

i.e. $N \equiv s \pmod 9$

Now suppose $9 \mid N$

$$N \equiv 0 \pmod 9$$

Date
Page

$\Rightarrow \quad S \equiv 0 \pmod 9$

$\Rightarrow \quad 9 \mid S$

conversely,

suppose that $9 \mid S$

$$S \equiv 0 \pmod 9$$

$$\Rightarrow N \equiv 0 \pmod 9$$

$$\Rightarrow 9 \mid N.$$

* Theorem -:

If $N = a_m 10^m + a_{m-1} 10^{m-1} + \cdots + a_1 \cdot 10 + a_0$ be the decimal expansion of positive integer N where $0 \leq a_k \leq 10$ and let $T = a_0 - a_1 + a_2 - a_3 + \cdots + (-1)^m a_m$ then $11 \mid N$ iff $11 \mid T$.

Proof:

Consider the polynomial $P(x) = \sum_{k=0}^{n} a_k x^k$ with integer coefficients.

We see that, $10 \equiv -1 \pmod{11}$

By above theorem,

$$P(10) \equiv P(-1) \pmod{11}$$

$$\Rightarrow \sum_{k=0}^{m} a_k 10^k \equiv \sum_{k=0}^{m} a_k (-1)^k \pmod{11}$$

$$\Rightarrow a_0 + a_1 \cdot 10 + \cdots + a_m 10^m \equiv a_0 - a_1 + a_2 - a_3) + \cdots + (-1)^m a_m. \pmod{11}$$

$$\Rightarrow N \equiv T \pmod{11} \quad \text{--- (1)}$$

suppose $11 \mid N$

$$\Leftrightarrow N \equiv 0 \pmod{11} \quad \text{--- (2)}$$

Form (1) and (2),

$$T \equiv 0 \pmod{11}$$

$$\Leftrightarrow 11 \mid T$$

Hence $11 \mid N$ iff $11 \mid T$.

Tuesday
01/10/2019

* Linear Congruences -:

A linear congruence is a congruence relation of the form $ax \equiv b \pmod{n}$.

* Theorem -:

The linear congroence $ax \equiv b \pmod{n}$ has a solution iff $d \mid b$ where $d = \gcd(a,n)$. If $d \mid b$ then it has 'd' mutually incongruent solutions modulo 'n'.

Proof:

Consider the linear congruence $ax \equiv b \pmod{n}$ which is equivalent to diophantine equation

$ax - ny = b$ —— ① ; 'y' is an integer.

We know that, eq^n ① has solution iff

$\gcd(a,-n) \equiv \gcd(a,n) \mid b$

i.e. $d \mid b$: where $d = \gcd(a,n)$

suppose $ax \equiv b \pmod{n}$ is solvable and (x_0, y_0) is particular solution of eq^n ①. Then general solution of eq^n ① is,

$$x = x_0 + \left(\frac{-n}{d}\right)t, \quad y = y_0 - \frac{a}{d}t.$$

Where 't' is arbitory integer.

Let us consider the following 'd' solutions,

$$x_0,\ x_0 + \frac{n}{d},\ x_0 + \frac{2n}{d},\ ---,\ x_0 + \frac{(d-1)n}{d}$$

Claim - These 'd' solutions are incongruent modulo 'n' and any other solutions is congruent to one of these 'd' solutions.

Let if possible,

$$x_0 + \frac{n}{d}t_1 \equiv x_0 + \frac{n}{d}t_2 \pmod{n} ;\ 0 \le t_1 < t_2 < d$$

$$\frac{n}{d}t_1 \equiv \frac{n}{d}t_2 \pmod{n} \; ; \; \gcd\left(n, \frac{n}{d}\right) = \frac{n}{d}$$

$$t_1 \equiv t_2 \left(\bmod\, n/\tfrac{n}{d}\right)$$

$$t_1 \equiv t_2 \pmod{d}$$

Which is impossible

Hence $x_0, x_0+\frac{n}{d}, x_0+\frac{2n}{d}, \dots, x_0+\frac{(d-1)n}{d}$ are

incongruent modulo 'n'.

Let $x_0+\frac{n}{d}t$ be any solution of $ax \equiv b \pmod{n}$

then by division algorithm we have,

$$t = dq + r \quad ; \quad 0 \leq r < d$$

$$\therefore x_0 + \frac{n}{d}t = x_0 + \frac{n}{d}(dq+r)$$

$$= x_0 + \frac{n}{d}r + nq \pmod{n}$$

$$\therefore x_0 + \frac{n}{d}t \equiv x_0 + \frac{n}{d}r \pmod{n} \quad ; \; 0 \leq r < d$$

Hence the proof.

* Corollary :-

If $\gcd(a,n) = 1$ then the linear congruence $ax \equiv b \pmod{n}$ has a unique sol^n modulo 'n'

Ex. Find all solutions of $7x \equiv 1 \pmod{11}$

→ Let $7x \equiv 1 \pmod{11}$ —— ①

Now comparing given linear congruence relation with $ax \equiv b \pmod{n}$

$\therefore \; a = 7, \; b = 1$ and $n = 11$.

$\therefore \; \gcd(a,n) = \gcd(7,11) = 1$

Here $1 \mid b$.

② $7x \equiv 4 \pmod{28}$ ⑤ $3x \equiv 21 \pmod{30}$

③ $6x \equiv 15 \pmod{21}$

④ $9x \equiv 3 \pmod{10}$

$\therefore$ Eqⁿ ① has exactly one solution modulo 11.

From ①, $11 \mid 7x - 1$

$\Rightarrow 11 \mid (7 \times 8) - 1$

$\Rightarrow x_0 = 8$

Which is required solution.

<u>Ex.</u> Find all solutions of $5x \equiv 2 \pmod{26}$.

$\rightarrow$ Let $5x \equiv 2 \pmod{26}$ —①

Now, comparing given linear congruence relation with $ax \equiv b \pmod{n}$.

$\therefore a = 5,\ b = 2$ and $n = 26$

$\therefore \gcd(a, n) = \gcd(5, 26) = 1$.

Here $1 \mid b$

$\therefore$ Eqⁿ ① has exactly one solution modulo 26

From ①, $26 \mid 5x - 2$

$\Rightarrow 26 \mid (5 \times 16) - 2$

$\Rightarrow x_0 = 16$.

Which is required solution.

<u>Ex.</u> Find all solutions of $18x \equiv 30 \pmod{42}$

$\rightarrow$ Let $18x \equiv 30 \pmod{42}$ —①

Now, comparing given linear congruence relation with $ax \equiv b \pmod{n}$.

$\therefore a = 18,\ b = 30$ and $n = 42$.

$\therefore \gcd(a, n) = \gcd(18, 42) = 6$.

Here $6 \mid b \Rightarrow 6 \mid 30$

$\Rightarrow \exists$ a solution to the given eqⁿ ①.

Now, we have to find particular solutions

$\therefore 18x \equiv 30 \pmod{42}$

$\Rightarrow 3x \equiv 5 \pmod{7}$ [$\because ac \equiv bc \pmod{n}$ then $a \equiv b \pmod{n/d}$; $(c, n) = d$]

$\Rightarrow 7 \mid 3x - 5$

$\Rightarrow \quad 3x - 5 = 7$

$\Rightarrow \quad 3x = 12$

$\Rightarrow \quad x_0 = 4.$

$\therefore$ The other solutions are given by,

Here $x_0 = 4, \quad d = 16, \quad t = 0, 1, 2, 3, 4, 5.$

Now, $x_1 = x_0 + \frac{n}{d} t = 4 + \frac{42}{6} = 11$

$$x_2 = x_0 + \frac{2n}{d} t = 4 + 2 \cdot \frac{42}{6} = 18$$

$$x_3 = x_0 + \frac{3n}{d} t = 4 + 3 \cdot \frac{42}{6} = 25$$

$$x_4 = x_0 + \frac{4n}{d} t = 4 + 4 \cdot \frac{42}{6} = 32$$

$$x_5 = x_0 + \frac{5n}{d} t = 4 + 5 \cdot \frac{42}{6} = 39.$$

Ex. Find all solutions of $7x \equiv 4 \pmod{28}$

$\rightarrow$ Let $7x \equiv 4 \pmod{28}$ ——— ①

Now, comparing given linear congruence relation with $ax \equiv b \pmod{n}$

$\therefore \quad a = 7, \quad b = 4$ and $n = 28.$

$\therefore \quad \gcd(a, n) = \gcd(7, 28) = 7$

Here $7 \nmid 4$

$\therefore$ Given congruence relation has no solution.

Ex. Find all solutions of $6x \equiv 15 \pmod{21}$

$\rightarrow$ Let $6x \equiv 15 \pmod{21}$ ——— ①

Now, comparing given linear congruence relation with $ax \equiv b \pmod{n}$

$\therefore \quad a = 6, \quad b = 15$ and $n = 21.$

$\therefore \quad \gcd(a, n) = \gcd(6, 21)$

$= 3.$

Here $3 | 15$.

$\therefore$ Eqⁿ ① has exactly one solution. modulo 21.

From ①, $21 | 6x - 15$

$\Rightarrow 21 | (6 \times 20) - 15$

$\Rightarrow x_0 = 20$.

OR

Comparing eqⁿ ① with $ax \equiv b \pmod{n}$

$\therefore a = 6$, $b = 15$ and $n = 21$

$\therefore g(a, n) = \gcd(6, 21) = 3$.

Here $3 | 21$

$\therefore 6x \equiv 15 \pmod{21}$

$\Rightarrow (3 \cdot 2)x \equiv (3 \cdot 5) \pmod{21}$

$\Rightarrow 2x \equiv 5 \pmod{7}$ —— ⊛

Here $a = 2$, $b = 5$ and $n = 7$

$\therefore \gcd(a, n) = \gcd(2, 7) = 1$

$\therefore 1 | 5$

$\Rightarrow$ Eqⁿ ⊛ has exactly on solⁿ modulo 7.

$\therefore$ From ⊛,

$7 | 2x - 5$

$\Rightarrow 7 | (2 \times 6) - 5$

$\Rightarrow x_0 = 6$

Which is required solution for given congruence relation.

Ex. Find all solutions of $x \equiv 9 \pmod{10}$

→ Let $x \equiv 9 \pmod{10}$ —— ①

Now, comparing given linear congruence relation with $ax \equiv b \pmod{n}$

$\therefore a = 1$, $b = 9$ and $n = 10$.

$\therefore \gcd(a, n) = \gcd(1, 10)$

$= 1$

Here $1 | 9$

$\therefore$ Eqⁿ (1) has exactly one solution modulo 10.

$\therefore$ From (1), $10 \mid x-9$

$\Rightarrow 10 \mid (1\times 19)-9$

$\Rightarrow x_0 = 19$

Which is required solution of congruence relation.

Ex. Find all solutions of $9x \equiv 21 \pmod{30}$

→ Let $9x \equiv 21 \pmod{30}$ —— (1)

Now, comparing given linear congruence relation with $ax \equiv b \pmod{n}$

$\therefore a = 9,\ b = 21$ and $n = 30$

But we can write eqⁿ (1) as,

$9x \equiv 21 \pmod{30}$

$\Rightarrow (3\cdot 3)x \equiv (3\cdot 7) \pmod{30}$

$\Rightarrow 3x \equiv 7 \pmod{10}$ —— (2)

Now, comparing above eqⁿ (2) with $ax \equiv b \pmod{n}$

$\therefore a = 3,\ b = 7$ and $n = 10$

$\therefore \gcd(a, n) = \gcd(3, 10)$

$= 1.$

Here $1 \mid 21$

$\therefore$ Eqⁿ (1) has exactly one solution modulo 30.

$\therefore$ From (1),

$30 \mid 9x - 21$

$\Rightarrow 10 \mid 3x - 7$

$\Rightarrow 10 \mid (3\times 9) - 7$

$\Rightarrow x_0 = 9$

Which is required solution for given congruence relation.

Monday 07/10/2019

* Theorem [Chinese Remainder Theorem]-:

* Statement:

Let $n_1, n_2, n_3, \ldots, n_r$ be positive integers such that $\gcd(n_i, n_j) = 1$ for $i \neq j$. Then the system of linear congruences,

$$x \equiv a_1 \pmod{n_1}$$
$$x \equiv a_2 \pmod{n_2}$$
$$\vdots$$
$$x \equiv a_r \pmod{n_r}$$

has unique solution with respect to multiplication modulo $n_1 n_2 n_3 \cdots n_r$.

Let $\overline{x}$ is solution of congruences then,

$$\overline{x} = [a_1 N_1 N_1^{-1} \pmod{n_1} + a_2 N_2 N_2^{-1} \pmod{n_2} + \cdots + a_r N_r N_r^{-1} \pmod{n_r}] \pmod{n}$$

where $n = n_1 \cdot n_2 \cdot n_3 \cdots n_r$ and $N_K = \frac{n}{n_K}$; $K = 1, 2, 3, \ldots, r$

Proof:

Let $n = n_1 n_2 n_3 \cdots n_r$ and

For each $K = 1, 2, 3, \ldots, r$.

$$N_K = \frac{n}{n_K}$$
$$= \frac{n_1 n_2 n_3 \cdots n_{K-1} n_K n_{K+1} \cdots n_r}{n_K}$$
$$= n_1 n_2 n_3 \cdots n_{K-1} \cdot n_{K+1} \cdots n_r.$$

By hypothesis, $\gcd(n_i, n_K) = 1$; $i \neq K$

$\therefore \gcd(n_K, N_K) = 1$

$\therefore$ It is possible to solve linear congruence

$$N_K x \equiv 1 \pmod{n_K} \quad \text{--- (1)}$$

and it has unique solution say x_K.

Claim - $\overline{x} = a_1 N_1 x_1 + a_2 N_2 x_2 + a_3 N_3 x_3 + \cdots + a_r N_r x_r$.

is the required simultaneous solution of given system.

Clearly, $N_i \equiv 0 \pmod{n_k}$; $i \neq k$
because $N_i = n_1 n_2 n_3 \cdots n_{i-1} n_{i+1} \cdots n_r$.

$\Rightarrow \quad a_i N_i x_i \equiv 0 \pmod{n_k}$; $i \neq k$.

$\Rightarrow \quad \sum_{i=1}^{r} a_i N_i x_i \equiv 0 \pmod{n_k}$; $i \neq k$

$\Rightarrow \quad \sum_{i=1}^{r} a_i N_i x_i - a_k N_k x_k \equiv 0 \pmod{n_k}$

$\Rightarrow \quad \sum_{i=1}^{r} a_i N_i x_i \equiv a_k N_k x_k \pmod{n_k}$

$\Rightarrow \quad \sum_{i=1}^{r} a_i N_i x_i \equiv a_k \pmod{n_k}$

$\Rightarrow \quad \bar{x} \equiv a_k \pmod{n_k}$; $k = 1, 2, \ldots, r$.

Thus, $\bar{x}$ is the simultaneous solution of the given system.

Uniqueness:

Suppose $\bar{x}'$ is any other solution of the given system.

$\therefore \quad \bar{x}' \equiv a_k \pmod{n_k}$ and also we have
$\bar{x} \equiv a_k \pmod{n_k}$

$\therefore$ By transitivity of congruence relation we have,

$$\bar{x}' \equiv \bar{x} \pmod{n_k}$$

$\Rightarrow \quad n_k \mid \bar{x}' - \bar{x}$; $k = 1, 2, 3, \ldots, r$.

$\Rightarrow \quad n_1 n_2 n_3 \cdots n_r \mid \bar{x}' - \bar{x}$; $(n_i, n_j) = 1$, $i \neq j$

$\Rightarrow \quad n \mid \bar{x}' - \bar{x}$

$\Rightarrow \quad \bar{x}' \equiv \bar{x} \pmod{n}$

Hence the uniqueness.

Ex. Solve $x \equiv 1 \pmod 3$, $x \equiv 2 \pmod 4$, $x \equiv 3 \pmod 5$

$\rightarrow$ Here $a_1 = 1$, $a_2 = 2$, $a_3 = 3$ and
$n_1 = 3$, $n_2 = 4$, $n_3 = 5$.

$\therefore \quad n = n_1 \cdot n_2 \cdot n_3 = 3 \times 4 \times 5 = 60$.

Now,

$$N_1 = \frac{n}{n_1} = \frac{60}{3} = 20$$

$$N_2 = \frac{n}{n_2} = \frac{60}{4} = 15$$

$$N_3 = \frac{n}{n_3} = \frac{60}{5} = 12.$$

$\therefore$ Solution of given system of congruences,

$$\bar{x} = [a_1 N_1 N_1^{-1} (\text{mod } n_1) + a_2 N_2 N_2^{-1} (\text{mod } n_2) + a_3 N_3 N_3^{-1} (\text{mod } n_3)] \ (\text{mod } n)$$

$$= [1 \cdot 20 \cdot 20^{-1} (\text{mod } 3) + 2 \cdot 15 \cdot 15^{-1} (\text{mod } 4) + 3 \cdot 12 \cdot 12^{-1} (\text{mod } 5)] \ (\text{mod } 60)$$

$$= [1 \cdot 20 \cdot 2^{-1} (\text{mod } 3) + 2 \cdot 15 \cdot 3^{-1} (\text{mod } 4) + 3 \cdot 12 \cdot 2^{-1} (\text{mod } 5)] \ (\text{mod } 60)$$

$$= [20 \times 2 + 30 \times 3 + 36 \times 3] \ (\text{mod } 60)$$

$$= [40 + 90 + 108] \ (\text{mod } 60)$$

$$= 238 \ (\text{mod } 60)$$

$$\bar{x} = 58 \ (\text{mod } 60)$$

Ex. Solve $x \equiv 5 (\text{mod } 6)$, $x \equiv 4 (\text{mod } 11)$, $x \equiv 3 (\text{mod } 17)$

$\rightarrow$ Here $a_1 = 5$, $a_2 = 4$, $a_3 = 3$ and

$n_1 = 6$, $n_2 = 11$, $n_3 = 17$.

$$\therefore \ n = n_1 \cdot n_2 \cdot n_3$$

$$= 6 \times 11 \times 17$$

$$= 1122$$

Now,

$$N_1 = \frac{n}{n_1} = \frac{1122}{6} = 187$$

$$N_2 = \frac{n}{n_2} = \frac{1122}{11} = 102$$

$$N_3 = \frac{n}{n_3} = \frac{1122}{17} = 66.$$

$\therefore$ Solution of given system of congruences,

$\bar{x} = [a_1 N_1 N_1^{-1} (\text{mod } n_1) + a_2 N_2 N_2^{-1} (\text{mod } n_2) + a_3 N_3 N_3^{-1} (\text{mod } n_3)] \ (\text{mod } n)$

$= [5 \cdot 187 \cdot 187^{-1} (\text{mod } 6) + 4 \cdot 102 \cdot 102^{-1} (\text{mod } 11) + 3 \cdot 66 \cdot 66^{-1} (\text{mod } 17)] \ (\text{mod } 1122)$

$= [5 \cdot 187 \cdot 1^{-1} (\text{mod } 6) + 4 \cdot 102 \cdot 3^{-1} (\text{mod } 11) + 3 \cdot 66 \cdot 15^{-1} (\text{mod } 17)] \ (\text{mod } 1122)$

$= [935 \times 7 + 408 \times 4 + 198 \times 8] \ (\text{mod } 1122)$

$= [6545 + 1632 + 1584] \ (\text{mod } 1122)$

$= 9761 \ (\text{mod } 1122)$

$\bar{x} = 785 \ (\text{mod } 1122)$

Ex. $2x \equiv 1 (\text{mod } 3)$, $2x \equiv 2 (\text{mod } 4)$, $x \equiv 3 (\text{mod } 5)$.

$\rightarrow$ Here, $2x \equiv 1 (\text{mod } 3)$

$\Rightarrow x \equiv 2^{-1} (\text{mod } 3)$

$\Rightarrow x \equiv 2 (\text{mod } 3)$ —— ①

and $2x \equiv 2 (\text{mod } 4)$

$\Rightarrow x \equiv 1 (\text{mod } 4/2)$

$\Rightarrow x \equiv 1 (\text{mod } 2)$ —— ②

and $x \equiv 3 (\text{mod } 5)$ —— ③

$\therefore$ Required system of congruence is,

$x \equiv 2 (\text{mod } 3)$, $x \equiv 1 (\text{mod } 2)$, $x \equiv 3 (\text{mod } 5)$

Here $a_1 = 2$, $a_2 = 1$, $a_3 = 3$ and

$n_1 = 3$, $n_2 = 2$, $n_3 = 5$.

$\therefore n = n_1 \cdot n_2 \cdot n_3$

$= 3 \times 2 \times 5$

$= 30$.

Now, $N_1 = \frac{n}{n_1} = \frac{30}{3} = 10$

$N_2 = \frac{n}{n_2} = \frac{30}{2} = 15$

$N_3 = \frac{n}{n_3} = \frac{30}{5} = 6$.

$\therefore$ Solution of given system of congruences,

$\bar{x} = [a_1 N_1 N_1^{-1} (\text{mod } n_1) + a_2 N_2 N_2^{-1} (\text{mod } n_2) + a_3 N_3 N_3^{-1} (\text{mod } n_3)] \; (\text{mod } n)$

$= [2 \cdot 10 \cdot 10^{-1} (\text{mod } 3) + 1 \cdot 15 \cdot 15^{-1} (\text{mod } 2) + 3 \cdot 6 \cdot 6^{-1} (\text{mod } 5)] \; (\text{mod } 30)$

$= [2 \cdot 10 \cdot 1^{-1} (\text{mod } 3) + 1 \cdot 15 \cdot 1^{-1} (\text{mod } 2) + 3 \cdot 6 \cdot 1^{-1} (\text{mod } 5)] \; (\text{mod } 30)$

$= [20 \times 4 + 15 \times 3 + 18 \times 6] \; (\text{mod } 30)$

$= [80 + 45 + 108] \; (\text{mod } 30)$

$= 233 \; (\text{mod } 30)$

$\bar{x} = 23 \; (\text{mod } 30)$

* Linear Congruences in two variables -:

The congruences of the form $ax + by \equiv c \; (\text{mod } n)$ are called linear congruences in two variables. such a congruences has solution iff $\gcd(a, b, n) \mid c$.

* Theorem -:

The system of linear congruences $ax + by \equiv r \; (\text{mod } n)$ and $cx + dy \equiv s \; (\text{mod } n)$ has unique solution modulo 'n' if $\gcd(ad - bc, n) = 1$.

Proof:

Here given linear congruences are

$ax + by \equiv r \; (\text{mod } n)$ ——— ① and

$cx + dy \equiv s \; (\text{mod } n)$ ——— ②

Multiply eqⁿ ① by 'd' and eqⁿ ② by 'b' and substracting we get,

$(ad - cb) x \equiv (rd - sb) \; (\text{mod } n)$ ——— ③

since $\gcd(ad - bc, n) = 1$ we have,

$(ad - bc) z \equiv 1 \; (\text{mod } n)$ ——— ④

has unique solution modulo 'n'.

Let 't' be a solution of eq^n ④ then

$(ad-bc)\,t \equiv 1 \pmod{n}$ ⟶ ⑤

Multiplying on both sides of eq^n ③ by 't'

$(ad-bc)\,t x \equiv (rd-sb)\,t \pmod{n}$.

∴ From eq^n ⑤ we have,

$x \equiv (rd-sb)\,t \pmod{n}$

Similarly,

Multiply eq^n ① by 'c' and eq^n ② by 'a' and substracting we get,

$(bc-ad)\,y \equiv (cr-as) \pmod{n}$

$\Rightarrow (ad-bc)\,y \equiv (as-cr) \pmod{n}$

$\Rightarrow y \equiv (as-cr) \pmod{n}$.

Ex: Find the solution of system of congruences

$3x+4y \equiv 5 \pmod{13}$, $2x+5y \equiv 7 \pmod{13}$

→ Here $a=3$, $b=4$, $c=2$, $d=5$, $r=5$, $s=7$, $n=13$

∴ $\gcd(ad-bc, n) = \gcd(15-8, 13)$

$= \gcd(7, 13) = 1$.

∴ Given system has unique solution.

Here, $3x+4y \equiv 5 \pmod{13}$ ⟶ ①

$2x+5y \equiv 7 \pmod{13}$ ⟶ ②

multiply eq^n ① by 5 and eq^n ② by 4 and substracting we get,

$15x - 8x \equiv (25-28) \pmod{13}$

$7x \equiv (-3) \pmod{13}$

$7x \equiv 10 \pmod{13}$

$\Rightarrow x \equiv 7^{-1}\cdot 10 \pmod{13}$

$\Rightarrow x \equiv 2\cdot 10 \pmod{13}$

$\Rightarrow x \equiv 20 \pmod{13}$

$\Rightarrow x \equiv 7 \pmod{13}$

Similarly,

Multiply eq^n (1) by 2 and eq^n (2) by 3 and substracting we get,

$$8y - 15y \equiv (10-21) \pmod{13}$$
$$-7y \equiv -11 \pmod{13}$$
$$7y \equiv 11 \pmod{13}$$
$$\Rightarrow y \equiv 7^{-1} \cdot 11 \pmod{13}$$
$$\Rightarrow y \equiv 2 \cdot 11 \pmod{13}$$
$$\Rightarrow y \equiv 22 \pmod{13}$$
$$\Rightarrow y \equiv 9 \pmod{13}$$

Ex: Find the solution of system of congruences,
$5x + 3y \equiv 1 \pmod 7$, $3x + 2y \equiv 4 \pmod 7$.

→ Here $a=5$, $b=3$, $c=3$, $d=2$, $r=1$, $s=4$, $n=7$.

$\therefore \gcd(ad-bc, n) = \gcd(10-9, 7)$
$= \gcd(1, 7) = 1$.

$\therefore$ Given system has unique solution.

$$5x + 3y \equiv 1 \pmod 7 \quad \text{—— (1)}$$
$$3x + 2y \equiv 4 \pmod 7 \quad \text{—— (2)}$$

multiply eq^n (1) by 2 and eq^n (2) by 3 and substracting we get,

$$10x - 9x \equiv (2-12) \pmod 7$$
$$\Rightarrow x \equiv -10 \pmod 7$$
$$\Rightarrow x \equiv -3 \pmod 7$$
$$\Rightarrow x \equiv 4 \pmod 7$$

Similarly,
multiply eq^n (1) by 3 and eq^n (2) by 5 and subtracting we get,

$$9y - 10y \equiv (3-20) \pmod 7$$
$$\Rightarrow -y \equiv -17 \pmod 7$$
$$\Rightarrow y \equiv 17 \pmod 7$$
$$\Rightarrow y \equiv 3 \pmod 7$$

Date
Page

* Fermat's Theorem-:

* **Statement:**

Let 'p' be a prime and $p \nmid a$ then $a^{p-1} \equiv 1 \pmod p$

Proof:

consider first $(p-1)$ multiples of 'a'. are $a, 2a, 3a, \ldots, (p-1)a$. none of these number is congruent to modulo p, nor is any congruent to zero.

Because $ra \equiv sa \pmod p$; $0 < r < s < p$

since $p \nmid a$

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

$\Rightarrow r \equiv s \pmod p$

$\Rightarrow p \mid r-s$

Which contradicts $0 < r < s < p$.

Which shows that $a, 2a, 3a, \ldots, (p-1)a$ are incongruent modulo p.

Hence $a, 2a, 3a, \ldots, (p-1)a$ leave different remainder when divided by p.

$\therefore a \cdot 2a \cdot 3a \cdots (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \pmod p$.

$[1 \cdot 2 \cdot 3 \cdots (p-1)] a^{p-1} \equiv (p-1)! \pmod p$

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

since $\gcd[(p-1)!, p] = 1$

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

Hence the proof.

* Corollary-:

If 'p' is prime then $a^p \equiv a \pmod p$ for any integer a.

Proof: case ①- $p \nmid a$.

By using Fermat's theorem,

$a^{p-1} \equiv 1 \pmod p$ ←①

also $a \equiv a \pmod p$ —— ②

$\therefore$ From ① and ② we have,

$a^p \equiv a \pmod p$

case ② - $p \mid a$

$\Rightarrow p \mid a^p$

$\therefore p \mid a^p - a$

$\Rightarrow a^p \equiv a \pmod p$

Ex Find the remainder when 5^{38} is divided by 11

→ Here $p = 11$, $a = 5$

$\therefore$ By Fermat's Theorem,

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

$\therefore 5^{11-1} \equiv 1 \pmod{11}$

$\therefore 5^{10} \equiv 1 \pmod{11}$

$\Rightarrow (5^{10})^3 \equiv 1^3 \pmod{11}$

$\Rightarrow 5^{30} \equiv 1 \pmod{11}$ —— ①

Now,

$5^2 \equiv 3 \pmod{11}$

$(5^2)^2 = 3^2 \pmod{11}$

$5^4 \equiv 9 \pmod{11}$

$5^4 \equiv (-2) \pmod{11}$

$(5^4)^2 \equiv (-2)^2 \pmod{11}$

$5^8 \equiv 4 \pmod{11}$ —— ②

multiplying eqⁿ ① and eqⁿ ② we get,

$5^{30} \cdot 5^8 \equiv 4 \cdot 1 \pmod{11}$

$\Rightarrow 5^{38} \equiv 4 \pmod{11}$

Tuesday 08/10/2019

* Euler's ϕ Function-:

A mapping $\phi : \mathbb{N} \to \mathbb{N}$ defined by,

$\phi(n) = \{ x \in \mathbb{N} \mid 1 \leq x \leq n, \ (x, n)_{gcd} = 1 \}$ is called as Euler's ϕ function.

e.g. i) $\phi(1) = \{ x \in \mathbb{N} \mid 1 \leq x \leq 1, \ (x, 1) = 1 \}$

$\Rightarrow |\phi(1)| = 1.$

Tuesday 08/10/2019

Date ____
Page ____

ii) $\phi(2) = \{x \in \mathbb{N} \mid 1 \leq x \leq 2, (x,2)=1\}$
$\Rightarrow |\phi(1)| = 1$

iii) $\phi(3) = \{x \in \mathbb{N} \mid 1 \leq x \leq 3, (x,3)=1\}$
$\Rightarrow |\phi(3)| = 2$, $\phi(3) = \{1, 2\}$

iv) $\phi(4) = \{x \in \mathbb{N} \mid 1 \leq x \leq 4, (x,4)=1\}$
$\Rightarrow |\phi(4)| = \{1, 3\}$ $\therefore$ $\phi(4) = 2$.

* Note-:

① $\phi(p^n) = p^n - p^{n-1} = p^n(1 - 1/p)$; if 'p' is prime

②

$\phi(mn) = \phi(m) \cdot \phi(n)$ if $\gcd(m,n) = 1$.

Ex: If $n = 1000$, find $\phi(n)$

→ Here $\phi(1000) = \phi(10^3) = \phi(5^3 \cdot 2^3)$
$= \phi(5^3) \cdot \phi(2^3)$
$= \phi(5^3 - 5^2) \cdot \phi(2^3 - 2^2)$
$= (125 - 25) \cdot (8 - 4)$
$= 100 \times 4$

$\therefore$ $\phi(1000) = 400$

Ex If $n = 100$, find $\phi(n)$.

→ $\phi(100) = \phi(10^2)$
$= \phi(5^2 \cdot 2^2)$
$= \phi(5^2) \cdot \phi(2^2)$
$= \phi(5^2 - 5) \cdot \phi(2^2 - 2)$
$= (25 - 5) \cdot (4 - 2)$
$= 20 \times 2$
$= 40.$

* Note -:

① How many integers which are relatively prime to zero.
$\Rightarrow$ 1 and -1 i.e. Two integers.

② How many integers which relatively prime to 1.
$\Rightarrow$ Infinite integers.

Ex. Euler's ϕ function is one-one?

→ We observe that,

$\phi(5) = \phi(10) = 4$

But $5 \neq 10$

$\therefore$ ϕ is not one-one.

Ex. Euler's ϕ function is onto?

→ Let $\phi : \mathbb{N} \to \mathbb{N}$ and $x \in \mathbb{N}$ $\exists$ $y \in \mathbb{N}$.

$\therefore$ $\phi(y) = x$

If $n > 2$ then ϕ is always even.

$\phi(1) = 1$

$\phi(2) = 1$

$\therefore$ $\phi(x)$ is not onto.

* Euler's Theorem -:

Let 'n' be a positive integer and $\gcd(a,n)=1$ then $a^{\phi(n)} \equiv 1 \pmod{n}$.

e.g. $n = 10$, $a = 3$.

Here $\gcd(3,10) = 1$

$\therefore$ $3^{\phi(10)} \equiv 1 \pmod{10}$

$\therefore$ $3^4 \equiv 1 \pmod{10}$

Ex. Find last digit of $(133)^{2011}$.

OR

Ex Find the value of $(133)^{2011} \pmod{10}$

→ Let $a = 133$ and $n = 10$

$\therefore$ $\gcd(133, 10) = 1$

$\therefore$ $(133)^{\phi(10)} \equiv 1 \pmod{10}$

$(133)^4 \equiv 1 \pmod{10}$

$[(133)^4]^{502} \equiv 1^{502} \pmod{10}$

$(133)^{2008} \equiv 1 \pmod{10}$ —— (1)

$133 \equiv 3 \pmod{10}$

$\therefore 133^3 \equiv 3^3 \pmod{10}$

$133^3 \equiv 27 \pmod{10}$

$133^3 \equiv 7 \pmod{10}$ —— (2)

From (1) and (2),

$133^{2008} \cdot 133^3 \equiv 7 \pmod{10}$

$133^{2011} \equiv 7 \pmod{10}$

Hence last digit of 133^{2011} is 7.

Ex. Find the last two digit of 7^{81}.

→ Here, $\gcd(7, 100) = 1$

$\therefore$ By Euler's theorem,

$7^{\phi(100)} \equiv 1 \pmod{100}$

$7^{40} \equiv 1 \pmod{100}$

$(7^{40})^2 \equiv 1^2 \pmod{100}$

$7^{80} \equiv 1 \pmod{100}$ —— (1)

also,

$7 \equiv 7 \pmod{100}$ —— (2)

$\therefore$ From (1) and (2),

$7^{81} \equiv 7 \pmod{100}$

$\therefore$ Last two digits are 07.

Ex Find last two digits of $(2003)^{2006}$.

→ Here $\gcd(2003, 100) = 1$.

$\therefore$ By Euler's theorem

$2003^{\phi(100)} \equiv 1 \pmod{100}$

$(2003)^{40} \equiv 1 \pmod{100}$

$[(2003)^{40}]^{50} \equiv 1^{50} \pmod{100}$

$(2003)^{2000} \equiv 1 \pmod{100}$ —— (1)

Now,

$2003 \equiv 3 \pmod{100}$

$(2003)^6 \equiv 3^6 \pmod{100}$

Date
Page

$$(2009)^6 \equiv 729\ (100)$$
$$(2009)^6 \equiv 29\ (\text{mod } 100) \longrightarrow (2)$$
$\therefore$ From (1) and (2),
$$(2009)^{2000} \cdot (2009)^6 \equiv 29\ (\text{mod } 100)$$
$$(2009)^{2006} \equiv 29\ (\text{mod } 100)$$
$\therefore$ Last two digits are 29.

Ex. Find unit digit of 247^{247}.

$\rightarrow$ Here $\gcd(247, 10) = 1$

$\therefore$ By Euler's theorem,
$$247^{\phi(10)} \equiv 1\ (\text{mod } 10)$$
$$247^4 \equiv 1\ (\text{mod } 10)$$
$$[(247)^4]^{61} \equiv 1\ (\text{mod } 10)$$
$$247^{244} \equiv 1\ (\text{mod } 10) \longrightarrow (1)$$
also
$$247 \equiv 7\ (\text{mod } 10)$$
$$(247)^3 \equiv 7^3\ (\text{mod } 10)$$
$$247^3 \equiv 343\ (\text{mod } 10)$$
$$247^3 \equiv 3\ (\text{mod } 10) \longrightarrow (2)$$
$\therefore$ From (1) and (2),
$$(247)^{244} \cdot 247^3 \equiv 3\ (\text{mod } 10)$$
$$247^{247} \equiv 3\ (\text{mod } 10)$$
$\therefore$ Unit digit of 247^{247} is 3.

H.W

Ex. Find unit digit of 2^{100}.

Ex. Find unit digit of 38^{100}

Ex. Find $(21)^{500}\ (\text{mod } 23)$

Ex. Find last digit of 2^{2019}

* Note-:

If $a^n \equiv a \pmod n$ fails to hold good for some choice of 'a' then 'n' is necessarly composite

Ex. Verify that $n = 117$ is composite.

→ Claim - $2^{117} \not\equiv 2 \pmod{117}$

Here $2^{117} = (2^7)^{16} \cdot 2^5$ —— ①

But $2^7 = 128 \equiv 11 \pmod{117}$

$\Rightarrow 2^7 \equiv 11 \pmod{117}$

$\Rightarrow (2^7)^{16} \equiv 11^{16} \pmod{117}$ —— ②

Now,

$11^2 = 121 \equiv 4 \pmod{117}$

$\Rightarrow (11^2)^8 \equiv 4^8 \pmod{117}$

$\Rightarrow 11^{16} \equiv 4^8 \pmod{117}$

$\Rightarrow 11^{16} \equiv (2^2)^8 \pmod{117}$

$= 2^{16} \pmod{117}$

$= 2^7 \cdot 2^7 \cdot 2^2 \pmod{117}$

$= 11 \cdot 11 \cdot 2^2 \pmod{117}$

$= 121 \cdot 2^2 \pmod{117}$

$= 4 \cdot 2^2 \pmod{117}$

$11^{16} = 16 \pmod{117}$

$\therefore$ From ②,

$(2^7)^{16} \equiv 16 \pmod{117}$

$\therefore (2^7)^{16} \cdot 2^5 \equiv 2^4\, 2^5 \pmod{117}$

$\equiv 2^7 \cdot 2^2 \pmod{117}$

$\equiv 11 \cdot 4 \pmod{117}$

$2^{117} \equiv 44 \pmod{117}$

$\therefore 2^{117} \not\equiv 2 \pmod{117}$

$\therefore$ 117 is composite

Date
Page

* Lemma-:

If 'p' and 'q' are distinct primes with $a^p \equiv a \pmod q$ and $a^q \equiv a \pmod p$ then $a^{pq} \equiv a \pmod{pq}$.

Proof:

We have,

$a^q \equiv a \pmod p$

$(a^q)^p \equiv a^p \pmod p$ — ①

Here p is prime.

$\therefore a^p \equiv a \pmod p$ — ②

$\therefore$ From ① and ②.

$a^{pq} \equiv a \pmod p$ — ③

also,

$a^p \equiv a \pmod q$

$(a^p)^q \equiv a^q \pmod q$ — ④

Here q is prime.

$\therefore a^q \equiv a \pmod q$ — ⑤

$\therefore$ From ④ and ⑤.

$a^{pq} \equiv a \pmod q$ — ⑥

From ③ and ⑥

$p \mid a^{pq} - a$ and $q \mid a^{pq} - a$

Here 'p' and 'q' are distinct primes

$\Rightarrow pq \mid a^{pq} - a$

$\Rightarrow a^{pq} \equiv a \pmod{pq}$

Ex. Show that $2^{340} \equiv 1 \pmod{341}$

→ We want to show that,

$2^{340} \equiv 1 \pmod{341}$ — ①

But $341 = 11 \cdot 31$

i.e to show that,

$2^{340} \equiv 1 \pmod{11 \cdot 31}$

$\Rightarrow 2^{340} \cdot 2 \equiv 2 \pmod{11 \cdot 31}$

$\Rightarrow 2^{341} \equiv 2 \pmod{11 \cdot 31}$

$\Rightarrow 2^{11 \cdot 31} \equiv 2 \pmod{11 \cdot 31}$ —— ②

To prove ② we have to prove,

i) $2^{11} \equiv 2 \pmod{31}$

ii) $2^{31} \equiv 2 \pmod{11}$

Now,

i) Here $2^5 = 32 \equiv 1 \pmod{31}$

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

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

$\Rightarrow 2^{10} \equiv 1 \pmod{31}$

$\Rightarrow 2^{10} \cdot 2 \equiv 1 \cdot 2 \pmod{31}$

$\Rightarrow 2^{11} \equiv 2 \pmod{31}$

Hence the required

ii) Here, $\gcd(2, 11) = 1$

$\therefore$ By Euler's theorem.

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

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

$(2^{10})^3 \equiv 1^3 \pmod{11}$

$2^{30} \equiv 1 \pmod{11}$

also,

$2^{30} \cdot 2 \equiv 1 \cdot 2 \pmod{11}$

$\therefore 2^{31} \equiv 2 \pmod{11}$

Date
Page

* Pseudo Prime -:

A composite number n is said to be pseudo prime if $2^n \equiv 2 \pmod{n}$.

e.g. 341 is smallest pseudo prime and 561, 645, 1105 are also pseudo primes.

Ex. Prove that if $d \mid n$ then $2^d - 1 \mid 2^n - 1$

→ We have, $d \mid n$.

$\Rightarrow n = dk \;;\; k \in \mathbb{Z}$.

consider,

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

$\Rightarrow 2^d - 1 \mid 2^n - 1$

* Theorem -:

If 'n' is pseudo prime then $M_n = 2^n - 1$ is also pseudo prime.

Proof:

since 'n' is a pseudo prime

$\therefore 2^n \equiv 2 \pmod{n}$

$\Rightarrow n \mid 2^n - 2$

$\Rightarrow 2^n - 2 = nk \;;\; k \in \mathbb{Z}$

consider,

$$M_n - 1 = 2^n - 1 - 1$$
$$= 2^n - 2$$
$$= nk$$

Now,

$$2^{(M_n - 1)} - 1 = 2^{nk} - 1$$
$$= (2^n)^k - 1^k$$
$$= (2^n - 1)\left[2^{n(k-1)} + 2^{(k-2)n} + \cdots + 1\right]$$

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

$\Rightarrow \quad M_n \mid 2^{(M_n-1)} - 1$

$\Rightarrow \quad 2^{M_n-1} \equiv 1 \pmod{M_n}$

$\Rightarrow \quad 2^{M_n} \equiv 2 \pmod{M_n}$

$\therefore \quad M_n = 2^n - 1$ is pseudo prime

* **Pseudo Prime to the base 'a' -:**

A pseudo prime 'n' is said to be pseudo prime to the base 'a' if $a^n \equiv a \pmod n$.

e.g. 341 is pseudo prime to the base 2.

* **Absolute Pseudo Prime -:**

A composite number 'n' is said to be absolute pseudo prime if $a^n \equiv a \pmod n$ $\forall a$ such that $\gcd(a, n) = 1$.

e.g. 561 is the smallest absolute pseudo prime

Ex. Show that 561 is absolute pseudo prime

→ Suppose an integer 'a' with the property that $\gcd(a, 3\times 11\times 17) = 1$

$\therefore$ We have, $\gcd(a, 3) = 1$

$\gcd(a, 11) = 1$

$\gcd(a, 17) = 1$.

$\therefore$ By using Fermat's theorem we have,

$a^{3-1} \equiv 1 \pmod 3$ $\qquad \uparrow (a^2)^{280}$

i.e. $a^2 \equiv 1 \pmod 3 \Rightarrow a^{560} \equiv 1 \pmod 3$

$a^{11-1} \equiv 1 \pmod{11}$ $\qquad \uparrow (a^{10})^{56}$

i.e. $a^{10} \equiv 1 \pmod{11} \Rightarrow a^{560} \equiv 1 \pmod{11}$

$a^{17-1} \equiv 1 \pmod{17}$ $\qquad \uparrow (a^{16})^{35}$

i.e. $a^{16} \equiv 1 \pmod{17} \Rightarrow a^{560} \equiv 1 \pmod{17}$

$\Rightarrow \quad 3 \mid a^{560} - 1$

$11 \mid a^{560} - 1$

$17 \mid a^{560} - 1$

$\Rightarrow \quad 3 \cdot 11 \cdot 17 \mid a^{560} - 1$

$\Rightarrow \quad 561 \mid a^{560} - 1$

$\Rightarrow \quad a^{560} \equiv 1 \pmod{561}$

$\Rightarrow \quad a^{560} \cdot a \equiv 1 \cdot a \pmod{561}$

$\Rightarrow \quad a^{561} \equiv a \pmod{561}$

$\therefore$ 561 is absolute pseudo prime.

H.W.

Ex. Show that the following numbers are absolute pseudo primes.

① 1105 ③ 6601

② 1729 ④ 10585

Ex. Use Fermat's theorem and verify $17 \mid 11^{104} + 1$

* Square Free integers -:

A composite number 'n' is said to be square free if $k^2 \nmid n$; $k > 1$

e.g. ① 28.

$\Rightarrow \quad 2^2 = 4 \mid 28$

$\therefore$ 28 is not square free integer.

② 10

$\Rightarrow \quad 2^2 = 4 \nmid 10$

$\therefore$ 10 is square free integer.

* Theorem -:

Let 'n' be a composite square free integer say $n = p_1 \cdot p_2 \cdot p_3 \cdots p_r$ where p_i are distinct primes $(1 \le i \le r)$. If $p_i - 1 \mid n-1 \ \forall i$ then 'n' is absolute Pseudo Prime.

Proof:

Suppose that 'a' is any integer such that $\gcd(a, n) = 1$.

i.e. $\gcd(a, p_1) = \gcd(a, p_2) = \cdots = \gcd(a, p_r) = 1$

$\Rightarrow \quad p_i \nmid a \ \forall i ; \ 1 \le i \le r.$

$\therefore$ By using Fermat's theorem,

$$a^{p_i - 1} \equiv 1 \pmod{p_i} \quad \text{——} ①$$

But we know that,

$$p_i - 1 \mid n-1$$

$$\Rightarrow \quad n-1 = (p_i - 1)k \ ; \ k \in \mathbb{Z} \quad \text{——} ②$$

On multiply congruence ① k times,

$$(a^{p_i-1})^k \equiv 1 \pmod{p_i}$$

$$a^{(p_i-1)k} \equiv 1 \pmod{p_i}$$

$$\Rightarrow \quad a^{n-1} \equiv 1 \pmod{p_i} \quad \text{—— from ②}$$

i.e. $p_i \mid a^{n-1} - 1 \quad \forall i$

$\Rightarrow \quad p_1 \mid a^{n-1} - 1, \ p_2 \mid a^{n-1} - 1, \ \cdots, \ p_r \mid a^{n-1} - 1.$

$\Rightarrow \quad p_1 p_2 p_3 \cdots p_r \mid a^{n-1} - 1$

$\Rightarrow \quad n \mid a^{n-1} - 1$

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

$\Rightarrow \quad a^n \equiv a \pmod{n}$

$\therefore$ 'n' is absolute pseudo prime.

VImp * Wilson's Theorem -:

* Statement:

For any prim p,

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

Proof:

i) For $p = 2$

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

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

Date
Page

$\therefore$ The result is hold for $p=2$.

ii) For $p=3$:

$(3-1)! \equiv -1 \pmod 3$

$2! \equiv -1 \pmod 3$

$2 \equiv -1 \pmod 3$

$\therefore$ The result is hold for $p=3$.

Let $p>3$.

Let 'a' be any one of the integers $1,2,\dots,p-1$

Then $\gcd(a,p)=1$

consider the linear congruence. $ax \equiv 1 \pmod p$

since $\gcd(a,p)=1$ then the linear congruence $ax \equiv 1 \pmod p$ has unique solution modulo p.

Let 'a' is one amongst $1,2,3,\dots,p-1$.

Thus a' is unique integer such that $1 \le a' \le p-1$ satisfying $aa' \equiv 1 \pmod p$

Claim: $a=a'$ iff either $a=1$ or $a=p-1$

consider $a=a'$

$\therefore \; a^2 \equiv 1 \pmod p$

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

$\Rightarrow (a-1)(a+1) \equiv 0 \pmod p$

$\Rightarrow (a-1) \equiv 0 \pmod p$ or $(a+1) \equiv 0 \pmod p$

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

Thus, for any 'a' other than '1' and '$p-1$', a' is distinct from 'a'.

Thus, we obtain $\frac{(p-3)}{2}$ pairs of (a,a') such that $aa' \equiv 1 \pmod p$

Hence $2\cdot3\cdot4\cdots(p-2) \equiv 1 \pmod p$

$\Rightarrow (p-2)! \equiv 1 \pmod p$

$\Rightarrow (p-1)(p-2)! \equiv (p-1) \pmod p$

$\Rightarrow (p-1)! \equiv -1 \pmod p$

Hence the proof.

Ex. Find the value of $(1.2.3.4.5.6)^{512} \pmod 7$

→ Here $1.2.3.4.5.6 = 6!$

For prime $p = 7$

$\therefore$ By Wilson's theorem we have,

$$(7-1)! \equiv -1 \pmod 7$$
$$6! \equiv -1 \pmod 7$$
$$(6!)^{512} \equiv (-1)^{512} \pmod 7$$
$$(6!)^{512} \equiv 1 \pmod 7$$

i.e. $(1.2.3.4.5.6)^{512} \equiv 1 \pmod 7$

$\therefore$ Value of $(1.2.3.4.5.6)^{512} \pmod 7$ is 1.

Ex. Find the value of $(9!)^{2019} \pmod{11}$

→ Here $1.2.3.4.5.6.7.8.9 = 9!$

For prime $p = 11$

$\therefore$ By Wilson's theorem we have,

$$(11-1)! \equiv -1 \pmod{11}$$
$$10! \equiv -1 \pmod{11}$$
$$10 \cdot 9! \equiv -1 \pmod{11}$$
$$9! \equiv -1 \pmod{11}$$
$$-1 \cdot 9! \equiv -1 \pmod{11}$$
$$9! \equiv 1 \pmod{11}$$
$$(9!)^{2019} \equiv 1^{2019} \pmod{11}$$
$$(9!)^{2019} \equiv 1 \pmod{11}$$

i.e. value of $(9!)^{2019} \pmod{11}$ is 1.

Ex. Find the value of $(99!) \pmod{101}$.

→ Here, $99!$

For prime, $P = 101$.

$\therefore$ By Wilson's theorem we have,

$$(101-1)! \equiv -1 \pmod{101}$$
$$100! \equiv -1 \pmod{101}$$
$$100 \cdot 99! \equiv -1 \pmod{101}$$

$-1 \cdot 99! \equiv -1 \pmod{101}$

$99! \equiv 1 \pmod{101}$

$(99!) \equiv 1 \pmod{101}$

$\therefore$ Value of $(99!) \pmod{101}$ is 1.

<u>Ex</u> Find the value of $(102!)^{212} \pmod{101}$

→ For prime $P = 101$

$\therefore$ By Wilson's theorem we have,

$(100-1)! \equiv -1 \pmod{101}$

$100! \equiv -1 \pmod{101}$

$(102)(101)\,100! \equiv -1\,(102)(101) \pmod{101}$

$(102)(101)\,100! \equiv -1 \cdot 0 \pmod{101}$

$102! \equiv 0 \pmod{101}$

$\therefore$ Value of $(102!)^{212} \pmod{101}$ is 0.

* Note-:

Converse of Wilson's theorem is also true i.e $(n-1!) \equiv (-1) \pmod{A}$ then 'n' must be prime.

<u>Proof:</u>

$(n-1)! \equiv (-1) \pmod{A}$

<u>Claim</u>- 'n' is prime.

On the contrary suppose that 'n' is not prime

i.e it has prime divisor 'd' such that $1<d<n$

since $d \leq n-1$.

$\therefore$ 'd' occures as one of the factors in $(n-1)!$

Hence $d \mid (n-1)!$

By assumption,

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

$\Rightarrow \quad n \mid (n-1)! + 1$

Now, $d \mid (n-1)+1$.

So $d \mid (n-1)!+1$ and $d \mid (n-1)!$

$\Rightarrow d \mid (n-1)! + 1 - (n-1)!$

$\Rightarrow d \mid 1$

Which is contradiction.

$\therefore$ 'n' must be prime.

* Examples of Wilson's Theorem :-

Ex. $x \equiv (20!)^{221} \pmod{23}$ then value of x is

(a) 12 (b) 11 (c) 22 (d) 1.

→ For prime $p = 23$.

$\therefore$ By Wilson's theorem we have,

$$(23-1)! \equiv -1 \pmod{23}$$
$$22! \equiv -1 \pmod{23}$$
$$22 \cdot 21 \cdot 20! \equiv -1 \pmod{23}$$
$$(-1)(-2)\, 20! \equiv -1 \pmod{23}$$
$$2 \cdot 20! \equiv -1 \pmod{23}$$
$$20! \equiv 2^{-1}(-1) \pmod{23}$$
$$20! \equiv -12 \pmod{23}$$
$$20! \equiv 11 \pmod{23}$$

$\Rightarrow 11 \equiv 20! \pmod{23}$

$\Rightarrow x = 11$.

Ex. Find the value of $(15!)^{102} \pmod{17}$

→ For prime. $p = 17$

$\therefore$ By Wilson's theorem we have,

$$16! \equiv -1 \pmod{17}$$
$$16 \cdot 15! \equiv -1 \pmod{17}$$
$$(-1)\, 15! \equiv -1 \pmod{17}$$
$$15! \equiv 1 \pmod{17}$$
$$(15!)^{102} \equiv (1)^{102} \pmod{17}$$
$$(15!)^{102} \equiv 1 \pmod{17}$$

$\therefore$ Value of $(15!)^{102} \pmod{17}$ is 1.

Date
Page

Ex. Find the value of $(21!)^{500} \pmod{23}$

→ For prime, $p = 23$

∴ By Wilson's theorem we have,

$$(23-1)! \equiv -1 \pmod{23}.$$

$$22! \equiv -1 \pmod{23}$$

$$22 \cdot 21! \equiv -1 \pmod{23}$$

$$(-1) \cdot 21! \equiv -1 \pmod{23}$$

$$21! \equiv 1 \pmod{23}$$

$$(21!)^{500} \equiv 1^{500} \pmod{23}$$

$$(21!)^{500} \equiv 1 \pmod{23}$$

∴ Value of $(21!)^{500} \pmod{23}$ is 1.

* Examples of Absolute Pseudo prime-:

Ex. Show that following numbers are absolute pseudo prime

i) 1105.

→ $1105 = 5 \times 17 \times 13$

Suppose an integer 'a' with the property that $\gcd(a, 5 \times 17 \times 13) = 1$.

∴ We have $\gcd(a,5) = 1$

$\gcd(a,17) = 1$

$\gcd(a,13) = 1$.

∴ By using Fermat's theorem we have,

$$a^{5-1} \equiv 1 \pmod{5}$$

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

$$\Rightarrow (a^4)^{276} \equiv 1^{276} \pmod{5}$$

$$\therefore a^{1104} \equiv 1 \pmod{5} \quad \text{--- (1)}$$

and

$$a^{17-1} \equiv 1 \pmod{17}$$

$$\Rightarrow a^{16} \equiv 1 \pmod{17}$$

$$\Rightarrow (a^{16})^{69} \equiv 1^{69} \pmod{17}$$

$$\therefore a^{1104} \equiv 1 \pmod{17} \quad \text{--- (2)}$$

and $a^{13-1} \equiv 1 \pmod{13}$

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

$\Rightarrow (a^{12})^{92} \equiv 1^{92} \pmod{13}$

$\therefore a^{1104} \equiv 1 \pmod{13}$ —— ③

From ①, ② and ③ we have,

$5 \mid a^{1104} - 1$

$17 \mid a^{1104} - 1$

$13 \mid a^{1104} - 1.$

$\Rightarrow 5 \cdot 17 \cdot 13 \mid a^{1104} - 1$

$\Rightarrow 1105 \mid a^{1104} - 1$

$\Rightarrow a^{1104} \equiv 1 \pmod{1105}$

$\Rightarrow a^{1104} \cdot a \equiv 1 \cdot a \pmod{1105}$

$\Rightarrow a^{1105} \equiv a \pmod{1105}$

$\therefore$ 1105 is absolute pseudo prime.

ii) 1729

→ $1729 = 13 \times 19 \times 7$

suppose an integer 'a' with the property that $\gcd(a, 13 \times 19 \times 7) = 1$.

$\therefore$ We have. $\gcd(a, 13) = 1$

$\gcd(a, 17) = 1$

$\gcd(a, 7) = 1.$

$\therefore$ By using Fermat's theorem we have,

$a^{13-1} \equiv 1 \pmod{13}$

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

$\Rightarrow (a^{12})^{144} \equiv 1^{144} \pmod{13}$

$\therefore a^{1728} \equiv 1 \pmod{13}$ —— ①

and

$a^{19-1} \equiv 1 \pmod{19}$

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

$\Rightarrow (a^{18})^{96} \equiv 1^{96} \pmod{19}$

$\therefore a^{1728} \equiv 1 \pmod{19}$ —— ②

and

$$a^{7-1} \equiv 1 \pmod 7$$

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

$$\Rightarrow (a^{6})^{288} \equiv 1^{288} \pmod 7$$

$$\therefore a^{1728} \equiv 1 \pmod 7 \quad \text{--- (3)}$$

From (1), (2) and (3) we have,

$$13 \mid a^{1178} - 1$$

$$19 \mid a^{1178} - 1$$

$$7 \mid a^{1178} - 1.$$

$$\Rightarrow 13 \cdot 19 \cdot 7 \mid a^{1178} - 1$$

$$\Rightarrow 1179 \mid a^{1178} - 1$$

$$\Rightarrow a^{1178} \equiv 1 \pmod{1179}$$

$$\Rightarrow a^{1178} \cdot a \equiv a \cdot 1 \pmod{1179}$$

$$\Rightarrow a^{1179} \equiv a \pmod{1179}$$

$\therefore$ 1729 is absolute pseudo prime

iii) 6601.

→ $6601 = 7 \times 23 \times 41$

suppose an integer 'a' with the property that $\gcd(7 \times 23 \times 41, a) = 1$

$\therefore$ We have $\gcd(a, 7) = 1$

$\gcd(a, 23) = 1$

$\gcd(a, 41) = 1$

$\therefore$ By Fermat's theorem we have,

$$a^{7-1} \equiv 1 \pmod 7$$

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

$$\Rightarrow (a^{6})^{1100} \equiv 1^{1100} \pmod 7$$

$$\therefore a^{6600} \equiv 1 \pmod 7 \quad \text{--- (1)}$$

and

$$a^{23-1} \equiv 1 \pmod{23}$$

$$\Rightarrow a^{22} \equiv 1 \pmod{23}$$

$$\Rightarrow (a^{22})^{300} \equiv 1^{300} \pmod{23}$$

$$\therefore a^{6600} \equiv 1 \pmod{23} \quad \text{--- (2)}$$

and

$$a^{41-1} \equiv a \pmod{41}$$

$\Rightarrow \quad a^{40} \equiv 1 \pmod{41}$

$\Rightarrow \quad (a^{40})^{165} \equiv 1^{165} \pmod{41}$

$\therefore \quad a^{6600} \equiv 1 \pmod{41}$ —— (3)

From (1), (2) and (3) we have,

$7 \mid a^{6600} - 1$

$23 \mid a^{6600} - 1$

$41 \mid a^{6600} - 1$

$\Rightarrow \quad 7 \cdot 23 \cdot 41 \mid a^{6600} - 1$

$\Rightarrow \quad 6601 \mid a^{6600} - 1$

$\Rightarrow \quad a^{6600} \equiv 1 \pmod{6601}$

$\Rightarrow \quad a^{6600} \cdot a \equiv 1 \cdot a \pmod{6601}$

$\Rightarrow \quad a^{6601} \equiv a \pmod{6601}$

$\therefore$ 6601 is absolute pseudo prime.

iv) 10585

→ $10585 = 5 \times 29 \times 73$

suppose an integer 'a' with the property that $\gcd(5 \times 29 \times 73, a) = 1$.

$\therefore$ We have $\gcd(a, 5) = 1$

$\gcd(a, 29) = 1$

$\gcd(a, 73) = 1$

$\therefore$ By Fermat's theorem we have,

$$a^{5-1} \equiv 1 \pmod 5$$

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

$\Rightarrow \quad (a^{4})^{2646} \equiv 1^{2646} \pmod 5$

$\therefore \quad a^{10584} \equiv 1 \pmod 5$ —— (1)

and

$$a^{29-1} \equiv 1 \pmod{29}$$

$\Rightarrow \quad a^{28} \equiv 1 \pmod{29}$

$\Rightarrow \quad (a^{28})^{378} \equiv 1^{378} \pmod{29}$

$\therefore \quad a^{10584} \equiv 1 \pmod{29}$ —— (2)

and

$$a^{73-1} \equiv 1 \pmod{73}$$

$$\Rightarrow a^{72} \equiv 1 \pmod{73}$$

$$\Rightarrow (a^{72})^{147} \equiv 1^{147} \pmod{73}$$

$$\therefore a^{10584} \equiv 1 \pmod{73} \quad \text{--- (3)}$$

From (1), (2) and (3) we have,

$$5 \mid a^{10584} - 1$$

$$29 \mid a^{10584} - 1$$

$$73 \mid a^{10584} - 1$$

$$\Rightarrow 5 \cdot 29 \cdot 73 \mid a^{10584} - 1$$

$$\Rightarrow 10585 \mid a^{10584} - 1$$

$$\Rightarrow a^{10584} \equiv 1 \pmod{10585}$$

$$\Rightarrow a^{10584} \cdot a \equiv 1 \cdot a \pmod{10585}$$

$$\Rightarrow a^{10585} \equiv a \pmod{10585}$$

$\therefore$ 10585 is absolute pseudo prime

v) Use Fermat's theorem and verify $17 \mid 11^{104} + 1$

→ We have to show that,

$$11^{104} \equiv -1 \pmod{17}$$

Here $a = 11$, $P = 17$

$\therefore$ By using Fermat's theorem,

$$11^{17-1} \equiv 1 \pmod{17}$$

$$\Rightarrow 11^{16} \equiv 1 \pmod{17}$$

$$\Rightarrow (11^{16})^{6} \equiv 1^{6} \pmod{17}$$

$$\therefore 11^{96} \equiv 1 \pmod{17} \quad \text{--- (1)}$$

and

$$11^{2} = 121 \equiv 2 \pmod{17}$$

$$\Rightarrow 11^{2} \equiv 2 \pmod{17}$$

$$\Rightarrow (11^{2}) \equiv 2 \pmod{17}$$

$$\Rightarrow 11^{8} \equiv 16 \pmod{17}$$

$$\therefore 11^{8} \equiv -1 \pmod{17} \quad \text{--- (2)}$$

From (1) and (2) we have,

$$11^{96} \cdot 11^{8} \equiv 1 \cdot (-1) \pmod{17}$$

$$\Rightarrow \quad 11^{104} \equiv -1 \pmod{17}$$

$$\Rightarrow \quad 17 \mid 11^{104} + 1$$

Thursday 10/10/2019

* Quadratic Congruence -:

A congruence of the form, $ax^2 + bx + c \equiv 0 \pmod{n}$ with $a \not\equiv 0 \pmod{n}$ is called the quadratic congruence.

* Theorem -:

The quadratic congruence $x^2 + 1 \equiv 0 \pmod{p}$ where 'p' is odd prime has a solution iff $p \equiv 1 \pmod{4}$

Proof:

Suppose the quadratic congruence $x^2 + 1 \equiv 0 \pmod{p}$ has a solution say 'a'.

$\therefore \quad a^2 + 1 \equiv 0 \pmod{p}$

$a^2 \equiv -1 \pmod{p} \longleftarrow (1)$

Suppose $p \mid a \Rightarrow a = pk \quad ; k \in \mathbb{Z}$

$\therefore$ Eq^n (1) becomes,

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

$$\Rightarrow \quad p \mid p^2k^2 + 1$$

also $p \mid p^2k^2$

$$\Rightarrow \quad p \mid p^2k^2 + 1 - p^2k^2$$

$$\Rightarrow \quad p \mid 1$$

Which is a contradiction.

$\therefore \quad p \nmid a$

$\therefore$ By using Fermat's theorem,

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

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

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

$\Rightarrow \quad 1 \equiv (-1)^{p-1/2} \pmod p \quad$; from ① —— ②

As 'p' is an odd prime.

$\therefore$ 'p' is of the form :

$4k+1$ or $4k+3$; $k \geq 0$ and $k \in \mathbb{Z}^+$

Suppose $p = 4k+3$

$\therefore (-1)^{p-1/2} = (-1)^{4k+3-1/2}$

$= (-1)^{4k+2/2}$

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

$= (-1)$

$\therefore$ Eq^n ② becomes,

$1 \equiv -1 \pmod p$

$\Rightarrow \quad p \mid 2$

Which is contradiction.

$\therefore \quad p \equiv 4k+1$

i.e. $p \equiv 1 \pmod 4$

Conversely,

Suppose that $p \equiv 1 \pmod 4$

Claim- $x^2+1 \equiv 0 \pmod p$ has solution.

We know that,

$p-1 \equiv -1 \pmod p$

$p-2 \equiv -2 \pmod p$

$p-3 \equiv -3 \pmod p$

$\vdots$

$\frac{p+1}{2} \equiv -\left(\frac{p-1}{2}\right) \pmod p$ $\Rightarrow \frac{p}{2}+\frac{1}{2} \equiv -\frac{p}{2}+\frac{1}{2} \pmod p$

$\Rightarrow \frac{p}{2}+\frac{p}{2} \equiv -\frac{1}{2}+\frac{1}{2} \pmod p$

consider, $\Rightarrow p \equiv 0 \pmod p \Rightarrow p \mid p$

$(p-1)! = 1 \cdot 2 \cdot 3 \cdot \cdots (p-1/2)(p+1/2) \cdots (p-1)$

$= 1(p-1) \cdot 2(p-2) \cdots \left(\frac{p-1}{2}\right)\left(\frac{p+1}{2}\right)$

Thus we obtain,

$(p-1)! \equiv 1(-1) \cdot 2(-2) \cdots \left(\frac{p-1}{2}\right)(-1)\left(\frac{p-1}{2}\right) \pmod p$

$\Rightarrow (P-1)! \equiv (-1)^{\frac{P-1}{2}} \left[1.1.2.2 \cdots \left(\frac{P-1}{2}\right)\left(\frac{P-1}{2}\right)\right] (\text{mod } P)$

$\Rightarrow (P-1)! \equiv (-1)^{P-1/2} \left[\left(\frac{P-1}{2}\right)!\right]^2 (\text{mod } P)$

since $P \equiv 1 (\text{mod} 4)$

$\therefore (-1)^{P-1/2} = 1.$

$\therefore (P-1)! \equiv \left[\left(\frac{P-1}{2}\right)!\right]^2 (\text{mod } P).$

since 'P' is prime

$\therefore$ By Wilson's theorem,

$$(P-1)! \equiv -1 (\text{mod } P)$$

$$\Rightarrow -1 \equiv \left[\left(\frac{P-1}{2}\right)!\right]^2 (\text{mod } P)$$

$$\Rightarrow 0 \equiv \left[\left(\frac{P-1}{2}\right)!\right]^2 + 1 (\text{mod } P)$$

$$\Rightarrow \left[\left(\frac{P-1}{2}\right)!\right]^2 + 1 \equiv 0 (\text{mod } P).$$

$\therefore x = \left(\frac{P-1}{2}\right)!$ is a solution of quadratic congruence $x^2+1 \equiv 0 (\text{mod } P)$.

Ex. Find the solution of $x^2+1 \equiv 0 (\text{mod } 13)$

→ Here $P = 13$.

$\therefore 4 \mid P-1$

$\Rightarrow 4 \mid 12$

i.e. $4 \mid 13-1$

$\Rightarrow 13 \equiv 1 (\text{mod} 4)$

$\therefore$ Given quadratic congruence has a solution. and the required solution is given by,

$$x = \left(\frac{P-1}{2}\right)!$$

$$= \left(\frac{13-1}{2}\right)!$$

$$= 6!$$
$$= 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6$$
$$= 720.$$

Ex. Find the remainder when $2(26!)$ is divided by 2

→ For prime $p = 29$.

∴ By Wilson's theorem we have,

$$(29-1)! \equiv -1 \pmod{29}$$
$$\Rightarrow \quad 28! \equiv -1 \pmod{29}$$
$$\Rightarrow \quad 28 \cdot 27 \cdot 26! \equiv -1 \pmod{29}$$
$$\Rightarrow \quad (-1)(-2)\, 26! \equiv -1 \pmod{29}$$
$$\Rightarrow \quad 2 \cdot 26! \equiv -1 \pmod{29}$$
$$\Rightarrow \quad 2 \cdot 26! \equiv 28 \pmod{29}$$

* Fermat's Factorisation Method -:

Ex. Using Fermats factorisation method factorise 119143.

observe that, $345^2 < 119143 < 346^2$

consider,

$$346^2 - 119143 = 119716 - 119143$$
$$= 573$$
$$345^2 - 119143 = 120409 - 119143$$
$$= 1266$$
$$348^2 - 119143 = 121104 - 119143$$
$$= 1961$$
$$349^2 - 119143 = 121801 - 119143$$
$$= 2658$$
$$350^2 - 119143 = 122500 - 119143$$
$$= 3357$$
$$351^2 - 119143 = 123201 - 119143$$
$$= 4058$$

① $23449 \Rightarrow 153^2 < 22449 < 154^2$

② $2279 \Rightarrow 47^2 < 2279 < 48^2$

③ $10541 \Rightarrow 102^2 < 10541 < 103^2$

④ $340663 \Rightarrow 583^2 < 340663 < 584^2$

Date ________
Page ________

$$352^2 - 119143 = 123904 - 119143$$

$$= 4761$$

$$\therefore \quad 352^2 - 119143 = 69^2$$

$$\Rightarrow \quad 352^2 - 69^2 = 119143$$

$$\Rightarrow \quad (352 - 69)(352 + 69) = 119143$$

$$\Rightarrow \quad 283 \times 421 = 119143$$