Number Theory

(Handwritten Classroom Study Material)

Submitted by
Sarojini Mohapatra
(MSc Math Student)
Central University of Jharkhand

No of Pages: 66

Your Note/Remarks

Submitted by
Sarojini Mohapatra
(MSc Math Student)
Central University of Jharkhand

Dt:- 08/01/2020

* Divisibility

* Congruent relation

An integer 'a' is said to be congruent to an integer 'b' modulo a fixed positive integer 'm' if $a-b$ is divisible by m i.e. $m \mid a-b$ written as

$a \equiv b \pmod{m}$

Q:- Show that congruence relation is an equivalence relation.

Proof:- We have to show that congruence relation is an equivalence relation.

(1) Reflexive relation

Consider a fixed integer m, then for any $a \in \mathbb{Z}$

$a-a=0$ is divisible by m.

i.e. $m \mid a-a$

$\Rightarrow a \equiv a \pmod{m}$

$\therefore$ The relation is reflexive.

(2) Symmetric relation

Let aRb

i.e. $a \equiv b \pmod{m}$, for some fixed integer m

$\Rightarrow m \mid a-b$

$\Rightarrow a-b = km, \ k \in \mathbb{Z}$

$\Rightarrow -(b-a) = km$

$\Rightarrow b-a = (-k)m$

$\Rightarrow b-a = tm$, where $t=-k \in \mathbb{Z}$

$\Rightarrow m \mid b-a$

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

$\Rightarrow bRa$

$\therefore aRb \Rightarrow bRa$

Hence the relation is symmetric.

(3) Transitive relation:-

Let aRb and bRc

i.e. $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$ for a fixed integer m.

i.e. $m \mid a-b$ and $m \mid b-c$

$\Rightarrow a-b = k_1 m, \ k_1 \in \mathbb{Z}$ —— (i)

$b-c = k_2 m, \ k_2 \in \mathbb{Z}$ —— (ii)

Adding (i) & (ii), we get

$a-c = (k_1+k_2)m$

$\Rightarrow a-c = sm$, where $s = k_1+k_2 \in \mathbb{Z}$

$\Rightarrow m \mid a-c$

$\Rightarrow a \equiv c \pmod{m}$

$\Rightarrow aRc$

$\therefore aRb$ and $bRc \Rightarrow aRc$

Hence the relation is transitive relation.

$\therefore$ Congruence relation is an equivalence relation.

Q:- $+ \cdot + = +$

$+ \cdot - = -$

$- \cdot + = -$

$- \cdot - = +$, why ?

A:- Let $x \in \mathbb{Z}^+$, then we have to show that

$(-x)\cdot(-x) = +x^2$

i.e. $(-x)^2 = +x^2$

Proof:- By the existence of additive inverse, we can write $x + (-x) = 0$

$\Rightarrow (-x)\{x + (-x)\} = (-x)\cdot 0$

$\Rightarrow (-x)x + (-x)(-x) = 0$

$\Rightarrow (-x)(-x) = +(x \cdot x)$

$\Rightarrow (-x)^2 = +x^2$

$\square$

09.01.2020

↳ G.C.D

A positive integer d is said to be gcd of two integers a & b (not both zero) if

(i) $d|a$ & $d|b$

(ii) If $c|a$ & $c|b$ then $c|d$

↳ The gcd of a & b is denoted by (a, b) or $\gcd(a, b)$.

↳ If gcd of a & b is 1, then a & b are co-prime or relatively prime to each other.

*1. If $a \equiv b \pmod{m}$ & $c \equiv d \pmod{m}$ then

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

2. If $a \equiv b \pmod{m}$ & $c \equiv d \pmod{m}$, then

$ac \equiv bd \pmod{m}$

3. If $a \equiv b \pmod{m}$ & $d > 0$, $d \mid m$, then

$a \equiv b \pmod{d}$

4. If $a \equiv b \pmod{m}$, then $ac \equiv bc \pmod{mc}$, $c > 0$

5. $ax \equiv ay \pmod{m}$ iff $x \equiv y \left(\bmod \frac{m}{(a,m)}\right)$

Complete Residue System modulo m (C.R.S):-

Let m be a fixed positive integer. The C.R.S modulo m is a finite set S of integers such that

① $|S| = m$

② $a_i \not\equiv a_j \pmod{m}$ for all $a_i, a_j \in S$.

Ex:- $m = 7$

$S = \{0, 1, 2, 3, 4, 5, 6\}$

Reduced Residue System modulo m (R.R.S) :-

Let m be a fixed positive integer. The R.R.S. modulo m is a finite set S of integers such that

(1) $|S| = \phi(m)$

(2) $a_i \not\equiv a_j \pmod{m}$ for all $a_i, a_j \in S$.

(3) $(a_i, m) = 1 \ \forall\ a_i \in S$.

Theorem-1

Let S be a CRS modulo m and $(a,m)=1$, then prove that $S' = \{ax \mid x \in S\}$ is also a CRS modulo m.

Theorem-2

Let S be a R.R.S modulo m and $(a,m)=1$, then prove that $S' = \{ax \mid x \in S\}$ is also a R.R.S. modulo m.

1) Proof:-

Given $a \equiv b \pmod{m}$ & $c \equiv d \pmod{m}$

Now, $a \equiv b \pmod{m}$

$\Rightarrow m \mid a-b$

$\Rightarrow a-b = mk_1$, for some $k_1 \in \mathbb{Z}$ ——(1)

$c \equiv d \pmod{m}$

$\Rightarrow m \mid c-d$

$\Rightarrow c-d = mk_2$, for some $k_2 \in \mathbb{Z}$ ——(2)

Adding eq(1) & (2), we get

$(a-b)+(c-d) = mk_1 + mk_2$

$\Rightarrow (a+c)-(b+d) = m(k_1+k_2)$

$\Rightarrow (a+c)-(b+d) = mt$, where $t = k_1+k_2 \in \mathbb{Z}$.

$\Rightarrow a+c \equiv b+d \pmod m$. $\square$

2) **Proof:-** Given $a \equiv b \pmod m$ & $c \equiv d \pmod m$

i.e. $m | a-b$

$\Rightarrow a-b = mk_1$, for some $k_1 \in \mathbb{Z}$

$\Rightarrow a = b + mk_1$

and $m | c-d$

$\Rightarrow c-d = mk_2$, for some $k_2 \in \mathbb{Z}$

$\Rightarrow c = d + mk_2$

Now, $ac = (b+mk_1)(d+mk_2)$

$= bd + mbk_2 + mdk_1 + m^2 k_1 k_2$

$\Rightarrow ac - bd = m(bk_2 + dk_1 + mk_1k_2)$

$\Rightarrow ac - bd = ml$, where $bk_2 + dk_1 + mk_1k_2 = l \in \mathbb{Z}$.

$\therefore ac \equiv bd \pmod m$. $\square$

3) **Proof:-** Given, $a \equiv b \pmod m$

$\Rightarrow m | a-b$

$\Rightarrow a-b = mk_1$, for some $k_1 \in \mathbb{Z}$ ——— (1)

Also given, $d > 0$ and $d | m$

$\Rightarrow m = dk_2$, for some $k_2 \in \mathbb{Z}$ ——— (2)

Putting the value of m in eq(1),

$a-b = (dk_2)k_1$

$\Rightarrow a-b = d(k_2k_1)$

$\Rightarrow a-b = dk_3$, where $k_3 = k_1k_2 \in \mathbb{Z}$

$\Rightarrow d \mid a-b$

$\therefore$ $a \equiv b \pmod d$ $\square$

4) Given $a \equiv b \pmod m$

$\Rightarrow m \mid a-b$

$\Rightarrow a-b = mk_1$, for some $k_1 \in \mathbb{Z}$.

Multiplying c on both sides, we get

$ac - bc = mk_1c$

$\Rightarrow ac - bc = mc(k_1)$

$\Rightarrow mc \mid ac-bc$

$\therefore$ $ac \equiv bc \pmod{mc}$ $\square$

5) <u>Proof:-</u> Given $ax \equiv ay \pmod m$

$\Rightarrow m \mid ax - ay$

$\Rightarrow ax - ay = mk_1$, for some $k_1 \in \mathbb{Z}$.

$\Rightarrow a(x-y) = mk_1$

$\Rightarrow \dfrac{a}{(a,m)}(x-y) = \dfrac{m}{(a,m)}k_1$

$\Rightarrow \dfrac{m}{(a,m)} \,\Big|\, \dfrac{a}{(a,m)}(x-y)$,

But $\left(\dfrac{a}{(a,m)}, \dfrac{m}{(a,m)}\right) = 1$ [We know that, if $d \mid a$ and $d \mid b$ and $d > 0$, then $\left(\dfrac{a}{d}, \dfrac{b}{d}\right) = \dfrac{1}{d}\gcd(a,b)$

if $(a,b) = g$, then

$\left(\dfrac{a}{g}, \dfrac{b}{g}\right) = 1$.

$\therefore \frac{m}{(a,m)} \Big| (x-y)$ [If $c|ab$ and $(b,c)=1$, then $c|a$].

$\Rightarrow x \equiv y \left(\text{mod } \frac{m}{(a,m)}\right)$.

Dt: 10.01.2020

Q:-1 Show that a decimal number n is divisible by 2 iff its unit digit is divisible by 2.

Q:-2 Show that a decimal number n is divisible by 3 or 9 iff the sum of its digits is divisible by 3 or 9.

Q:-3 Show that a decimal number n is divisible by 4 iff the number formed by last two digits is divisible by 4.

Q:-4 Show that a decimal number n is divisible by 11 iff the difference of the sum of the digits at odd places and even places is divisible by 11.

Theorem:-2

Let S be a RRS modulo m and $\gcd(a,m)=1$. Then prove that $S'=\{ax \mid x \in S\}$ is also a RRS modulo m

Proof:-

By definition of $S'=\{ax \mid x \in S\}$ it is clear that $|S'|=\phi(m)$, as S is a RRS modulo m.

Let us consider, ax_1 and ax_2 are two elements in S' such that

$$ax_1 \equiv ax_2 \pmod m$$

$$\Rightarrow m \mid ax_1 - ax_2$$

$\Rightarrow m \mid a(x_1 - x_2)$

$\Rightarrow m \mid x_1 - x_2 \quad [\because (a,m) = 1]$

$\Rightarrow x_1 \equiv x_2 \pmod m$

As $x_1, x_2 \in S$, there is a contradiction that S is a RRS modulo m.

$\therefore \quad ax_1 \not\equiv ax_2 \pmod m$

Let us consider that $\gcd(ax, m) = d$, for any $ax \in S'$

Since $\gcd(a,m) = 1$ and $x \in S \Rightarrow (x,m) = 1$

$\Rightarrow (ax, m) = 1$

$\Rightarrow d = 1$.

Thus S' is a RRS modulo m. □

Theorem - 1:-

Let S be a CRS modulo m and $(a,m) = 1$, then prove that $S' = \{ax \mid x \in S\}$ is also a CRS modulo m.

Proof:- By definition of $S' = \{ax \mid x \in S\}$ it is clear that $|S'| = m$, as S is a CRS modulo m.

Let us consider, ax_1 and ax_2 are two elements in S' such that

$ax_1 \equiv ax_2 \pmod m$

$\Rightarrow m \mid ax_1 - ax_2$

$\Rightarrow m \mid a(x_1 - x_2)$

$\Rightarrow m \mid x_1 - x_2 \quad [\because (a, m) = 1]$

$\Rightarrow x_1 \equiv x_2 \pmod m$

As $x_1, x_2 \in S$, there is a contradiction that S is a CRS modulo m.

Thus $\therefore ax_1 \not\equiv ax_2 \pmod m$

Thus S' is a CRS modulo m. □

Linear Congruence :-

For a fixed +ve integer, the linear congruence mod m is defined as $ax \equiv b \pmod m$, where a and b are integers.

Theorem - 3 :-

Let $(a, m) = 1$. Then the linear congruence $ax \equiv b \pmod m$ has unique solution.

Proof :-

Let us consider a CRS mod m is,

$$S = \{0, 1, \ldots\ldots, m-1\}$$

Since $(a, m) = 1$, the set $S' = \{a \cdot 0, a \cdot 1, \ldots, a(m-1)\}$ is also a CRS mod m.

Since S is a CRS mod m, there is a unique element $r \in S$ such that $b \equiv r \pmod m$ and with same argument there is a unique element $ak \in S'$ such that $ak \equiv r \pmod m$.

$\therefore ak \equiv b \pmod m$ for unique k in S.

$\therefore ax \equiv b \pmod m$ has unique solution k in S. □

Theorem – 4:-

Let $\gcd(a,m) = d$, then the linear congruence $ax \equiv b \pmod m$ has d solutions if $d|b$ and no solution if $d \nmid b$.

Dt:- 15.01.2020

Proof:- Let $d|b$ and $b = dk_1$, k_1 is an integer

Given that $(a,m) = d$

$\Rightarrow$ There exists integers k_2 & k_3 such that
$a = dk_2$ & $m = dk_3$ with $(k_2, k_3) = 1$.

Now, the linear congruence $ax \equiv b \pmod m$ ---(1)
i.e. $dk_2 x \equiv dk_1 \pmod{dk_3}$

reduced to $k_2 x \equiv k_1 \pmod{k_3}$ ----(2)

Since $(k_2, k_3) = 1$, the linear congruence (2) has unique solution say x_0.

Now, consider a set $S = \{x_0, x_0 + k_3, x_0 + 2k_3, \ldots, x_0 + (d-1)k_3\}$

Consider a general element $x_0 + tk_3$ of S, where
$t = 0, 1, \ldots, d-1$

Now, $a(x_0 + tk_3) - b = ax_0 + atk_3 - b$

$= dk_2 x_0 + dk_2 t\, k_3 - dk_1$

$= dk_3 k_2 t + d(k_2 x_0 - k_1)$

$= mk_2 t + dk_3 s$, for some integers s.

$= mk_2 t + ms$

$= m(k_2 t + s)$

$\Rightarrow m \mid [a(x_0 + tk_3) - b]$

$\Rightarrow a(x_0 + tk_3) \equiv b \pmod{m}$

Hence $x_0 + tk_3$ is a solution of (1) and since S is a solution set of C.R.S modulo m

So S is a solution set of (1).

So (1) has d solution.

Let $d \nmid b$ and consider that the linear congruence $ax \equiv b \pmod{m}$ has a solution say x'.

Then $m \mid (ax' - b)$

$\Rightarrow ax' - b = mk$, for some integer k.

$\Rightarrow b = ax' - km$

$\Rightarrow d \mid (ax' - km) = b \quad [\because (a, m) = d]$

which is a contradiction.

Therefore if $d \nmid b$ then it has no solution.

Ex:-1 Solve

$12x \equiv 5 \pmod{13}$

A:- Since $(12, 13) = 1$, it has unique solution.

$13 = 12 \cdot 1 + 1$

$12 = 1 \cdot 12 + 0$

$1 = 13 \cdot 1 - 12 \cdot 1$

$5 = 13 \cdot 5 - 12 \cdot 5$

$12 \cdot 5 + 5 = 13 \cdot 5$

$\Rightarrow (-12)(-5) + 5 = 13 \cdot 5$

$\Rightarrow 12(-5) - 5 = 13 \cdot (-5)$

$\therefore x \equiv -5 \pmod{13}$ $\quad 8 \equiv -5 \pmod{13}$ $\quad \{0, 1, 2, \ldots, 12\}$

i.e $\quad x \equiv 8 \pmod{13}$

$\therefore$ 8 is the required solution.

Ex:-2 $\quad 8x \equiv 3 \pmod{13}$

Since $(8, 13) = 1$, so it has unique solution.

$13 = 8 \cdot 1 + 5$

$8 = 5 \cdot 1 + 3$

$5 = 3 \cdot 1 + 2$

$3 = 2 \cdot 1 + 1$

$2 = 1 \cdot 2 + 0$

~~$1 = 3 \cdot 1 - 2 \cdot 1$~~

~~$2 = 5 \cdot 1 - 3 \cdot 1$~~

$1 = 3 - 2 \cdot 1$

$= 3 - (5 - 3 \cdot 1) \cdot 1$

$= 3 \cdot 2 - 5 \cdot 1$

$= (8 - 5 \cdot 1) \cdot 2 - 5 \cdot 1$

$= 8 \cdot 2 - 5 \cdot 3$

$= 8 \cdot 2 - (13 - 8 \cdot 1) \cdot 3$

$1 = 8 \cdot 5 - 13 \cdot 3$

$\Rightarrow 3 = (8 \cdot 5) \cdot 3 - 13 \cdot 3 \cdot 3$

$\Rightarrow \underset{b}{3} = \underset{a}{8} \cdot \underset{x}{15} - \underset{m}{13} \cdot 9$

$\therefore \quad x \equiv 15 \pmod{13}$

i.e. $\quad x \equiv 2 \pmod{13}$ is the required solution.

$\therefore$ 2 is the req. solution.

* Simple Continued Fraction :-

$$\frac{a}{m} = \frac{8}{13} = 0 + \frac{1}{\frac{13}{8}}$$

$$= \frac{1}{1+\frac{5}{8}}$$

$$= \frac{1}{1+\frac{1}{8/5}}$$

$$= \frac{1}{1+\frac{1}{1+\frac{3}{5}}}$$

$$= \frac{1}{1+\frac{1}{1+\frac{1}{5/3}}}$$

$$= \frac{1}{1+\frac{1}{1+\frac{1}{1+\frac{2}{3}}}}$$

$$= 0 + \frac{1}{1+\frac{1}{1+\frac{1}{1+\frac{1}{1+\frac{1}{2}}}}}$$

$$\text{S.C.F}\left(\frac{8}{13}\right) = [0, 1, 1, 1, 1, 2]$$

$$[0, 1, 1, 1, 1] = 0 + \frac{1}{1+\frac{1}{1+\frac{1}{1+\frac{1}{1}}}}$$

$$= 0 + \frac{1}{1+\frac{1}{1+\frac{1}{2}}} = 0 + \frac{1}{1+\frac{2}{3}} = \frac{3}{5}$$

$\frac{8}{13} \times \frac{3}{5}$

$8 \cdot 5 - 13 \cdot 3 = 1$

$\underset{a}{\underline{8}} \cdot \underset{x}{\underline{15}} - \underset{m}{\underline{13}} \cdot 9 = \underset{b}{\underline{3}}$

For multiple solution

$8x \equiv 4 \pmod{14}$ ——— (1)

$\because (8, 14) = 2$ & $2|4$, so it has 2 sol^{n}s

$4x \equiv 2 \pmod 7$ ——— (2)

$x_0 = 4$ is a sol^n of (2).

$S = \{x_0, x_0 + k_3, \text{- - - -}, x_0 + (d-1)k_3\}$, $k_3 = \frac{m}{d} = \frac{14}{2} = 7$

$S = \{4, 4+7\}$

$S = \{4, 11\}$

$\therefore$ 4 & 11 are two solutions of (1).

1) Show that a decimal number n is divisible by 2 iff its unit digit is divisible by 2.

A:- Let $n = a_k a_{k-1} \dots a_2 a_1 a_0$

$$= a_k 10^k + a_{k-1} 10^{k-1} + \dots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0$$

$10 \equiv 0 \pmod 2$

$10^j \equiv 0 \pmod 2$, $j = 0, 1, 2, \dots, k$

$\therefore a_k 10^k + a_{k-1} 10^{k-1} + \dots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0 \equiv a_0 \pmod 2$

$\therefore$ If $2 | a_0$, then $2 | n$.

2) Show that a decimal number n is divisible by 3 or 9 if the sum of its digits is divisible by 3 or 9.

A:- Let $n = a_k a_{k-1} \dots a_2 a_1 a_0$

$$= a_k 10^k + a_{k-1} 10^{k-1} + \dots + a_2 10^2 + a_1 \cdot 10 + a_0$$

$10 \equiv 1 \pmod 3$

$10^j \equiv 1^j = 1 \pmod 3$, $j = 0, 1, 2, \dots, k$

$\therefore a_k 10^k + a_{k-1} 10^{k-1} + \dots + a_2 10^2 + a_1 \cdot 10 + a_0 \equiv a_k + a_{k-1} + \dots + a_1 + a_0 \pmod 3$

$\Rightarrow n \equiv a_k + a_{k-1} + \dots + a_1 + a_0 \pmod 3$

$\therefore n$ is divisible by 3 if $a_k + a_{k-1} + \dots + a_1 + a_0$ is divisible by 3.

Similarly n is divisible by 9 if sum of its digit is divisible by 9.

3) Show that a decimal number n is divisible by 4 iff the number formed by last two digits is divisible by 4.

A:- Let $n = a_k a_{k-1} \dots a_2 a_1 a_0$

$$= a_k 10^k + a_{k-1} 10^{k-1} + \dots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0$$

$10^2 \equiv 0 \pmod 4$

$\therefore a_k 10^k + a_{k-1} 10^{k-1} + \dots + a_2 10^2 \equiv 0 \pmod 4$

$\Rightarrow a_k 10^k + a_{k-1} 10^{k-1} + \dots + a_2 10^2 + a_1 \cdot 10 + a_0 \equiv a_1 \cdot 10 + a_0 \pmod 4$

$\Rightarrow n \equiv a_1 \cdot 10 + a_0 \pmod 4$

$\therefore$ n is divisible by 4 if the number formed by last two digits is divisible by 4.

4) Show that a decimal number n is divisible by 11 iff the difference of the sum of the digits at odd places and even places is divisible by 11.

A:- Let $n = a_k a_{k-1} \dots a_2 a_1 a_0$

$$= a_k 10^k + a_{k-1} 10^{k-1} + \dots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0$$

$10 \equiv -1 \pmod{11}$

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

$\therefore a_k 10^k + a_{k-1} 10^{k-1} + \dots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0$

$$\equiv (-1)^k a_k + (-1)^{k-1} a_{k-1} + \dots + (-1)^2 a_2 - a_1 + a_0 \pmod{11}$$

$\Rightarrow n \equiv (-1)^k a_k + (-1)^{k-1} a_{k-1} + \dots + a_2 - a_1 + a_0 \pmod{11}$

$\Rightarrow n \equiv (a_0 + a_2 + a_4 + \dots) - (a_1 + a_3 + a_5 + \dots) \pmod{11}$

$\therefore$ n is divisible by 11 if the difference of the sum of the digits at odd places and even places is divisible by 11.

Dt:- 16.01.2020

Fermat's little Theorem :-

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

Furthermore, for any integer a, $a^p \equiv a \pmod p$

Proof:-

If $p|a$, then $p \mid (a^p - a) = a(a^{p-1} - 1)$

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

If $p \nmid a$, then we have to show that

$$p \mid (a^{p-1} - 1) \quad \text{i.e.} \quad a^{p-1} \equiv 1 \pmod p$$

Let $S = \{a_1, a_2, \ldots, a_{\phi(p)}\}$ be a R.R.S mod p.

Since $p \nmid a$, $(a, p) = 1$ and hence

$S' = \{aa_i \mid a_i \in S\}$ is also a R.R.S mod p.

It is clear that for each $aa_i \in S'$, there exists exactly one element say $a_j \in S$ such that

$$aa_i \equiv a_j \pmod p$$

Then $\prod_{i=1}^{\phi(p)} aa_i \equiv \prod_{j=1}^{\phi(p)} a_j \pmod p$

$$\Rightarrow a^{\phi(p)}\left(\prod_{i=1}^{\phi(p)} a_i\right) \equiv \left(\prod_{j=1}^{\phi(p)} a_j\right) \pmod p$$

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

$$\Rightarrow p \mid a^{\phi(p)}\left(\prod_{i=1}^{\phi(p)} a_i\right) - \left(\prod_{i=1}^{\phi(p)} a_i\right)$$

$$\Rightarrow p \mid \prod_{i=1}^{\phi(p)} a_i \left(a^{\phi(p)} - 1\right)$$

$$\Rightarrow p \mid a^{\phi(p)} - 1 \qquad [\because (a_i, p) = 1]$$

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

$$\Rightarrow a^{p-1} \equiv 1 \pmod{p} \qquad [\because \phi(p) = p-1]$$

$\square$

Euler's Theorem:-

If $(a, m) = 1$, then $a^{\phi(m)} \equiv 1 \pmod{m}$

Proof:- Let $S = \{a_1, a_2, \ldots, a_{\phi(m)}\}$ be a R.R.S mod m.

Since $(a, m) = 1$ and hence,

$S' = \{aa_i \mid a_i \in S\}$ is also a R.R.S mod m.

It is clear that for each $aa_i \in S'$, there exists exactly one element $a_j \in S$ such that

$$aa_i \equiv a_j \pmod{m}$$

Then $\displaystyle\prod_{i=1}^{\phi(m)} aa_i \equiv \prod_{j=1}^{\phi(m)} a_j \pmod{m}$

$$\Rightarrow a^{\phi(m)}\left(\prod_{i=1}^{\phi(m)} a_i\right) \equiv \left(\prod_{j=1}^{\phi(m)} a_j\right) \pmod{m}$$

$$\Rightarrow m \mid a^{\phi(m)}\left(\prod_{i=1}^{\phi(m)} a_i\right) - \left(\prod_{j=1}^{\phi(m)} a_j\right)$$

$$\Rightarrow m \,\Big|\, a^{\phi(m)}\left(\prod_{i=1}^{\phi(m)} a_i\right) - \left(\prod_{i=1}^{\phi(m)} a_i\right)$$

$$\Rightarrow m \,\Big|\, \prod_{i=1}^{\phi(m)} a_i \left(a^{\phi(m)} - 1\right)$$

$$\Rightarrow m \,\Big|\, a^{\phi(m)} - 1 \quad [\because (a_i, m) = 1]$$

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

* $\boxed{\phi(m) = m \prod_{p|m}\left(1 - \frac{1}{p}\right), \; m \geq 1}$

$\boxed{\phi(1) = 1}$.

Theorem:-

* Prove that $\phi(m) = m \prod_{p|m}\left(1 - \frac{1}{p}\right), \; m \geq 1$

Proof:-

Q) Find the number of integers from 1 to 250 (inclusive) which are not divisible by any of 3, 4 and 6

A:- A = Set of all integers from 1 to 250 which are divisible by 3.

B = Set of all integers from 1 to 250 which are divisible by 4

C = Set of all integers from 1 to 250 which are divisible by 6.

$|A| = \left\lfloor \frac{250}{3} \right\rfloor = 83$

$|B| = \left\lfloor \frac{250}{4} \right\rfloor = 62$

$|C| = \left\lfloor \frac{250}{6} \right\rfloor = 41$

$|A \cap B| = \left\lfloor \frac{250}{12} \right\rfloor = 20$

$|B \cap C| = \left\lfloor \frac{250}{12} \right\rfloor = 20$

$|A \cap C| = \left\lfloor \frac{250}{6} \right\rfloor = 41$

$|A \cap B \cap C| = \left\lfloor \frac{250}{12} \right\rfloor = 20$

$|A \cup B \cup C| = 83 + 62 + 41 - (20 + 20 + 41) + 20$

$= 206 - 81$

$= 125$

$|(A \cup B \cup C)'| = 250 - 125 = 125$

Q) Find the number of integers from 50 to 250 (inclusive) which are not divisible by any of 3, 4 and 6

A:- The numbers from 1 to 250 (inclusive) which are not divisible by any of 3, 4 and 6 = 125.

Now, consider the numbers from 1 to 49

$|A| = \left\lfloor \frac{49}{3} \right\rfloor = 16$

$|B| = \left\lfloor \frac{49}{4} \right\rfloor = 12$

$|C| = \left\lfloor \frac{49}{6} \right\rfloor = 8$

$|A\cap B| = \left\lfloor \frac{49}{12} \right\rfloor = 4$

$|B\cap C| = \left\lfloor \frac{49}{12} \right\rfloor = 4$

$|A\cap C| = \left\lfloor \frac{49}{6} \right\rfloor = 8$

$|A\cap B\cap C| = \left\lfloor \frac{49}{12} \right\rfloor = 4$.

$\therefore |A\cup B\cup C| = |A| + |B| + |C| - |A\cap B| - |B\cap C| - |A\cap C| + |A\cap B\cap C|$

$= 16 + 12 + 8 - 4 - 4 - 8 + 4$

$= 24$

$\therefore |(A\cup B\cup C)'| = 49 - 24 = 25$

$\therefore$ The number of integers from 50 to 250 (inclusive) which are not divisible by any of 3, 4 and 6 is

= The number of integers from 1 to 250 (inclusive) w.a.r d.b.a of 3,4 and 6 − T. N. of i.f. 1 to 49 (") "

" " " $= 125 - 25 = 100$

Dt:- 17.01.2020

$$\phi(m) = m \prod_{p|m}\left(1-\frac{1}{p}\right), \quad m>1$$

Proof:- Since $m>1$, by fundamental theorem of arithmetic consider $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, where $p_1, p_2, \ldots, p_k$ are distinct primes.

By definition, $\phi(m)$ = the no. of positive integers less than or equal to m which are co-prime to m.
= the no. of integers between 1 to m which are not divisible by any of the primes $p_1, p_2, \ldots, p_k$

Let A_i be the set of integers between 1 to m which are divisible by p_i

$$\therefore |A_i| = \left\lfloor \frac{m}{p_i} \right\rfloor = \frac{m}{p_i}$$

$$|A_i \cap A_j| = \left\lfloor \frac{m}{p_i p_j} \right\rfloor = \frac{m}{p_i p_j}, \quad i \neq j$$

$$\cdots |A_1 \cap A_2 \cap \cdots \cap A_k| = \left\lfloor \frac{m}{p_1 p_2 \cdots p_k} \right\rfloor = \frac{m}{p_1 p_2 \cdots p_k}$$

Now by the ~~P.I.E~~ Principle of inclusion & Exclusion,

$$\phi(m) = m - \sum_{i=1}^{k} |A_i| + \sum_{\substack{i,j=1 \\ i\neq j}}^{k} |A_i \cap A_j| - \cdots + (-1)^k |A_1 \cap A_2 \cap \cdots \cap A_k|$$

$$= m - \sum_{i=1}^{k} \frac{m}{p_i} + \sum_{\substack{i,j=1 \\ i \neq j}}^{k} \frac{m}{p_i p_j} - \cdots + (-1)^k \frac{m}{p_1 p_2 \cdots p_k}$$

$$= m \left[1 - \sum_{i=1}^{k} \frac{1}{p_i} + \sum_{\substack{i,j=1 \\ i \neq j}}^{k} \frac{1}{p_i p_j} - \cdots + (-1)^k \frac{1}{p_1 p_2 \cdots p_k} \right]$$

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

$$= m \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)$$

$$= m \prod_{p|m} \left(1 - \frac{1}{p}\right).$$ □

Theorem:- (theorem on gcd)

Let $d = (a, b)$, then there exists integers x_0 and y_0 such that $d = ax_0 + by_0$

Proof:- Let us consider a set S defined as,

$S = \{ax + by \mid x, y \in \mathbb{Z}\}$

It is clear that $0 \in S$, when $x = y = 0$

Let g be the smallest positive integer in S.

Let us consider $g = ax_0 + by_0$

If possible let us consider $g \nmid a$, then there exists two integers q and r such that

$a = g \cdot q + r \quad , 0 < r < g$

Then, $r = a - gq$

$= a - (ax_0 + by_0)q$

$= a(1 - x_0 q) + b(-y_0 q) \in S$

$\therefore r \in S$

which is a contradiction that g is the smallest positive integer in S

$\therefore g | a$

Similarly $g | b$

$\Rightarrow g | d$ ——— (1)

Again $(a,b) = d \Rightarrow d | a$ and $d | b$

since $g = ax_0 + by_0$

$\Rightarrow d | g$ ——— (2)

From (1) & (2), we have $g = d$

$\therefore d = ax_0 + by_0$

Theorem – 1.16

(The fundamental theorem of arithmetic, or the unique factorization theorem.)

The factoring of any integer $n > 1$ into primes is unique apart from the order of the prime factors.

* First proof:–

Suppose that there is an integer n with two different factorings. Dividing out any primes common to the two representations, we would have an equality of the form

$$p_1 p_2 \cdots\cdots p_r = q_1 q_2 \cdots\cdots q_s$$

where the factors p_i and q_j are primes, not necessarily all distinct, but where no primes on the left side occurs on the right side. But this is impossible because

$$p_1 \mid q_1 q_2 \cdots\cdots q_s ,$$

So p_1 is a divisor of at least one of the q_j i.e. p_1 must be identical with at least one of the q_j which is a contradiction.

* Second proof:-

Suppose that the theorem is false and let n be the smallest positive integer having more than one representation as the product of primes, say

$$n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s \qquad \text{——(1)}$$

It is clear that r and s are greater than 1.

Now the primes $p_1, p_2, \ldots, p_r$ have no members in common with $q_1, q_2, \ldots, q_s$, because if for example p_1 were a common prime, then we could divide it out of both sides of (1) to get two distinct factorings of $\frac{n}{p_1}$. But this would contradict our assumption that all integers smaller than n are uniquely factorable.

Next, without loss of generality assume that $p_1 < q_1$ and we define the positive integer N as,

$$N = (q_1 - p_1) q_2 q_3 \cdots\cdots q_s = p_1 p_2 \cdots p_r - p_1 q_2 q_3 \cdots q_s$$

$$= p_1 (p_2 p_3 \cdots\cdots p_r - q_2 q_3 \cdots\cdots q_s) \quad \text{---(2)}$$

It is clear that $N < n$, so that N is uniquely factorable into primes.

But $p_1 \nmid (q_1 - p_1)$

So eq(2) gives us two factorings of N one involving p_1 and other not, thus we have a contradiction.

So any integer $n > 1$ is uniquely factorable into primes apart from the order of prime factors.

Theorem:-

23.01.2020

For any integer x, $(a,b) = (b,a) = (a,-b) = (a, b+ax)$

Proof:-

Let $(a,b) = d$ & $(a, b+ax) = g$

Therefore there exists two integers x_0 and y_0 such that

$d = ax_0 + by_0$

$= a(x_0 - xy_0) + (b + ax) y_0$

Since $g = (a, b+ax)$ and $d = a(x_0 - xy_0) + (b+ax) y_0$

$\Rightarrow g | d$ as g is the smallest positive integers in

$S = \{ au + (b+ax)v \mid u, v \in \mathbb{Z} \}$

Since $d|a$ and $d|b$

$\Rightarrow d|a$ & $d | b+ax$

$\therefore d|g$

$\Rightarrow d = \pm g$

But both d and g are positive, so $d = g$.

$\therefore (a,b) = (a, b+ax)$.

Theorem:— (Wilson's theorem)

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

Proof:— For $p = 2$, $(2-1)! = 1! = 1 \equiv -1 \pmod 2$

$p = 3$, $(3-1)! = 2! = 2 \equiv -1 \pmod 3$

For $p \geq 5$, suppose $1 \leq a \leq p-1$, then $(a,p) = 1$ and the Linear congruence $ax \equiv 1 \pmod p$ (1) has uniqe solution

It is clear that $x = 0$ is not a solution of (1) for any a, $1 \leq a \leq p-1$

Now, we are interested to find the values of 'a' for which the solution of (1) is 'a' itself.

For this, we have

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

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

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

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

Thus for any a, $2 \le a \le p-2$, the congruence (1) has solution $a' \ne a$.

Then $2 \le a' \le p-2$

So there are $\frac{p-3}{2}$ pairs of elements (a, a') in $2 \le a, a' \le p-2$ such that $aa' \equiv 1 \pmod p$

So $\prod_{a=2}^{p-2} a \equiv 1 \pmod p$

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

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

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

24.01.2020

$a_1x_1 + b_1x_2 = c_1$
$a_2x_1 + b_2x_2 = c_2$

$\begin{vmatrix} a_1 & b_1 \\ a_2 & b_2 \end{vmatrix} \ne 0 \rightarrow$ unique solⁿ

$= 0 \rightarrow$ infinite solⁿ
$\rightarrow$ No solⁿ.

Chinese Remainder Theorem:-

Let $m_1, m_2, \ldots, m_r$ are mutually co-prime positive integers, then the system of linear congruences

$$x \equiv b_1 \pmod{m_1}$$
$$x \equiv b_2 \pmod{m_2}$$
$$\vdots$$
$$x \equiv b_r \pmod{m_r}$$

has unique solution modulo $M = m_1 \cdot m_2 \cdots m_r$.

Proof:- We have $M = m_1 \cdot m_2 \cdots m_r$

Consider $M_i = \dfrac{M}{m_i} \quad \forall \ i = 1, 2, \ldots, r$.

Then $(M_i, m_i) = 1$ as $(m_i, m_j) = 1 \ \forall \ j = 1, 2, \ldots, r$ & $j \neq i$.

Then the linear congruences $M_i x \equiv 1 \pmod{m_i}$ has unique solution for each $i = 1, 2, \ldots, r$.

Let c_i be the solution of ith congruence

i.e. $M_i c_i \equiv 1 \pmod{m_i}$

Consider an integer, $x_0 = \sum_{i=1}^{r} M_i c_i b_i$

$$\equiv M_i c_i b_i \pmod{m_i}$$
$$\equiv b_i \pmod{m_i}$$

$\therefore \ x_0 \equiv b_i \pmod{m_i} \ \forall \ i = 1, 2, \ldots, r$

So x_0 is a solution of the given system of linear congruence.

For uniqueness let us consider that y_0 is also a solution of the given system of linear congruence in modulo M.
So for each $i = 1, 2, \dots, r$

$$x_0 \equiv b_i \pmod{m_i} \quad \& \quad y_0 \equiv b_i \pmod{m_i}$$

$\Rightarrow x_0 \equiv y_0 \pmod{m_i}$

$\Rightarrow m_i \mid (x_0 - y_0) \quad \forall\ i = 1, 2, \dots, r$

$\Rightarrow M \mid (x_0 - y_0)$

$\Rightarrow x_0 \equiv y_0 \pmod{M}$

$\therefore$ The system of linear congruence has unique solution modulo M.

Q:- Solve
$$x \equiv 3 \pmod 8$$
$$x \equiv 5 \pmod 9$$
$$x \equiv 6 \pmod 7$$

A:- $m_1 = 8, \quad m_2 = 9, \quad m_3 = 7$

$M = m_1 m_2 m_3 = 8 \times 9 \times 7 = 504$

$M_1 = 9 \times 7 = 63$

$M_2 = 8 \times 7 = 56$

$M_3 = 8 \times 9 = 72$

Now, we have to solve the congruences
$$M_i x \equiv 1 \pmod{m_i} \quad \forall\ i = 1, 2, 3$$

$M_1 x = 63x \equiv 1 \pmod 8$ ——— (1)

$M_2 x = 56x \equiv 1 \pmod 9$ ——— (2)

$M_3 x = 72x \equiv 1 \pmod 7$ ——— (3)

eq(1) $63x \equiv 1 \pmod 8$

$\Rightarrow (-1)x \equiv 1 \pmod 8$

$\therefore$ $c_1 = -1$ is the solution of (1)

eq(2) $56x \equiv 1 \pmod 9$

$\Rightarrow 2x \equiv 1 \pmod 9$

$\therefore$ $c_2 = 5$ is the solution of (2)

eq(3) $72x \equiv 1 \pmod 7$

$\Rightarrow 2x \equiv 1 \pmod 7$

$\therefore$ $c_3 = 4$ is the solution of (3).

$\therefore$ $x_0 = \sum_{i=1}^{3} M_i c_i b_i$

$= M_1 c_1 b_1 + M_2 c_2 b_2 + M_3 c_3 b_3$

$= (63)(-1)3 + (56)(5)(5) + (72)(4)(6)$

$= -189 + 1400 + 1728$

$= 2939 \equiv 419 \pmod{504}$

Now, $\frac{2939}{504} = 419.$

Solve this .

* $5x \equiv 3 \pmod 8 \Rightarrow x \equiv 7 \pmod 8$

$7x \equiv 5 \pmod 9 \Rightarrow x \equiv 2 \pmod 9$

$2x \equiv 6 \pmod 7 \Rightarrow x \equiv 3 \pmod 7$

$m_1 = 8, \; m_2 = 9, \; m_3 = 7$

$M = m_1 m_2 m_3 = 8 \times 9 \times 7 = 504$

$M_1 = 9 \times 7 = 63$

$M_2 = 8 \times 7 = 56$

$M_3 = 8 \times 9 = 72$

Now, we have to solve the congruences

$M_i x \equiv 1 \pmod{m_i} \;\; \forall \; i = 1, 2, 3 .$

$M_1 x = 63x \equiv 1 \pmod 8$ ——— (i)

$M_2 x = 56x \equiv 1 \pmod 9$ ——— (ii)

$M_3 x = 72x \equiv 1 \pmod 7$ ——— (iii)

eq (i) $\Rightarrow 63x \equiv 1 \pmod 8$

$\Rightarrow 7x \equiv 1 \pmod 8$

$\therefore \; c_1 = 7$ is the solution of (i)

eq(ii) $\Rightarrow 56x \equiv 1 \pmod 9$

$\Rightarrow 2x \equiv 1 \pmod 9$

$\therefore \; c_2 = 5$ is the solution of (ii)

eq(iii) $\Rightarrow 72x \equiv 1 \pmod 7$

$\Rightarrow 2x \equiv 1 \pmod 7$

$\therefore \; c_3 = 4$ is the solution of (iii)

$$\therefore x_0 = \sum_{i=1}^{3} M_i c_i b_i$$

$$= (63)(7)(7) + (56)(2)(5) + (72)(3)(4)$$

$$= 3087 + 560 + 864$$

$$= 4511 \equiv 479 \pmod{504}$$

Q:-

$$6x \equiv 3 \pmod 9 \quad \text{———} (1)$$

$$2x \equiv 6 \pmod 8 \quad \text{———} (2)$$

$$21x \equiv 14 \pmod 7 \quad \text{———} (3)$$

eq(1) has 3 sol^n let 1 1

1 2 $\quad$ 3

1 3

$\times$

eq(2) has 2 sol^n let 2 1

2 2 $\quad$ 2 $\quad$ = 42 systems

and have

eq(3) has 7 sol^n let 3 1 $\quad \times \quad$ 42 sol^ns.

3 2

3 3

3 4 $\quad$ 7

3 5

3 6

3 7

27.01.2020

Find the primitive root of Z_8

$\{1, 2, 3, 4, 5, 6, 7\}$

$\phi(8) = 4$

$2 = 2$ $\quad$ $3 = 3$ $\quad$ $5 = 5$ $\quad$ $7 = 7$

$2^2 = 4$ $\quad$ $3^2 = 1$ $\quad$ $5^2 = 1$ $\quad$ $7^2 = 1$

$2^3 = 0$

$\therefore Z_8$ has no primitive roots

$2^2 \cdot 8$

$12 \times \frac{1}{2} \times \frac{2}{3}$

$Z_{12} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$

$5 = 5$ $\quad$ $7 = 7$ $\quad$ $11 = 11$

$5^2 = 1$ $\quad$ $7^2 = 1$ $\quad$ $11^2 = 1$

$\times_8$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

$n = 1, 2, 4, p^\alpha, 2p^\alpha$, p is odd prime

then primitive root exist.

and the group is cyclic under multiplication.

Exponent of a number :-

29.01.2020

The smallest positive integer f such that $a^f \equiv 1 \pmod{n}$ is called the exponent of a modulo n.

↳ It is denoted by $f = \exp_n(a)$

↳ If $\exp_n(a) = \phi(n)$, then a is called a primitive root modulo n.

Note:- Using Fermat's theorem $\boxed{\exp_n(a) \leq \phi(n)}$

Theorem:-

Given, $m \geq 1$, $(a,m) = 1$, let $\exp_m(a) = f$, then prove that

(1) $a^k \equiv a^h \pmod{m}$ iff $k \equiv h \pmod{f}$

H.W (2) $a^k \equiv 1 \pmod{m}$ iff $k \equiv 0 \pmod{f}$. In particular $f \mid \phi(m)$

(3) The numbers $1, a, a^2, \dots, a^{f-1}$ are incongruent modulo m.

1) Proof:-

$\Rightarrow$ Let us consider that $a^k \equiv a^h \pmod{m}$

$$\Rightarrow a^{k-h} \equiv 1 \pmod{m}$$

Then there exists two integers q and r such that

$$k-h = fq + r \quad , 0 \leq r < f$$

Then $1 \equiv a^{k-h} = a^{fq+r} = a^{fq} \cdot a^r = (a^f)^q \cdot a^r \equiv a^r \pmod{m}$

$\Rightarrow r = 0$

$\Rightarrow k \equiv h \pmod f$.

$\Leftarrow$ Conversely if $k \equiv h \pmod f$,

$\Rightarrow k-h = fq$, for some integer q.

$\therefore a^{k-h} = a^{fq} = (a^f)^q \equiv 1 \pmod m$

$\Rightarrow a^k \equiv a^h \pmod m$

$\square$

3) If possible let us consider that $a^t \equiv a^s \pmod m$,

where $0 \le t, s \le f-1$.

$\Rightarrow t \equiv s \pmod f$

$\Rightarrow f \mid (t-s)$

which is a contradiction

$\therefore a^t \not\equiv a^s \pmod m$, for $0 \le t, s \le f-1$

2) Let us consider that,

$a^k \equiv 1 \pmod m$

Then there exists two integers q and r such that

$k = fq + r$, $0 \le r < f$

Then $1 \equiv a^k = a^{fq+r} = a^{fq} \cdot a^r = (a^f)^q \cdot a^r$

$\equiv a^r \pmod m$

$\Rightarrow r = 0$

$\Rightarrow k \equiv 0 \pmod f$

$\Leftarrow$ If $k \equiv 0 \pmod f$

$\Rightarrow k = fq$, for some integer q.

$\therefore a^k = a^{fq} = (a^f)^q \equiv 1 \pmod m$

$\Rightarrow a^k \equiv 1 \pmod m$.

Thm:-

Let $(a,m) = 1$, then a is a primitive root modulo m iff the numbers $a, a^2, a^3, \ldots, a^{\phi(m)}$ form a reduced residue system modulo m.

Proof:-

Let a is a primitive root modulo m i.e. $exp_m(a) = \phi(m)$

~~then~~ and $S = \{a, a^2, a^3, \ldots\ldots, a^{\phi(m)} = 1\}$

then $|S| = \phi(m)$ and

the elements of S are incongruent modulo m.

Also $(a,m) = 1 \Rightarrow (a^t, m) = 1$

Thus S is a RRS modulo m.

Conversely,

let us consider that $S = \{a, a^2, \ldots, a^{\phi(m)}\}$ is a RRS modulo m.

$\therefore exp_m(a) = \phi(m)$

otherwise if $\exp_m(a) = t$, & $t < \phi(m)$, then

$$a^t \equiv 1 \pmod m$$

Then $a^t \equiv a^{\phi(m)} \pmod m$

Arise a contradiction that S is a R.R.S modulo m.

$\therefore$ a is primitive root modulo m.

$\square$

Theorem:- 30.01.2020

Let x be an odd integer. If $\alpha \geq 3$ we have

$$x^{\frac{\phi(2^\alpha)}{2}} \equiv 1 \pmod{2^\alpha} \quad \text{---(1)}$$

So there is no primitive root modulo 2^α.

Proof:- If $\alpha = 3$, then for any odd integer $x = 2k+1$

$$x^{\frac{\phi(8)}{2}} = (2k+1)^2 = 4k^2 + 4k + 1 = 4k(k+1) + 1$$
$$\equiv 1 \pmod 8$$

$\therefore$ (1) is true for $\alpha = 3$.

Assume that (1) is true for α.

~~then,~~ $\cancel{\phi(2^{\alpha+1}}$ $\cancel{x}$

then $x^{\frac{\phi(2^\alpha)}{2}} - 1 = t\,2^\alpha$, for some integer t.

or $x^{\frac{\phi(2^\alpha)}{2}} = 1 + t\,2^\alpha$

Squaring both sides,

$$x^{\phi(2^\alpha)} = (1+t2^\alpha)^2$$

$$\Rightarrow x^{\phi(2^\alpha)} = 1+t2^{\alpha+1}+t^2 2^{2\alpha}$$

$$\equiv 1 \pmod{2^{\alpha+1}} \quad \text{------ (2)}$$

as $2\alpha > \alpha+1$, $\alpha \geq 3$

Now, $\phi(2^{\alpha+1}) = 2^{\alpha+1}\left(1-\frac{1}{2}\right) = 2^\alpha = 2\cdot 2^{\alpha-1} = 2\phi(2^\alpha)$

$$\therefore \phi(2^\alpha) = \frac{\phi(2^{\alpha+1})}{2}$$

$$\therefore (2) \Rightarrow x^{\frac{\phi(2^{\alpha+1})}{2}} \equiv 1 \bmod (2^{\alpha+1}).$$

Thus $x^{\frac{\phi(2^\alpha)}{2}} \equiv 1 \pmod{2^\alpha}$ for $\alpha \geq 3$.

$$\Rightarrow \exp_{2^\alpha}(x) \leq \frac{\phi(2^\alpha)}{2}$$

$$\Rightarrow \exp_{2^\alpha}(x) \neq \phi(2^\alpha)$$

So x is not a primitive root modulo 2^α.

Lemma:-

Given $(a,m)=1$, let $f=\exp_m(a)$. Then $\exp_m(a^k)=\dfrac{\exp_m(a)}{(k,f)}$

In particular $\exp_m(a^k)=\exp_m(a)$ iff $(k,f)=1$

Proof:- The $\exp_m(a^k)$ is the smallest positive integer x such that $(a^k)^x \equiv 1 \pmod m$

or, $a^{kx} \equiv 1 \pmod m$

This is also smallest $x>0$ such that $kx \equiv 0 \pmod f$

But this congruence is equivalent to the congruence $x \equiv 0 \pmod{\frac{f}{d}}$, where $d=(k,f)$

$\Rightarrow$ x is the smallest positive integer which is multiple of $\frac{f}{d}$.

$\therefore$ $x = \dfrac{f}{d}$

$\therefore$ $\exp_m(a^k) = \dfrac{f}{d} = \dfrac{\exp_m(a)}{(k,f)}$

Theorem:- 31.01.2020

Let p be an odd prime and d be any positive divisor of $p-1$, then in every R.R.S modulo p, there exists exactly $\phi(d)$ numbers a such that $\exp_p(a)=d$

In particular, when $d=\phi(p)=p-1$, there are exactly $\phi(p-1)$ primitive roots.

Proof:-

$* \; n=10$
$d = 1, 2, 5, 10$
$\sum_{d|n} \phi(d) = \phi(1)+\phi(2)+\phi(5)+\phi(10)$
$= 1+1+4+4 = 10 = n$

We know that,

$$\sum_{d|n} \phi(d) = n \quad \text{———} (1)$$

The numbers $1, 2, \ldots, p-1$ are distributed into disjoint sets $A(d)$ each set corresponding to a divisor d of $p-1$ and defined as,

$$A(d) = \{x : 1 \le x \le p-1 \text{ and } \exp_p(x) = d\}$$

Let $f(d)$ be the no. of elements in $A(d)$.

then $f(d) \geq 0$, for each d.

We have to prove that $f(d) = \phi(d)$

Since the sets $A(d)$ are disjoints and since each $x = 1, 2, \ldots, p-1$ belongs to some $A(d)$.

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

From (1), we have $\sum_{d|p-1} \phi(d) = p-1 \quad \text{———} (3)$

$$\therefore \sum_{d|p-1} (\phi(d) - f(d)) = 0 \quad \text{———} (4)$$

To show each term in this sum is zero, it is sufficient to prove that $f(d) \le \phi(d)$

We show this ~~considering~~ proving either $f(d)=0$ or $f(d) = \phi(d)$.

Suppose $f(d) \neq 0$, then $A(d)$ is non-empty. So there exists $a \in A(d)$

$\therefore \exp_p(a) = d$, hence $a^d \equiv 1 \pmod p$

But every power of a satisfies the same congruence, so the d numbers $a, a^2, \dots, a^d$ are solution of the congruence $x^d - 1 \equiv 0 \pmod p$ ——— (5)

These solutions are incongruent modulo p as $\exp_p(a) = d$

But (5) has at most 'd' solutions, since the modulous is prime.

$\therefore$ The d numbers $a, a^2, \dots, a^d$ are all solutions of (5)

Hence each number in $A(d)$ must be in the form a^k for some $k = 1, 2, \dots, d$, there are some elements a^k such that $\exp_p(a^k) = d$ and they are a^k with $(k, d) = 1$.

$\therefore f(d) = |A(d)| = \phi(d)$.

$\therefore$ Each term of (4) are ≥ 0

$\Rightarrow f(d) = \phi(d)$ for each d.

06.02.2020

If $x^2 \equiv a \pmod{n}$ has a solution then 'a' is a quadratic residue.

Theorem :-

Let g be a primitive root mod p, where p is an odd prime, then the even powers $g^2, g^4, \ldots\ldots, g^{p-1}$ are quadratic residues and the odd powers $g, g^3, \ldots\ldots, g^{p-2}$ are ~~non~~ non-quadratic residues.

Proof:- If n is even, then $n = 2m$ (say)

and $g^n = g^{2m} = (g^m)^2$

$\therefore g^n \equiv x^2 \pmod{p}$, where $x = g^m$

$\therefore g^n$ is a quadratic residue.

We know that for $exp_n(a) = f$, the numbers $a, a^2, \ldots\ldots, a^f$ are incongruent to each other.

So $g, g^2, g^3, \ldots, g^{p-1}$ are pairwise incongruent.

So the even powers of g i.e. $g^2, g^4, \ldots, g^{p-1}$ are $\frac{p-1}{2}$ incongruent numbers each of which is a quadratic residues.

Since there are exactly $\frac{p-1}{2}$ quadratic residues for odd prime p, so the remaining numbers with odd power of g i.e. $g, g^3, g^5, \ldots\ldots, g^{p-2}$ are $\frac{p-1}{2}$

quadratic non-residues.

Theorem:-

Let g be a primitive root modulo p such that $g^{p-1} \not\equiv 1 \pmod{p^2}$ ---(1), then for every $\alpha \geq 2$ we have

$$g^{\phi(p^{\alpha-1})} \not\equiv 1 \pmod{p^\alpha} \quad ---(2)$$

Proof:- We shall prove the result by mathematical induction on α.

For $\alpha = 2$, it is clear that (2) reduce, to (1) which is our assumption.

So the result is true for $\alpha = 2$.

Suppose that (2) holds for α.

By Euler's Fermat's theorem, we have

$$g^{\phi(p^{\alpha-1})} \equiv 1 \pmod{p^{\alpha-1}}$$

$$\Rightarrow g^{\phi(p^{\alpha-1})} = 1 + k \cdot p^{\alpha-1}$$

, where $p \nmid k$ because of (2).

$$\therefore \left(g^{\phi(p^{\alpha-1})}\right)^p = \left(1 + k \cdot p^{\alpha-1}\right)^p$$

or $$g^{\phi(p^\alpha)} = 1 + kp^\alpha + \frac{p(p-1)}{2} k^2 p^{2(\alpha-1)} + r p^{3(\alpha-1)}$$

where r is an integer

Since $2(\alpha-1) \geq \alpha+1$ and $3(\alpha-1) \geq \alpha+1$,

Therefore,

$$g^{\phi(p^\alpha)} \equiv 1 + kp^\alpha \pmod{p^{\alpha+1}}$$

But $p \nmid k \Rightarrow g^{\phi(p^{\alpha})} \not\equiv 1 \pmod{p^{\alpha+1}}$

So the result (2) is true for $\alpha+1$ which completes the proof of the result.

07.02.2020

Statement :-

Let p be an odd prime, then we have

(a) If g is a primitive root modulo p, then g is also a primitive root modulo p^{α} $\forall$ $\alpha \geq 1$ iff

$$g^{p-1} \not\equiv 1 \pmod{p^2} \quad \text{——— (1)}$$

(b) There is at least one primitive root modulo p which satisfies (1), hence there is a primitive root modulo p^{α} for all $\alpha \geq 2$.

Proof of (b)

Let g be a primitive root mod p.

If g satisfies (1) then nothing to prove.

If not we have, $g^{p-1} \equiv 1 \pmod{p^2}$

Now consider the primitive root,

$$g_1 = g + p \quad \text{mod } p$$

We shall show that, $g_1^{p-1} \not\equiv 1 \pmod{p^2}$

We have, $g_1^{p-1} = (g+p)^{p-1} = g^{p-1} + (p-1)g^{p-2}p + \frac{(p-1)(p-2)}{2} g^{p-3}p^2 + \dots$

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

$$\equiv 1 + p(p-1)g^{p-2} \pmod{p^2}$$

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

Since $(g,p)=1$, $p^2 \nmid pg^{p-2}$, so

$$g_1^{p-1} \not\equiv 1 \pmod{p^2}$$

$\Rightarrow g_1$ satisfies (1).

Proof of (a)

$\Rightarrow$ Let g be a primitive root modulo p which is also a primitive root modulo p^α for all $\alpha \geq 1$.

In particular if $\alpha = 2$, then

$$\exp_{p^2}(g) = \phi(p^2) = p^2\left(1-\frac{1}{p}\right) = p(p-1)$$

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

12.02.2020

$\Leftarrow$ Suppose that g is a primitive root modulo p which satisfies (1).

Then we have to show that g is also a primitive root modulo p^α, $\alpha \geq 2$

Let us consider that t is the exponent of g modulo p^α

Now, we are interested to show that, $t = \phi(p^\alpha)$.

Since $g^t \equiv 1 \pmod{p^\alpha}$

$$\Rightarrow g^t \equiv 1 \pmod{p}$$

As g is a primitive root modulo p, we have

$\phi(p) \mid t$

Consider, $t = q \cdot \phi(p)$

Also $t \mid \phi(p^\alpha)$

$$\left[\begin{array}{l} g^t \equiv 1 \pmod{p^\alpha} \\ g^{\phi(p^\alpha)} \equiv 1 \pmod{p^\alpha} \end{array}\right]$$

$\Rightarrow q \cdot \phi(p) \mid \phi(p^\alpha)$

But $\phi(p^\alpha) = p^{\alpha-1}(p-1)$

$\Rightarrow q(p-1) \mid p^{\alpha-1}(p-1)$

$\Rightarrow q \mid p^{\alpha-1}$

Consider $q = p^\beta$, where $\beta \le \alpha - 1$

$\therefore t = p^\beta (p-1)$

Now, we have to show that, $\beta = \alpha - 1$

If possible let us consider that $\beta < \alpha - 1$

i.e. $\beta \le \alpha - 2$

$\Rightarrow t = p^\beta(p-1) \mid p^{\alpha-2}(p-1) = \phi(p^{\alpha-1})$

$\Rightarrow \phi(p^{\alpha-1})$ is a multiple of t.

$\Rightarrow g^{\phi(p^{\alpha-1})} \equiv 1 \pmod{p^\alpha}$ ——— (2)

We know that for any primitive root g modulo p which satisfies $g^{p-1} \not\equiv 1 \pmod{p^2}$, we have
$g^{\phi(p^{\alpha-1})} \not\equiv 1 \pmod{p^\alpha}$ for all $\alpha \geq 2$.

Thus ② rise a contradiction and hence $\beta = \alpha - 1$ and $t = p^{\alpha-1}(p-1) = \phi(p^\alpha)$

Theorem:-

If p is an odd prime & $\alpha \geq 1$, there exists an odd primitive root g mod p^α. Each such g is also a primitive root modulo $2p^\alpha$

Proof:-

If g is a primitive root modulo p^α so is $g + p^\alpha$. But one of g or $g+p^\alpha$ is odd primitive root modulo p^α exist.

Let g be an odd primitive root modulo p^α. Then we have to show that g is also a primitive root mod $2p^\alpha$. Let us consider t be the exponent of g mod $2p^\alpha$. Then we have to show that $t = \phi(2p^\alpha)$.

It is clear that $t \mid \phi(2p^\alpha)$ $\left[\begin{array}{l} g^t \equiv 1 \pmod{2p^\alpha} \\ g^{\phi(2p^\alpha)} \equiv 1 \pmod{2p^\alpha} \end{array} \right.$

Also $\phi(2p^\alpha) = \phi(2)\phi(p^\alpha)$
$= \phi(p^\alpha)$

$\Rightarrow t \mid \phi(p^\alpha)$

On the otherhand, $g^t \equiv 1 \pmod{2p^\alpha}$

$\Rightarrow g^t \equiv 1 \pmod{p^\alpha}$

As g is a primitive root mod p^α, $g^{\phi(p^\alpha)} \equiv 1 \pmod{p^\alpha}$

$\Rightarrow \phi(p^\alpha) \mid t$

Therefore $t = \phi(p^\alpha) = \phi(2p^\alpha)$

$\therefore g$ is a primitive root modulo $2p^\alpha$.

HW

Q:- Find a primitive root modulo 250.

A:- $250 = 2 \times 5^3$

$\phi(5) = 4$

primitive root modulo $5 = 2, 3$

Now, 5 is an odd prime

2 is primitive root modulo 5

$2^{5-1} = 2^4 \not\equiv 1 \pmod{5^2}$

$\Rightarrow$ 2 is a primitive root modulo 5^3.

But 2 is not odd. So it is not primitive root modulo 2×5^3.

$\therefore 2 + 5^3 = 127$ is an odd primitive root modulo 250.

Now, $3^{5-1} = 3^4 \not\equiv 1 \pmod{5^2}$

$\Rightarrow$ 3 is a primitive root modulo 5^3.

Since 3 is odd, so it is primitive root modulo 250.

$\therefore$ 3 is a primitive root modulo 250.

13.01.2020

$\cancel{250} \times \frac{1}{\cancel{2}} \times \frac{4}{5} = 100$ $\quad 5^2 \times 2^2, \; \cancel{100} \times \frac{4}{5} \times \frac{1}{2} = 40$

$\phi(\phi(250)) = \phi(100) = 40$

No. of primitive roots modulo $n = \phi(\phi(n))$

Let $n = 10$
$= 2 \times 5$

primitive root mod 5 $\rightarrow 2, 3$

3 is a primitive root mod 10

$\phi(10) = 4$

$\underbrace{3^1, 3^2, 3^3, 3^4}$ co-prime

$3^3 \equiv 7 \pmod{10}$

$\therefore$ 3, 7 are primitive root mod 10.

Q:- Find all primitive root modulo 50.

A:- $50 = 2 \times 5^2$

$\therefore$ Primitive root mod 50 exists.

Primtive root modulo 5 is 2 and 3

Let 3 is primitive root mod 5

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

~~Since 3 is odd~~

$\therefore$ 3 is a primitive root mod 5^2

Since 3 is odd primitive root mod 5^2

So 3 is a primitive root mod 50

$\phi(50) = 50 \times \frac{1}{2} \times \frac{4}{5} = 20$

$\phi(20) = \phi(2^2 \times 5) = 20 \times \frac{1}{2} \times \frac{4}{5} = 8$

$\therefore 3, 3^3, 3^7, 3^9, 3^{11}, 3^{13}, 3^{17}, 3^{19}$ are primitive roots modulo 50.

3, 9, 37, 33,

Theorem:-

20.02.2020

Given, $m \geq 1$, where m is not in the form of $1, 2, 4, p^\alpha$ and $2p^\alpha$, where p is an odd prime, then for any a with $(a, m) = 1$, we have

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

So there are no primitive roots modulo m.

Proof:-

We know that, there are no primitive roots modulo 2^α, $\alpha \geq 3$.

Also we have seen that for any odd integer x

$$x^{\frac{\phi(2^\alpha)}{2}} \equiv 1 \pmod{2^\alpha}$$

Therefore the result is true for 2^α, $\alpha \geq 3$.

Therefore we can suppose that m has the factorisation.
$m = 2^{\alpha} p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$, where p_i's are odd primes, $s \geq 1$ and $\alpha \geq 0$.

Since m is not of the form 1, 2, 4, p^{α} and $2p^{\alpha}$. We have $\alpha \geq 2$ if $s = 1$ and $s \geq 2$ if $\alpha = 0$ or $\alpha = 1$

Note that, $\phi(m) = \phi(2^{\alpha}) \cdot \phi(p_1^{\alpha_1}) \phi(p_2^{\alpha_2}) \cdots \phi(p_s^{\alpha_s})$

Now consider integer a with $(a, m) = 1$

then we have to show that, $a^{\frac{\phi(m)}{2}} \equiv 1 \pmod{m}$

Let g be a primitive root modulo $p_1^{\alpha_1}$

Then there exists an integer k such that $g \equiv a^k \pmod{p_1^{\alpha_1}}$

Therefore $a^{\frac{\phi(m)}{2}} \equiv g^{k\frac{\phi(m)}{2}}$

This is congruent to $g^{t\phi(p_1^{\alpha_1})}$ modulo $p_1^{\alpha_1}$

i.e. $a^{\frac{\phi(m)}{2}} \equiv g^{k\frac{\phi(m)}{2}} \equiv g^{t\phi(p_1^{\alpha_1})} \pmod{p_1^{\alpha_1}}$ ——(1)

where $t = \dfrac{k \cdot \phi(2^{\alpha}) \cdot \phi(p_2^{\alpha_2}) \cdots \phi(p_s^{\alpha_s})}{2}$

We claim that t is an integer.

If $\alpha \geq 2$ the factor $\phi(2^{\alpha})$ is even implies that t is an integer.

If $\alpha = 0$ or 1, $s \geq 2$ and the factor $\phi(p_2^{\alpha_2})$ is even implies that t is an integer.

$\therefore$ ① $\Rightarrow a^{\frac{\phi(m)}{2}} \equiv \left(g^{\phi(p_1^{\alpha_1})}\right)^{t} \equiv 1 \pmod{p_1^{\alpha_1}}$ —— ②

In the same way we can find that

$$a^{\frac{\phi(m)}{2}} \equiv 1 \pmod{p_i^{\alpha_i}} \quad \forall\ i = 1, 2, \dots, s. \quad \text{—— ②}$$

Also we have $a^{\frac{\phi(2^\alpha)}{2}} \equiv 1 \pmod{2^\alpha}$, $\alpha \geq 3$

$$\Rightarrow a^{\frac{\phi(m)}{2}} \equiv 1 \pmod{2^\alpha} \quad \text{as } \phi(2^\alpha) \mid \phi(m) \quad \text{—— ③}$$

If $\alpha \leq 2$, then $a^{\phi(2^\alpha)} \equiv 1 \pmod{2^\alpha}$

But $s \geq 1$, so $\phi(m) = \phi(2^\alpha)\,\phi(p_1^{\alpha_1}) \cdots \phi(p_s^{\alpha_s})$
$= 2r\,\phi(2^\alpha)$, where r is an integer.

Therefore $a^{\frac{\phi(m)}{2}} \equiv a^{r\phi(2^\alpha)} = \left(a^{\phi(2^\alpha)}\right)^{r} \equiv 1 \pmod{2^\alpha}$ — ④

Combining ②, ③ and ④ we have

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

$\Rightarrow$ exponent of a modulo m, $\exp_m(a) \leq \frac{\phi(m)}{2}$

So a is not a primitive root modulo m. □

Theorem:- 04.03.2020

If m has a primitive root g, then m has exactly $\phi(\phi(m))$ incongruent primitive roots and they are given by the numbers in the set

$$S = \{ g^n, 1 \le n \le \phi(m) \text{ and } (n, \phi(m)) = 1 \}$$

Proof:- Since g is a primitive root modulo m, $\exp_m(g) = \phi(m)$.
We know that $\exp_m(g^k) = \exp(g)$ iff $(k, \phi(m)) = 1$.
Therefore each element of S is a primitive root modulo m.

Conversely if a is a primitive root modulo m, then $a \equiv g^k \pmod m$ for some $k = 1, 2, \ldots, \phi(m)$
Hence, $\exp_m(a) = \exp_m(g^k) = \exp_m(g)$, so $(k, \phi(m)) = 1$
$\Rightarrow a \in S$

Therefore S contains $\phi(\phi(m))$ primitive roots modulo m
Hence m has exactly $\phi(\phi(m))$ primitive roots.

Q:- Find all primitive roots of 50 if exists.

A:- $50 = 2 \times 5^2$

$\phi(50) = 5\cancel{0} \times \frac{1}{\cancel{2}} \times \frac{4}{\cancel{5}} = 20$

Defn :- An arithmetic function f is said to be multiplicative if $f(ab) = f(a)f(b)$, where $(a,b)=1$.

An arithmetic function is said to be completely multiplicative if $f(ab) = f(a)f(b)$ $\forall$ $a,b \in \mathbb{Z}$.

$\sigma_0(n)$ = no. of divisors of n (not σm but m)

$\sigma_1(n)$ = sum of the divisors of n (not σm but m)

$\sigma_2(n)$ = sum of the square of divisors of n

$$\sigma_k(n) = \sum_{d|n} d^k$$

$\sigma_k(n)$ is not completely multiplicative but multiplicative

Q:- Show that $\phi(n)$ is multiplicative but not completely multiplicative.

Lagrange's Theorem

05.08.2020

Given, a prime p, let $f(x) = c_0 + c_1 x + c_2 x^2 + \dots + c_n x^n$ be a polynomial of degree n with integer co-efficients, $c_n \not\equiv 0 \pmod p$. Then the polynomial congruence $f(x) \equiv 0 \pmod p$ has at most n solutions. —①

Proof:-

We shall prove the result using mathematical induction on the degree of polynomial n.

For $n=1$, the congruence is $c_0 + c_1 x \equiv 0 \pmod p$, $c_1 \not\equiv 0 \pmod p$.

Then it has unique solution.

So the result is true for $n=1$.

Assume that the result is true for polynomials of degree $n-1$.

Furthermore, assume that ① has $n+1$ solutions, say $x_0, x_1, \dots, x_n$

Therefore, $f(x_k) \equiv 0 \pmod p \ \forall \ k = 0, 1, 2, \dots, n$

Now consider the following identity ~~f(x) - f(x₀)~~

$$f(x) - f(x_0) = \sum_{r=1}^{n} (x^r - x_0^r) c_r = (x - x_0) g(x)$$

where $g(x)$ is a polynomial of degree $(n-1)$ with integer co-efficients and leading co-efficient c_n.

It is clear that $f(x_k) - f(x_0) \equiv 0 \pmod{p}$ $\forall$ $k=1,2,\ldots,n$

as $f(x_k) \equiv 0 \pmod{p}$ $\forall$ $k = 0,1,2,\ldots,n$

Therefore $f(x_k) - f(x_0) = (x_k - x_0)g(x) \equiv 0 \pmod{p}$ $\forall k \neq 0$

But $x_k - x_0 \not\equiv 0 \pmod{p}$ $\forall$ $k \neq 0$ as $x_0, x_1, \ldots, x_n$ are incongruent solutions of ① mod p.

$\Rightarrow g(x_k) \equiv 0 \pmod{p}$ $\forall$ $k \neq 0$

$\Rightarrow$ The polynomial congruence $g(x) \equiv 0 \pmod{p}$ has n solutions $x_1, x_2, \ldots, x_n$

and $g(x)$ is a polynomial of degree $n-1$.

which is a contradiction

$\therefore$ ① has atmost n solutions.

□

Q:- Solve this,

$f(x) = 2x^2 + 3x + 1 \equiv 0 \pmod{5^2}$

Solⁿ:- Consider,

$f(x) \equiv 0 \pmod{5}$

$2x^2 + 3x + 1 \equiv 0 \pmod{5}$ ——— ①

$\therefore$ $r = 2$ is a solution of ①

$r = 4$ is a solution of ①

r = 2

$f'(x) = 4x + 3$

$f'(r) = f'(2) = 11$

$(f'(r), 5) = 1$

$f(2) = 15 = 5 \cdot 3$

$k = 3$

$qf'(r) + k \equiv 0 \pmod 5$

$\Rightarrow 11q + 3 \equiv 0 \pmod 5$

$\Rightarrow 11q \equiv -3 \pmod 5$

$\Rightarrow q \equiv -3 \pmod 5$

$\therefore q = 2$.

$a = r + qp = 2 + 2 \times 5 = 12$

$\underline{r = 4}$

$f'(4) = 19$

$(19, 5) = 1$

$\therefore$ So $r = 4$ can be lifted in one way

$f(4) = 45 = 5 \cdot 9$

$k = 9$

$qf'(4) + k \equiv 0 \pmod 5$

$\Rightarrow 19q + 9 \equiv 0 \pmod 5$

$\Rightarrow 19q \equiv -9 \pmod 5$

$\Rightarrow 4q \equiv -9 \pmod 5$

$\Rightarrow 4q \equiv 1 \pmod 5$

$\therefore q = 4$

$\therefore a = r + qp = 4 + 4 \cdot 5 = 24$

* Show that ϕ function is multiplicative.

i.e. $\phi(mn) = \phi(m)\cdot\phi(n)$, where $(m,n)=1$.

Proof:- Let $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$

$n = q_1^{\beta_1} q_2^{\beta_2} \cdots q_r^{\beta_r}$

with $p_i \neq q_j$ for any $i=1,2,\dots,k$ and $j=1,2,\dots,r$

then , $\phi(m) = m\prod_{i=1}^{k}\left(1-\frac{1}{p_i}\right)$ and

$\phi(n) = n\prod_{i=1}^{r}$

13.02.202

Theorem:-

Assume $\alpha \geq 2$ and let r be a solution of the congruence $f(x) \equiv 0 \pmod{p^{\alpha-1}}$ — ① lying in the interval $0 \leq r < p^{\alpha-1}$

ⓐ Assume $f'(r) \not\equiv 0 \pmod{p}$, then r can be lifted in a unique way from $p^{\alpha-1}$ to p^{α}. i.e. there is a unique 'a' in the interval $0 \leq a < p^{\alpha}$ which is generated by r and satisfies the congruence

$f(x) \equiv 0 \pmod{p^{\alpha}}$ — ②

ⓑ Assume $f'(r) \equiv 0 \pmod{p}$, then there are two possibilities.

(b1) If $f(r) \not\equiv 0 \pmod{p^{\alpha}}$, then r can be lifted from $p^{\alpha-1}$ to p^{α} in p distinct ways.

(b2) If $f'(r) \not\equiv 0 \pmod{p^{\alpha}}$, r can not be lifted from $p^{\alpha-1}$ to p^{α}.

Proof:-

If n is the degree of f, by Taylor's theorem

$$f(x+h) = f(x) + hf'(x) + \frac{h^2}{2!} f''(x) + \frac{h^3}{3!} f^{(3)}(x) + \cdots + \frac{h^n}{n!} f^{n}(x), \quad \text{— ③}$$

for every x and h.

We note that each polynomial $\frac{f^k(x)}{k!}$ has integer co-efficients.

Now take $x = r$, where r is a solution of (1) & $0 \le r < p^{\alpha-1}$

Let $h = q \cdot p^{\alpha-1}$, where q is an integer to be specified presently.

Since $\alpha \geq 2$, the terms in (3) involving h^2 and higher power of h are integer multiple of p^α.

Therefore (3) becomes

$h^2 = q^2 p^{2\alpha-2}$, $2\alpha - 2 \geq \alpha$ for $\alpha \geq 2$

$$f(r + qp^{\alpha-1}) \equiv f(r) + qp^{\alpha-1} f'(r) \pmod{p^\alpha} \quad \text{--- (4)}$$

Since r satisfies (1), we can write

$f(r) = kp^{\alpha-1}$, for some integer k.

Therefore (4) becomes

$$f(r + qp^{\alpha-1}) \equiv \left(kp^{\alpha-1} + qp^{\alpha-1} f'(r)\right) \pmod{p^\alpha}$$

$$= p^{\alpha-1}\left(k + qf'(r)\right) \pmod{p^\alpha}$$

Now, let $a = r + qp^{\alpha-1}$, then 'a' satisfies (2) iff the linear congruence $qf'(r) + k \equiv 0 \pmod{p}$ --- (5)

If $f'(r) \not\equiv 0 \pmod{p} \Rightarrow (f'(r), p) = 1$ and we can find unique q which satisfies (5), and hence unique 'a' generated by r.

If $f'(r) \equiv 0 \pmod{p}$ and $p|-k$ i.e. $p|k = \frac{f(r)}{p^{\alpha-1}}$

i.e. $f(r) \equiv 0 \pmod{p^\alpha}$

then (5) has p solution.

Hence there are p solutions of (2) generated by r.

If $f'(r) \equiv 0 \pmod p$ and $p \nmid -k$ i.e. $f(r) \not\equiv 0 \pmod p$

there is no solution of (5), hence r can not be lifted from $p^{\alpha-1}$ to p^{α}.

Solve:- $3x^2+2x+1 \equiv 0 \pmod{7^3}$ —— (1)

Sol^n:- $f(x) = 3x^2+2x+1$

$f'(x) = 6x+2$

Consider, $3x^2+2x+1 \equiv 0 \pmod 7$ —— (2)

$r=1$ and $r=3$ are solutions of (2).

$r=1$

$f'(r) = f'(1) = 8 \not\equiv 0 \pmod 7$

$\therefore$ $r=1$ can be lifted in unique way from 7 to 7^2.

$(f'(r), 7) = (8,7) = 1$.

$$k = \frac{f(r)}{p^{\alpha-1}} = \frac{7}{7} = 1 \quad [\text{Here } \alpha = 2]$$

$8q+1 \equiv 0 \pmod 7$

$\Rightarrow q+1 \equiv 0 \pmod 7$

$\therefore q = 6$

The req. sol^n is,

$a = r + qp^{\alpha-1}$

$= 1+6\cdot 7 = \underline{43}$

$r = 3$

$f'(r) = f'(3) = 20 \not\equiv 0 \pmod{7}$

$\therefore$ $r = 3$ can be lifted in unique way from 7 to 7^2.

$k = \frac{f(r)}{p^{\alpha-1}} = \frac{35}{7} = 5$

$f'(r)q + k \equiv 0 \pmod{p}$

$20q + 5 \equiv 0 \pmod{7}$

$\Rightarrow$ $-q + 5 \equiv 0 \pmod{7}$

$\therefore$ $q = 5$

$\therefore$ The req. solution is,

$a = r + qp^{\alpha-1}$

$= 3 + 5 \cdot 7$

$= \underline{\underline{38}}$

$\therefore$ The solutions $f(x) \equiv 0 \pmod{7^2}$ are $r = 43$, $r = 38$

✍
Submitted by
Sarojini Mohapatra
(MSc Math Student)
Central University of Jharkhand

Some Useful Links:

1. Free Maths Study Materials (https://pkalika.in/2020/04/06/free-maths-study-materials/**)**

2. BSc/MSc Free Study Materials (https://pkalika.in/2019/10/14/study-material/**)**

3. MSc Entrance Exam Que. Paper: (https://pkalika.in/2020/04/03/msc-entrance-exam-paper/**)**
[JAM(MA), JAM(MS), BHU, CUCET, ...etc]

4. PhD Entrance Exam Que. Paper: (https://pkalika.in/que-papers-collection/**)**
[CSIR-NET, GATE(MA), BHU, CUCET,IIT, NBHM, ...etc]

5. CSIR-NET Maths Que. Paper: (https://pkalika.in/2020/03/30/csir-net-previous-yr-papers/**)**
[Upto 2019 Dec]

6. Practice Que. Paper: (https://pkalika.in/2019/02/10/practice-set-for-net-gate-set-jam/**)**
[Topic-wise/Subject-wise]

(Provide your Feedbacks/Comments at maths.whisperer@gmail.com)