Number Theory: Notes

by

Anwar Khan

Partial Contents

These are the handwritten notes. We are very thankful to Mr. Anwar Khan for providing these notes.

1. Number Theory 1
2. Divisibility 2
3. Euclids Theorem 15
4. Base of Radix Representation 19
5. Common Division 21
6. Method of finding great common divisor 23
7. G.C.D. more than two integers 38
8. Least Common Multiple 39
9. The Linear Diophantine Equation 45
10. Theory of Primes 54
11. Composite Number 54
12. Prime Divisor 54
13. Congruence 61
14. Complete Residue System 85
15. Solutions of the Congruence 102
16. Perfect Number 107
17. Reduce residue System 123
18. Quadratic residue 191
19. Arithmetic Function 205

Number Theory:-

Number Theory is also called arithematic. It is mathematical theory that study the property and relations of integers and their extension both algebric and analytic.

Number:- This also called a natural number one of the unique sequence of element used for counting a collection of individual. For e.g The number of english alphabits is 26.

Divisblity:- let $a, b \in \mathbb{Z}$, we say that 'a' divides 'b' if $\exists$ an integer $c \in \mathbb{Z}$. Then s.t

$b = ac$, Then a is called divisor or facter of b and b is called multiple of a.

Symbolically it can be written as.

$a \mid b$ and read as 'a' divides 'b'

If a doesnot divides b then we write

$a \nmid b$.

Theorem:-

i) Prove that $a|0 \quad \forall \; a \in Z$ $(a \neq 0)$

Proof:- we can write

$$0 = a(0) \text{ where } 0 \in Z.$$

$$\Rightarrow a|0$$

Hence Proved.

ii) Prove that $a|a \quad \forall \; a \in Z$.

Proof:- we can write

$$a = a(1) \quad \text{where } 1 \in Z$$

$$\Rightarrow a|a \quad \text{Hence proved.}$$

iii) if $a|b$ and $c \in Z$. Then

$a|bc$

Proof

Since $a|b$. Therefore $\exists$ an integer c_1 such that

$$b = ac_1$$

multipling both sides by c.

$$bc = ac_1c$$
$$= ac_2 \qquad c_2 \in Z$$

$$\Rightarrow a|bc \quad \text{Hence Proof}$$

Q. if $a|b$ then $ac|bc$

Sol. if $a|b$ then $\exists c_1$ s.t $b = ac_1$ $\Rightarrow bc = acc_1$ $c_1 \in Z$

$\Rightarrow ac|bc$

(3)

iv) if $a|b$ and $b|a$ Then Prove that $a = \pm b$.

Proof Since $a|b$ Therefore $\exists$ an integer $c_1 \in Z$ such that

$$b = ac_1 \text{ ——— } (1)$$

and

$b|a$ Therefore $\exists$ an integer $c_2 \in Z$ Such that

$$a = bc_2 \text{ ——— } (2)$$

using (1) in (2) we get

$$a = (ac_1)c_2$$
$$a = ac_1c_2.$$
$$a - ac_1c_2 = 0$$
$$\Rightarrow a(1 - c_1c_2) = 0$$
$$\Rightarrow a \neq 0 \text{ Therefore } 1 - c_1c_2 = 0$$
$$\Rightarrow c_1c_2 = 1$$
$$\Rightarrow c_1 = c_2 = \pm 1$$

Putting $c_2 = \pm 1$ in eqn (2) we get

$$a = \pm b.$$

which is the required result.

v) $-1 \mid a$ & $1 \mid a$ $\forall a \in Z$.

Proof :-
we can write

$$a = (-1)(-a) \quad \text{where } -a \in Z$$

$\Rightarrow -1 \mid a$

Similarly we can write

$$a = 1(a) \quad \text{where } a \in Z$$

$\Rightarrow 1 \mid a$ Hence the result.

---

vi) if $a \mid b$ and $b \mid c$ Then $a \mid c$.

Proof:-
Since $a \mid b$ Therefore $\exists$ an element $c_1 \in Z$ s.t.

$$b = ac_1 \quad \text{--- (1)}$$

and $b \mid c$
$\therefore \exists$ an integer $c_2 \in Z$ such that

$$c = bc_2 \quad \text{--- (2)}$$

using (1) in (2) we get.

$$c = ac_1c_2$$

$$c = ac_3$$

$\Rightarrow a \mid c$ which is required result.

vii) if $a|b$ and $a|c$ Then $a|bx+cy$ $\forall\ x, y \in Z$.

Proof:

Since $a|b$

$\therefore$ $\exists$ an integer c_1 s.t.

$b = ac_1$ —— (1)

and

$a|c$

$\therefore$ $\exists$ an integer c_2 s.t.

$c = ac_2$ —— (2)

Multiplying eqn (1) by x and (2) by y then adding

$$bx + cy = ac_1x + ac_2y.$$

$$= ac_3 + ac_4$$

$$= a(c_5)$$

$\Rightarrow$ $a | bx+cy$.

viii) if $a | b_1+b_2$ & $a|b_1$ Then $a|b_2$.

Proof: Since $a|b_1+b_2$ therefore There exist an integer c_1 s.t.

$b_1 + b_2 = ac_1$ —— (1)

and

Since $a|b_1$ therefore exist an integer c_2 s.t $b_1 = ac_2$ —— (2)

putting (2) in (1) we get.

$$b_1 + b_2 = ac_1$$
$$\Rightarrow b_2 = ac_1 - b_1$$
$$\Rightarrow b_2 = ac_1 - ac_2$$
$$= a(c_1 - c_2)$$
$$b_2 = ac_3$$

$\Rightarrow a \mid b_2$ which is required result.

For e.g. $2 \mid 4+6$ & $2 \mid 4$

Then $2 \mid 6$

e.g $3 \mid 9+6$ & $3 \mid 9$

Then $3 \mid 6$.

e.g $5 \mid 15+5$ and $5 \mid 15$

Then $5 \mid 5$

Theorem: Prove That $a-b \mid a^n - b^n \ \forall \ n \geq 0$ where $n \in \mathbb{Z}$

Proof:- We prove it by mathematical Induction.

For $n = 0$

$$a-b \mid a^0 - b^0$$

$$\Rightarrow a-b \mid 0$$

which is true

bcs $a \mid 0 \ \forall \ a \in \mathbb{Z}$.

Suppose that the statement is true for $n=k$

So

$$a-b \mid a^k - b^k \quad \text{——— (1)}$$

We now prove that the statement is true for $n = k+1$ Then

$$a^{k+1} - b^{k+1} = a^k \cdot a - b^k \cdot b + ab^k - ab^k$$

$$a^{k+1} - b^{k+1} = a(a^k - b^k) + b^k (a-b) \quad ?$$

Since $a-b \mid a^k - b^k$ There

$$a-b \mid a(a^k - b^k) \quad \because \ a \mid b \text{ Then } a \mid bc$$

also

$$a-b \mid (a-b) b^k \quad \text{Then}$$

$$a-b \mid a(a^k - b^k) + b^k (a-b)$$

Hence $a-b \mid a^{k+1} - b^{k+1}$ which is required result.

Hence the statement is true for $n \geq 0$

8

Theore (Q#2) $a+b \mid a^n+b^n$ if n is odd.

Proof:- we prove it by matematical inductio

For $n=1$

$a+b \mid a+b$ is true.

Suppose that the statement is true for $n = 2k+1$

i.e $a+b \mid a^{2k+1}+b^{2k+1}$

we are to show that the statement is true for $n = 2(k+1)+1 = 2k+2+1 = 2k+3$.

Then

$$a^{2k+3}+b^{2k+3} = a^{2k+1}\cdot a^2 + b^{2k+1}\cdot b^2$$

$$= a^{2k+1}a^2 + b^{2k+1}b^2 + b^{2k+1}a^2 - b^{2k+1}\cdot a^2$$

$$= a^2\left(a^{2k+1}+b^{2k+1}\right) \mp b^{2k+1}\left(a^2-b^2\right)$$

?

$$a^{2k+3}+b^{2k+3} = a^2\left(a^{2k+1}+b^{2k+1}\right)+b^{2k+1}(a+b)(a-b)$$

As $a|b$ Then $a|bc$ There if

$a+b \mid a^{2k+1}+b^{2k+1}$ Then

$a+b \mid a^2\left(a^{2k+1}+b^{2k+1}\right)$ —— (1)

and $a+b \mid b^{2k+1}(a+b)(a-b)$ —— (2)

Therefore from (1) & (2) we have

$a+b \mid a^2(a^{2k+1}+b^{2k+1}) - b^{2k+1}(a+b)(a-b)$

$\Rightarrow a+b \mid a^{2k+3}+b^{2k+3}$

Hence the statment is true for

$n = 2k+3$.

Hence the given statment is true $\forall\, n \in$ odd.

—— ※ —— ※ —— ※ —— ※ ——

Q No# 3. $a+b \mid a^n - b^n$ if n is even.

Sol: By M. Induction for

$n = 2$.

$a+b \mid a^2 - b^2$

$\Rightarrow a+b \mid (a+b)(a-b)$

which is true $\because$ $a \mid b$ Then $a \mid bc$.

Suppose that the statement is true for

$n = 2k$.

$a+b \mid a^{2k} - b^{2k}$ —— (1)

we are to show that the statement is true for

$n = 2(k+1) = 2k+2$.

$a^{2k+2} - b^{2k+2} = a^{2k}.a^2 - b^{2k}b^2$

$= a^{2k}.a^2 - b^{2k}b^2 - a^2b^{2k} + a^2b^{2k}$

$= a^2(a^{2k} - b^{2k}) + b^{2k}(a^2 - b^2)$

$= a^2(a^{2k} - b^{2k}) + b^{2k}(a+b)(a-b)$

(2)

$n = 1, 3, 5, 7.$
$8|0,\ 8|8,\ 8|24,\ 8|48$

As $a+b \mid a^{2k} - b^{2k}$ Therefore

$$a+b \mid a^2(a^{2k} - b^{2k}) \quad \text{—③}$$

and

$$a+b \mid b^{2k}(a+b)(a-b) \quad \text{—④}$$

from ③ and ④ we have

$$a+b \mid a^{2k+2} - b^{2k+2}.$$

Hence the statement $\forall\ n \in E$ mean +ve even integer. ?

Q ④* If n is odd Then $8 \mid n^2 - 1$.

Solution :—
As n is odd Then we can write $n = 2k+1$ where $k \in \mathbb{Z}$.

Take

$$n^2 - 1 = (2k+1)^2 - 1$$
$$= 4k^2 + 4k + \cancel{1} - \cancel{1}$$
$$n^2 - 1 = 4k(k+1) \quad \text{—①}$$

Either k is even or odd.

Case I if k is even Then $\exists$ an integer k_1 s.t $k = 2k_1$ putting in eq ①

$$n^2 - 1 = 4(2k_1)(2k_1 + 1)$$
$$= 8k_1(2k_1 + 1)$$

$3 = 4(1) - 1$

(11)

— ?

As $8 \mid 8k_1(2k_1+1)$

There $8 \mid n^2 - 1$

Case II

if n is ~~odd~~ odd Then $\exists$ an integer k_2 s.t

$$k = 2k_2 + 1$$

Putting in Equation (1) we get.

$$n^2 - 1 = 4(2k_2+1)((2k_2+1)+1)$$

$$= 4(2k_2+1)(2k_2+2)$$

$$= 4(2k_2+1)2(k_2+1).$$

$$n^2 - 1 = 8(2k_2+1)(k_2+1)$$

$$\Rightarrow 8 \mid 8(2k_2+1)(k_2+1)$$

$$\Rightarrow 8 \mid n^2 - 1.$$

Hence $8 \mid n^2 - 1$ if n is odd.

Q 11 Show that the product of any three consecutive integer is divisible by 6.

Proof:- let $n, n+1, n+2$ be three consecutive integers. Then we are to show that

$$6 \mid n(n+1)(n+2).$$

for $n = 1$ $\quad 6 \mid 1(1+1)(1+2) = 6 \mid 6$ (True)

Suppose that the statement is true for $n = k$ i.e

$$6 \mid k(k+1)(k+2).$$

we are to show that the statement is true for $n = k+1$.

$$(k+1)(k+2)(k+3) = k(k+1)(k+2) + 3(k+1)(k+2) \quad \text{—(1)}$$

Since

$6 \mid k(k+1)(k+2)$ is True by Assumption and for

$3(k+1)(k+2)$ ~~therefore~~ $\because$ k is integer there are two possibilies i.e k is even or k is odd. if

k is even then $\exists$ an integer k_1 S.t

$k = 2k_1$ Then $3(k+1)(k+2)$ becomes

$$3(k+1)(k+2) = 3(2k_1+1)(2k_1+2)$$
$$= 6(2k_1+1)(k_1+1)$$
$$\Rightarrow 6 \mid 3(k+1)(k+2)$$

Secondly if

k is odd Then $\exists$ an integer k_2 Such that

$k = 2k_2+1$ Then $3(k+1)(k+2)$

becomes $3(k+1)(k+2) = \cancel{3(2k_2+2)(2k_2+3}$

Show that

$$14 \,\big|\, 3^{4n+2} + 5^{2n+1}$$

for $n = 0$

$$14 \,\big|\, 3^{2} + 5^{1}$$

$$= 14 \,|\, 14 \quad (\text{True})$$

for $n = 1$ $\quad 14 \,\big|\, 3^{6} + 5^{3}$

$$= 14 \,\big|\, 729 + 125 \;=\; 14 \,\big|\, 854.$$

Suppose That the statment is true for $n = k$ i.e

$$14 \mid 3^{4k+2} + 5^{2k+1}$$

we are to show That the statement is true for $n = k+1$. i.e

$$14 \mid 3^{4(k+1)+2} + 5^{2(k+1)+1}$$

$$= 14 \mid 3^{4k+6} + 5^{2k+3} \quad \text{——} \quad (1)$$

$$3^{4k+6} + 5^{2k+3} = 3^{4k+2} \cdot 3^4 + 5^{2k+1} \cdot 5^2$$

$$= 3^{4k+2} \cdot 3^4 + 5^{2k+1} \cdot 5^2 + 5^{2k+1} \cdot 3^4 - 5^{2k+1} \cdot 3^4$$

$$= 3^{4k+2} \cdot 3^4 + 5^{2k+1} \cdot 3^4 + 5^{2k+1} \cdot 5^2 - 5^{2k+1} \cdot 3^4$$

$$= 3^4\left(3^{4k+2} + 5^{2k+1}\right) + 5^{2k+1}\left(5^2 - 3^4\right)$$

$$= 3^4\left(3^{4k+2} + 5^{2k+1}\right) + 5^{2k+1}\left(25 - 81\right)$$

$$= 3^4\left(3^{4k+2} + 5^{2k+1}\right) + 5^{2k+1}\left(-56\right)$$

Since $14 \mid 3^{4k+2} + 5^{2k+1}$ Then $14 \mid 3^4\left(3^{4k+2} + 5^{2k+1}\right)$

and $14 \mid -56$ Then $14 \mid 5^{2k+1}(-56)$

So $14 \mid 3^4\left(3^{4k+2} + 5^{2k+1}\right) + 5^{2k+1}(-56)$

$a\overline{)b}(q$ $a = bq + r$

So from (1)

$$14 \mid 3^{4k+6} + 5^{2k+3}.$$

Hence The statment is true for $n = k+1$

Hence

$$14 \mid 3^{4n+2} + 5^{4n+1} \quad \forall\ n \in \mathbb{Z}^{+} \text{ i.e } n \geq 0$$

~ ~ ~ ~ ~ ~ ~ ~ ~

~~Theorem of Euclid~~). (Euclid's Theorem)

let $a, b \in \mathbb{Z}$, $b > 0$ There exist unique integer q and r such that

$$a = bq + r \qquad 0 \leq r < b.$$

Proof :- let A be a set such that

$$A = \{a - bx \geq 0\} \text{ where } x \in \mathbb{Z}$$

$A \neq \phi$

$$a - b(-a) \in A.$$

If

$0 \in A$ Then 0 is the least element of A.

If $0 \notin A$ Then 'A' being the a subset of +ve integers must have least element. let us call it 'r'. for some $x = q \in \mathbb{Z}$

$$r = a - bq$$

$$a - bq \geq 0$$

$$\Rightarrow r \geq 0 \quad \because r = a - bq$$

Now we have to prove that $r < b$.
Suppose that $r \geq b$.

$$\Rightarrow r - b \geq 0$$

$$= a - bq - b \geq 0 \quad \because r = a - bq$$

$$= a - b(q+1) \geq 0 \qquad a - bx$$

$$\Rightarrow r - b \in A.$$

$r - b < r$. This contradiction to the fact that r is the least element of A. Hence our supposition $r \geq b$ is wrong. Hence

$$r < b$$

so $0 \leq r < b$

$$r = a - bq$$

$$a = bq + r \quad \text{where } 0 \leq r < b$$

For uniqueness let $a = bq_1 + r_1$ -
also $\qquad 0 \leq r_1 < b$.

$$a = bq + r$$

$$0 \leq r_1 < b$$

so $\quad bq_1 + r_1 = bq + r$

$$|bq_1 - bq| = |r - r_1| \quad \text{--- (1)}$$

From (i)

$$|bq_1 - bq| = |r - r_1|$$

$$0 = |r - r_1|$$

$$\Rightarrow r = r_1$$

$$\Rightarrow bq + r = bq_1 + r \qquad 0 \le r < b$$

This implies that expression is unique.

Remarks:- (In Euclid's Theorem).

i) "a" is divided by 'b' if $r = 0$

ii) "q" is called quotient and 'r' is called remainder

iii) if $r = 0$ then $b|a$ and conversely if $b|a$ then $r = 0$

iv) if $b=2$ Then $r=0$ or 1 it means every integer is either of the form $2k$ or $2k+1$.
If it is of the form $2k+1$ Then it is called odd integer if it is of the form $2k$ Then it is called even integer.

Preposition:- if $r=0$ Then b/a and Conversely if b/a Then $r=0$.

Proof:- By Euclid's Theorem we know That

$$a = bq + r \quad \text{--- (1)}$$

Since $r=0$ Therefore eq (1) $\Rightarrow$ $a = bq$ where $q \in \mathbb{Z}$.
Then by definition of divisiblity

$$b|a$$

Conversely Suppose that

$$b|a$$

Then $\exists$ an element $q \in \mathbb{Z}$ Such that

$$a = bq \quad \text{--- (2)}$$

also by Euclid's Theorem

$$a = bq + r \quad \text{--- (3)}$$

$\therefore$ From eqn (2) and (3)

$$bq + r = bq$$

$$r = 0$$ Hence proved.

$$1325 = 1\times10^3 + 3\times10^2 + 2\times10^1 + 5\times10^0$$

4/2 r_3 r_2 r_1 r_0.

~~Base~~ or Radix ~~representation~~

Every positive integer can be written as

$$a = r_n \times 10^n + r_{n-1}\times 10^{n-1} + \cdots + r_1\times 10^1 + r_0$$

where $r_n > 0$ and $r_n < 10$ & $0 \leq r_i < 10$

This is called representation of "a" in the scale (base) 10 and 10 is called Base or radix. In fact every fixed integer $g > 1$ can be used as base or radix.

where $i = 1, 2, 3, \ldots, n-1$. Then $0 \leq r_i < 10$.

NOTE:-

In abbrivated from we write

$(r_n r_{n-1} r_{n-2} \ldots r_1 r_0)_{10}$ for any base $g > 1$. The base is specified at the right end. If no base is specified then integer is written in the scale of 10.

Ex:-

$(\alpha\alpha)_{12} + (\beta\beta)_{12}$

where $\alpha = 10$ and, $\beta = 11$.

$(\alpha\alpha)_{12} + (\beta\beta)_{12}$

$\Rightarrow ((10)(10))_{12}$

$+ ((11)(11))_{12}$

$(1(10)9)_{12}$ $\Rightarrow (1\alpha 9)_{12}$ Ans.

$$\begin{array}{r|l} 12 & 21 \\ & \underline{12} \\ & 9 \end{array} \quad 1$$

$$\begin{array}{r|l} 12 & 13 \\ & \underline{12} \\ & 1 \end{array} \quad 1$$

Q:-

If $\alpha = 10$, $\beta = 11$

(i) $(2\alpha 34)_{12} \times (\beta 934)_{12}$

ii) $(2129)_{12} \times (\beta 370)_{12}$

Sol:-

$(2\alpha 34)_{12} \times (\beta 934)_{12}$

$$\begin{array}{r}
(2\,(10)\,3\,4)_{12} \\
\times\ (11)\,9\,3\,4\ )_{12} \\
\hline
11\,5\,1\,4 \\
8\,6\,10\,0\,\times \\
21\,8\,6\,0\,\times\,\times \\
27\,7\,0\,8\,\times\,\times\,\times \\
\hline
(4\,5\,11\,0\,10\,14)_{12}
\end{array}$$

$(4\,5\,\beta\,0\,\alpha\,14)_{12}$ Ans.

ii) $(2129)_{12} \times (\beta 370)_{12}$

$$\begin{array}{r}
(2129)_{12} \\
(11\,3\,7\,0)_{12} \\
\hline
0\,0\,0\,0 \\
1\,2\,8\,7\,3\,\times \\
6\,3\,8\,3\,\times\,\times \\
1\,11\,1\,6\,3\,\times\,\times\,\times \\
\hline
(1\,11\,9\,0\,7\,10\,3\,0)_{12}
\end{array}$$

$(1\beta 907\alpha 30)_{12}$ Answer.

Common Divisor :-

let $a, b \in Z$ Then $c \in Z$ is called common divisor of a and b if $c|a$ and $c|b$.

for e.g $4, 8 \in Z$ Then $2 \in Z$ is C.D $\because$ $2|4$ and $2|8$.

Annual 10 2nd

Greatest Common Divisor :- (GCD).

let $a, b \in Z$ and Then $d \in Z$ is called G.C.D of 'a' and 'b' if

(i) $d > 0$ (ii) $d|a$ and $d|b$.
iii) $c|a$ and $c|b$ Then $c|d$.

for. $4, 8 \in Z$ Then $4|4$ & $4|8$.
and $4 > 0$ and
$2|4$ & $2|8$ also $2|4$.

So 4 is G.C.D.

for e.g $(-2, -4)$

$-1, -2, 1, 2$ are c.D of $(-2, -4)$.

Therefore G.C.D = 2 which is always positive. we denote

G.C.D of 'a' and 'b' as
$(a, b) = d$ for e.g $(a, b) = d$
(4) $(4, 12) = d$ //

Theorem:- The G.C.D of 'a' and 'b' is unique. where $a, b \in \mathbb{Z}$.

Proof:- let d_1 and d_2 be the two G.C.D of 'a' and 'b'.

$$(a,b) = d_1 \text{ — (i) and } (a,b) = d_2 \text{ — (ii)}$$

If d_1 is G.C.D of 'a' & 'b'. Then d_2 being the common divisor of 'a' and "b" divides d_1

i.e

$$d_2 \mid d_1 \text{ —— (iii)}$$

Similarly if d_2 is G.C.D of 'a' & 'b'. Then we have

$$d_1 \mid d_2 \text{ —— (iv)}$$

From (iii) & (iv)

$$d_1 = \pm d_2 \quad \because \text{ if } a|b \text{ \& } b|a \text{ Then } a = \pm b.$$

$$\Rightarrow d_1 = d_2 \text{ or } d_1 = -d_2$$

$$\Rightarrow d_1 = d_2 \quad (\because d_1, d_2 > 0)$$

Hence G.C.D of "a" & "b" is unique.

Method of finding G.C.D:

we suppose $a > b$ and $b > 0$ Then by Euclid's Theorem $\exists$ unique integers q_1 and r_1 such that

$$\begin{array}{r|l} b & a \\ & \underline{bq_1} \\ & r_1 \end{array} \quad q_1$$

$$a = bq_1 + r_1 \quad \text{---} (1)$$

$$0 \leq r_1 < b.$$

Then b is called G.C.D of 'a' & 'b' if $r_1 = 0$. But if $r_1 \neq 0$ Then $\exists$ unique integers q_2 and r_2 such that

$$b = r_1 q_2 + r_2$$

If $r_2 \neq 0$ Then There exist q_3, r_3 s.t

$$r_1 = r_2 q_3 + r_3 \qquad 0 \leq r_3 < r_2.$$

we repeat this process untill we obtained a remainder r_{n+1} which is zero. Then

$$r_{n-2} = r_{n-1} q_n + r_n$$

$$r_{n-1} = r_n q_{n+1} + 0 \rightarrow (n+1) \quad r_{n+1} = 0$$

Here we note the following properties

i) $r_n > 0$

ii) $r_n | a$ and $r_n | b$

iii) From (1) to (n+1) if $c|a$ & $c|b$. Then $c | r_n$.

Hence r_n is G.C.D of 'a' and 'b'

i.e

$$(a, b) = r_n.$$

Theore (Just Statement
proof not included in the cours)

If $(a,b) = d$ Then d can be written as the linear Combination of 'a' & 'b' i.e.

$$d = ax + by \quad \text{where } x, y \in \mathbb{Z}$$

For e.g $(4, 8) = 4$.
Then
$$4 = 4(-1) + 8(+1)$$

EXERCISE

Q#:-
Find G.C.D of $(275, 105)$, and Express it as liner Combination of 275 and 105.

Sol:-

$a = bq + r$

$$275 = 2.105 + 65$$
$$105 = 1.65 + 40$$
$$65 = 1.40 + 25$$
$$40 = 1.25 + 15$$
$$25 = 1.15 + 10$$
$$15 = 1.10 + 5$$
$$10 = 2.5 + 0$$

Hence
$$\text{G.c.d } (275, 105) = 5$$

$105 \overline{)275}$ 2
210
$65 \overline{)105}$ 1
65
$40 \overline{)65}$ 1
40
$25 \overline{)40}$ 1
25
$15 \overline{)25}$ 1
15
$10 \overline{)15}$ 1
10
$5 \overline{)10}$ 2
0

Now for linear Combination

$$
\begin{aligned}
5 &= 15 - 1\cdot 10 \\
&= 15 - 1\cdot(25 - 1\cdot 15) \\
&= 15 - 1\cdot 25 + 1\cdot 15 \\
&= 2\cdot(15) - 1\cdot(25) \\
&= 2\cdot(40 - 1\cdot 25) - 1\cdot(25) \\
&= 2(40) - 2\cdot(25) - 1(25) \\
&= 2(40) - 3(25) \\
&= 2(40) - 3(65 - 1(40)) \\
&= 2(40) - 3(65) + 3(40) \\
&= 5(40) - 3(65) \\
&= 5(105 - 1\cdot 65) - 3(65) \\
&= 5(105) - 5(65) - 3(65) \\
&= 5(105) - 8(65) \\
&= 5(105) - 8(275 - 2\cdot(105)) \\
&= 5(105) - 8(275) + 16(105) \\
&= 21(105) - 8(275)
\end{aligned}
$$

$$5 = 105(21) + 275(-8)$$

$5 = 275(-8) + 105(21)$ is Required L. Combination

where $x = -8$ & $y = 21$.

Q# Find the G.C.D of (10672, 4147) and express it as linear Combination of 10672, 4147.

$10672 = 2 \cdot 4147 + 2378$

$4147 = 1 \cdot 2378 + 1769$

$2378 = 1 \cdot 1769 + 609$

$1769 = 2 \cdot 609 + 551$

$609 = 1 \cdot 551 + 58$

$551 = 9 \cdot 58 + 29$

$58 = 2 \cdot 29$

So G.C.D of

$(10672, 4147) = 29.$

$4147 \overline{)10672}(2$
8294

$2378)4147 (1$
2378

$1769)2378 (1$
1769

$609)1769 (2$
1218

$551)609 (1$
551

$58)551 (9$
522

$29)58 (2$
58
$\times$

Now for linear Combination.

$$29 = 1 \cdot 551 - 9 \cdot 58.$$
$$= 1 \cdot 551 - 9 \cdot (609 - 1 \cdot 551)$$
$$= 1 \cdot 551 - 9 \cdot 609 + 9 \cdot 551$$
$$= 10 \cdot 551 - 9 \cdot 609$$
$$= 10 \cdot (1769 - 2 \cdot 609) - 9 \cdot 609$$

$$29 = 10(1769) - 20(609) - 9(609)$$

$$\text{"} \quad = 10(1769) - 29(609).$$

$$\text{"} \quad = 10(1769) - 29(2378 - 1(1769))$$

$$\text{"} \quad = 10(1769) - 29(2378) + 29(1769)$$

$$\text{"} \quad = 39(1769) - 29(2378).$$

$$\text{"} \quad = 39(4147 - 2378) - 29(2378)$$

$$\text{"} \quad = 39(4147) - 39(2378) - 29(2378)$$

$$\text{"} \quad = 39(4147) - 68(2378)$$

$$\text{"} \quad = 39(4147) - 68(10672 - 2(4147))$$

$$\text{"} \quad = 39(4147) - 68(10672) + 136(4147)$$

$$\text{"} \quad = \cancel{68}\ 175(4147) - 68(10672)$$

$$29 = 10672(-68) + 4147(175)$$

Hence The linear Combination

$$10672(-68) + 4147(175) = 29$$

Corollary:-

If $c \mid ab$ and $(c,b)=1$ Then $c \mid a$

Since $(c,b)=1$

$\Rightarrow$ $x,y \in \mathbb{Z}$ such that

$cx+by=1$ —— (1)

multiplying eq (1) by a

Therefore

$acx+aby=a$

As $c \mid c \Rightarrow c \mid acx$

also

$c \mid ab \Rightarrow c \mid aby$

$\Rightarrow c \mid acx+aby$

$\Rightarrow c \mid a$ Hence the Proved.

$3 \mid 6(5)$

$(3,5)=1$

Then $3 \mid 6$.

But

$(3,6) \neq 1$

$\therefore 3 \nmid 5$.

Theorem

If $(a,b)=1$ Then $(a-b,a+b)=1$ or 2

Proof let G.C.D of $(a-b,a+b)=d$

$\Rightarrow d \mid a-b$ —— (1)

also

$d \mid a+b$ —— (2)

$\Rightarrow d \mid a-b+a+b$

$\Rightarrow d \mid 2a$ —— (3)

Ex: If $(b,c)=1$ and a/c Then $(a,b)=1$.

Proof: Since b and c are relatively prime so $\exists\ x,y \in Z$ such that

$$bx + cy = 1 \quad \text{---} (1)$$

Also a/c

$\exists$ an integer $c_1 \in Z$ s.t.

$(5,11)=1$ Then $c=5$ $(5,11)=1$ $(12,7)$ $(7,12)$ and $2/12$ Then $(2,7)=1$

$$c = ac_1 \quad \text{---} (2) \quad \text{(By Divisibility definition)}$$

$$eq(1) \Rightarrow bx + ac_1y = 1$$

$$bx + ay_1 = 1$$

$$\Rightarrow (a,b) = 1 \quad \text{Hence proved}$$

Ex:-

1/ If $(a,b)=d$ Then $(ma, mb) = md$.

Sol:-

Since $(a,b)=d$.

Then

$\exists$ integers $x, y \in \mathbb{Z}$ such that

$$ax+by = d$$

$$max + mby = md \quad \text{—} (1)$$

Suppose That $(ma, mb) = d_1$

$\Rightarrow d_1 | ma, \; d_1 | mb$.

$\therefore d_1 | max$ and $d_1 | mby$.

$\Rightarrow d_1 | max + mby$. $\because md = max + mby$

$\Rightarrow d_1 | md$. — (2)

As

$(a,b) = d$.

$\Rightarrow d|a$ and $d|b$.

$\Rightarrow md | ma$ and $md | mb$.

$\Rightarrow md$ is C.D of ma and mb. Therefore

$\Rightarrow md | d_1$ — (3) $\because (ma, mb) = d_1$

From (2) & (3)

$$md = \pm d_1$$

But d_1 is G.C.D Therefore

$$md = d_1$$

$md = m(a,b) = (ma, mb)$

Hence

$(ma, mb) = d_1$ // Hence Proved

Problem

If $(k_1, k_2) = 1$ and $k_1 | a$ and $k_2 | a$ Then $k_1 k_2 | a$.

Sol: Since $k_1 | a$ Then
By definition of divisibility
$\exists$ an integer $c_1 \in \mathbb{Z}$ such that
$$a = c_1 k_1 \quad \text{--- (1)}$$
Also
$k_2 | a \Rightarrow \exists$ an integer
$c_2 \in \mathbb{Z}$ such that
$$a = c_2 k_2 \quad \text{--- (2)}$$

If $(3,7) = 1$
$3|21$, $7|21$
$(3)(7) | 21$.

As
$(k_1, k_2) = 1$ Then $\exists$ $x, y \in \mathbb{Z}$ s.t
$$k_1 x + k_2 y = 1$$
Multiplying both sides by 'a' we have
$$a k_1 x + a k_2 y = a$$
$$c_2 k_2 k_1 x + c_1 k_1 k_2 y = a \quad \text{From (1) \& (2)}$$

As $k_1 k_2 | c_2 k_1 k_2 x$ & $k_1 k_2 | c_1 k_1 k_2 y$.

Therefore
$$k_1 k_2 | c_2 k_1 k_2 x + c_1 k_1 k_2 y$$
$$\Rightarrow k_1 k_2 | a \quad \because a = c_2 k_1 k_2 x + c_1 k_1 k_2 y$$
which is required result.

If $k_1 | a$ and $k_2 | b$. Then $k_1k_2 | ab$.

Since $k_1 | a$ Therefore There exist an integer c_1 such that

$$a = k_1 c_1 \quad \text{—(1) and}$$

Similarly $k_2 | b$ Therefore $\exists$ $c_2 \in \mathbb{Z}$ such that

$$b = k_2 c_1 \quad \text{—(2)}$$

multiplying eqn (1) and (2) we have.

$$ab = k_1 k_2 c_1 . c_2 \Rightarrow ab = k_1k_2 c$$

$$\Rightarrow k_2k_1 | ab \; \cancel{\text{and } k_2 | ab}.$$

Hence the prove

$2 | 4,\ 4 | 4$

$4 = 2(2)$

$4 = 4(1)$

~~Since $k_1 | ab$ Again by definition of divisibility $\exists$ an integer c_3 such that. $ab = k_1 c_3$ and Also $k_2 | ab$ Therefore $\exists$ an integer $c_4 \in \mathbb{Z}$ s/t $ab = k_2 c_4$.~~

Imp.
* Theorem:

If $(b,c)=1$ Then $(a,bc)=(a,b)\cdot(a,c)$

Proof let $(a,bc)=d$

, $(a,b)=d_1$

and $(a,c)=d_2$.

we will prove that

$d=d_1d_2$.

Now

$(b,c)=1$, $(a,b)=d_1$

$(a,c)=d_2$.

a b c
2, 5, 7.
$(5,7)=1$
$(2,(5)(7))$
$=(2,5)\cdot(2,7)$
$1=(1)(1)$
$1=1$.

$\Rightarrow$ $d_1|a$ and $d_1|b$.

Also $d_2|a$ and $d_2|c$

$\Rightarrow$ $d_1|b$ and $d_2|c$.

$(9,10)=1$
$3|9$ & $5|10$
$(3,5)=1$

$\Rightarrow$ $(d_1,d_2)=1$. $\because (b,c)=1$

As $d_1|a$ and $d_2|a$ Then $d_1d_2|a$ — (1)

As $d_1|b$ and $d_2|c$. $\because$ if $a|c$ & $b|c$ then $ab|c$.

Then $d_1d_2|bc$ ——— (2) $\because$ if $k_1|a$, $k_2|b$ $\Rightarrow k_1k_2|ab$.

From (1) & (2)

$\Rightarrow$ d_1d_2 is C.D of a & bc.

but G.C.D of a & bc

is d. Therefore

$d_1d_2|d$ ——— (3)

Again as $(a,b) = d_1$ & $(a,c) = d_2$
Then $\exists$ $x_1, y_1 \in \mathbb{Z}$ and $x_2, y_2 \in \mathbb{Z}$
such that.

$$ax_1 + by_1 = d_1 \quad \text{—— (4)}$$
&
$$ax_2 + cy_2 = d_2 \quad \text{—— (5)}$$

multiplying eqn (4) & (5)

$$(ax_1 + by_1)(ax_2 + cy_2) = d_1 d_2.$$

$$\Rightarrow a^2x_1x_2 + acx_1y_2 + abx_2y_1 + bcy_1y_2 = d_1d_2$$

As $d \mid a$ & $d \mid bc$

so $d \mid a^2x_1x_2 + acx_1y_2 + abx_2y_1 + bcy_1y_2$

$$\Rightarrow d \mid d_1 d_2 \quad \text{—— (6)}$$

From (3) & (6) we have

$$d_1 d_2 = \pm d.$$

But G.C.D is alway +ve Therefore

$$d_1 d_2 = d \Rightarrow d = d_1 d_2$$
$$\Rightarrow (a, bc) = (a,b)\cdot(b,c) \;//$$

Ex:- If $(a,c)=1$ Then $(a,bc)=(a,b)$.

Sol:- Given $(a,c)=1$ &

let $(a,bc)=d$ and $(a,b)=d_1$

Then we have to prove that $d=d_1$.

$(a,b)=d_1$

$\Rightarrow d_1|a$ and $d_1|b$.

$\Rightarrow d_1|a$ and $d_1|bc$.

$\Rightarrow d_1$ is Common Divisor of a & bc.

but $(a,bc)=d$.

Therefore $d_1|d$. — ①

As $(a,c)=1$ Therefore ∃ two integers x and $y \in \mathbb{Z}$ s.t.

$ax+cy=1$

$\Rightarrow$ ~~bax+bcy=b~~ $abx+bcy=b$

as $d|a$ & $d|bc$

$\Rightarrow d|abx+bcy$.

$\Rightarrow d|b$ $\because abx+bcy=b$.

As $d|a$ and $d|b$.
$\therefore$ d is C.D of a and b.

But $(a,b) = d_1$ Therefore

$$d | d_1 \quad \text{——} \quad (2)$$

From (1) & (2) we have

$$d = \pm d_1.$$

But d_1 is G.C.D Therefore

$$d = d_1$$

$$\Rightarrow d_1 = d$$

$$(a,bc) = (a,b).$$

which is required result

---

exercise:–

If $a = bq + r$ Then
$(a,b) = (b,r)$.

Sol:– Let $(a,b) = d$ and
$(b,r) = d_1$
Then we have to show that

$$d = d_1$$

Since

$$a = bq + r \quad \text{——} \quad (1)$$

$$a - bq = r$$

As $d|a$ and $d|b$ Then $d|a-bq$.

$\Rightarrow d|r \quad \because a-bq=r$.

As $d|b$ and $d|r$

$\Rightarrow d$ is C.D of 'b' and 'r'

but

$(b,r)=d_1$

$\Rightarrow d|d_1$. —— (2)

Now again as

$a=bq+r$.

as $d_1|b$ and $d_1|r$.

$\Rightarrow d_1|bq+r$.

$\Rightarrow d_1|a \quad \because a=bq+r$.

As $d_1|a$ and $d_1|b$

$\Rightarrow d_1$ is C. Divisor of a & b.

But

$(a,b)=d$.

i.e. $d_1|d$. —— (3)

from (2) & (3) we have

$d=\pm d_1$

But G.C.D is always positive

i.e. $d=d_1$

So $(a,b)=(b,r)$ which is required result.

G.C.D of more then two integer

d is called G.C.D of $a_1, a_2, a_3, \ldots, a_n$

i) $d > 0$

ii) $d \mid a_i$ for $i = 1, 2, 3, \ldots, n$.

iii) If $e \mid a_i$ for $i = 1, 2, 3, \ldots, n$

Then $e \mid d$

and we writted as.

$$(a_1, a_2, a_3, \ldots, a_n) = d.$$

* Method of finding G.C.D for more then two integers.

let $a_1, a_2, a_3, \ldots, a_n$ are integers.

let $(a_1, a_2) = d_1$

$(d_1, a_3) = d_2$

$(d_2, a_4) = d_3$

$\vdots$

$(d_{n-2}, a_n) = d_{n-1}$

$$\Rightarrow d_{n-1} = (a_1, a_2, a_3, \ldots, a_n).$$

$(6,8) = 2$
$(6/2, 8/2) = 1$
$(3,4) = 1$

EXERCISE

$(a,b) = d$ Then $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$

As $(a,b) = d$
Then $\exists$ $x, y \in \mathbb{Z}$ such

$$ax + by = d$$
$$\frac{a}{d}x + \frac{b}{d}y = 1$$

$\Rightarrow \left(\frac{a}{d}, \frac{b}{d}\right) = 1$ where $x, y \in \mathbb{Z}$. which required result.

Annual obj

Least Common Multiple:- (L.C.M).

An integer 'm' is the L.C.M of a and b if

i) $m > 0$
ii) $a|m$ and $b|m$.
iii) $a|c$ and $b|c$ Then $m|c$

L.C.M of 'a' and 'b' will be denoted by

$\langle a, b \rangle = m$. or L.C.M.$(a,b) = m$

Theorem:- Show that L.C.M of two number is unique.

or

Prove that L.C.M of 'a' and 'b' is unique.

Proof: let $\langle a,b\rangle = m_1$
and
$\langle a,b\rangle = m_2$.

Case-I

If m_1 is L.C.M of 'a' and 'b'. Then m_2 being common multiple of 'a' and 'b' is divisible by m_1. i.e m_1 / m_2 — (1)

Case II

If m_2 is L.C.M of 'a' and 'b' Then m_1 being common multiple of 'a' and 'b' is divisible by m_2.

i.e m_2 / m_1 — (2)

From (1) & (2) we have.

$\Longrightarrow$

$m_2 = \pm m_1$

But m_1 is L.C.M. Therefore.

$m_2 = m_1 \Longrightarrow m_1 = m_2$

Hence L.C.M of a & b is unique.

x — x — x — x — x —

* * Imp;

Theorem:

If $(a,b) = d$ Then

$$m = \langle a,b \rangle = \frac{|ab|}{d} = \frac{|ab|}{d}$$

Proof we prove that $m = \langle a,b \rangle = \frac{|ab|}{d}$ satisfy all three properties

i) Since $d > 0$ and $|ab| > 0$

$$\Rightarrow \frac{|ab|}{d} > 0.$$

ii) Since $(a,b) = d$

$$\Rightarrow d \mid a \text{ and } d \mid b.$$

Then $\exists$ an integer $a_1, a_2 \in \mathbb{Z}$ Such that

$$a = a_1 d \quad \text{---} (1)$$
$$b = a_2 d \quad \text{---} (2)$$

$$\left|\frac{ab}{d}\right| = \frac{|a_1 d\, a_2 d|}{d}$$

$$m = |a_1 a_2 d| \rightarrow (3) \quad \because \left|\frac{ab}{d}\right| = m$$

$$m = |a\, a_2| \quad \because a_1 d = a.$$

$$\Rightarrow a \mid m$$

Also

$$m = |a_1 b| \quad \text{---} \because \text{By putting } b = a_2 d \text{ in eq (3)}$$

$\Rightarrow b \mid m$ $\quad n \mid c$

iii) If $a \mid c$ & $b \mid c$ Then we are to show that $m \mid c$.

$\Rightarrow \exists\, d_1, d_2 \in \mathbb{Z}$ s.t.

$$c = ad_1 \text{ --- } (4)$$
$$c = bd_2 \text{ --- } (5)$$

$$c = ad_1 = bd_2 \text{ --- } (A)$$

As $(a, b) = d$
$\Rightarrow d \mid a$ and $d \mid b$.
$\Rightarrow \exists\, a_1, a_2 \in \mathbb{Z}$ s.t
$\Rightarrow a = a_1 d$ & $b = a_2 d$
using in (A)

$$c = a_1 d d_1 = a_2 d d_2 \text{ --- } (B)$$

$$a_1 \cancel{d} d_1 = a_2 \cancel{d} d_2.$$

$$a_1 d_1 = a_2 d_2.$$

or

$$a_2 d_2 = a_1 d_1.$$

$$\Rightarrow a_1 \mid a_2 d_2$$

~~$\Rightarrow \exists$ an integer $t \in \mathbb{Z}$ s.t~~

~~$a_2 d_2 = a_1 t$.~~

$$\Rightarrow a_1 \mid d_2 \quad \because (a_1, a_2) = 1$$

$\Rightarrow \exists \; t \in Z$ s.t.

$$d_2 = a_1 t$$

eqn (B) becomes.

$C = a_2 d \, a_1 t$

$C = a_1 a_2 d \, t \Rightarrow$

$C = m t$ $\quad$ $m = a_1 a_2 d$ from eqn (3)

$\Rightarrow m \mid C$.

Hence all the three conditions are satisfied so l.c.m of

$$m = \langle a, b \rangle = \frac{|ab|}{d}$$

— .x. — .x. — .x. — .x. — .x. —

The Linear Diophantine Equation:

The equation of the form

$ax+by=c$ where $a,b,c\in\mathbb{Z}$ is called diophantine equation.

for e.g $7x+8y=15$

Theorem:

$ax+by=c$, $a,b,c\in\mathbb{Z}$ has an integral solution iff $(a,b)\mid c$.

If (x_0,y_0) is solution of equation then solution set is

$$S=\left\{\left(x_0+\frac{b}{d}t,\ y_0-\frac{a}{d}t\right);\ t\in\mathbb{Z}\right\}$$

or

$$S=\left\{\left(x_0-\frac{b}{d}t,\ y_0+\frac{a}{d}t\right);\ t\in\mathbb{Z}\right\}$$

Proof Suppose that

$ax+by=c$ has integral solution Then we have to prove

$(a,b)\mid c$.

let $(a,b)=d$

$\Rightarrow d\mid a$ and $d\mid b$.

$d \mid ax$ and $d \mid by$

$d \mid ax+by$.

$\Rightarrow d \mid c \quad \because \; ax+by = c$

so $(a,b) \mid c$.

Conversely If $(a,b) \mid c$ Then we have to prove that the equation $ax+by=c$ has integral solution

let $(a,b) = d$ ✓

$\Rightarrow d \mid a$ and $d \mid b$.

$\Rightarrow \exists \; a_1, b_1 \in \mathbb{Z}$ such that

$a = a_1 d$ & $b = b_1 d$ where $(a_1, b_1) = 1$ ✓

As $d \mid c \Rightarrow \exists \; c_1 \in \mathbb{Z}$ such that

$c = c_1 d$

Also as $(a,b) = d \Rightarrow \exists \; x_0, y_0 \in \mathbb{Z}$ such that

$ax_0 + by_0 = d$ Then

$1 \Rightarrow \quad ac_1x_0 + bc_1y_0 = c_1 d$ by putting value of d.

$ac_1x_0 + bc_1y_0 = c$ ✓

$\Rightarrow x = c_1x_0$ and $y = c_1y_0$ is an integral solution of $ax+by=c$.

This complet the first part of theorem.

Now Suppose x_0, y_0 and x_1, y_1 be two solution of $ax + by = c$

$\Rightarrow$

$$ax_0 + by_0 = c \quad \text{--- (1)}$$

and

$$ax_1 + by_1 = c \quad \text{--- (2)}$$

Substracting (2) from (1) we get.

$$a(x_0 - x_1) + b(y_0 - y_1) = 0$$

$$\Rightarrow a_1 d(x_0 - x_1) + b_1 d(y_0 - y_1) = 0$$

$$\Rightarrow a_1(x_0 - x_1) = b_1(y_1 - y_0) \quad \text{--- (3)}$$

$10 = 2$
$\Rightarrow 2 | 10$
$5.$

$$\Rightarrow a_1 \mid b_1(y_1 - y_0) \text{ and}$$

$$(x_0 - x_1) \mid b_1(y_1 - y_0)$$

As

$$(a_1, b_1) = 1$$

$a = a_1 d$
$a_1 = \frac{a}{d}$

Therefore

$$a_1 \mid y_1 - y_0.$$

$\Rightarrow$ $\exists$ an integer $t \in \mathbb{Z}$ s.t.

$$y_1 - y_0 = a_1 t.$$

$$y_1 = y_0 + a_1 t$$

$$y_1 = y_0 + \frac{a}{d} t$$

using $y_1 = y_0 + \frac{a}{d}t$ in eqn 3

$a_1(x_0 - x_1) = b_1(\cancel{y_0} + a_1 t - \cancel{y_0})$

$a_1(x_0 - x_1) = b_1 a_1 t$

$x_0 - x_1 = b_1 t$

$x_1 = x_0 - b_1 t$

$x_1 = x_0 - \frac{b}{d}t \quad \because b = b_1 d$

For each value of $t \in \mathbb{Z}$

$$a x_1 + b y_1 = c.$$

$$a\left(x_0 - \frac{b}{d}t\right) + b\left(y_0 + \frac{a}{d}t\right) = c$$

$$a x_0 - \cancel{\frac{ab}{d}t} + b y_0 + \cancel{\frac{ab}{d}t} = c$$

$$a x_0 + b y_0 = c.$$

$\Rightarrow a x_0 + b y_0 = c$

Hence Solution Set.

$$S.S = \left\{ x_0 - \frac{b}{d}t \,,\, y_0 + \frac{a}{d}t \right\}$$

Ex Find all integral Solutions of

$$69x + 111y = 9000 \quad \text{—— (1)}$$

Sol:
As $(69, 111) = 3 \mid 9000$
Hence Solution of eqn (1) exist.

$(a, b) = d$

69 | 111 (1
69
42 | 69 (1
42
27 | 42 (1
27
15 | 27 (1
15
12 | 15 (1
12
3 | 12 (4
12
x

3 | 9000

$$69x + 111y = 9000$$

$$23x + 37y = 3000$$

$$\Rightarrow 23x + (23 + 14)y = 23(130) + 10$$

$$\Rightarrow 23x + 23y + 14y - 23(130) = 10$$

$$\Rightarrow 23(x + y - 130) + 14y = 10$$

put $x + y - 130 = z$ —— (2)

$$23z + 14y = 10$$
$$(14 + 9)z + 14y = 10$$
$$14(z + y) + 9z = 10$$

put $z + y = v$ —— (3)

$$14v + 9z = 10.$$

$$\Rightarrow (9 + 5)v + 9z = 9 + 1$$

$$\Rightarrow 9(v + z - 1) + 5v = 1.$$

$\Rightarrow$ put $v + z - 1 = w$ —— (4)

$9w + 5v = 1$

$(4+5)w + 5v = 1$

$5(w+v) + 4w = 1$

put $w + v = u$ — (5)

$5u + 4w = 1$

$\Rightarrow u = 1$ & $w = -1$

from (5)

$v = u - w$

$= 1 - (-1)$

$v = 2$

put $v = 2$, $w = -1$ in eqn (4)

$2 + z \cancel{-1} = \cancel{-1}$

$z = -2$.

put $z = -2$, $v = 2$ in eq (3) we have

$-2 + y = 2$

$y = 4$.

put $z = -2$, $y = 4$ in eq (2) we have

$x + 4 - 130 = -2$

$x - 126 = -2$

$x = 126 - 2$

$x = 124$.

$a = 69$ $\frac{b}{d} = \frac{111}{3} = 37$

$b = 111$ $\frac{a}{d} = \frac{69}{3} = 23$

$d = 3$

$x = x_0 = 124$

$y = y_0 = 4$

$S.S = \{ (x_0 - b/d\,t,\ y_0 + a/d\,t);\ t \in Z \}$

$S.S = \{ (124 - 37t,\ 4 + 23t);\ t \in Z \}$.

[redacted] Find the solution set of

i) $23x - 49y = 179.$

ii) $321x + 105y = 11$

iii) $3x + 6y = 1$

$$105\overline{)321}(3$$
$$315$$
$$6\overline{)105}(17$$
$$102$$
$$3\overline{)6}(2$$
$$6$$
$$\times$$

But $3 \nmid 11$

Sol:-

Given linear diophantine equation is

$$23x - 49y = 179.$$

First we find G.C.D of $(23, 49)$

so

$$(23, 49) = 1.$$

Hence $1 \mid 179.$

So Integral solution of the given equation exist.

$$23\overline{)49}(2$$
$$46$$
$$3\overline{)23}(7$$
$$21$$
$$2\overline{)3}(1$$
$$2$$
$$1\overline{)2}(2$$
$$2$$
$$\times$$

$$23x - 49y = 179.$$

$$23x - (23(2) + 3)y = 23(7) + 18.$$

$$23x - 23(2y) + 3y - 23(7) = 18.$$

$$23(x - 2y - 7) + 3y = 18$$

put

$$x - 2y - 7 = z \quad \text{--- (1)}$$

$$23z + 3y = 18$$

$$(7(3) + 2)z + 3y = 3(6)$$

$3(7z) + 2z + 3y = 3(6)$.

$3(7z) + 3(y) - 3(6) + 2z = 0$.

$3(7z + y - 6) + 2z = 0$.

Put $7z + y - 6 = u$. — (2)

$3u + 2z = 0$

$\Rightarrow u = (-2)$ & $z = -3$

$u = -2$ & $z = -3$.

putting these values in equation (2)

$7(-3) + y - 6 = -2$

$-27 + y = -2$

$y_0 = y = -2 + 27 = 25$

putting $y = 25$, $z = -3$ in eqn (1)

$x - 2(25) - 7 = -3$.

$x - 57 = -3$

$x_0 = x = \cancel{57 - 3}$

$= x = 54$.

Hence the integral solution of given eqn is $S.S = \left\{ x_0 + \frac{b}{d}t,\ y_0 + \frac{a}{d}t \right\}$

$S.S = \left\{ 54 - \frac{(-49)}{1}t,\ 25 + 23t \right\}$

Theorem:

Every Composit number has prime divisor $\leq \sqrt{n}$.

Proof: Since n is composit it has at least prime divisor p. let $n = n_1 p$. if $p > \sqrt{n}$. Then $n = n_1 p$ shows that

$$n_1 < \sqrt{n} < p$$

i.e There exists a divisor n_1 of n less then the least which is contradiction

Hence

$$p \leq \sqrt{n}.$$

Let $P = 2$ then divisor of 2 is 2.
If composite no is 4.
then $4 = 1, 2, 4$,
then $1 < 2, 2 < 4$

Ch#2. Theory of Primes.

* [redacted]

A positive integer p is called prime number if it has no divisor 'd' $1 < d < p$

or

If $p \in Z$ & $p > 0$ Then p is said to be prime number if $\pm 1, \pm p$ are only divisors of p.

e.g: $2, 3, 5, 7, \ldots\ldots$

* [redacted]

A number m which is not prime is called composit number and it can be written as

$m = d_1 d_2$ where d_1 & d_2 are divisor of m.

and $1 < d_1, d_2 < m$.

1 is neither prime nor composite.
2 is only even prime number.

* [redacted]

Every integer 'm' > 1 has prime divisor.

Proof If 'm' is prime then 'm' is prime divisor of 'm'.

If m is composite then we can write $m = d_1 d_2$. $1 < d_1, d_2 < m$

$m = d_1 d_2$

let $d_1 < d_2$.

If d_1 is prime Then m has prime diviser That is d_1.

If d_1 is composite then we can write

$$d_1 = d_3 d_4 \qquad 1 < d_3, d_4 < d_1$$

let $d_3 < d_4$

If d_3 is prime Then m has Prime diviser i.e d_3.

But If d_3 is composite we proceed in the same way altimely we arrive

$$1 < d_k, d_{k+1} < m.$$

Such that d_k cannot be factored more Then d_k is prime number. and m has prime divisor.

NOTE:- Every Composit number has prime divisor $\leq \sqrt{n}$.

∴ ———— ∴ ———— ∴ ————

[redacted]

If p is a prime divisor and $p|ab$ Then $p|a$ or $p|b$.

Proof:-

Suppose That $p \nmid a$

Since p is prime Then

$$(p, a) = 1$$

$\Rightarrow \exists\ x, y \in \mathbb{Z}$ Such that.

$$px + ay = 1$$
$$pbx + aby = b \quad \text{---} (1)$$

As $p \mid p$ & $p \mid ab$

$\Rightarrow p \mid pbx$ and $p \mid aby$

$\Rightarrow p \mid pbx + aby$

$\Rightarrow p \mid b \quad \because \quad pbx + aby = b.$

[redacted] If 'p' is a prime number and $p \mid a_1 a_2 a_3, \ldots, a_k$ Then

$p \mid a_i$ for some $i = 1, 2, 3, \ldots, k$.

If $p \mid p_1 p_2 p_3 \ldots p_k$ where p_i's are prime. Then $p = p_j$ for some $j = 1, 2, 3, \ldots, k$.

[redacted] (The Fundamental Theorem of Airthmatics
OR
Unique Factorization Theorem

Statement

Every integer $n > 1$ can be expressed as a product of primes and this representation is unique ~~exp~~ except for the order in which they are written.

P.T.O. for proof

Proof :- we prove The Theorem by induction on 'n'

For $n = 2$

$2 = 2$ (True).

let us Suppose that the statement is true for $n = 2, 3, 4, \ldots, k$.

Now prove it for $n = k+1$.

If $k+1$ is prime. Then the induction is complete. If $k+1$ is composit. Then It can be written as

$$k+1 = k_1 k_2.$$

Then by induction hypothesis k_1, k_2 can be expressed as product of prime. So The induction is complete and Theorem is True. That is $n = p_1 p_2 p_3 \ldots p_r$ where p_i for $i = 1, 2, 3 \ldots r$ are primes.

— x — x — x To be Continoue. — x —

For Uniqueness.

let $n = p_1 p_2 p_3 \ldots p_r$. where $i = 1, 2, 3, \ldots, r$

$n = q_1 q_2 q_3 \ldots q_s$ where $j = 1, 2, 3, \ldots, s$.

Then

$$q_1 q_2 q_3 \ldots q_s = p_1 p_2 p_3 \ldots p_r. \quad \text{—} (1)$$

Then we cancelled common factors from both sides of (1)
we obtained

$$q_1 \cdot q_2 \cdot q_3 \cdots q_i = p_1 p_2 p_3 \cdots p_j \quad \text{——— (2)}$$

Then by result
of $p \mid p_1 p_2 p_3 \cdots p_k$ where p_i $i = 1, 2, 3, \ldots, k$ are primes Then $p = p_i$ for some $i = 1, 2, 3, \ldots, k$.

Since
$$q_1 \mid q_1 q_2 q_3 \cdots q_i$$
Therefore
$$q_1 \mid p_1 p_2 p_3 \cdots p_j.$$
Then By above result.

$q_1 = p_j$ where for some $j = 1, 2, 3, \ldots, j$
which is a contradiction Hence This prove the uniqueness Theorem.

[redacted]: The number of primes is infinite.

Proof
Suppose that the number of prime is finite Then there Largest prime p (say) such that.

$$2, 3, 5, 7, 11, \ldots, p.$$

Now Consider the integer

$n = (2 \cdot 3 \cdot 5 \cdots P) + 1$

If n is prime Then n is greater Then P i.e $n > P$. ~~which is not Possible.~~

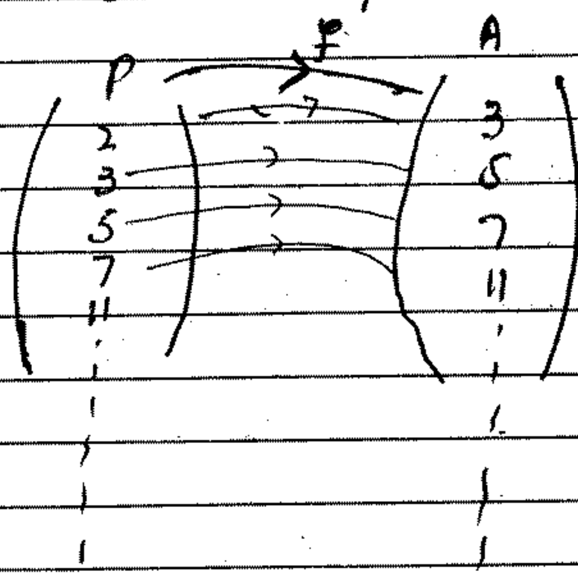
If n is composit. Then it has Prime divisor which is not in

$2, 3, 5, \cdots, P$

Consequently, It is a prime greater then P.

which is again a Controduction.

To Show By other way.



$$f(P_i) = \begin{cases} 3 & \text{if } P = 2 \\ P_{i+1} & \text{if } P > 2 \end{cases}$$

P_{i+1} mean ~~next~~ prime Then P_i

if a proper Subset is equivelent to the given set (i.e bijective mapping) is define b/w them. Then the given Set is infinite.

//

(4,9)=1 36

[redacted]

If $(b,c)=1$ and bc is perfect square Then prove That 'b' & c are perfect square.

Sol:-

let
$$b = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot p_3^{\alpha_3} \cdots p_r^{\alpha_r}.$$
$$c = q_1^{\beta_1} \cdot q_2^{\beta_2} \cdot q_3^{\beta_3} \cdots q_t^{\beta_t}$$
be the standard form of b & c

Since b & c are relatively prime.
$$(b,c) = 1.$$
So
$$q_i \neq p_j ?$$
$i \in \{1,2,3,\dots t\}$ & $j \in \{1,2,3,\dots,r\}$

Then
$$bc = \left(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot p_3^{\alpha_3} \cdots p_r^{\alpha_r}\right)\left(q_1^{\beta_1} \cdot q_2^{\beta_2} \cdots q_t^{\beta_t}\right) \quad (1)$$
Since bc is perfect square.

So every exponent is even. ~~Then~~.

Then
$$\alpha_i = 2r_i \text{ and each}$$
$$\beta_i = 2s_i$$
Then eqn (1) becomes.
$$bc = \left(p_1^{2r_1} \cdot p_2^{2r_2} \cdots p_r^{2r_r}\right) \cdot \left(q_1^{2s_1} \cdot q_2^{2s_2} \cdots q_t^{2s_t}\right).$$
$$bc = \left(p_1^{r_1} \cdot p_2^{r_2} \cdots p_r^{r_r}\right)^2 \cdot \left(q_1^{s_1} \cdot q_2^{s_2} \cdots q_t^{s_t}\right)^2.$$

Hence b & c are perfect square.

for e.g. As 36 is perfect square $(4,9)=1$.
$$36 = 9 \times 4.$$
$$= (3)^2 \cdot (2)^2 \implies 9 \text{ \& } 4 \text{ are also perfect square.}$$

$3\overline{)-11}^{\,3}$ $\;9$ $\;(-2)$

$m|\overline{a}$, b / $a \equiv b \pmod m$ or $m \mid a-b$.

[redacted]

Gauss (1777-1855) introduce the concept of congurences.

If $m>0$ and $a, b, m \in \mathbb{Z}$ we say 'a' is congurente to 'b' modulo 'm' if

$m \mid a-b$. Then we write

$$a \equiv b \pmod m.$$

We say that 'a' is rasidue of 'b' and 'b' is is residue of 'a'.

If $m \nmid a-b$ Then we say
a is inconguence to b (mod m)

$$a \not\equiv b \ (\text{modulo } m)$$

e.g

$$4 \equiv 1 \ (\text{modue } 3)$$

$\because$

$3 \mid 4-1$ i.e $3 \mid 3$. $\qquad 1 \equiv 1 \pmod m$

or

$3\overline{)4}(1$
$\;\;\underline{3}$
$\;\;1$.

$$3 \mid 4-1 \pmod 3$$

$$4 \equiv 1 \ (\text{modulo } 3)$$

$$-11 \equiv -2 \pmod 3.$$

[redacted] The Congurance relation in Z is an equivalence relation.

Proof Reflexive.

since $\forall a \in Z$.

$m \mid a-a$

$\Rightarrow a \equiv a \pmod m$.

Symmetric property.

If for $a, b \in Z$ & $m > 0$ $a \equiv b \pmod m$ Then $b \equiv a \pmod m$

Since $a \equiv b \pmod m$

$\Rightarrow m \mid a-b$

$\Rightarrow m \mid -(b-a)$

$\Rightarrow m \mid b-a$ $\because$ if $m \mid a$ Then $m \mid -a$

$\Rightarrow b \equiv a \pmod m$

Transitive property. (For $a, b, c \in Z$ & $m > 0$)

If $a \equiv b \pmod m$ — ①

and $b \equiv c \pmod m$ — ② Then

$a \equiv c \pmod m$.

from ① & ②

$m \mid a-b$ & $m \mid b-c$

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

$\Rightarrow m \mid a-c$

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

Hence Congruance relation in $\mathbb{Z}$ is an equivelence relation.

Remark:-

1) The integer $0, 1, 2, \ldots, m-1$ are incongruent modulo m. (For any two integers) { i.e $a \not\equiv b$. }

[redacted]

$a \equiv b \pmod{m}$ iff a & b have same remainder after division by m.

Proof:- Suppose that $a \equiv b \pmod{m}$

$\Rightarrow m \mid a-b$.

$\Rightarrow \exists$ an integer $q \in \mathbb{Z}$ such that

$$a - b = mq \quad \text{——} ①$$

let $a = mq_1 + r_1 \ldots \quad 0 \leq r_1 < m$.

& $b = mq_2 + r_2 \quad 0 \leq r_2 < m$.

where $q_1, q_2, r_1, r_2 \in \mathbb{Z}$.

$$a-b = mq_1 + r_1 - mq_2 - r_2.$$

$$a-b = m(q_1 - q_2) + r_1 - r_2.$$

$$mq = m(q_1 - q_2) + r_1 - r_2.$$

$$mq - m(q_1 - q_2) = r_1 - r_2$$

$$\Rightarrow m \mid r_1 - r_2.$$

but

$$0 \leq |r_1 - r_2| < m.$$

NOTE:- if $m \mid r$ and $r < m$. Then r must be equal to zero

$$|r_1 - r_2| = 0$$

$$r_1 = r_2$$

Conversely suppose that a & b have same remainders after division by m.

i.e

$$a = mq_1 + r \quad \text{Same remainder}$$

$$b = mq_2 + r \qquad 0 \leq r < m.$$

$$a-b = m(q_1 - q_2) + \cancel{r} - \cancel{r}$$

$$a-b = m(q_1 - q_2) = mq_3 \text{ where } q_3 = q_1 - q_2.$$

$$\Rightarrow m \mid a-b.$$

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

x — x — x — x — x — x

[redacted] If $a \equiv b \pmod m$

and $c \equiv d \pmod m$

Then (1)

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

2) $a-c \equiv b-d \pmod m$.

3) $ac \equiv bd \pmod m$.

Proof

Given That

1) $a \equiv b \pmod m$.

$m \mid a-b$ — ① also $c \equiv d \pmod m$

&

$m \mid c-d$ — ②

From ① & ②

$m \mid a-b+c-d$.

$m \mid (a+c)-(b+d)$

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

2)

As $a \equiv b \pmod m$

∴ $m \mid a-b$ — ①

&

$c \equiv d \pmod m$.

∴ $m \mid c-d$ — ②

From (1) & (2)

$m \mid a-b-(c-d)$.

$\Rightarrow m \mid a-c-b+d$.

$\Rightarrow m \mid (a-c)-(b-d)$

$\Rightarrow \quad a-c \equiv b-d \pmod{m}$.

iii) As $a \equiv b \pmod{m}$

$\therefore m \mid a-b$. —(1) $\Rightarrow a-b = mq_1$
$a = mq_1 + b$ —(3)

and $c \equiv d \pmod{m}$.

$\therefore m \mid c-d$. —(2)

~~From~~

$\Rightarrow c-d = mq_2$ By Definition of Divisibility

$c = mq_2 + d$ —(4)

multiplying (3) & (4) we get

$ac = (mq_1+b)(mq_2+d)$.

$ac = m^2 q_1 q_2 + mdq_1 + mbq_1 + bd$.

$ac - bd = m^2 q_1 q_2 + mdq_1 + mbq_1$.

$\Rightarrow m \mid ac-bd$

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

—x— x — x —x— x —

[redacted] If $a \equiv b \pmod m$

Then

1) $na \equiv nb \pmod m$.

2) $a^n \equiv b^n \pmod m$.

Proof

1) Since $a \equiv b \pmod m$.

$$\Rightarrow m \mid a-b.$$

$\Rightarrow \exists$ an integer $q \in \mathbb{Z}$ such that

$$a-b = mq.$$
$$na-nb = mnq.$$

$$\Rightarrow na-nb = mq_1. \quad \because nq = q_1$$

$$\Rightarrow m \mid na-nb$$

$$\Rightarrow na \equiv nb \pmod m$$

2) Since $a \equiv b \pmod m$.

$$\Rightarrow m \mid a-b.$$

& we are ~~$\Rightarrow \exists$ an~~ to prove that

$m \mid a^n - b^n$.

So by induction we have

for $n = 1$ ~~ath~~ we have

$a \equiv b \pmod m \Rightarrow m \mid a-b$

Hence the statment (1) is true.

let The statement is true for $n = k$

$$a^k \equiv b^k \pmod m.$$

$$\Rightarrow m \mid a^k - b^k \quad \text{——} (2)$$

Consider

$$a^{k+1} - b^{k+1} = a^k \cdot a - b^k \cdot b$$

$$= a^k \cdot a - b^k \cdot b + ab^k - ab^k$$

$$= a^k a - b^k \cdot a - b^k \cdot b + ab^k$$

$$a^{k+1} - b^{k+1} = a(a^k - b^k) + b^k(a - b)$$

Since $m \mid a(a^k - b^k)$ By (2)

& $m \mid b^k(a-b)$ By (1).

$$m \mid a(a^k - b^k) + b^k(a-b)$$

$$\Rightarrow m \mid a^{k+1} - b^{k+1}$$

$$\Rightarrow a^{k+1} \equiv b^{k+1} \pmod m$$

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

$\forall$ n non-negative integer.

i.e $n \in \mathbb{Z}^+ - \{0\}$ //.

Imp

[redacted]

If $na \equiv nb \pmod{m}$ and $(m,n) = d$ Then

$$a \equiv b \left(\bmod \frac{m}{d}\right)$$

Proof:- Since $na \equiv nb \pmod{m}$

$$\Rightarrow m \mid na - nb \quad \text{--- (1)}$$

a/80

$$(m,n) = d.$$

$$\Rightarrow d \mid m \ \& \ d \mid n.$$

$\Rightarrow \exists\, q_1, q_2 \in \mathbb{Z}$ Such that $m = q_1 d$, $n = q_2 d$ where $(q_1, q_2) = 1$

$$(1) \Rightarrow q_1 d \mid q_2 d(a-b)$$

$$\Rightarrow q_1 \mid q_2(a-b).$$

$$\Rightarrow q_1 \mid a-b \quad \because (q_1, q_2) = 1$$

$$a \equiv b \pmod{q_1}.$$

$\Rightarrow a \equiv b \left(\bmod \frac{m}{d}\right)$ Since $m = q_1 d$

[redacted]

If $na \equiv nb \pmod{m}$ and $(m,n)=1$
Then $a \equiv b \pmod{m}$.

Proof:

Since $na \equiv nb \pmod{m}$

i.e.

$$m \mid na - nb. \quad \text{---} (1)$$

also

~~$(m,n)=1$~~

~~Then $1 \mid m$ & $1 \mid n$~~
~~$\Rightarrow$ There exist two integers $q_1, q_2 \in \mathbb{Z}$ such that.~~

~~$m = q_1$ and $n = q_2$~~

~~Putting $m = q_1$ & $n = q_2$ Then eqn (1) becomes~~

~~$q_1 \mid q_1 a -$~~

$$m \mid n(a-b).$$

Since $(m,n)=1$ Therefore

$$m \mid a-b \quad \because \text{ If } a \mid bc \ \& \ (a,b)=1 \text{ Then } a \mid c.$$

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

— x — x — x — x —

[redacted]

If $a \equiv b \pmod{m_1}$

&

$a \equiv b \pmod{m_2}$ and

$(m_1, m_2) = 1$ Then

$a \equiv b \pmod{m_1}$

$m_1 \mid a - b$

[redacted]

If $f(x) = c_0 + c_1 x + c_2 x^2 + c_3 x^3 + \cdots + c_n x^n$

where $c_i \in \mathbb{Z}$

& $i = 1, 2, 3, \cdots, n$

and if $a \equiv b \pmod{m}$

Then $f(a) \equiv f(b) \pmod{m}$.

Proof :- we know that

$$1 \equiv 1 \pmod{m}$$

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

$$a^2 \equiv b^2 \pmod{m}$$

$$a^3 \equiv b^3 \pmod{m}$$

$$\vdots$$

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

Multiplying the congruences by $c_0, c_1, c_2, \cdots, c_n$ respectively and then adding

$$c_0 + c_1 a + c_2 a^2 + \cdots + c_n a^n \equiv c_0 + c_1 b + c_2 b^2 + \cdots + c_n b^n \pmod{m}.$$

$$\Rightarrow f(a) \equiv f(b) \pmod{m}$$

//

[redacted] Find The remainder when $f(15)$ is divided by 7 where

$f(x) = x^4 - 3x^2 + 2x - 1$.

Since

$$15 \equiv 1 \pmod 7$$

$$\Rightarrow f(15) \equiv f(1) \pmod 7.$$

$f(1) = 1 - 3(1) + 2 - 1$

$f(1) = -1$

$$-1 \equiv 6 \pmod 7.$$

Hence $\because$ remainder is positive

$$f(15) \equiv 6 \bmod (7).$$

Hence 6 is remainder $f(15)$ is divided by 7.

— ☆ — ☆ — ☆ — ☆ —

[redacted] Find remainder when 3^{21} is divided by 8.

As

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

$$\Rightarrow (3^2)^{10} \equiv (1)^{10} \pmod 8$$

Find the rem...

3^{10} is divided by 51.

(c) Find remainder.

5^{21} is divided by 127.

5^{65} is divided by 127.

Sol:-

[redacted]

As $7^4 \equiv 4 \pmod{51}$

$(7^4)^2 \equiv (4)^2 \pmod{51}$.

$7^8 \equiv 16 \pmod{51}$

$7^{10} \equiv 49 \times 16 \pmod{51}$

$7^{10} \equiv 19 \pmod{51}$

$7^{8} \cdot 7^{2}$

$49 \times 16 = 784$

$51 \overline{)784}(15$

765

19

[redacted] Find the remainder when 3^{10} is divided by 51.

As.

$$3^4 \equiv 30 \bmod (51).$$

$$(3^4)^2 \equiv 900 \bmod (51)$$

$$(3^4)^2 \equiv 11 \pmod{51}.$$

[redacted] Find the remainder when 5^{21} is divided by 127.

$$5^6 \equiv 4 \pmod{127}.$$

$$5^{18} \equiv (4)^3 \pmod{127}.$$

$$5^{18} \equiv 64 \pmod{127}.$$

$$5^3 \cdot 5^{18} \equiv 5^3 \cdot 64 \pmod{127}.$$

$$5^{21} \equiv 8{,}000 \pmod{127}$$

$$5^{21} \equiv 126 \pmod{127}.$$

$$127 \overline{)8000} (62$$
$$7874$$
$$\overline{126}$$

— x — x — x — x — x —

[redacted] Prove that $2^{11}-1$ has the factor 23.

Proof:-

Since $2^2 \equiv 4 \pmod{23}$

$$(2^2)^5 \equiv (4)^5 \pmod{23}$$

$$2^{10} \equiv 1024 \pmod{23}$$

$$\therefore 2^{10} \equiv 12 \pmod{23}$$

$$2 \cdot 2^{10} \equiv 2 \cdot 12 \pmod{23}$$

$$2^{11} \equiv 24 \pmod{23}$$

$$2^{11} \equiv 1 \pmod{23}$$

$$2^{11} - 1 \equiv 1 - 1 \pmod{23}$$

$$2^{11} - 1 \equiv 0 \pmod{23}$$

$\Rightarrow 23 \mid 2^{11} - 1$

$\Rightarrow$ 23 is factor of

$2^{11} - 1$ //

— x — x — x —

[redacted]

$2^{23}-1$ has the factor 47.

Since

$$2^4 \equiv 2^4 \pmod{47}$$

$$2^4 \equiv 16 \pmod{47}.$$

$$(2^4)^5 \equiv (16)^5 \pmod{47}$$

$$2^{20} \equiv 6 \pmod{47}.$$

$16.16.16.16.16$

$(16)^5 = 1048$

$$2^3 \cdot 2^{20} \equiv 2^3 \cdot 6 \pmod{47}.$$

$$2^{23} \equiv 48 \pmod{47}$$

$$2^{23} \equiv 1 \pmod{47}.$$

$$2^{23}-1 \equiv 0 \pmod{47}.$$

$\Rightarrow 47 \mid 2^{23}-1$

$\Rightarrow$ 47 is the factor of $2^{23}-1$.

[redacted]

If $ab \equiv c \pmod{m}$
and $b \equiv d \pmod{m}$

Then
$$ad \equiv c \pmod{m}.$$

Proof: Since $ab \equiv c \pmod{m}$.
$m \mid ab-c$

$\Rightarrow \exists$ an integer say $q_1 \in \mathbb{Z}$ s.t.

$$ab - c = m q_1 \quad \text{——} \ (1)$$

Also
$$b \equiv d \pmod{m}.$$

$\Rightarrow m \mid b-d$

$\Rightarrow \exists$ an integer $q_2 \in \mathbb{Z}$
s.t.

$$b - d = q_2 m$$
$$\Rightarrow b = d + m q_2 \quad \text{——}$$

Then
eq (1) $\Rightarrow a(d + m q_2) - c = m q_1$.

$$ad + a m q_2 - c = m q_1.$$

$$ad - c = m q_1 - a m q_2.$$

$$ad - c = m(q_1 - a q_2).$$

$$ad - c = m q_3.$$

$\Rightarrow m \mid ad - c \Rightarrow ad \equiv c \pmod{m}$ //

[redacted]

// Show that an integer written in the scale of 10 is divisible by 9 iff the sum of its digit is divisible by 9.

Proof

Let

$$a = (r_n \, r_{n-1} \, r_{n-2} \cdots r_1 \, r_0)_{10}$$ be the integer then.

$$a = r_n \times 10^n + r_{n-1} \times 10^{n-1} + \cdots r_1 \times 10 + r_0$$

Since

$$1 \equiv 1 \pmod 9$$

$$10 \equiv 1 \pmod 9$$

$$(10)^2 \equiv (1)^2 \pmod 9$$

$$10^2 \equiv 1 \pmod 9$$

$$10^3 \equiv 1 \pmod 9$$

$$\vdots$$

$$10^n \equiv 1 \pmod 9$$

Now

$$r_n 10^n \equiv r_n \pmod 9 \quad (i)$$

&

$$r_{n-1} 10^{n-1} \equiv r_{n-1} \pmod 9 \quad (ii)$$

$$\vdots \qquad\qquad \vdots$$

$$r_1 10 \equiv r_1 \pmod 9 \quad (n)$$

$$r_0 \cdot 1 \equiv r_0 \pmod 9 \quad (n+1).$$

Now adding all congurancies from (i) to (n+1) eqns.

$$r_n 10^n + r_{n-1} 10^{n-1} + \cdots + r_1 10 + r_0 \equiv \underline{r_n + r_{n-1} + \cdots r_1 + r_0} \pmod 9$$

$$\Rightarrow \quad a \equiv r_n + r_{n-1} + r_{n-3} + \cdots + r_1 + r_0 \pmod 9$$

$$\Rightarrow \quad 9 \mid a \text{ iff } 9 \mid r_1 + r_2 + r_3 + \cdots + r_n.$$

Theorem:- Show that an integer divisble by 8 iff the integer formed by its last three digit is divisble by 8.

Proof let

$a = (r_n r_{n-1} r_{n-2} \cdots r_1 r_0)_{10}$ be the integer then

$$a = r_n \times 10^n + r_{n-1} \times 10^{n-1} + \cdots + r_2 \times 10^2 + r_1 \times 10 + r_0$$

Since

$1 \equiv 1 \pmod 8$.

$10 \equiv 2 \pmod 8$.

$100 \equiv 50 \pmod{25}$

$5^0 \equiv 2 \pmod{25}$

$10^2 \equiv 4 \pmod 8$.

$10^3 \equiv (4)^3 \pmod 8$

$10^3 \equiv 64 \pmod 8$.

$10^3 \equiv 0 \pmod 8$.

$10^4 \equiv 0 \pmod 8$

— — — — —

— —

$10^{n-1} \equiv 0 \pmod 8$

$10^n \equiv 0 \pmod 8$.

Now

$r_n 10^n \equiv 0 \pmod 8$ — (i)

$r_{n-1} 10^{n-1} \equiv 0 \pmod 8$ — (ii)

— (iii)

$r_{n-2} 10^{n-2} \equiv 0 \pmod 8$. — (iv)

— — — — —

— — — —

— — —

$r_2 10^2 \equiv 4r_2 \pmod 8$.

$r_1 10 \equiv 2r_1 \pmod 8$

$r_0 \equiv r_0 \pmod 8$ (n+1)

Now adding all the congruences from (1) to (n+1) Then

$$r_n 10^n + r_{n-1} 10^{n-1} + \cdots + r_2 10^2 + r_1 10 + r_0 \equiv 4r_2 + 2r_1 + r_0 \pmod 8$$

$\therefore$ $a \equiv 4r_2 + 2r_1 + r_0 \pmod 8$.

$a \equiv 10^2 r_2 + 10 r_1 + r_0 \pmod 8$.

$a \equiv (r_2 r_1 r_0)_{10} \pmod 8$.

Hence $8 \mid a$ iff $8 \mid (r_2 r_1 r_0)_{10}$.

* — * — * — *

[redacted]

We know that the Conguesence selation (mod m) in Z is an equivelence relation and hence by the fundamental Theorem of equivelence selation. [If partition 'Z' into disjoint equivelence classes called congruent classes (mod m)] Such that all members of same equivalence class are conguesent to each other (mod m) and two member of distinct classes are incongusent (mod m). Since every integer is congusent to one of

$0, 1, 2, 3, ---, m-1 \pmod{m}$.

Then there are exactly m Congurent classes.

Example:-

If $m = 4$. Then

$$C_i = \{ x \in Z : x \equiv i \pmod{4} \}$$
$$i = 0, 1, 2, 3$$

Solution when $i = 0$

$$C_0 = \{ x_0 \in Z : x \equiv 0 \pmod{4} \}$$

$$C_0 = \{ ---, -12, -8, -4, 0, 4, 8, 12, --- \}.$$

for $i = 1$

$$C_1 = \{ x_i \in Z : x \equiv 1 \pmod{4} \}$$

$$C_1 = \{ ---, -11, -7, -3, 1, 5, 9, 13, -- \}$$

$$C_2 = \{ x \in Z : x \equiv 2 \pmod 4 \}$$

$$C_2 = \{ \dots, -10, -6, -2, 2, 6, 10, 14, \dots \}$$

for $i = 3$.

$$C_3 = \{ x \in Z : x \equiv 3 \pmod 4 \}$$

$$C_3 = \{ \dots -9, -5, -1, 3, 7, 11, 15, \dots \}$$

Imp NOTE: Number of equivalence classes are equal to modulo.

$$\bigcup_{i=0}^{3} C_i = \{ 0, \pm 4, \pm 8, \pm 12 \} \cup \{ \dots -11, -7, -3, 1, 5, 9, 13, \dots \}$$

$$\cup \{ \dots, -10, -6, -2, 2, 6, 10, 14 \dots \}$$

$$\cup \{ \dots, -9, -5, -1, 3, 7, 11, 15, \dots \}$$

$= Z$ (set of integer).

[redacted]

(C. R. S).

[redacted]

A set 'A' is Complete Residue System (mod m) iff 'A' satisfy the following properties

i) A has 'm' elements.

ii) If $x_i, x_j \in A$; $i \neq j$ Then

$$x_i \not\equiv x_j \pmod{m}.$$

OR

A Set 'A' is C.R.S if any integer 'a' is congruent to one of the following elements i.e $0, 1, 2, 3, \ldots, m-1 \pmod{m}$.

i.e.

For $a \in \mathbb{Z}$.

$$a_i \equiv m-1 \pmod{m}$$

where $i = 0, 1, 2, 3, \ldots, m-1$

For Ex.

$$A = \{0, 1, 2, 3, 4\}$$ is

C.R.S (mod 5).

$\because$ A has 5 elements.

& for any $x, y \in A$.

$$x \not\equiv y \pmod 5.$$

=x———x———x———x———x=

Imp.

[redacted]

If $\{x_0, x_1, x_2, ---, x_{m-1}\}$ is C.R.S of (mod m) Then for any $a, b \in Z$ with $(a, m) = 1$ Then

$A = \{ax_0+b, ax_1+b, ax_2+b, ---, ax_{m-1}+b\}$ is C.R.S. (mod m).

Proof :- As

$$A = \{ax_0+b, ax_1+b, + ---, ax_{m-1}+b\}$$

Clearly A has 'm' element.

let $ax_i + b$ and $ax_j + b \in A$. where $i \neq j$ s.t

$$ax_i + b \equiv ax_j + b \ (\text{mod } m).$$

$$\Rightarrow ax_i \equiv ax_j \ (\text{mod } m).$$

$$\Rightarrow x_i \equiv x_j \ (\text{mod } m) \quad \because (a, m) = 1$$

which is contreduction as x_i and x_j are members of C.R.S. Hence our supposition is wrong. and any two member of A are incongruence under (mod m). Consequantly A is complete Residue system.

—:—:—:—

Imp

[redacted]

If $\{x_0, x_1, x_2, \dots, x_{m-1}\}$ is C.R.S $(\text{mod } m)$ and $\{y_0, y_1, y_2, \dots, y_{n-1}\}$ is C.R.S $(\text{mod } n)$ where $(m,n)=1$ Then

$A = \{nx_i + my_j,\ i = 0,1,2,\dots,m-1,\ j = 0,1,2,\dots,n-1\}$ is C.R.S of $(\text{mod } mn)$.

Proof

As

$$A = \{nx_i + my_j,\ i = 0,1,2,\dots,m-1,\ j = 0,1,2,\dots,n-1.\}$$

Clearly **A** has 'mn' elements.

Now let

$nx_i + my_j,\ nx_l + my_k$ where $i \neq l$ or $j \neq k$.

$$nx_i + my_j \equiv nx_l + my_k \pmod{mn}.$$

$$n(x_i - x_l) \equiv m(y_k - y_j) \pmod{mn}$$

$$\Rightarrow n(x_i - x_l) + m(y_j - y_k) \equiv 0 \pmod{mn}.$$

$$\Rightarrow n(x_i - x_l) + m(y_j - y_k) \equiv 0 \pmod{m}$$

&

$$n(x_i - x_l) + m(y_j - y_k) \equiv 0 \pmod{n}.$$

$$\Rightarrow n(x_i - x_l) \equiv m(y_k - y_j) \pmod{m}$$

& $m(y_j - y_k) \equiv n(x_l - x_i) \pmod{n}$

$\Rightarrow n(x_i - x_l) \equiv 0 \pmod m$

&

$m(y_j - y_k) \equiv 0 \pmod n$

$\Rightarrow x_i - x_l \equiv 0 \pmod m$

&

$y_j - y_k \equiv 0 \pmod n$.

$\because (m, n) = 1$

$\Rightarrow x_i \equiv x_l \pmod m$

&

$y_j \equiv y_k \pmod n$.

which is contradiction as x_i's and y_j's are members of complete residue systems. Hence our supposition is wrong, and any two members of A are incongruent (mod mn). That is 'A' is C.R.S.

EX:

$\{0, 1, 2\}$, $\{0, 1, 2, 3\}$

are C.R.S. und (mod 3) & (mod 4) resp.

Then $m = 3$, $n = 4$.

$A = \{nx_i + my_j : i = 0, 1, 2, \ldots, m-1; j = 0, 1, 2, \ldots, n-1\}$

$A = \{0, 4, 8, 3, 7, 11, 6, 10, 14, 9, 13, 17\}$

or

$A = \{0, 3, 4, 6, 7, 8, 9, 10, 11, 13, 14, 17\}$

we are to show that
A is C.R.S (mod 12).
Since A has 12 element
and for any $x, y \in A$

$x \not\equiv y \pmod{12}$.
Hence A is complete
residue system (mod 12).

imp obj q

[redacted]

An arithmatical function which associates with every integer 'm', the number of positive integers less than or equal to m and prime to 'm' is called Euler's Function and is denoted by $\phi(m)$.

e.g

$\phi(1) = 1$

$\phi(2) = 1$

$\phi(3) = 2$

$\phi(4) = 2$ ✓

$\phi(5) = 4$

$\phi(8)=$

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

$4 = 2^2$

$\phi(4) = 2^2$

$\phi(4) = m(1-\frac{1}{P_1})$
$= 4(1-\frac{1}{2})$
$= 4(\frac{1}{2}) = 2$

NOTE:- If m is prime then
$\phi(m) = m-1$.

$\phi(6) = 2 \cdot 3$
$= 6(1-\frac{1}{2})(1-\frac{1}{3})$
$= 6(\frac{1}{2})(\frac{2}{3})$
$\phi(6) = 2$

$\phi(8) = 2^3$
$= 8(1-\frac{1}{2})$
$\phi(8) = 8(\frac{1}{2}) = 4$

[redacted]

$$\varphi(m) = m-1 \text{ iff } 'm' \text{ prime}$$

Proof:- Suppose m is prime then all the +ve integer less then m are relatively prime to 'm'.

$\Rightarrow \varphi(m) = m-1$ $\because$ There are $m-1$ +ve integers relativ prime to m.

Conversely

let

$$\varphi(m) = m-1$$

i.e there are '$m-1$' +ve integers which relatively prime to 'm'. which is only possible if m is prime.

for e.g

$$\varphi(5) = 4. \quad \because 5 \text{ is prime}$$

9. [redacted] - If m is not prime then $\varphi(m)$ is less than $m-1$.

Consider p^{α} where p is prime Then There are exactly p^{α} integer not exceeding p^{α} out of which $p^{\alpha-1}$ are not prime to p^{α}.

Then

$$\varphi(m) = p^{\alpha} - p^{\alpha-1}$$

for e.g $8 = 2^3$, $2^{3-1} = 4$

$$\varphi(8) = 2^3 - 2^{3-1} = 8 - 4 = 4.$$

$$\beta_0^{n-1} P\left(\frac{x}{\beta_0}\right) = x^n + \beta_1 x^{n-1} + \beta_0\beta_2 x^{n-2} + \cdots + \beta_0^{n-1}\beta_n = q(x)$$

Then

'$\beta_0\theta$' is zero of $q(x)$ having coeffients are algebraic integers and also $q(x)$ is monic. Hence '$\beta_0\theta$' is an algebraic integer.

Definition:- Norm of an element $\alpha \in R(\theta)$.

If 'α' is any element of $R(\theta)$ of degree 'n'. Then the product of $\alpha', \alpha'', \alpha''', \ldots, \alpha^n$ all are field conjugates of 'α' is called the norm of 'α' and it is denoted by $N\alpha$.

or

$$\underset{R(\theta)}{N\alpha} = \alpha'.\alpha''.\alpha''' \ldots \alpha^{n}$$

Imp * Annual 09

Theorem:- 'The norm of an algebraic integer is a rational integer.

Proof:- Let 'α' be an algebraic integer and let $P(x) = x^m + s_1 x^{m-1} + \cdots + s_m$ be the defining polynomial of 'α' and let.

$$f(x) = (x-\alpha')(x-\alpha'') \cdots (x-\alpha^{(n)}).$$

where 'α'', α'', α''', $\ldots$, α^n are the conjugate of α.

$$f(x) = [P(x)]^{n/m}$$

$$(x-\alpha')(x-\alpha'')\cdots(x-\alpha^{(n)}) = [P(x)]^{n/m}$$

$$\Rightarrow (x-\alpha')(x-\alpha'')\cdots(x-\alpha^{(n)})$$
$$= [x^m + s_1 x^{m-1} + \cdots + S_m]^{n/m}$$

Comparing the constant terms of of both polynomials we have

$$\alpha'\alpha''\alpha'''\cdots\alpha^{(n)} = (S_m)^{n/m}. \quad \boxed{t = \tfrac{n}{m}}$$

$$N\alpha = (S_m)^{n/m}.$$

Norm of α is power of S_m where S_m is an integer. Hence $N\alpha$ is a rational integer.

x ——— x ——— x ———

Annual of Parel.

Theorem: If α and β are element of $R(\theta)$ Then

$\alpha = \frac{q_1(\theta)}{q_2(\theta)}$

$$N_{\alpha\beta} = N\alpha \cdot N\beta$$

Proof:-

Let
$P(x) = x^n + r_1 x^{n-1} + \cdots + r_n$ be the defining polynomial of θ.
and
Let

$\phi(m) = m - 1$

If m is prime.

If m is not prime

$m = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_r^{\alpha_r}$

2^{4}

$= 16(1 - 1/2)$

ASSIGNMENT Eq ③ $\Longrightarrow a_1(x_0 - x_1) = b_1(y_0 - y_1)$

From eqn ③

$$a_1(x_0 - x_1) = b_1(y_0 - y_1)$$

$$b_1 \mid a_1(x_0 - x_1)$$

since $(a_1, b_1) = 1$

Then

$$b_1 \mid x_0 - x_1$$

$\exists$ integer $t \in \mathbb{Z}$ s.t

$$x_0 - x_1 = b_1 t \Longrightarrow x_1 = x_0 - b_1 t.$$

$$x_1 = x_0 - b_1 t.$$

$$x_1 = x_0 - \frac{b}{d}t.$$

Putting $x_1 = x_0 - \frac{b}{d}t$ in eqn ③

$= x_0 - b_1 t$

$$a_1(x_0 - x_0 + b_1 t) = b_1(y_0 - y_1)$$

$$a_1 b_1 t = b_1(y_1 - y_0)$$

$$a_1 t = y_1 - y_0 \Longrightarrow y_1 = y_0 + a_1 t.$$

$$y_1 = y_0 + \frac{a}{d}t.$$

S.S. $\left\{ \left(x_0 - \frac{b}{d}t,\ y_0 + \frac{a}{d}t\right) \right\}$

Theorem:-

Let f be a bounded function and E be mable set of finit measure Then for simple function φ and ψ show that

$$\inf_{\psi \geq f} \int \psi \, dx = \sup_{\varphi \leq f} \int \varphi \, dx \quad \text{iff } f \text{ is mable.}$$

Proof:- Suppose that f is bounded by M and f is mable. Then set.

$$E_k = \left\{ \frac{Mk}{n} \geq f(x) \geq \frac{M(k-1)}{n} \right\} \quad -n < k < n.$$

are mable disjoint and have union E i.e

$$m \cup E_k = mE$$

$$\Rightarrow \sum_{k=-n}^{n} mE_k = mE.$$

The simple function is define as.

$$\psi_n(x) = \frac{M}{n} \sum_{k=-n}^{n} k \chi_{E_k}(x)$$

and

$$\varphi_n(x) = \frac{M}{n} \sum_{k=-n}^{n} (k-1) \chi_E(x).$$

Satisfy

$$\psi_n(x) \geq f(x) \geq \varphi_n(x).$$

or

$$\varphi_n(x) \leq f(x) \leq \psi_n(x)$$

Thus

$$\inf \int_E \psi_n(x) dx \leq \int_E \psi_n(x) dx = \frac{M}{N} \sum_{k=-n}^{n} k \, mE_k$$

&

$$\sup \int_E \varphi_n(x) dx \geq \int_E \varphi_n(x) dx = \frac{M}{N} \sum_{k=-n}^{n} (k-1) \, mE_k.$$

we have.

$$0 \leq \inf \int_E \psi_n(x)\,dx - \sup \int_E \varphi_n(x) \leq \frac{M}{N}\left(\sum_{k=n}^{n} mE_k\right)$$

Since n is arbitrary $= \frac{M}{N} mE.$

$$\inf \int_E \psi_n(x)\,dx - \sup \int_E \varphi_n(x)\,dx = 0$$

$$\Rightarrow \quad \inf \int_E \psi_n(x)\,dx = \sup \int_E \varphi_n(x)\,dx.$$

$$\psi \geq f \qquad \varphi \leq f.$$

Conversely suppose that.

$$\inf \int_E \psi_n(x)\,dx = \sup \int_E \varphi_n(x)\,dx.$$

Then given for given n there is a simple fn φ_n and ψ_n

$$\varphi_n(x) \leq f(x) \leq \psi_n(x).$$

$$\int \psi_n(x)\,dx - \int \varphi_n(x)\,dx < \frac{1}{n}$$

Then the function.

$$\psi^* = \inf \psi_n \text{ and } \varphi^* = \sup \varphi_n$$

are meble by theorem and.

$$\varphi^* \leq f(x) \leq \psi^*$$

now the set.

$$\Delta = \{x : \varphi^*(x) < \psi^*(x)\}$$

is the union of the sets

$$\Delta_V = \left\{x : \varphi^*(x) < \psi^*(x) - \frac{1}{V}\right\}$$

But each Δv is contained in the set

$$A_v = \left\{x;\ \varphi_n(x) < \psi_n(x) - \frac{1}{v}\right\}$$ and this

latter set has measure less than v/n. Since n is arbitrary; $m\Delta v = 0$ and $m\Delta = 0$. Thus φ^* and ψ^* except on a of measure zero. Thus f is mable.

NOTE: $\inf\limits_{\psi \geq f} \int_E \psi = \int_E \varphi$ and $\sup\limits_{\varphi \leq f} \int_E \varphi = \int_E f$.

Bounded cgt Theorem:

Let $\langle f_n \rangle$ be a sequence of mable functions define on a set E of finite measure bounded by M i.e $|f_n(x)| \leq M\ \forall n$

and if

$$f(x) = \lim_{n\to\infty} f_n \quad \text{for each } x \text{ in } E$$

Then

$$\int_E f(x) = \lim \int_E f_n.$$

Proof:- Suppose that $f(x) = \lim\limits_{n\to\infty} f_n$. Then for given $\varepsilon > 0$ there is natural no and a subset $A \subset E$ s.t for all $n \geq n_0$

$$mA < \frac{\varepsilon}{4M}$$

we have. $|f_n(x) - f(x)| < \frac{\varepsilon}{2mE}$ where $x \notin A$.

$$\left|\int_E f_n(x) - \int_E f\right| = \left|\int_E f_n - f\right| \le \int_E |f_n - f|$$

$$= \int_A |f_n - f| + \int_{E-A} |f_n - f| \quad \text{(1)}$$

NOW

$$\int_{E-A} |f_n - f| < \frac{\varepsilon}{2mE}\, m(E-A) \le \frac{\varepsilon}{2mE} \cdot mE = \varepsilon/2.$$

$$\int_{E-A} |f_n - f| < \frac{\varepsilon}{2} \quad \text{——— (i)}$$

Next

$$|f_n(x) - f(x)| \le |f_n(x)| + |f(x)|$$
$$\le 2M.$$

$$\int_A |f_n - f| \le 2M \cdot mA < 2M \cdot \frac{\varepsilon}{4M} = \varepsilon/2$$

$$\int_A |f_n - f| < \varepsilon/2 \quad \text{——— (ii)}$$

using (i) and (ii) in eqn (1)

$$\left|\int_E f_n - \int_E f\right| < \varepsilon/2 + \varepsilon/2 = \varepsilon$$

$$\boxed{\int_E f = \lim \int_E f_n.}$$

Case III If $c<0 \Rightarrow -c>0$ Then

$(-c)f^+$ and $(-c)f^-$ are non-negative function

$$cf = -(-cf^+) + (-cf^-).$$

$$\int_E cf = \int_E -(-cf^+) + (-cf^-)$$

$$= -c\int_E f^- + c\int_E f^+$$

$$= c\left[\int_E f^+ - \int_E f^-\right]$$

$$\int_E cf = c\int_E f.$$

(iii) $f \leq g$ (a.e)

$0 \leq f - g$ (a.e).

Since integral fun of non-negative fun is non-negative

$$0 \leq \int g - f = \int g - \int f.$$

$$\Rightarrow \int f \leq \int g.$$

(iv) $$\int_{A\cup B} f = \int_{A\cup B} f \chi_{A\cup B}$$

$$= \int_{A\cup B} f(\chi_A + \chi_B)$$

$$= \int_A f\chi_A + \int_B \chi_B \Rightarrow \int_A f + \int_B f.$$

MathCity.org
Merging Man and maths
MathCity.org
Merging Man and maths
MathCity.org
Merging Man and maths
MathCity.org
Merging Man and maths

102

Solution of the Congruences;

1) By substituting the integers of the c.r.s.

2) $ax \equiv b \pmod m$

has diophantine forme $ax - my = b$

3) A liner Congruence $ax \equiv b \pmod m$ where $(a,m) = 1$ can sometimes be solved easily by adding or substracting suitble multiple of m such that cofficient of x divides the other side.

for e.g.

$$3x \equiv 4 \pmod 5.$$
$$3x \equiv 9 \pmod 5.$$

$x \equiv 3^3 \cdot 4 (\ldots$

$x \equiv 3.$

$x \equiv 3 \pmod 5$ is the Solution of the given Congruence.

4) Some time it is possible to find the Solution of the Congruence

$$ax \equiv b \pmod m, \quad (a,m) = 1$$

with the Euler's Theorem.

By putting $x = b a^{\phi(m) - 1}$.

for e.g.

$$4x \equiv 7 \pmod 9.$$

$$\phi(9) = 6.$$

$$x \equiv 7 \cdot 4^5 \pmod 9$$

$$x \equiv 4 \pmod 9.$$

Imp annual 09

Show That Mobious function is multiplicative.

$\mu(m \cdot n) = \mu(m) \cdot \mu(n)$.

let $m = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot p_3^{\alpha_3} \cdots p_k^{\alpha_k}$.

& $n = q_1^{\beta_1} \cdot q_2^{\beta_2} \cdot q_3^{\beta_3} \cdots q_r^{\beta_r}$.

$mn = \underline{p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot p_3^{\alpha_3} \cdots p_k^{\alpha_k}} \cdot \underline{q_1^{\beta_1} \cdots q_r^{\beta_r}}$.

$\mu(mn) = \mu(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot p_3^{\alpha_3} \cdots p_k^{\alpha_k} \cdot q_1^{\beta_1} \cdots q_r^{\beta_r})$

$= \mu(m)\,\mu(n)$.

$\mu(m) = 0$ if any $\alpha_i > 0$

$\mu(n) = 0$ if any $\beta_i > 0$

$\mu(mn) =$

Show that

$d(mn) = d(m)\,d(n)$.

$\sigma(mn) = \sigma(m)\,\sigma(n)$

$8 = 2^3$

$12 = 2^2 \times 4$.

$96 = 2^5 \times 4 = 2^7$.

$\mu(96) =$

Theorem ~~of~~ Annual 09

Prove if p is an odd prime, the integer a is a quadratic residue of $p \Leftrightarrow a^{(p-1)/2} \equiv 1 \pmod{p}$.

Proof Suppose that a is quadratic residue of p. Then

$x^2 \equiv a \pmod{p}$ is solvable. Let $x \equiv r \pmod{p}$ is the solution of given congruence. Then by transitive property of congruencies

$$r^2 \equiv a \pmod{p}.$$

Since p is odd prime therefore

$$\phi(p) = p-1.$$

So

$$(r^2)^{\frac{\phi(p)}{2}} \equiv a^{\frac{\phi(p)}{2}} \pmod{p}.$$

$$r^{\phi(p)} \equiv a^{\frac{\phi(p)}{2}} \pmod{p}.$$

Since $(r, p) = 1$ therefore by Fermat's Theorem.

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

So

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

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

Conversely suppose that

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

and Consider

$$\cancel{x^2 \equiv a \pmod p} \quad x^2 \equiv a \pmod p$$

let $x \equiv a^{\frac{p-1}{2}}$ ($\cancel{\text{mod}}$)

$$\left(a^{\frac{p-1}{2}}\right)^2 \equiv a \pmod p.$$

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

Since

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

$$\Rightarrow a \equiv 1 \pmod p.$$

$$x^2 \equiv \left(a^{\frac{\phi(p)}{2}}\right)^2 \equiv 1 \pmod p$$

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

$$x \equiv 1 \pmod p$$

is the solutions of

$$x^2 \equiv a \pmod p.$$

Hence a is the square residue of p.

(2) (166)

Theorem If

$n = P_1^{\alpha_1} \cdot P_2^{\alpha_2} \cdots P_r^{\alpha_r}$, where P_i's are distinct prime Then show That:

i) $d(n) = \prod_{i=1}^{r} (\alpha_i + 1)$.

ii) $\sigma(n) = \prod_{i=1}^{r} \dfrac{P_i^{\alpha_i+1} - 1}{P_i - 1}$

Proof: Since P_i's is Prime, therefore the only Divisor of

$P_i^{\alpha_i}$ are $1, P_i, P_i^2, P_i^3, \ldots, P_i^{\alpha_i - 1}, P_i^{\alpha_i}$

$\Rightarrow d(P_i^{\alpha_i}) = \alpha_i + 1$

Then $d(P_1^{\alpha_1} \cdot P_2^{\alpha_2} \cdots P_r^{\alpha_r}) = d(P_1^{\alpha_1}) \cdot d(P_2^{\alpha_2}) \cdots d(P_r^{\alpha_r})$

$= (\alpha_1 + 1)(\alpha_2 + 2) \cdots (\alpha_r + r)$

$2^n + 1$ F.N

$2^n - 1$ M_n

$d(n) = \prod_{i=1}^{r} (\alpha_i + 1)$.

and

$\sigma(P_i^{\alpha_i}) = 1 + P_i + P_i^2 + \cdots + P_i^{\alpha_i}$

is Geometric series. $S_n = \dfrac{a(r^n - 1)}{r - 1}$

$\sigma(P_i^{\alpha_i}) = \dfrac{P_i^{\alpha_i+1} - 1}{P_i - 1}$

So

$\sigma(P_i^{\alpha_i}) = \prod_{i=1}^{r} \dfrac{P_i^{\alpha_i+1} - 1}{P_i - 1}$.

$\sigma(P_i^{\alpha_i})$
$= 1 + P_i + P_i^2 + \cdots + P_i^{\alpha_i}$

$d(P_i^{\alpha_i}) =$

$P_i^{\alpha_i} = 1, P_i^1, P_i^2, \ldots, P_i^{\alpha_i - 1}, P_i^{\alpha_i}$

$4n-1$

Perfect Number: A number $n \in Z$ is said to be perfect if its sum of +ve divisor can be expressed as

$$\sigma(n) = 2n.$$

NOTE:- All perfect numbers are even.

Theorem: An even integer is perfect $\Leftrightarrow$ it is of the form

$2^{p-1}(2^p - 1)$ where '$2p-1$' is prime.

$\rightarrow$ $d(n)$ is odd $\Leftrightarrow$ if n is in square.

$\rightarrow$ if $\sigma(n)$ is odd Then n is square are double of n.

$\rightarrow$ Every integer $n>1$ has prime divisor.

$\rightarrow$ Every composite number n has prime divisor $\leq \sqrt{n}$.

$\rightarrow$ if $x_1, x_2 \in R$ Then $[x_1 + x_2] \geq [x_1] + [x_2]$

$\rightarrow$ if n is positive integer and $x \in R$ Then number of multiple of $n \leq x$ is equal $\left[\frac{x}{n}\right]$.

Proof: The multiple of $n \leq x$ are the following integer,

$1 \cdot n, 2 \cdot n, 3 \cdot n, \ldots, n_1 n$ where $n_1 n$ is largest multiple of $n \leq x$.

$$\Rightarrow n_1 n \leq x < (n_1 + 1) n.$$

$$n_1 \leq \frac{x}{n} < n_1 + 1$$

$$0 \leq \frac{x}{n} - n_1 < 1.$$

$$\Rightarrow \left[\frac{x}{n} - n_1\right] = 0 \Rightarrow \left[\frac{x}{n}\right] - n_1 = 0$$

$\left[\frac{x}{n}\right]$

ii) ~~let~~ prov $[x_1+x_2] \geq [x_1]+[x_2]$

Since

$$x_1 = [x_1]+\theta_1 \ , \ x_2 = [x_2]+\theta_2$$

$$x_1+x_2 = [x_1]+[x_2]+\theta_1+\theta_2$$

$$[x_1+x_2] = [x_1]+[x_2], \text{ if } 0 \leq \theta_1+\theta_2 < 1.$$

$$= [x_1]+[x_2]+1 \text{ if } 0 \leq \theta_1+\theta_2 < 2.$$

Hence

$$[x_1+x_2] \geq [x_1]+[x_2].$$

Theorem. If n is an integer >0 Then highest power of a prime p which divides $n!$ is

$$\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\left[\frac{n}{p^3}\right]+\cdots$$

→ Number of integers which are $\leq n$ and divisible p is $\left[\frac{n}{p}\right]$ and these integers are

$$p, 2p, 3p, \cdots, \left[\frac{n}{p}\right]\cdot p.$$

→ Find the highest power of 7 dividing the integer 100!

~~$\left[\frac{100}{7}\right]+[\ ]$~~

$$\left[\frac{100}{7}\right]+\left[\frac{100}{7^2}\right]+\left[\frac{100}{7^3}\right]+\cdots$$

$$= 14+2+0+0$$

$$= 16$$

15

$$\left[\frac{15}{7}\right]+\left[\frac{15}{7^2}\right]$$

→ Lagrange's Theorem is not true if p is not prime.

Solve the congruence

$$4x^2+4x-1 \equiv 0 \pmod 7$$

The given congruence can be written as.

$$4x^2+4x \equiv 1 \pmod 7.$$

$$4x^2+4x+1 \equiv 2 \pmod 7 \quad \text{adding } 1.$$

$$(2x+1)^2 \equiv 3^2 \pmod 7$$

$\because 3^2 \equiv 2 \pmod 7$

$$2x+1 \equiv \pm 3 \pmod 7.$$

$$2x \equiv 2 \pmod 7$$

and

$$2x \equiv -4 \pmod 7$$

$$x \equiv 1, -2 \pmod 7.$$

$x \equiv 1, 5 \pmod 7$ are the sol of given congruence.

ii) $$x^3-4x^2+5x-6 \equiv 0 \pmod{27}.$$

First we solve.

$$x^3-4x^2+5x-6 \equiv 0 \pmod 3$$

Trying $x = 0, 1, 2$ we find $x \equiv 0 \pmod 3$ is the only solution.

let $x = 3t,\ t \in \mathbb{Z}$.

(110) (3)

Show That 33 is quardratic non-residue of 89.

Sol: we are to show That

$$\left(\frac{33}{89}\right) = -1.$$

Since $\left(\frac{33}{89}\right) = \left(\frac{3}{89}\right)\left(\frac{11}{89}\right)$.

First we check

$\left(\frac{11}{89}\right)$ Appling the reciprocically laws

$$\left(\frac{11}{89}\right)\left(\frac{89}{11}\right) = (-1)^{\frac{11-1}{2}\cdot\frac{89-1}{2}}$$

$$= (-1)^{5\cdot 44}$$

$$= 1$$

$\Rightarrow \left(\frac{11}{89}\right)\left(\frac{89}{11}\right)$ both have same quardratic character.

Since

$$\frac{89}{11} \equiv \frac{1}{11} \pmod{29}.$$

Since

$$x^2 \equiv 1 \pmod{11}.$$

has sol

$$x \equiv 1 \pmod{11}$$

So $\left(\frac{1}{11}\right) = 1$

These

$$\left(\frac{89}{11}\right) = 1$$

Now we check $\left(\frac{3}{89}\right)$

$$\left(\frac{3}{89}\right)\left(\frac{89}{3}\right) = (-1)^{1\cdot 44}$$ (111)

$$= 1.$$

Both have same quardratic character.

Since

$$\frac{89}{3} \equiv \frac{2}{3}(29).$$

Since 29 is odd prime

$$\left(\frac{2}{3}\right) = (-1)^{\frac{p-1}{8}}$$
$$= (-1)^{\frac{9-1}{8}}$$
$$= -1$$

$$\left(\frac{89}{3}\right) = -1$$

Hence

$$\left(\frac{33}{89}\right) = \left(\frac{3}{89}\right)\left(\frac{11}{89}\right)$$
$$= (-1)(1)$$
$$= -1$$

Hence $\frac{33}{98}$ is non-quardratic residue.

Show that

$$\frac{67}{89}$$

Available at
www.mathcity.org

Since $67 \equiv -22 \pmod{89}$.

$$\left(\frac{-22}{89}\right) = \left(\frac{-1}{89}\right)\left(\frac{2}{89}\right)\left(\frac{11}{89}\right)$$
$$= (-1)^{\frac{89-1}{2}} \cdot (-1)^{\frac{(89)^2-1}{8}} \cdot \left(\frac{11}{\ }\right)$$

$\left(\frac{11}{89}\right)\left(\frac{89}{11}\right) = (-1)^{\frac{11-1}{2}\cdot\frac{89-1}{2}}$

$= 1.$

$\therefore$ 11/89, 89/11 have same character

$\left(\frac{89}{11}\right) = \left(\frac{1}{11}\right) = 1$

$\therefore \left(\frac{11}{89}\right) = 1$

Hence $\left(\frac{67}{89}\right) = \left(\frac{-22}{89}\right) = 1$

Hence $\frac{67}{89}$ is quadratic Residue

1) $\frac{182}{271}$. ~~217~~

Since
$182 \equiv -89 \pmod{271}$

$\frac{-89}{271} = -\frac{1}{271} \cdot \frac{89}{271}$

$= \left(\frac{-1}{271}\right) \cdot \frac{89}{271}$

$= (-1)^{\frac{271-1}{2}} \cdot \frac{89}{271}$

$= (1)\left(\frac{89}{271}\right)$

$\frac{89}{27}$ Appling resiprocally law

$\left(\frac{89}{271}\right)\left(\frac{271}{89}\right) = (-1)^{44\cdot135} = 1$

Hence

$\left(\frac{89}{271}\right)$ & $\left(\frac{271}{89}\right)$ both have Character

$\therefore$ $\left(\frac{271}{89}\right) = \frac{4}{89}$.

$4 \equiv -85 \pmod{89}$.

$\frac{-85}{89} = \left(\frac{-1}{89}\right)\left(\frac{5}{89}\right)\left(\frac{17}{89}\right)$.

$= (-1)^{\frac{89-1}{2}} = 1$

Both

$\left(\frac{5}{89}\right)\left(\frac{89}{5}\right)$ have the quadratic character.

$\left(\frac{89}{271}\right) = (-1)^{135} \cdot (-1)^{5940}$

Hence 182 is quadratic non-residue of 271.

Annual 09

$\left(\frac{783}{997}\right)$

$783 \equiv -188 \pmod{997}$.

$$\begin{array}{r|l} 3 & 189 \\ 3 & 63 \\ 3 & 21 \\ 7 & 7 \end{array}$$

$\left(\frac{783}{997}\right) = \left(\frac{-188}{997}\right)$

$= \left(\frac{-1}{997}\right)\left(\frac{189}{197}\right)\left(\frac{7}{197}\right)($

$= 7.$

Prove That

i) $x = [x] + \theta \quad 0 \le \theta < 1.$

ii) $[x+n] = [x] + n \quad , x \in R, n \in Z.$

if $x, y \in R \quad y \ne 0$ and;

$x = qy + r$ where $0 \le r < y.$

Then $\left[\frac{x}{y}\right] = q$

iii) $\left[\frac{[x]}{n}\right] = \left[\frac{x}{n}\right]$

Proof:- i) $x = [x] + \theta \quad 0 \le \theta < 1$

true by Definition.

ii) Prove That $[x+n] = [x] + n.$

Since $x = [x] + \theta \quad 0 \le \theta < 1.$

$[x] = x - \theta.$

adding n we have

$[x] + n = \underline{x + n} - \theta.$

$[x] + n = \underline{[x+n]} + \theta_1 - \theta \quad 0 \le \theta_1 < 1.$

as

$[x]$, n, and $[x+n]$ are integer so

$\theta_1 - \theta$ must be integer but

$0 \le \theta_1 - \theta < 1.$

$\theta_1 - \theta = 0.$ ✓

Hence $[x] + n = [x+n]$ //

II if $x, y \in \mathbb{Z}$

$$x = qy + r \qquad 0 \le r < y$$

Then

$$\left[\frac{x}{y}\right] = q.$$

Since

$$x = qy + r.$$

Dividing on both sides by y.

$$\frac{x}{y} = q + \frac{r}{y}$$

taking Bracket function.

$$\left[\frac{x}{y}\right] = \left[q + \frac{r}{y}\right]$$

$$= q + \left[\frac{r}{y}\right] \quad \because q \in \mathbb{Z}.$$

Since $0 \le r < y$ Therefore

By definition

$$\left[\frac{r}{y}\right] = 0 \quad \because 0 \le \frac{r}{y} < 1$$

Hence

$$\left[\frac{x}{y}\right] = q.$$

Hence Prove //.

x ——— x ——— x ——— x ———

Prove That $\left[\frac{[x]}{n}\right] = \left[\frac{x}{n}\right]$. (116)

Since $[x] \in \mathbb{Z}$ so $\exists$ q and r such that

$$[x] = nq + r \quad \exists \quad 0 \le r < n. \quad (1)$$

$$\frac{[x]}{n} = q + \frac{r}{n}.$$

$\because$

$$x = [x] + \theta \Rightarrow [x] = x - \theta \quad 0 \le \theta < 1.$$

using in eq (1).

$$x - \theta = nq + r.$$

$$x = nq + r + \theta$$

$$\frac{x}{n} = q + \frac{r}{n} + \frac{\theta}{n}.$$

$$\left[\frac{x}{n}\right] = \left[\underline{q + \frac{r}{n}} + \theta/n\right]$$

$$= \left[\frac{[x]}{n} + \theta/n\right]$$

$$\left[\frac{x}{n}\right] = \left[\frac{[x]}{n}\right] \quad \because \quad 0 \le \theta/n < 1.$$

From Register

Theorem

117

$$\left[\frac{\left[\frac{x}{y}\right]}{z}\right] = \left[\frac{x}{yz}\right]$$

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

Since $x, y \in \mathbb{Z}$ There exist

$X^2 \equiv a \pmod{p}$

$x = qy + r.$

$X \equiv r \pmod{p}$

$\frac{x}{y} = q + r.$

$r^2 \equiv a \pmod{p}$

$(r^2)^{\phi(p)/2} \equiv (a)^{\phi(p)/2}$ (—

$\left[\frac{x}{y}\right] = \left[q + \frac{r}{y}\right].$

$r^{\phi(p)} \equiv a^{\phi(p)/2} \pmod{p}$

$1 \cdot n, 2 \cdot n \ldots n \cdot x$

$n x \le x < (n+1) n$

$= q + \left[\frac{r}{y}\right]$

$r^{\phi(p)} \equiv 1$ (—)

$a^{\phi(p)/2} \equiv 1 \pmod{p}$

$$\left[\frac{\left[\frac{x}{y}\right]}{z}\right] = \left[\frac{q}{z}\right] \neq 0$$

$a^{\phi(p)/2} \equiv 1 \pmod{p}$

$= \left[\frac{q}{z}\right] + \theta \quad 0 \le \theta < 1.$

$= \frac{q}{z} + \theta.$

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

NOW

$x^2 \equiv a$ (—)

$x = a^{\frac{p-1}{2}}$

$x = qy + r.$

$x^{\frac{p-1}{2}} \equiv a \pmod{p}$

$$\frac{x}{yz} = \frac{q}{z} + \frac{r}{yz}$$

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

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

$$\left[\frac{x}{yz}\right] = \frac{q}{z} + \ldots$$

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

$x^2 = a^{\phi(p)/2}$

[redacted] is (Proof) ?

[redacted] . i.e ?? Imp Annual 2010

pli

$$\phi(mn) = \phi(m)\phi(n).$$

$12 = 4 \times 3$
$= 2^2 \times 3^1 \times$

[redacted]

If $m > 1$.

$m = p_1^{\alpha_1} . p_2^{\alpha_2} . \dots p_r^{\alpha_r}$ be the standard form of m. Then

$$\phi(m) = \phi(p_1^{\alpha_1}) . \phi(p_2^{\alpha_2}) \dots \phi(p_r^{\alpha_r})$$

$$\phi(m) = [p_1^{\alpha_1} - p_1^{\alpha_1 - 1}] . [p_2^{\alpha_2} - p_2^{\alpha_2 - 1}] \dots [p_r^{\alpha_r} - p_r^{\alpha_r - 1}]$$

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

or

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

$$= p_i^{\alpha_i} . p_i^{-1} \prod_{i=1}^{r} (p_i - 1)$$

$$\phi(m) = \prod_{i=1}^{r} p_i^{\alpha_i - 1} (p_i - 1).$$

Proof

let p^α be the ~~stander~~ factrization of m. Then There exactly p^α integers not exceeding p^α & out of which $p^{\alpha-1}$ are ? not relatively prime to p^α. so remaing $p^\alpha - p^{\alpha-1}$ will be relatively prime to p^α. i.e.

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

$$= p^\alpha - \frac{p^\alpha}{p} = p^\alpha\left(1 - \frac{1}{p}\right).$$

Similarly

$$\phi(p_1^{\alpha_1}) = p_1^{\alpha_1}\left(1-\frac{1}{p_1}\right)$$

$$\phi(p_2^{\alpha_2}) = p_2^{\alpha_2}\left(1-\frac{1}{p_2}\right).$$

$$\vdots$$

$$\phi(p_r^{\alpha_r}) = p_r^{\alpha_r}\left(1-\frac{1}{p_r}\right)$$

Since

$$m = p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot p_3^{\alpha_3}\cdots p_r^{\alpha_r}$$

$$\phi(m) = \phi\left(p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot p_3^{\alpha_3}\cdots p_r^{\alpha_r}\right)$$

$$= \phi(p_1^{\alpha_1})\,\phi(p_2^{\alpha_2})\,\phi(p_3^{\alpha_3})\cdots\phi(p_r^{\alpha_r})$$

$$= p_1^{\alpha_1}\left(1-\frac{1}{p_1}\right)\cdot p_2^{\alpha_2}\left(1-\frac{1}{p_2}\right)\cdot p_3^{\alpha_3}\left(1-\frac{1}{p_3}\right)$$

$$\cdots\cdots\; p_r^{\alpha_r}\left(1-\frac{1}{p_r}\right).$$

$$= p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdots p_r^{\alpha_r}\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_r}\right)$$

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

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

$$= \cancel{\prod_{i=1}^{r} p_i^{\alpha_i-1}(p_i-1)}.$$

Since

$$\phi(m) = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_r^{\alpha_r} \left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\left(1-\frac{1}{p_3}\right)\cdots\left(1-\frac{1}{p_r}\right)$$

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

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

$$\phi(m) = \prod_{i=1}^{r} p_i^{\alpha_i-1}(p_i-1)$$

— x — x — x —

[redacted] $\phi(500) = ?$ $\phi(8)$.

$$500 = 2^2 \times 5^3$$

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

$$\phi(500) = 500\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right)$$

$$= 500\left(\frac{1}{2}\right)\left(\frac{4}{5}\right)$$

2	500
2	250
5	125
5	25
5	5
	1

$$\phi(500) = 200$$

i.e exactly 200 positive integers are relatively prime to 500.

— x — x —

$$\varphi(7562) = ?$$
$$\varphi(5000) = ?$$

2	7562
	3781

$$7562 = 2 \cdot 3781.$$

$$\varphi(7562) = \varphi(2) \cdot \varphi(3781)$$
$$= 1 \cdot 3780$$
$$= 3780 \quad \because \; 2 \,\&\, 3781 \text{ are prime numbers.}$$

Then $\varphi(n) = n-1$

$$5000 = 2^3 \cdot 5^4.$$

2	5000
2	2500
2	1250
5	625
5	125
5	25
5	5
	1

Hence.

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

$$= 5000\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right)$$

$$= 5000\left(\frac{1}{2}\right)\left(\frac{4}{5}\right).$$

$$= 500(4)$$

$$= 2000$$

— α — α —

NOTE:

[redacted] Prove That $\phi(m^2) = m\,\phi(m)$.

Proof:- let

$m = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ be the Standard form of 'm' Then

$m^2 = p_1^{2\alpha_1} \cdot p_2^{2\alpha_2} \cdots p_r^{2\alpha_r}$ is Standar form of m^2.

Also

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

Now

$$\phi(m^2) = m^2 \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right)$$

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

$$= m\,\phi(m).$$

Hence $\phi(m^2) = m\,\phi(m)$

$\phi(500^2)$
$= 500\,\phi(500)$
$= 500(200)$
$= 100000$.

Generally $\phi(m^n) = m^{n-1}\phi(m)$

under decision

[redacted] (Reduce Residue System (mod m))

R. R. S.

Let 'A' be a C.R.S (mod m) and 'B' be a subset of 'A' containing all those members of A which prime to 'm' Then B is R.R.S (mod m).

for e.g $m = 7$. Then C.R.S (mod 7) is

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

$B = \{1, 2, 3, 4, 5, 6\}$ is R.R.S (mod 7)

if $m = 8$.

$A = \{0, 1, 2, 3, 4, 5, 6, 7\}$ is C.R.S. Then

$B = \{1, 3, 5, 7\}$

$\varphi(8) = 4$, $(3,5) = 1$

$3 \not\equiv 5 \pmod 8$.

Def.

" A Set 'A' is R.R.S (mod m) if

i) 'A' has $\varphi(m)$ elements.

ii) If $a_i \in A$ Then $(a_i, m) = 1$

iii) If $a_i, a_j \in A$ & $i \neq j$ Then $a_i \not\equiv a_j \pmod m$

$\forall a \in \mathbb{Z}$ $a \equiv x_i$ for some $x_i \in A$.

Result: Corolly:- If $m > 2$ Then $\varphi(m)$ is always even. (2^{ii})

* — * — * — * — *

[redacted] If $\{a_1, a_2, a_3, \dots, a_{\varphi(m)}\}$ is a R.R.S (mod m) and if $(a, m) = 1$ Then $A = \{aa_1, aa_2, \dots, aa_{\varphi(m)}\}$ is also a R.R.S (mod m).

Proof As $A = \{aa_1, aa_2, \dots, aa_{\varphi(m)}\}$.

(i) clearly A has $\varphi(m)$ elements.

(ii) let $aa_i, aa_j \in A$ for $i \neq j$

$$aa_i \equiv aa_j \pmod m.$$

$$aa_i - aa_j \equiv 0 \pmod m$$

$$a(a_i - a_j) \equiv 0 \pmod m.$$

$$\Rightarrow a_i - a_j \equiv 0 \pmod m \quad \text{Since } (a, m) = 1$$

$$\Rightarrow a_i \equiv a_j \pmod m.$$

which is a contraduction as a_i and a_j are elements of R.R.S Hence our Suppostion is wrong and

$$aa_i \not\equiv aa_j \pmod m \quad \text{for } i \neq j$$

(iii) Since $(a, m) = 1$. also

$$(a_i, m) = 1 \quad \forall \; i = 1, 2, 3, \dots, \varphi(m)$$

$$\Rightarrow (aa_i, m) = 1$$

All the three condition satisfied.

Hence 'A' is R.R.S.

//

* — * — *

[redacted] write C.R.S of modulo 17. as multiple of 3.

b) write R.R.S (mod 17) as multip of 3.

Sol:-

for $m = 17$.

C.R.S of (mod 17) as follow.

$\{0, 1, 2, 3, ---, 16\}$

$\{0, 3, 6, 9, ---, 48\}$ is C.R.S (mod 17) as a multiple of 3.

(b) R.R.S of mod (17) is

$\{1, 2, 3, 4, 5, ---, 16\}$

$\{3, 6, 9, 12, 15, ---, 48\}$

is R.R.S as multiple of 3.

NOTE :- If m is prime then R.R.S is the maximal proper Subset of C.R.S.?

— q. — x —

$\Omega(m)$ $32=$

if $(m, n) = 1$ Then $(m-n, m) = 1$

$\frac{1}{2} m\varphi(m)$

$\varphi(8) = \{1,3,5,7\} = 4 = \frac{1}{2} 8 \cdot 4 = \frac{32}{2} = 16$

$1+3+5+7 = 16$

(126)

a^2

[redacted]n:- Show that the sum of integers of R.R.S of (mod m) is $\frac{1}{2} m\varphi(m)$.

Proof: we first ~~note~~ show that if $(m, n) = 1$ Then $(m-n, m) = 1$

for $(m-n, m) = d$

$\Rightarrow d | m-n, \; d | m.$

$\Rightarrow d | -n$ & $d | m$ $\quad\because d | a+(-b)$ & $d | b$ Then $d | a$.

$\Rightarrow d | n$ & $d | m$.

$\Rightarrow d = 1$ as $(m, n) = 1$.

Hence

$(m-n, m) = 1.$

let $\{a_1, a_2, a_3, \ldots, a_{\varphi(m)}\}$ be the integers less then m and prime to 'm'. Then for each $(a_i, m) = 1$ $\because$ The set R.R.S.

$\Rightarrow (m - a_i, m) = 1$

$m - a_i$ is also one of $a_1, a_2, a_3, \ldots, a_{\varphi(m)}$

Then a_i and $m - a_i$ occurs in the form of pairs among $a_1, a_2, a_3, \ldots, a_{\varphi(m)}$ Then

$$a_1 + a_2 + a_3 + \cdots + a_{\varphi(m)} = \frac{1}{2}\left(\cancel{a_1} + m - \cancel{a_1} + \cancel{a_2} + m - \cancel{a_2} + \cancel{a_3} + m - \cancel{a_3} + \cdots + \cancel{a_{\varphi(m)}} + m - \cancel{a_{\varphi(m)}}\right)$$

$= \frac{1}{2}(m + m + m + \cdots + m) \quad \{\varphi(m) \text{ times}\}$

Hence $= \frac{1}{2} m\varphi(m)$.

$\frac{1}{2}(m\varphi(m))$

(40, 20)

[redacted] Prove That If $m > 2$ Then $\varphi(m)$ is always even.

Proof: if m is even. Then

i) $m = 2^\alpha$.

$\Rightarrow \varphi(m) = 2^\alpha - 2^{\alpha-1}$

$= 2^\alpha\left(1 - \frac{1}{2}\right)$

$= 2^\alpha\left(\frac{1}{2}\right)$

$= 2^{\alpha-1}$

$\varphi(m) = 2 \cdot 2^{\alpha-2}$

(ii) if $m \neq 2^\alpha$. Then

$m = 2^\alpha \cdot p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_3^{\alpha_r}$

$\varphi(m) = \varphi(2^\alpha \cdot p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_3^{\alpha_r})$

$= \varphi(2^\alpha) \cdot \varphi(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_3^{\alpha_3})$

Since $\varphi(2^\alpha)$ is even

Therefore $\varphi(2^\alpha) \cdot \varphi(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_3^{\alpha_3})$ is even. Hence $\varphi(m)$ is even If m is even.

Since $2 \cdot 2^{\alpha-1}$ is the multiple of 2 so is even. Then $\varphi(m)$ is even.

if m is odd.

Then we discuss two cases.

i) If m is prime.

Then $\varphi(m) = m - 1$

Since m is odd. Therefore $m-1$ is even

Hence $\varphi(m)$ is even.

ii) If m is not prime.

There $m = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ where $i = 1, 2, 3, \cdots r$ & $p_i \neq 2$ Bes m is ~~even~~ odd.

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

Since each p_i is odd & prime Therefore Then $(p_i - 1)$ is even each $\left(1 - \frac{1}{p_i}\right)$ is even. ~~Hence~~; it is multiple of $(p_i - 1)$ which is even.

Hence $m\left(1 - \frac{1}{p_i}\right)$ is even $\forall\ i = 1, 2, 3, \cdots, n$

$\Rightarrow \varphi(m)$ is even //

2.2.2 / 5.2.3.2.2

is not even base ← 0.48
dose not 1

$2(0.24) = 0.48$

~~$a \mid b \quad \exists \ c \in \mathbb{Z}$~~

~~$b = ac$~~

[redacted]

If $d \mid n$ Then $\varphi(d) \mid \varphi(n)$.

Sol: Let $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot p_3^{\alpha_3} \cdots p_r^{\alpha_r}$ be the Standared form of n. Now $d \mid n$. Hence the prime factorization of d.
i.e
$$d = p_{i_1}^{\alpha_{i_1}} \cdot p_{i_2}^{\alpha_{i_2}} \cdots p_{i_k}^{\alpha_{i_k}}$$
The primes p_{i_j} : $j \in \{1, 2, 3, \ldots, k\}$ are among the primes $p_1, p_2, p_3, \ldots, p_r$ and $\alpha_{i_j} \le \alpha_i$.
Then
$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right)$$
Also
$$\varphi(d) = d\left(1 - \frac{1}{p_{i_1}}\right)\left(1 - \frac{1}{p_{i_2}}\right) \cdots \left(1 - \frac{1}{p_{i_k}}\right)$$
now all the factor $\left(1 - \frac{1}{p_{i_j}}\right)$ are involved in the product $\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right)$.
$$\Rightarrow \left(1 - \frac{1}{p_{i_1}}\right)\left(1 - \frac{1}{p_{i_2}}\right) \cdots \left(1 - \frac{1}{p_{i_k}}\right) \Big| \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right)$$
also $d \mid n$.
$$\Rightarrow d\left(1 - \frac{1}{p_{i_j}}\right) \Big| n\left(1 - \frac{1}{p_i}\right) \quad \text{where } j \in \{1, 2, \ldots, r\}$$
$$\Rightarrow \varphi(d) \mid \varphi(n)$$
which is required result.

[redacted]

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

Proof: let

$A = \{a_1, a_2, a_3, \ldots, a_{\phi(m)}\}$

be a R.R.S $\pmod m$

and if $(a, m) = 1$ Then

$B = \{aa_1, aa_2, aa_3, \ldots, aa_{\phi(m)}\}$

is also R.R.S $\pmod m$.

Its mean elements of A are congruent to elements of B but may not in the same order.

Then

$a_1 \cdot a_2 \cdot a_3 \cdots a_{\phi(m)} \equiv a a_1 \cdot aa_2 \cdots aa_{\phi(m)} \pmod m$

$a_1 a_2 \cdot a_3 \cdots a_{\phi(m)} \equiv a^{\phi(m)} \cdot a_1 a_2 \cdot a_3 \cdots a_{\phi(m)} \pmod m$ — (1)

Since each

$(a_i, m) = 1$ where $i = 1, 2, 3, \ldots, \phi(m)$

So

$(a_1 a_2 a_3 \cdots a_{\phi(m)}, m) = 1$ $\because$ $na \equiv nb \pmod m$, $(m, n) = 1$ Then $a \equiv b \pmod m$

So (1) becomes

$1 \equiv a^{\phi(m)} \pmod m$ $\because$ if $na \equiv nb \pmod m$ & $(n, m) = 1$ Then $a \equiv b \pmod m$

or

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

$(3, 4) = 1$

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

$3^2 \equiv 1 \pmod 4$

$9 \equiv 1 \pmod 4$

R.R.S (mod 6)

$\{1, 5\}$

& $(5, 6) = 1$

$\{5, 25\} \pmod 6$

Then

$5 \equiv 5 \pmod 6$

& $25 \equiv 1 \pmod 6$

Then $25(5) \equiv 5(1) \pmod 6$

$1 \equiv 8 \pmod 7$

i.e $7 \mid 1 - 8 = 7 \mid -7$

Then $8 \equiv 1 \pmod 7$

i.e $8 - 1 \mid 7 = 7 \mid 7$.

[redacted]

If $m_1, m_2, m_3, \ldots, m_k$ are positive integers greater than one relatively prime in pairs then system of simultaneous linear congruences

$$x \equiv c_1 \pmod{m_1}$$
$$x \equiv c_2 \pmod{m_2}$$
$$\vdots$$
$$x \equiv c_k \pmod{m_k}$$

$8 \equiv 1 \pmod 7$
$8 \equiv 3 \pmod 5$
$8 \equiv 5 \pmod 3$
Then
$8 \equiv 1 \pmod{105}$
$8 \equiv 3 \pmod{105}$
$8 \equiv 5 \pmod{105}$

has a unique solution $\pmod m$ where $m = m_1 \cdot m_2 \cdot m_3 \cdots m_k$.

Proof let $M_i = \dfrac{m_1 \cdot m_2 \cdot m_3 \cdots m_i \cdots m_k}{m_i}$

$M_1 = \dfrac{\cancel{3} \cdot 5 \cdot 7}{\cancel{3}}$
$M_1 = 35$
$M_2 = 21$
$M_3 = 15$

So m_i is not a factor of M_i. Since m_i's are prime in pair so

$$(M_i, m_i) = 1$$

Then the linear congruence

$$M_i y_i \equiv 1 \pmod{m_i}$$

$8x \equiv 1 \pmod 7$

where

$$M_i \not\equiv 0 \pmod{m_i} \quad \because m_i \text{ is not the factor of } M_i.$$

and $(M_i, m_i) = 1$ has exactly one solution for y_i's.

Now consider the integer

$$y = M_1 y_1 c_1 + M_2 y_2 c_2 + \cdots + M_k y_k c_k.$$

$a \equiv b \pmod{m_i}$
$\Rightarrow an \equiv bn \pmod{mn}$

$2 | 8$
$\Rightarrow 8 \equiv 0 \pmod{2}$

(131)

$$y = \sum_{j=1}^{k} M_j y_j c_j$$

$$Y \equiv M_i Y_i C_i \pmod{m_i} \quad \text{---(A)}$$

$(\because m_i | M_j \text{ for } i \neq j)$

and
Since

$$M_i Y_i \equiv 1 \pmod{m_i}$$

$\Rightarrow$

$$M_i y_i C_i \equiv C_i \pmod{m_i} \quad \text{---(B)}$$

From (A) & (B) By transitive

$$\Rightarrow y \equiv C_i \pmod{m_i}.$$

It means 'y' satisfies all the congruences

$$x \equiv C_i \pmod{m_i}$$

for 'm_i', $i = 1, 2, 3, \ldots k$ are relatively prime in pairs. So we have

$$Y \equiv C_i \pmod{m}.$$

where

$$m = m_1 \cdot m_2 \cdot m_3 \cdots m_k$$ //

For uniqueness let

$$Z \equiv C_i \pmod{m}.$$

Then

$$Z \equiv C_i \equiv Y \pmod{m}$$

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

$\Rightarrow Z \equiv Y \pmod{m_i}$.

Since m_i's are relatively prime in pairs

$\Rightarrow Z \equiv C_i \pmod{m}$

or

$Z \equiv Y \equiv C_i \pmod{m}$ is unique solution.

Chinese remainder ~~Sol~~ Theorem

Solve the system (Annual 09 Same)

$x \equiv 1 \pmod{4}$

$x \equiv 3 \pmod{5}$

$x \equiv 2 \pmod{7}$.

$M_i = \dfrac{m_1 m_2 m_3 \cdots m_n}{m_i}$

Soln $M_1 = \dfrac{m_1 \cdot m_2 \cdot m_3}{m_1}$

$M_1 = m_2 \cdot m_3 = 5 \times 7 = 35$

$M_2 = m_1 \cdot m_3 = 4 \times 7 = 28$

$M_3 = m_1 \cdot m_2 = 4 \times 5 = 20$

$M_1 y_1 \equiv 1 \pmod{m_1}$, $M_2 y_2 \equiv 1 \pmod{m_2}$

& $M_3 y_3 \equiv 1 \pmod{m_3}$. So we have

$35 y_1 \equiv 1 \pmod{4}$.

$a \equiv b \pmod{m}$

$m \mid a-b$

$mq = a-b$

$a - mq = b$

$\Rightarrow 35 y_1 - 4u_1 = 1$

$\Rightarrow (4 \cdot 8 + 3) y_1 - 4u_1 = 1$

$4 \mid 35y_1 - 1$

$35y_1 - 1 = 4u_1$

$35y_1 - 4u_1 = 1$

$4(8y_1 - u_1) + 3y_1 = 1$

$4u_2 + 3y_1 = 1$

$$4u_2 + 3y_1 = 1 \quad \text{where } u_2 = 8y_1 - u_1$$

$$\Rightarrow \quad u_2 = 1 \text{ and } y_1 = -1$$

as $\because$

$$-1 \equiv 3 \pmod 4 \qquad \therefore y_1 = 3$$

$$\Rightarrow \boxed{y_1 \equiv 3 \pmod 4}$$

Similarly

$$28y_2 \equiv 1 \pmod 5.$$

$$28y_2 - 5v_1 = 1$$

$$(5.5 + 3)y_2 - 5v_1 = 1$$

$$5(5.y_2 - v_1) + 3y_2 = 1$$

$$5v_2 + 3y_2 = 1 \quad \text{where } v_2 = 5y_2 - v_1$$

$$\Rightarrow v_2 = -1, \therefore y_2 = 2$$

$$\because \boxed{y_2 \equiv 2 \pmod 5} \qquad \therefore y_2 = 2$$

if we select $5(2) + 3(-3) = 1$, $v_2 = 2$, $y_2 = -3$

$2 \equiv -3 \pmod 5$, $-3 \equiv 2 \pmod 5$

$\Rightarrow y_2 \equiv 2 \pmod 5$

also

$$20y_3 \equiv 1 \pmod 7$$

$$20y_3 - 7s_1 = 1 \quad \text{for } s_1 \in \mathbb{Z}.$$

$$(7.2 + 6)y_3 - 7s_1 = 1$$

$7(2y_3 - s_1) + 6y_3 = 1$

$\Rightarrow 7s_2 + 6y_3 = 1$ where

$s_2 = 2y_3 - s_1$

$s_2 = 1, \; y_3 = -1$

$-1 \equiv 6 \pmod 7$ $\quad y_3 = 6$

so $\boxed{y_3 \equiv 6 \pmod 7}$

Now $y = M_1 y_1 c_1 + M_2 y_2 c_2 + M_3 y_3 c_3$

$y = (35)(3)(1) + 28(2)(3) + 20(6)(2)$

$y = 513$

$4 \times 5 \times 7$

$y \equiv 93 \pmod{140}$

is a solution of the system.

35
28
20
93

$140 \mid 513 - 93$

$m \mid a - b$

$a - m(q) = b$

Solve The System.

$$x \equiv 2 \pmod{5}$$
$$x \equiv 3 \pmod{7}$$
$$x \equiv 5 \pmod{11}$$

Solution:

$$M_1 = \frac{m_1 m_2 m_3}{m_1}$$

$$M_1 = m_2 m_3 = (7)(11) = 77.$$
$$M_2 = m_1 m_3 = (5)(11) = 55$$
$$M_3 = m_1 m_2 = (5)(7) = 35$$

$$M_1 y_1 \equiv 1 \pmod{m_1}$$

$$77 y_1 \equiv 1 \pmod{5}$$

$$\Rightarrow 77 y_1 - 5u_1 = 1$$
$$(5(15 y_1) + 2y_1) - 5u_1 = 1$$

$$\Rightarrow 5(15y_1 - u_1) + 2y_1 = 1$$

$$5u_2 + 2y_1 = 1 \quad \text{where } 15y_1 - u_1 = u_2$$

$$(2+3)u_2 + 2y_1 = 1$$

$$2(u_2 + y_1) + 3u_2 = 1 \quad \text{where}$$

$$u_2 + y_1 = u_3$$

$$2u_3 + 3u_2 = 1 \qquad -2 + y_1 = 3$$

$$u_3 = 3,\ u_2 = -2 \qquad y_1 = 5$$

$$\boxed{y_1 \equiv 5 \pmod 5}$$

$$M_2 y_2 \equiv 1 \pmod{m_2}$$

$$55 y_2 \equiv 1 \pmod 7$$

$$55 y_2 - 7u_1 = 1$$
$$(7(8)y_2 - y_2) - 7u_1 = 1$$

$$7(8y_2 - u_1) - y_2 = 1 \quad \text{where}$$
$$7u_2 - y_2 = 1 \quad u_2 = 8y_2 - u_1$$

$u_2 = 1 \quad y_2 = 6$

$6 \equiv$

$$y_2 = 7.$$
$$\Rightarrow \boxed{y_2 = 7 \pmod 7}$$

$48 = 3 + 2(5) + 5(7)$

$48 \equiv 3 \pmod 5$

$48 \equiv$

$$M_3 y_3 \equiv 1 \pmod{m_3}$$

$$35 y_3 \equiv 1 \pmod{11}.$$

$$35 y_3 - 11u_1 = 1$$
$$(11(3y_3) + 2y_3) - 11u_1 = 1$$

$$11(3y_3 - u_1) + 2y_3 = 1$$

$$11u_2 + 2y_3 = 1$$
$$u_2 = -2,\ y_3 = 11$$

$u_2 = 1 \quad y_3 = -5$

$-5 \equiv - \pmod{11}.$

$6.$

$$\boxed{y_3 \equiv 11 \pmod{11}}$$

$\rightarrow y_3 \equiv 6 \pmod{11}$

Now

$$y = M_1 y_1 C_1 + M_2 y_2 C_2 + M_3 y_3 C_3.$$

$$y = 77(5)(2) + 55(7)(3) + 77(11)(5)$$

$$y = 770 + 1155 + 385$$

$$y = 2310$$

$$y \equiv 14 \pmod{82}$$

——— x ——— x ———

Theorem Every Composite number n has a prime divisor $\leq \sqrt{n}$.

Proof

Since n is Composite. It will have a least prime divisor p.

Let $n = n_1 p$.

If $p > \sqrt{n}$ Then

$n = n_1 p$ shows That

$n_1 < \sqrt{n} < p$.

i.e There exist a divisor n_1 of n less than the least, which is Contradiction

Hence

$p \leq \sqrt{n}$.

— x — x —

Def:-

A polynomial Congruence

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

if

$$f(a) \equiv 0 \pmod{m}.$$

[redacted]: (Factor Theorem)

A polynomial Congruence

$f(x) \equiv 0 \pmod{m}$ has

solution

$x \equiv a \pmod{m}$ iff there is a polynomial Congruence $q(x)$ with integral cofficent s.t

$$f(x) \equiv q(x)(x-a) \pmod{m}$$

Proof:

Let $x \equiv a \pmod{m}$ is solution of $f(x) \equiv 0 \pmod{m}$. Now dividing by '$x-a$' we obtained a polynomial $q(x)$ with integral cofficient and remainder 'r' s.t

$$f(x) \equiv (x-a)\,q(x) + r \quad \text{--- (i)}$$

Now

$x \equiv a \pmod{m}$ is solution of

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

$$\Rightarrow f(a) \equiv 0 \pmod{m}.$$

eq ①

$\Rightarrow f(a) \equiv (a-a)\,q(a) + r \pmod{m}$

$\Rightarrow 0 \equiv 0 + r \pmod{m}$.

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

So using in eq ①

$f(x) \equiv q(x)\,(x-a) \pmod{m}$.

Conversely

$f(x) \equiv q(x)\,(x-a) \pmod{m}$.

Then

let $x \equiv a \pmod{m}$.

$\Rightarrow f(a) \equiv q(a)(a-a) \pmod{m}$

$\Rightarrow f(a) \equiv 0 \pmod{m}$

$\Rightarrow x \equiv a \pmod{m}$ is the solution of $f(x) \equiv 0 \pmod{m}$ BY Definition

$=\!=\!\times\!=\!=\; \times \;=\!=\; \times \;=\!=\; \times \;=\!=$

[redacted] of

$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$

& $g(x) = b_n x^n + b_{n-1} x^{n-1} + \cdots + b_0$

are polynomial of degree 'n' in x

and

$f(x) \equiv g(x) \pmod{m}$

Then

$a_i \equiv b_i \pmod{m}$

for $i = 1, 2, 3, \ldots, n$.

[redacted]

Let p a prime. Than a congurance $f(x) \equiv 0 \pmod{p}$ of degree 'n' has atmost 'n' solution.

Proof

we prove The Theorem by induction on. Theorem is True for $n=1$ as the Congurence

$$ax \equiv b \pmod{p}$$

of degree one has exactly one solution.

Suppose The Theorem is true for congurence of degree $n-1$ i.e a congurence of degree '$n-1$' has at most '$n-1$' solution

Now if

$$x \equiv a \pmod{p} \text{ is}$$

solution of the congurence of degree n. Then by facter Theorem

$$f(x) \equiv (x-a)\,q(x) \pmod{p} \quad \text{--- (1)}$$

where $q(x)$ is of degree '$n-1$'.
Therefore The congruence $q(x) \equiv 0 \pmod{p}$ has atmost '$n-1$' solutions. (By hypothesis)
let $c_1, c_2, \ldots, c_{n-1}$ be the solutions of $q(x)$.
i.e $q(x) \equiv 0 \pmod{p}$.

Now if

$$x \equiv c \pmod{p} \text{ is an}$$

any solution of the congurence

$$f(x) \equiv 0 \pmod{p}. \implies f(c) \equiv 0 \pmod{p}$$

?

using in ①

$$(c-a)\,q(c) \equiv 0 \pmod{p}$$

either

$$c-a \equiv 0 \pmod{p}$$

or

$$q(c) \equiv 0 \pmod{p}.$$

if

$$c-a \equiv 0 \pmod{p}$$

$$c \equiv a \pmod{p}$$

Now

if

$$q(c) \equiv 0 \pmod{p}$$

$\Rightarrow x \equiv c \pmod{p}$ is solution of

$$q(x) \equiv 0 \pmod{p}.$$

$$\Rightarrow \cancel{c \in} \; \cancel{\equiv} \; c \equiv c_i \pmod{p}$$

for some

$i = 1, 2, 3, \ldots, n-1$

$$\Rightarrow c \in \{a, c_1, c_2, c_3, \ldots, c_{n-1}\}$$

$\Rightarrow f(x) \equiv 0 \mod (p)$ has at most 'n' solutions.

$\therefore \quad \times \quad \therefore$

Fermat's Theorem : If p is odd prime and $(a,p)=1$ Then $a^{p-1}\equiv 1 \pmod p$ or $a^{p-1}-1\equiv 0 \pmod p$.

[redacted]

Let p be an odd prime Then The Congruence ~~$f(x)\equiv 0 \pmod$~~

$x^{p-1}-1\equiv 0 \pmod p$ has exactly '$p-1$' solution.

Proof:

By Fermats Theorem

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

So The Congruence

$x^{p-1}-1\equiv 0 \pmod p$ is satisfied by all the integer $1,2,3,\dots,p-1$.

Hence all The '$p-1$' integers are the solution of

$$x^{p-1}-1\equiv 0 \pmod p.$$

But by Lagrange's Theorem a Congruence of degree '$p-1$' has at most $p-1$ solution.

$$f(x)\equiv (x-1)\,(x^{n-1}\cdots)(\ -\ -\ -\ )$$

-x- -x- -x-

[redacted] $x^2+x+1 \equiv 0 \pmod 7$

C.R.S of $7 = \{0,1,2,3,4,5,6\}$ or $\{0,\pm1,\pm2,\pm3\}$

Hence only solution are

$x \equiv 2 \pmod 7$

& $x \equiv 4 \pmod 7$

By Putting 2 & 4 in x^2+x+1 which satisfied.

Q11 $x^2+4x+2 \equiv 0 \pmod{23}$

$x^2+4x+2+2 \equiv 2 \pmod{23}$

$(x+2)^2 \equiv 2 \pmod{23}$.

$\Rightarrow (x+2)^2 \equiv 25 \pmod{23}$ $\because 2 \equiv 25 \pmod{23}$

$\Rightarrow (x+2)^2 \equiv 5^2 \pmod{23}$

$\Rightarrow x+2 \equiv \pm 5 \pmod{23}$

$x+2 \equiv 5 \pmod{23}$ & $x+2 \equiv -5 \pmod{23}$

$x \equiv 3 \pmod{23}$ & $x \equiv -7 \pmod{23}$

$\Rightarrow x \equiv 16 \pmod{23}$

Hence The solution set is

$\{3, 16\}$

22/ Same Annual 09

(145)

[redacted] Find all the solution of Congruence

$$x^3 - 4x^2 + 15x - 6 \equiv 0 \pmod{30}$$

As

$30 = 2 \cdot 3 \cdot 5$ Therefore the given congruence is equivalent to the system of congruences

$$x^3 - 4x^2 + 15x - 6 \equiv 0 \pmod 2 \quad \text{— (i)}$$

$$x^3 - 4x^2 + 15x - 6 \equiv 0 \pmod 3$$

$$x^3 - 4x^2 + 15x - 6 \equiv 0 \pmod 5$$

(i) $\Longrightarrow$

[2 divides $-4x^2$ & -6 so can not written and $15x = 14x + x$. So 2 divides 14 Hence we write only $x^3 + x$]

$$x^3 + x \equiv 0 \pmod 2.$$

$$x \equiv 0 \pmod 2$$

$$x \equiv 1 \pmod 2$$

[$-4x^2 = +2x^2$, $-6x$ (ii) So 3 divides -6 and only write $2x^2$] ~~$-4 \equiv 2 \pmod 3$~~

(-1)

$$x^3 + 2x^2 \equiv 0 \pmod 3$$

$$x \equiv 0 \pmod 3$$

$$x \equiv 1 \pmod 3$$

Now

eq (3) $\Rightarrow$ $x^3 + x^2 + 4 \equiv 0 \pmod 5$

$x \equiv 3 \pmod 5$

The possible combinations are

a) $x \equiv 0 \pmod 2$

$x \equiv 0 \pmod 3$

$x \equiv 3 \pmod 5$

b) $x \equiv 0 \pmod 2$

$x \equiv 1 \pmod 3$

$x \equiv 3 \pmod 5$.

c) $x \equiv 1 \pmod 2$.

$x \equiv 0 \pmod 3$

$x \equiv 3 \pmod 5$

d) $x \equiv 1 \pmod 2$

$x \equiv 1 \pmod 3$.

$x \equiv 3 \pmod 5$

a) $x \equiv 0 \pmod 2$

$x \equiv 0 \pmod 3$

$x \equiv 3 \pmod 5$

By Chainees Remainder Theorem

$M_1 = \frac{2\cdot 3\cdot 5}{2} = 15$

$M_2 = \frac{2\cdot 3\cdot 5}{3} = 10$

$M_3 = \frac{2\cdot 3\cdot 5}{5} = 6.$

now

$0, 1, 2, 3, 4$

$15y_1 \equiv 1 \pmod 2$

$10y_2 \equiv 1 \pmod 3$

$6y_3 \equiv 1 \pmod 5.$

Since

$15y_1 \equiv 0 \pmod 2.$

$15y_1 - 2u_1 = 0$

$(7\cdot 2y_1 + y_1) - 2u_1 = 0$

$2v_1 + y_1 = 0$ where $7y_1 - u_1 = v_1$

If $y_1 = -2, v_1 = 1$

$-2 \equiv 0 \pmod 2$

$y_1 \equiv 0 \pmod 2.$

0, 1, 2

$$10y_2 \equiv 0 \pmod 3$$

$$y_2 \equiv 3 \pmod 3$$

Since

$$0 \equiv 3 \pmod 3$$

$\therefore$

$$y_2 \equiv 0 \pmod 3$$

Since

$$6y_3 - 3u_1 = 5$$

$$2 \cdot 3y_3 - 3u_1 = 5$$

$$3(2y_3 - u_1) = 5$$

$ax + by = c$

$(a, b) \mid c$

$(6, 3) = 2 \nmid 5$

$$y_1 = 1, \quad y_2 = 1, \quad y_3 = 1 \implies ?$$

$$y = M_1 y_1 C_1 + M_2 y_2 C_2 + M_3 y_3 C_3$$

$$= (15)(1)(0) + 10(1)(3) + 6(3)(5)$$

$$= \cancel{30 + 30} \; 90$$

$$3\overline{)90}$$
90
α

$$y = 90$$

$$y \equiv 0 \pmod{30}$$

b) $x \equiv 0 \pmod{2}$

$x \equiv 1 \pmod{3}$

$x \equiv 3 \pmod{5}$

$M_1 = \dfrac{2\cdot 3\cdot 5}{2} = 15$

$M_2 = 10$

$M_3 = 6$

$M_1 y \equiv 1 \pmod{c_1}$

$15 y_1 \equiv 1 \pmod{2}$

$y_1 = 1$.

$10 y_2 \equiv 1 \pmod{3}$

$y_2 = 1$

$6 y_3 \equiv 3 \pmod{3}$

$y_3 = 1$

$y = (15)(1)(0) + (10)(1)(1) + 6(1)(3)$

$= 0 + 10 + 18$

$y = 28$

$\boxed{y \equiv -2 \mod (30)}$ $-2 \equiv 28$

$y \equiv 28 \pmod{30}$

c) $x \equiv 1 \pmod 2$

$x \equiv 0 \pmod 3$

$x \equiv 3 \pmod 5$

$M_1 = 15, \; M_2 = 10, \; M_3 = 6$

$y_1 = 1, \; y_2 = 1, \; y_3 = 1$

$x = 15(1)(1) + 10(1)(0) + 6(1)(3)$

$= 15 + 0 + 18$

$x = 33$

$\boxed{x \equiv 3 \pmod{30}}$

d) $x \equiv 1 \pmod 2$

$x \equiv 1 \pmod 3$

$x \equiv 3 \pmod 5$

$M_1 = 15, \; M_2 = 10, \; M_3 = 6$

$y_1 = 1, \; y_2 = 1, \; y_3 = 1$

$c_1 = 1, \; c_2 = 0, \; c_3 = 3$

$x = 15 + 10 + 18$

$x = 43$

$\boxed{x \equiv 13 \pmod{30}}$

Solve $x^3-4x^2+5x-6 \equiv 0 \pmod{27}$. (151)

we first $x^3-4x^2+5x-6 \equiv 0 \pmod 3$.

trying 0, 1, 2 we find $x \equiv 0 \pmod 3$ is the only solution.

Let $x=3t$ is also solution of the congruence $x^3-4x^2+5x-6 \equiv 0 \pmod{3^2}$.

put $x=3t$.

$(3t)^3-4(3t)^2+5(3t)-6 \equiv \bmod (3^2)$.

$9t^3-12t^2+15t-6 \equiv \bmod (3^2)$.

$-12+9$

$-\frac{4}{3}$

0

$15t-6 \equiv 0 \pmod{3^2}$.

or

$5t \equiv 2 \pmod 3$.

This congruence has unique solution

$t \equiv 1 \pmod 3$

let $t=1+3s$, $s \in Z$ so that

$x=3+9s$ is also of the congruence

$x^3-4x^2+5x-6 \equiv 0 \pmod{3^3}$.

Substituting $x \equiv 3+9s$

$72s \equiv 0 \pmod{27}$.

$s \equiv 0 \pmod 3$

$s=3r$, $r \in Z$. That

$x=3+27s$. Hence the given solution of the congruence is

$x \equiv 3 \pmod{27}$.

let: $x=3t$.

$5t \equiv 2$

$t \equiv 1$

$t=1+3s$

$x=9s+3$

$72s$

C.R.S of 5 = {0, 1, 2, 3, 4}

$x \equiv 3 \pmod 5$ ✓

$x \equiv 4 \pmod 5$

~~C.R.S of~~ 7 = {0, 1, 2, 3, 4, 5, 6}

$x \equiv 6 \pmod 7$.

$x \equiv 5 \pmod 7$.

The possibles Combinations are.

a) $x \equiv 3 \pmod 5$.
$x \equiv 5 \pmod 7$

b) $x \equiv 4 \pmod 5$
$x \equiv 6 \pmod 7$

c) $x \equiv 3 \pmod 5$
$x \equiv 6 \pmod 7$

d) $x \equiv 4 \pmod 5$
$x \equiv 5 \pmod 7$

a) $x \equiv 3 \pmod 5$

$x \equiv 5 \pmod 7$

$M_1 = \cancel{7}$, $M_2 = 5$.

$\cancel{7}y_1 \equiv 1 \pmod 5$

$y_1 \equiv 3 \pmod 5$

$5y_2 \equiv 1 \pmod 7$

$y_2 \equiv 3 \pmod 7$.

$y = M_1 y_1 C_1 + M_2 y_2 C_2$

$= (7)(3)(3) + (5)(3)(5)$

$= 63 + 75$

$y = 138$

$138 = 33$
$105 = 35$
3

$y \equiv 33 \pmod{35}$. ✓

b) $x \equiv 4 \pmod 5$

$x \equiv 6 \pmod 7$

$y_1 = 3$, $y_2 = 3$, $M_1 = 7$, $M_2 = 5$

$$y = 84 + 90$$

$$y = 174$$

$$y \equiv 34 \pmod{35}$$

e) $x \equiv 3 \pmod{5}$

$x \equiv 6 \pmod{7}$

$y_1 = 3$, $y_2 = 3$

$M_1 = 7$, $M_2 = 5$

$e_1 = 3$, $e_2 = 6$

$$y = 63 + 90$$

$$y = 153$$

$$y \equiv 13 \pmod{35}.$$

d) $x \equiv 4 \pmod{5}$

$x \equiv 5 \pmod{7}$

$y_1 = 3$ $y_2 = 3$

$M_1 = 7$ $M_2 = 5$

$c_1 = 4$ $c_2 = 5$

$$y = 84 + 75 = 159$$

$$y \equiv 19 \pmod{35}$$

* [redacted]

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

iff p is an odd prime.

Proof: we know that the congruence

$$x^{p-1} - 1 \equiv 0 \pmod p$$ has $p-1$ solution which are given by

$$x \equiv 1, 2, 3, \ldots, p-1 \pmod p.$$

If p is an odd prime then by factor theorem.

$$x^{p-1} - 1 \equiv (x-1)(x-2)(x-3) \cdots (x-(p-1)) \pmod p$$

As both polynomials of degree '$p-1$' are congruence implies the constant term on both sides will be congruent $(\bmod p)$.

i.e

$$-1 \equiv (-1)(-2)(-3) \cdots (-(p-1)) \pmod p$$

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

$$-1 \equiv (1)(2)(3) \cdots (p-1) \pmod p$$ since $(-1)^{p-1} = 1$ as p is odd prime.

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

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

Conversely suppose that
$(P-1)! \equiv -1 \pmod{P}$ & P is composite
~~Sup~~ Then $\exists$ an integer m_1, m_2 i.e

$1 < m_1, m_2 < P$

St
$P = m_1 m_2.$

Then
$(P-1)! \equiv -1 \pmod{m_1 m_2}$ $\because P = m_1 m_2$

$\Rightarrow (P-1)! \equiv -1 \pmod{m_1}$

Now
$m_1 < P$
$\Rightarrow m_1 < P-1$ $\because$

$10 = 2 \cdot 5$
$2 < 10$ & $2 \mid 10$
$2 < 10 - 1 = 9$
$2 \mid 9! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9$

$\Rightarrow m_1 \mid (P-1)!$

$\Rightarrow (P-1)! \equiv 0 \pmod{m_1}$

$\Rightarrow -1 \equiv 0 \pmod{m_1}$ $\because (P-1)! \equiv -1 \pmod{m_1}$

which is a contradiction Hence P must be prime.

$4! = 1 \cdot 2 \cdot 3 \cdot 4, = 2 \mid 4!$

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

~~$P.0$~~! $(P-1)! \equiv -1 \pmod{P}$
$-1 \equiv (P-1)! \pmod{P}$
$(P-1)! \equiv 0 \pmod{P}$

$-1 \equiv 0 \pmod{P}$

Imp

* [redacted]

Order of an integer (mod m)

If $(a, m) = 1$ and $a^n \equiv 1 \pmod{m}$ where 'n' is the least positive integer for which the congruence is true. Then we say 'a' belongs to 'n' (mod m) or 'a' has order 'n' for modulus 'm' & we write order of $ord_m(a) = n$.

NOTE :- By Euler's Theorem we know That for $(a, m) = 1$ Then

Imp

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

It means order of 'a' (mod m) always exist, and less Then or equal to $\phi(m)$.

[redacted]

If $(a, m) = 1$ & $ord_m(a) = n$ Then $a^r \equiv 1 \pmod{m}$ iff $n \mid r$.

Proof

Since $ord_m(a) = n$

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

$\Rightarrow$ n is least positive integer for which the congruence is true.

Suppose that
$$a^r \equiv 1 \pmod m$$
and also suppose that
$$r = nq_1 + r_1 \quad \text{—(1)} \quad \text{where } 0 \leq r_1 < n.$$
now
$$a^r \equiv 1 \pmod m$$
$$\Rightarrow a^{nq_1 + r_1} \equiv 1 \pmod m \quad \because r = nq_1 + r_1$$
$$\Rightarrow a^{nq_1} \cdot a^{r_1} \equiv 1 \pmod m$$
$$\Rightarrow (a^n)^{q_1} \cdot a^{r_1} \equiv 1 \pmod m$$
$$\Rightarrow a^{r_1} \equiv 1 \pmod m. \quad \because a^n \equiv 1 \pmod m$$
as $r_1 < n$ which is not possible as n is least positive integer
$\Rightarrow$ r_1 must be equal to zero

so
eq (1) becomes
$$r = nq_1 + 0 \quad \because r_1 = 0$$
$$\Rightarrow r = nq_1$$
$$\Rightarrow n \mid r \quad \text{which is required.}$$
now Conversely
Suppose that
$n \mid r$ and we have prove that

$$a^{r} \equiv 1 \pmod{m}$$

Since

$$a^{n} \equiv 1 \pmod{m}$$

as $ord_m(a) = n$.

Now

as $n \mid r \Rightarrow r = nq$ for $q \in \mathbb{Z}$.

Now

$$a^{n} \equiv 1 \pmod{m}$$

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

$$\Rightarrow a^{nq} \equiv 1 \pmod{m}$$

$2^2 \equiv 1 \pmod{3}$
$\Rightarrow 2^3 \equiv 1 \pmod{3}$
$\Rightarrow 2^4 \equiv 1 \pmod{3}$

$$\Rightarrow a^{r} \equiv 1 \pmod{m} \quad \because r = nq.$$

which is required result.

[redacted] of $ord_m(a) = n$ Then

$n \mid \phi(m)$.

Proof Since $ord_m(a) = n$

$$\Rightarrow a^{n} \equiv 1 \pmod{m}.$$

That is 'n' is least positive integer for which the congruence is true.

Statement write φ(m) theorem.

Also by Euler's Theorem

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

But

$a^n \equiv 1 \pmod{m}$

i.e n is the order of a and hence

$n \mid \phi(m)$.

[redacted] If $(a, m) = 1$ & $\operatorname{ord}_m(a) = n$

Then for positive integers i & j

$a^i \equiv a^j \pmod{m}$

iff $i \equiv j \pmod{n}$.

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

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

$\Leftrightarrow 5 \equiv 3 \pmod{2}$

Proof

Suppose

$a^i \equiv a^j \pmod{m}$

& $i > j$ Then

$\underbrace{a \cdot a \cdot a \cdot a \cdots a}_{(i \text{ times})} \equiv \underbrace{a \cdot a \cdot a \cdots a}_{(j \text{ times})} \pmod{m}$

Since $(a, m) = 1$ Therefore

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

but

$a^n \equiv 1 \pmod{m}$

$\Rightarrow n \mid i-j$

$$\Rightarrow i - j \equiv 0 \pmod{n}.$$

$$\Rightarrow i \equiv j \pmod{n}.$$

Conversely suppose that

$$i \equiv j \pmod{n}.$$

$$\Rightarrow i - j \equiv 0 \pmod{n}$$

$$\Rightarrow n \mid i - j$$

$\exists\ q \in \mathbb{Z}$ s.t.

$$i - j = nq.$$

$$\Rightarrow i = j + nq.$$

Since $a^i \equiv a^j \pmod{m}$.

$$\Rightarrow a^i = a^{j+nq} \equiv a^j \cdot (a^n)^q \pmod{m}$$

$$\Rightarrow a^i \equiv a^j \pmod{m}.$$

which is required result.

[redacted]

i) If $a \equiv b \pmod{m}$

Then

$$\text{ord}_m(a) = \text{ord}_m(b)$$

ii) If $ab \equiv 1 \pmod{m}$ Then

$$\text{ord}_m(a) \equiv \text{ord}_m(b)$$

Proof

Suppose $\text{ord}_m(a) = n_1$ and
$\text{ord}_m(b) = n_2$

$$\Rightarrow a^{n_1} \equiv 1 \pmod{m}$$
and
$$b^{n_2} \equiv 1 \pmod{m}.$$

Since

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

$$\Rightarrow a^{n_1} \equiv b^{n_1} \pmod{m}.$$

$$\Rightarrow 1 \equiv b^{n_1} \pmod{m}$$

or

$$b^{n_1} \equiv 1 \pmod{m}$$ by Symmetric property of Congruence.

But $b^{n_2} \equiv 1 \pmod{m}$

$\Rightarrow$

$$n_2 \mid n_1 \quad \text{———} \quad (1) \qquad \because \text{ord}_m b = n_2$$

NOW

$$a^{n_2} \equiv b^{n_2} \pmod{m}$$

$$\Rightarrow a^{n_2} \equiv 1 \pmod{m} \qquad \because b^{n_2} \equiv 1 \pmod{m}$$

If $ab \equiv 1 \pmod{m}$

Then $ord_m(a) = ord_m(b)$

Proof: Suppose

$$order_m(a) = n_1$$

&

$$ord_m(b) = n_2.$$

$$\Rightarrow a^{n_1} \equiv 1 \pmod{m}$$

&

$$b^{n_2} \equiv 1 \pmod{m}$$

Since

$$ab \equiv 1 \pmod{m}$$

$$\Rightarrow (ab)^{n_1} \equiv (1)^{n_1} \pmod{m}$$

$$\Rightarrow a^{n_1} b^{n_1} \equiv 1 \pmod{m}$$

$$\Rightarrow b^{n_1} \equiv 1 \pmod{m} \quad \because a^{n_1} \equiv 1 \pmod{m}$$

But $\text{ord}_m(b) = n_2$

$\Rightarrow n_2 \mid n_1$ —— (1)

Now

$(ab)^{n_2} \equiv (1)^{n_2} \pmod m$

$a^{n_2} b^{n_2} \equiv 1 \pmod m$

$a^{n_2} \equiv 1 \pmod m \quad \because b^{n_2} \equiv 1 \pmod m$

But

$\text{ord}_m(a) = n_1$

$\Rightarrow n_1 \mid n_2$ —— (2)

From (1) & (2) we have

$n_1 = n_2$

$$\boxed{\text{ord}_m(a) = \text{ord}_m(b)}$$

[redacted] If $(s,t) = 1$ and 'a' belonges to 's' (mod m) and 'b' belongs to 't' (mod m) Then ab belongs to st (mod m).

Proof

we know

$a^s \equiv 1 \pmod m$

&

$b^t \equiv 1 \pmod m$

Let $\quad ord_m(ab) = k$

$$\Rightarrow \quad (ab)^k \equiv 1 \pmod{m}$$

Now

as

$$a^s \equiv 1 \pmod{m}$$

$$\Rightarrow a^{st} \equiv 1 \pmod{m} \quad \text{--- (1)}$$

&

also $\quad b^t \equiv 1 \pmod{m}$

$$b^{st} \equiv 1 \pmod{m} \quad \text{--- (2)}$$

Multiplying eqn (1) & (2) we get

$$a^{st} \cdot b^{st} \equiv 1 \pmod{m}$$

$$\Rightarrow (ab)^{st} \equiv 1 \pmod{m}$$

But

$$ord_m(ab) = k \quad \text{or} \quad (ab)^k \equiv 1 \pmod{m}$$

$$\Rightarrow \quad k \mid st \quad \text{--- (3)}$$

Next

$$(ab)^k \equiv 1 \pmod{m}$$

$$a^k b^k \equiv 1 \pmod{m}$$

$$(a^k b^k)^t \equiv 1 \pmod{m}$$

$$a^{kt} b^{kt} \equiv 1 \pmod{m}$$

$\Rightarrow a^{ki} \equiv 1 \pmod m \quad \because b^t \equiv 1 \pmod m$

But

$ord_m(a) = s$ or $a^s \equiv 1 \pmod m$ $\quad b^{ki} \equiv 1 \pmod m$

$\Rightarrow s \mid ki$ — (4) and $s \mid k \quad \because (s,t) = 1$.

Similarly

$(ab)^k \equiv 1 \pmod m$

$(ab)^{ks} \equiv 1 \pmod m$

$a^{ks} b^{ks} \equiv 1 \pmod m$

$b^{ks} \equiv 1 \pmod m \quad \because a^s \equiv 1 \pmod m$

But

$ord_m(b) = t$ or $b^t \equiv 1 \pmod m$ $\quad a^{ks} \equiv 1 \pmod m$.

$\Rightarrow t \mid ks$

$\Rightarrow t \mid k \quad \because (s,t) = 1$

$\Rightarrow st \mid k$ —— (5) $\because (s,t) = 1$

from (3) & (5) we get

$k = st$

$$\boxed{ord_m(ab) = st}$$

Imp

CWMS PR

* [redacted]

when $(a,m) = 1$ and 'a' belongs to $\phi(m)$ (mod m) Then a is called primitive root of 'm' i.e

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

① for e.g.

$\phi(1)$

$1 \equiv 1 \pmod 1$

i) 1 is primitive root of 1 and 2.

$1 \equiv 1 \pmod 1$

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

② $1 \equiv 1 \pmod 2$

NOTE: 1 is the primitive root for Those for which $\phi(m) = 1$ i.e 1 & 2.

ii) 2 is primitive root of 3.

$\phi(3) = 2$

$\therefore \quad 2^{\phi(3)} \equiv 1 \pmod 3$

$= 2^2 \equiv 1 \pmod 3$

$\phi(4)$

$3 \equiv 1 \pmod 4$

$3^2 \equiv 1 \pmod 4$

3 is the primitive root of 4.

The only integers which have primitive roots are

a. 1, 2, 4, p^n and $2p^n$. where p is an odd prime

1, 2, 3, 4, 5, 6, 7, 9, 10, 11, 13, 14, p^n and $2p^n$.

//.

Check the proof

If [redacted] of m has primitive root 'g'
Then 'm' has $\varphi(\varphi(m))$
primitive roots given by

$$1 \leq \alpha \leq \varphi(m) - 1, \ (\alpha, \varphi(m)) = 1$$

denoted by "g^{α}".

For e.g. for 13

$\varphi(13) = 12$ $\because$ 13 is odd prime

$\varphi(\varphi(13)) = \varphi(12) =$

$= 12(1 - \frac{1}{2})(1 - \frac{1}{3})$

$= 12(1/2)(2/3)$

$= 4$

& $\varphi(m) = m - 1$
if m is prime

$(1, 12) = 1$
$(5, 12) = 1$
$(7, 12) = 1$
$(11, 12) = 1$

— x — x — x —

$(a, 17) = 1 \quad a^{\varphi(17)} \equiv 1 \pmod{17}$

[redacted] Find all primitive roots of 17.

Sol:-

$$\varphi(17) = 16 \quad \because \text{ 17 is odd prime.}$$

$(2, 17) = 1$

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

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

$$2^3 \equiv 8 \pmod{17}$$

$$2^4 \equiv 16 \pmod{17} \text{ or } 2^4 \equiv -1 \pmod{17}$$

$$2^5 \equiv -2 \pmod{17}$$

$$2^6 \equiv -4 \pmod{17}$$

$$2^7 \equiv -8 \pmod{17}$$

$$2^8 \equiv -16 \pmod{17}$$

$$2^8 \equiv 1 \pmod{17} \quad \because -16 \equiv 1 \pmod{17}$$

so 2 is not primitive root of 17.

Now

$(3, 17) = 1$

$$3^1 \equiv 3 \pmod{17}.$$

$3^2 \equiv 9 \pmod{17}$

$3^3 \equiv 10 \pmod{17}$

$3^4 \equiv 13 \pmod{17}$

$3^5 \equiv 5 \pmod{17}$

$3^6 \equiv 15 \pmod{17}$

$3^7 \equiv 11 \pmod{17}$

$3^8 \equiv -1 \pmod{17}$

$3^{\phi(17)} = 3^{16} \equiv 1 \pmod{17}$ — $13^{\phi(17)} \equiv 1 \pmod{17}$

3 is primitive root of 17. ∵ By definition By Previous Theorem.

Now $\phi(\phi(17)) = \phi(16) = 16\left(1-\frac{1}{2}\right)$
$= \underline{\underline{8}}$ ∵ $16 = 2^4$.

$\phi(\phi(17)) = 8$ ✓.

So It has '8' numbers (primitive) Roots.

Now $1 \leq \alpha \leq 16-1$
$\Rightarrow 1 \leq \alpha \leq 15$

Such α's are i.e $(\alpha, 16) = 1$

~~$(\alpha, 16) = 1$~~

$(1,16)=1$

$(3,16)=1$

$(5,16)=1$

$(7,16)=1$

$(9,16)=1$

$(11,16)=1$

$(13,16)=1$

$(15,16)=1$

So all primitive roots of 17 given by g^a.

$$3^1, 3^3, 3^5, 3^7, 3^9, 3^{11}, 3^{13}, 3^{15}$$

—— x —— x —— x —— x ——

[redacted]

Find all primitive roots of 11, 13, 15 and 19.

Sol:

$\phi(19) = 18$

$(2,19) = 1$

$2 \equiv 2 \mod (19)$

$2^2 \equiv 4 \pmod{19}$

$2^3 \equiv 8 \pmod{19}$

$18 = 3^2 \cdot 2^1$

$= 18(1-\frac{1}{3})(1-\frac{1}{2})$

$= 18(\frac{2}{3})(\frac{1}{2})$

$= 6$

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

$2^5 \equiv 13 \pmod{19}$

$2^6 \equiv 7 \pmod{19}$.

$2^7 \equiv 14 \pmod{19}$

$2^8 \equiv 9 \pmod{19}$

$2^9 \equiv 18 \pmod{19}$

also $2^9 \equiv -1 \pmod{19}$

$2^{18} \equiv 1 \pmod{19}$

$\Rightarrow$ 2 is the primitive ~~period~~ root of 19.

Now $\varphi(\varphi(19)) = \varphi(18)$

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

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

$\varphi(\varphi(19)) = 6$ where $(\alpha, 6) = 1$

$1 \leq \alpha \leq \varphi(19) - 1$

$= 18 - 1 = 17$

Such α's which are $(\alpha, 18) = 1$

$(1, 18)$, $(5, 18) = 1$, $(7, 18) = 1$, $(11, 18) = 1$

$(13, 18) = 1$, $(17, 18) = 1$,

So all the primitive roots of 19 is given by g^{α},

i.e $2^{1}, 2^{5}, 2^{7}, 2^{11}, 2^{13}, 2^{17}$.

— * — * — * — * —

Q [redacted]

$$x \equiv 0 \pmod{2} \quad \text{—(i)}$$
$$x \equiv 0 \pmod{3} \quad \text{(ii)}$$
$$x \equiv 3 \pmod{5} \quad \text{(iii)}$$

Solution

So $x \equiv 0 \pmod{2}$

$x = 0 + 2r$

$x = 2r$ — (4)

using in (ii)

$2r \equiv 0 \pmod{3}$

$r \equiv 0 \pmod{3}$ $\because (2,3)=1$

$r = 0 + 3s$ for $s \in \mathbb{Z}$

$r = 3s$

(4) $\Rightarrow$

$$x = 2(3s) = 6s. \quad \text{—— (5)}$$

using in (iii) we get

$$6s \equiv 3 \pmod 5$$

Checking in C.R.S of $\pmod 5$

$\Rightarrow s \equiv 3 \pmod 5$.

$\Rightarrow s = 3 + 5t \quad \rightarrow$ by linear eqn form

eqn (5) $\Rightarrow x = 6(3 + 5t)$

$x = 18 + 30t$

$x \equiv 18 \pmod{30} \quad \because 30t \equiv 0 \pmod{30}$

[redacted] // If P_1 and P_2 are odd prime and

$$m \equiv a_1 \pmod{P_1}, \quad m \equiv a_2 \pmod{P_2}$$

Moreover if 'a_1' $\pmod{P_1}$ belongs to 'd_1' $\pmod{P_2}$. Then 'm' belongs to least common multiple of d_1 and d_2. mod P_1P_2.

Proof: let $L = \langle d_1, d_2 \rangle =$ L.C.M of d_1, d_2.

also given that

$$a_1^{d_1} \equiv 1 \pmod{P_1}$$

$$a_2^{d_2} \equiv 1 \pmod{P_2}.$$

d_1/L and d_2/L because L.C.M.

$$\Rightarrow \left(a_1^{d_1}\right)^{\frac{L}{d_1}} \equiv 1 \pmod{p_1}$$

and

$$\left(a_2^{d_2}\right)^{\frac{L}{d_2}} \equiv 1 \pmod{p_2}.$$

$$\Rightarrow \quad a_1^L \equiv 1 \pmod{p_1}$$

&

$$a_2^L \equiv 1 \pmod{p_2}$$

Then

$$m^L \equiv a_1^L \equiv 1 \pmod{p_1} \quad \because$$

i.e

$$m^L \equiv 1 \pmod{p_1}. \qquad m \equiv a_1 \pmod{p_1}$$

also

$$m^L \equiv a_2^l \equiv 1 \pmod{p_2}$$

i.e

$$m^L \equiv 1 \pmod{p_2}.$$

$$\Rightarrow \quad p_1 \mid m^l - 1 \quad \& \quad p_2 \mid m^l - 1$$

$$\Rightarrow \quad p_1 p_2 \mid m^l - 1 \quad \because \quad (p_1, p_2) = 1$$

$$m^l \equiv 1 \pmod{p_1 p_2}$$

Now if m belongs to $K \pmod{p_1 p_2}$

Then $\quad m^k \equiv 1 \pmod{p_1 p_2}.$

$\Rightarrow k \mid L$ —— ①

Then
$$m^k \equiv 1 \pmod{P_1P_2}$$

$$\Rightarrow m^k \equiv 1 \pmod{P_1}$$

& $m^k \equiv 1 \pmod{P_2}$ $\because (P_1, P_2) = 1$

Also
$$m^{d_1} \equiv a_1^{d_1} \equiv 1 \pmod{P_1}$$

$$\Rightarrow m^{d_1} \equiv 1 \pmod{P_1}$$

Similarly
$$m^{d_2} \equiv a_2^{d_2} \equiv 1 \pmod{P_2}$$

$$m^{d_2} \equiv 1 \pmod{P_2}.$$

$\Rightarrow d_1 \mid k$ and $d_2 \mid k$.

$\Rightarrow$ k is common multiple of d_1 & d_2 but $\langle d_1, d_2 \rangle = L$.

i.e. $L \mid k$ —— ②

From ① & ②

$$k = L$$

i.e
$$m^l \equiv 1 \pmod{P_1P_2}$$

$\Rightarrow$ m belongs to "L" $\pmod{P_1P_2}$

* [redacted] Let p be an odd prime and 'r' is a primitive root of p. and

$$n \equiv r^s \pmod{p}$$ Then the exponent 's' is called index of 'n' $(\bmod p)$ relative to base 'r'.

i.e

$$s = \text{index}_r\, n$$

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

* [redacted]

(i) If $(n,p)=1$

$\text{ind}_r n \pmod{p-1}$ is unique.

Proof: Let 'r' be the primitive root of p. let

$$\text{ind}_r n = s$$

&

$$\text{ind}_r n = t.$$

$\log_{10} a = n$

$$\Rightarrow n \equiv r^s \pmod{p}$$

&

$$n \equiv r^t \pmod{p}$$

Suppose $s > t$.

$r^s \cdot r^{-t} \equiv r^t \cdot r^{-t} \pmod{p}$

$r^s \equiv r^t \pmod{p}$

$\Rightarrow r^{s-t} \equiv 1 \pmod{p} \quad \because (r,p)=1.$

$r^s \equiv r^t \pmod{p}$

$r \cdot r \cdot r \cdots r \equiv r \cdot r \cdots t \pmod{p}$
(s time)

$r^{s-t} \equiv 1 \pmod{p}$

But By definition

$r^{\phi(p)} = r^{p-1} \equiv 1 \pmod{p}$

$\Rightarrow p-1 \mid s-t \quad \because \phi(p) = p-1$

$a/a-b$

$\Rightarrow s \equiv t \pmod{p-1}$ by def of ~~divisibility~~ congruence.

$\Rightarrow$ s and t lies in same congruence class.

Hence

$\operatorname{ind}_r n \pmod{p-1}$

is unique.

$m \equiv n \pmod{p}$

iff

$\operatorname{ind}_r m \equiv \operatorname{ind}_r n \pmod{p-1}.$

Proof :- Let 'r' be the premitive root of p. and

$\operatorname{ind}_r m = s$

and

$\operatorname{ind}_r n = t$

$\Rightarrow m \equiv r^s \pmod{p}$

& $n \equiv r^t \pmod{p}$

Now $m \equiv n \pmod{p}$

$\Rightarrow r^s \equiv r^t \pmod{p}$

$\Rightarrow r^{\text{ind } m} \equiv r^{\text{ind } n} \pmod{p}$

Now suppose $s > t$

$\Rightarrow r^{\text{ind } m - \text{ind } n} \equiv 1 \pmod{p}$

But $r^{\phi(p)} = r^{p-1} \equiv 1 \pmod{p}$

$p-1 \mid \text{ind } m - \text{ind } n.$

$\Rightarrow \text{ind } m \equiv \text{ind } n \pmod{p-1}$

$\because$ if $m \mid a-b$
$\Rightarrow a \equiv b \pmod{m}$

Conversely suppose that

$\text{ind}_r m \equiv \text{ind}_r n \pmod{p-1}$

By def of congruence

$p-1 \mid \text{ind } m - \text{ind } n$

$\Rightarrow \quad g^{ind\,m - ind\,n} \equiv 1 \pmod{p}$

$\Rightarrow \quad g^{ind\,m} \equiv g^{ind\,n} \pmod{p}$ | $\because \; g^{\phi(p)} \equiv 1 \pmod{p}$ if $\phi(p) \mid z$. Then $g^{z} \equiv 1 \pmod{p}$.

$\Rightarrow \quad g^{s} \equiv g^{t} \pmod{p}$.

As $g^{s} \equiv m \pmod{p}$ & $g^{t} \equiv n \pmod{p}$

Therefore $\boxed{m \equiv n \pmod{p}}$

.x. .x. .x.

[redacted] Imp Annual 10

If g is premitive root of 'q' and $a \equiv b \pmod{q}$ Then

(i) $ind_g(ab) \equiv ind_g a + ind_g(b) \pmod{\phi(q)}$

(ii) $ind_g a^n \equiv n\, ind_g a \pmod{\phi(q)}$

Proof: if 'g' be the primitive root of q.

let $ind_g(ab) = t$

$\Rightarrow ab \equiv \xi^{t} \pmod{q}$

also

Suppose that

$ind_{\xi} a = t_1$ and

$ind_{\xi} b = t_2$.

$\Rightarrow$

$a \equiv \xi^{t_1} \bmod (q)$ — (1)

& $b \equiv \xi^{t_2} \bmod (q)$. — (2)

Since

$a \equiv b \pmod{q}$

Therefore

$\xi^{t_1} \equiv \xi^{t_2} \pmod{q}$ Not include in the proof.

Suppose $t_1 > t_2$

$\xi^{t_1} \cdot \xi^{-t_2} \equiv 1 \pmod{q}$

$\Rightarrow \xi^{t_1 - t_2} \equiv 1 \pmod{q}$.

Root But By definition of perimitive

$\xi^{\varphi(q)} \equiv 1 \pmod{q}$

so $\varphi(q) \mid t_1 - t_2$.

$\Rightarrow t_1 \equiv t_2 \pmod{\phi(q)}$

Now from (1) & (2)

$ab \equiv g^{t_1} \cdot g^{t_2} \pmod{q}$.

$ab \equiv g^{t_1+t_2} \pmod{q}$.

$g^t \equiv g^{t_1+t_2} \pmod{q}$.

$\because ab \equiv t \pmod{q}$

$\Rightarrow g^{t-t_1+t_2} \equiv 1 \pmod{q}$.

By definition of premitive root

$g^{\phi(q)} \equiv 1 \pmod{q}$

$\Rightarrow \phi(q) \mid t - t_1 + t_2$.

$\Rightarrow t \equiv t_1 + t_2 \pmod{\phi(q)}$

$\Rightarrow \text{ind}_g ab \equiv \text{ind}_g a + \text{ind}_g b \pmod{\phi(q)}$

which is required result.

— × — × —

ii) $$\text{ind}_\xi a^n \equiv n \,\text{ind}_\xi a \pmod{\varphi(q)}$$

Since

$$\text{ind}_\xi a^n = \text{ind}_\xi (a.a.a.\cdots.a)_{(n\text{ times})}$$

$$\equiv \text{ind}_\xi a + \text{ind}_\xi a + \cdots + \text{ind}_\xi a_{(n\text{ times})} \pmod{\varphi(q)}$$

$$\text{ind}_\xi a^n \equiv n \,\text{ind}_\xi (a) \pmod{\varphi(q)}$$

---

* [redacted]

If ξ and h are primitive root of p. Then

$$\text{ind}_h (a) \equiv \text{ind}_\xi a \cdot \text{ind}_h \xi \pmod{p-1}$$

Proof Suppose

$$\text{ind}_h a = t.$$

$$\text{ind}_\xi a = t_1$$

$$\text{ind}_h \xi = t_2$$

$$\Longrightarrow \quad a \equiv h^t \pmod{p} \quad \text{— (1)}$$

$$a \equiv \xi^{t_1} \pmod{p} \quad \text{— (2)}$$

$$g \equiv h^{t_2} \pmod{p} \quad \text{--- (3)}$$

eqn (3) $\Rightarrow$

$$g^{t_1} \equiv h^{t_1 t_2} \pmod{p}$$

$$a \equiv h^{t_1 t_2} \pmod{p}$$

or

$$h^{t_1 t_2} \equiv a \pmod{p} \quad \because g^{t} \equiv a \pmod{p}$$

$$h^{t_1 t_2} \equiv h^{t} \pmod{p} \quad \because a \equiv h^{t} \pmod{p}$$

$$h^{t_1 t_2 - t} \equiv 1 \pmod{p}.$$

But

By definition of primitive root

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

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

$$\Rightarrow p-1 \mid t_1 t_2 - t$$

$$\Rightarrow t_1 t_2 \equiv t \pmod{p-1}$$

$$\Rightarrow t \equiv t_1 t_2 \pmod{p-1}$$

$$\text{ind}_h a \equiv \text{ind}_g a \cdot \text{ind}_h g \pmod{p-1}$$

22

[redacted] Solve with the help of indices

Sol $17x \equiv 10 \pmod{29}$.

Since '2' is the primitive root of 29.

So we have the table for indicies

a	2	4	8	16	3	6
ind a	1	2	3	4	5	6

a	12	19	9	18	7	14
ind a	7	9	10	11	12	13

a	28	27	25	21	13
ind a	14	15	16	17	18

a	26	23	17	5	10
ind a	19	20	21	22	23
a	20	11	22	15	1
ind a	24	25	26	27	28

Now as we know

$$\operatorname{ind}_g(ab) \equiv \operatorname{ind}_g a + \operatorname{ind}_g b \pmod{\phi(p)}$$

Now we have

$$17x \equiv 10 \pmod{29}$$

$$\operatorname{ind}_2(17x) \equiv \operatorname{ind}_2 10 \pmod{28}$$

$$\operatorname{ind}_2 17 + \operatorname{ind}_2 x \equiv \operatorname{ind}_2 10 \pmod{28}$$

$$\operatorname{ind}_2 x \equiv \operatorname{ind}_2 10 - \operatorname{ind}_2 17 \pmod{28}$$

$$\equiv 23 - 21 \pmod{28}$$

$$\operatorname{ind}_2 x \equiv 2 \pmod{28}$$

$$x \equiv 2^2 \pmod{29}$$

$$x \equiv 4 \pmod{29}$$

which is the required solution of

$$17x \equiv 10 \pmod{29}$$

Ex:

1, $5x^2 \equiv 3 \pmod{11}$

$17x^2 \equiv 10 \pmod{29}$

(Q# 1) $5x^2 \equiv 3 \pmod{11}$

First we find the primitive root of 11.

Since $\phi(11) = 10$

Since $(2, 11) = 1$
and

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

$\Rightarrow$ 2 is the primitive root

a	2	4	8	5	3	3	5	9	4	1
ind a	1	2	3	4	5	6	7	8	9	10

Now as we know that,

$ind_g ab = ind_g a + ind_g b \pmod{\phi(p)}$

&

$ind_g a^n = n\, ind_g a \pmod{\phi(p)}$

So we have

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

$$\Rightarrow \operatorname{ind}_2 5x^2 \equiv \operatorname{ind}_2 3 \pmod{10}$$

$\because$ if $m \equiv n \pmod p$ Then $\Rightarrow \operatorname{ind}_g m \equiv \operatorname{ind}_g n \pmod{\phi(p)}$

$$\Rightarrow \operatorname{ind}_2 5 + \operatorname{ind}_2 x^2 \equiv \operatorname{ind}_2 3 \pmod{10}$$

$$\Rightarrow \operatorname{ind}_2 5 + 2\operatorname{ind}_2 x \equiv \operatorname{ind}_2 3 \pmod{10}.$$

$$3 + 2\operatorname{ind}_2 x \equiv 8 \pmod{10}$$

$$2\operatorname{ind}_2 x \equiv 5 \pmod{10}.$$

$$\operatorname{ind}_2 x \equiv \frac{5}{2} \pmod{10}$$

$$x \equiv 2^{5/2} \pmod{10}.$$

Since 8 s

$$x_0 + \frac{m}{d} t.$$

Imp Annual 10

*

[redacted]

If $x^n \equiv c \pmod m$ is solvable and $(m,c)=1$ Then c is said to be nth power residue of 'm' otherwise n-th power non-residue.

If $x^2 \equiv c \pmod m$ is solvable and $(m,c)=1$ Then c is said to be quadratic residue of m, otherwise quadratic non-residue of m" i.e if the congruence has non solution. Then 'c' is said to be quadratic non-residue of 'm'.

e.g

Imp Annual

$x^2 \equiv 2 \mod (7)$ has a sol (5)

$x \equiv 3 \pmod 7$ and $(2,7)=1$ Then 2 is quadratic residue of 7.

now if

(2,5)=1

$x^2 \equiv 2 \pmod 5$.

This congruence has no solution So '2' is quadratic non-residue of 5.

$x=3$

— x — x —

[redacted] If 'a' is Quardratic Residue of $m > 2$ Then

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

Proof:

Suppose that the Congruence $x^2 \equiv a \pmod{m}$ has sol $x \equiv r \pmod{m}$ with $(r,m) = 1$

Then by transitive property of Congruences

$$\Rightarrow r^2 \equiv a \pmod{m}$$

Since $m > 2$ so $\phi(m)$ is even

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

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

Now By Euler's Theorem.

Since $(r,m) = 1$ so $r^{\phi(m)} \equiv 1 \pmod{m}$

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

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

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

$$2^{6} \equiv 1 \pmod{7}$$

so by above theorem

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

$\left(2/29\right)$ Solve L. symbol

Imp

*

[redacted]

If p is an odd prime and $(a,p)=1$ we defined the Legender ~~Symbol~~ as

$\left(\frac{a}{p}\right)=1$ if 'a' is a quardratic residue of p and

$\left(\frac{a}{p}\right)=-1$ if 'a' is quardratic non residue of p.

for e.g. $\left(\frac{2}{7}\right)=1$ $x^2\equiv 2 \pmod 7$

$(2,7)=1$

$x\equiv 3 \pmod 7$

&

(a.) $\left(\frac{2}{5}\right)=-1$ $\therefore$ $x^2\equiv 2 \pmod 5$

Since 2 is ~~quardratic~~ non-residue of 5. $(2,5)=1$

But solution does not exist.

Imp

[redacted] If $a_1\equiv a_2 \pmod p$ and if the Congruence $x^2\equiv a_1 \pmod p$ has a solution where $(a_1,p)=1$. Then a_1 is quardratic residue of p.

Since

$a_1\equiv a_2 \pmod p$ and

~~if the Congruence $x^2\equiv a_1 \pmod p$ has a solution~~

Then $x^2 \equiv a_2 \pmod{P}$ is also sorvable and 'a_2' is quardratic residue of p. i.e

$$\left(\frac{a_1}{p}\right) = 1 = \left(\frac{a_2}{p}\right)$$

Similarly if a_1 is quardratic non-residue then a_2 is also quardratic non-residue of p. i.e

$$\left(\frac{a_1}{p}\right) = -1 = \left(\frac{a_2}{p}\right)$$

imp

2) $\left(\frac{1}{p}\right) = 1$. Since $x^2 \equiv 1 \pmod{p}$, $(1, P) = 1$

so 1 is quardratic residue of p. (As $x \equiv 1 \pmod{p}$ is the solution of this congruence.

3) $\left(\frac{a^2}{p}\right) = 1$ if $(a, P) = 1$

* 4) product of two quardratic residues and two quardratic non-residues is a quardratic residue.

The product of a quardratic residue with a quardratic non-residue is quardratic non residue. i.e

If a_1, a_2 are quaratic residues

Then $\left(\frac{a_1 \cdot a_2}{P}\right) = 1 = \left(\frac{a_1}{P}\right)\left(\frac{a_2}{P}\right)$

Similarly

4) a_1 & a_2 are non-quardratic Residue.

$$\left(\frac{a_1 a_2}{P}\right) = 1 = \left(\frac{a_1}{P}\right) \cdot \left(\frac{a_2}{P}\right)$$

Similarly If a_1 is ~~a_2~~ quardratic and a_2 is non-quardratic Then

$$\left(\frac{a_1 \cdot a_2}{P}\right) = -1 = \left(\frac{a_1}{P}\right)\left(\frac{a_2}{P}\right)$$

5) for $(a_i, P) = 1$, $i = 1, 2, 3, \dots, n$

Then

$$\left(\frac{a_1 \cdot a_2 \cdot a_3 \cdot \dots \cdot a_n}{P}\right) = \left(\frac{a_1}{P}\right)\left(\frac{a_2}{P}\right)\left(\frac{a_3}{P}\right) \cdots \left(\frac{a_n}{P}\right)$$

6

$$\left(\frac{a_1}{P}\right)\left(\frac{a_2}{P}\right) = 1$$

$$\Rightarrow \left(\frac{a_1}{P}\right) = \left(\frac{a_2}{P}\right)$$

indicates that a_1 & a_2 both are residue are non-residue.

$\Rightarrow$ a_1, a_2 have ~~oppos~~ same quadratic character if both are

Quaratic Residue or Quardratic non-Residue.

$$\left(\frac{a_1}{p}\right)\left(\frac{a_2}{p}\right) = -1$$

$$\Rightarrow \left(\frac{a_1}{p}\right) = -\left(\frac{a_2}{p}\right).$$

& have opposite Quaratic char. if one is quadratic Residue & other is Quardratic non-Residue.

[redacted]

(i) If "p" is positive odd integer then

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

Quadratic residue. e.g. $\left(\frac{-1}{271}\right) = (-1)^{\frac{271-1}{2}}$

(ii) If p is an odd prime then

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$ is quadratic residue of 7.

Remark:-

(3) The quadratic Reciprocially law:- If "p" and "q" are distinct odd prime then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

Imp

[redacted] Show that 33 is the ~~Quadrat~~ quadratic non-residue of 89.

Sol:- Since $33 = 3 \times 11$

So $$\left(\frac{33}{89}\right) = \left(\frac{3\times 11}{89}\right)$$

$$\left(\frac{33}{89}\right) = \left(\frac{3}{89}\right)\left(\frac{11}{89}\right) \quad \text{--- (1)}$$

First we take 3/89

$$\left(\frac{3}{89}\right)\left(\frac{89}{3}\right) = (-1)^{\frac{3-1}{2}\cdot\frac{89-1}{2}}$$

$$= (-1)^{(1)(44)} = 1$$

Clearly $\left(\frac{3}{89}\right)$ and $\left(\frac{89}{3}\right)$ have same quadratic charactor.

So we check $89/3 \equiv 2/3 \bmod (2)$

$$\Rightarrow \left(\frac{2}{3}\right) = (-1)^{\frac{3^2-1}{8}} \quad \because \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$ if p is odd prime.

$$= (-1)^{\frac{9-1}{8}}$$

$$= (-1)^1$$

$$= -1$$

So $\boxed{3/89 = -1}$

Similarly $(11/89)(89/11)$

$$= (-1)^{\frac{11-1}{2}\cdot\frac{89-1}{2}}$$

$$= (-1)^{5\cdot 44}$$

$$= 1$$

clearly $(11/89)$ and L-S $(89/11)$ have same quardratic charactor.

So we check $(89/11) \equiv (1/11) \pmod 8$

$$\left(\frac{1}{11}\right) = 1$$

So $(11/89) = 1$

using these values in (1)

$$\frac{33}{89} = (-1)(1) = -1$$

$\Rightarrow$ 33 is quadratic non-residue of 89.

Q# $\left(\frac{67}{89}\right)$ is quadratic residue or quadratic non-residue.

$$67 \equiv -22 \pmod{89}$$

$$\left(\frac{-22}{89}\right) = \left(\frac{-1 \cdot 2 \cdot 11}{89}\right)$$

$$= \left(-1/89\right)\left(2/89\right)\left(11/89\right)$$

$$= (-1)^{\frac{89-1}{2}} \cdot (-1)^{\frac{(89)^2-1}{8}} \cdot \left(11/89\right) \quad \text{--- (1)}$$

$$\left(11/89\right)\left(89/11\right) = (-1)^{\frac{11-1}{2} \cdot \frac{89-1}{2}}$$

$$= (-1)^{5 \cdot 44}$$

$$= 1$$

As $11/89$ and $89/11$ have same quadratic character

$$\left(89/11\right) = \left(1/11\right) = 1$$

so

$$\left(11/89\right) = 1$$

eq (1) $\Rightarrow$ $\left(\frac{67}{89}\right) = \left(\frac{-22}{89}\right)$

$$= (-1)^{44}(-1)^{990} \cdot (1) = (1)(1)(1) = 1$$

$\Rightarrow$ 67 is quadratic residue of 89

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = 1$$

$\Rightarrow$ $\left(p/q\right) \doteq \left(q/p\right)$ Resiprocity property

If p and q are distinct odd prime. Then Legender Symbol $\left(p/q\right)$ will be equal q/p unless both p and q are of the form $4K-1$ or $4K+3$. In this case

$$\left(p/q\right) = -\left(q/p\right).$$

e.g

$$11/19 = \frac{4(2)+3}{4(4)+3} = -1.$$

Assingnment:-

$$182/271.$$

γ [redacted]" γ

Let $x \in R$ Then we define $[x]$ greatest integer not exceeding x, $[x]$ is called "Bracket Function".

e.g.

R.N

$$[7.2] = 7$$

If

Real nos

$$x = 5/2 = 2.5$$

$$[5/2] = [2.5] = 2.$$

Similarly

$$[5] = 5$$

$$[-3] = -3. \quad , \quad [-9/2] = [-4.5] = -5$$

Q.

[redacted] Is $\frac{182}{271}$ is Quadratic Residue or non-Quadratic Residue.

$$182 \equiv -89 \pmod{271}$$

$$\left(\frac{-89}{271}\right) = \left(\frac{-1}{271}\right) \cdot \left(\frac{89}{271}\right)$$

$$= (-1)^{\frac{271-1}{2}} \cdot \left(\frac{89}{271}\right) \quad \text{--- I}$$

$$\left(\frac{89}{271}\right)\left(\frac{271}{89}\right) = (-1)^{\frac{89-1}{2} \cdot \frac{271-1}{2}}$$

$$= (-1)^{(44)\cdot(135)}$$

$$= (-1)^{5946} = 1$$

$\left(\frac{89}{271}\right)$ and $\left(\frac{271}{89}\right)$ has Same quardratic charactor.

$\left(\frac{271}{89}\right) = \left(\frac{4}{89}\right)$?

$4 \equiv -85 \pmod{89}$.

$\frac{-85}{89} = \frac{(-1 \times 5 \times 17)}{89}$

$= \left({}^{-1}/89\right)\left({}^{5}/89\right)\left({}^{17}/89\right)$ —— ②

$= (-1)^{\frac{89-1}{2}}$

$= \left({}^{5}/89\right)\left({}^{89}/5\right)$

$= (-1)^{\frac{5-1}{2} \cdot \frac{89-1}{2}}$

$= (-1)^{(2)(44)} = 1$.

Both $\left({}^{5}/89\right)$ and $\left({}^{89}/5\right)$ has same quadratic character.

$\left({}^{89}/271\right) = -1$

eq ① $\Rightarrow \left(\frac{182}{271}\right) = (-1)^{135} \cdot (-1)^{5940}$

$= (-1)(1)$

$= -1$

Hence 182 is quadratic non-residue of 271.

[redacted]

Prove That

i) $x = [x] + \theta \quad , \quad 0 \leq \theta < 1.$

ii) $[x+n] = [x] + n, \quad x \in \mathbb{R}, n \in \mathbb{Z}.$

iii) If $x, y \in \mathbb{R}$ $y \neq 0$ and

$x = qy + r$ where

Then $\left[x/y \right] = q \quad 0 \leq r < y.$

iv) $\left[\dfrac{[x]}{n} \right] = \left[\dfrac{x}{n} \right]$

Proof:-

I) This is obviousely True by definition

$$x = [x] + \theta \quad 0 \leq \theta < 1$$

II $[x+n] = [x] + n$

Since

$$x = [x] + \theta \quad ; \quad 0 \leq \theta < 1$$

$$[x] = x - \theta$$

$$[x] + n = \underline{x + n} - \theta$$

$$\Rightarrow [x] + n = [x+n] + \theta_1 - \theta$$

where $\theta_1 \geq 0$
$\theta_1 < 1$

as $[x]$, n and $[x+n]$ are

integer so $\theta_1 - \theta$ must be an integer but $0 \le \theta_1 - \theta < 1$.

$$\Rightarrow \theta_1 - \theta = 0$$

$$\Rightarrow [x] + n = [x+n] + 0$$

$$\Rightarrow [x] + n = [x+n].$$

III

If $x, y \in \mathbb{R}$ and $x = qy + r$, $0 \le r < y$

Then $\left[\frac{x}{y}\right] = q$

Since

$$x = qy + r$$

$$\frac{x}{y} = q + \frac{r}{y}$$

$$\left[\frac{x}{y}\right] = \left[q + \frac{r}{y}\right]$$

$$= \left[\frac{r}{y}\right] + q \text{ for } 0 \le r < y$$

$$\Rightarrow 0 \le \frac{r}{y} < 1$$

$$\left[\frac{x}{y}\right] = q + 0$$

$$\left[\frac{x}{y}\right] = q$$

So

$$\left[\frac{x}{y}\right] = q.$$

—x—

IV $\left[\dfrac{[x]}{n}\right] = \left[\dfrac{x}{n}\right]$

Proof:- $\left[\dfrac{[x]}{n}\right] = \left[\dfrac{x}{n}\right]$

Since $[x] \in \mathbb{Z}$ so $\exists$ q and r Such that

$[x] = qn + r$ — (1) where $0 \leq r < n$

$\Rightarrow$ $0 \leq r/n < 1$

$\dfrac{[x]}{n} = q + r/n$ $\because$ $[x] = x - \theta$.

using in eqn (1)

$x - \theta = qn + r$

$x = qn + r + \theta$

$\dfrac{x}{n} = q + \dfrac{r}{n} + \theta/n$.

$\Rightarrow \left[\dfrac{x}{n}\right] = \left[q + \dfrac{r+\theta}{n}\right]$

$= q + \left[\dfrac{r+\theta}{n}\right]$

$\left[\dfrac{x}{n}\right] = q + 0$

$\left[\dfrac{x}{n}\right] = q$ — (2)

Since $[x] = qn + r$; $0 \leq r < n$

$$\frac{[x]}{n} = q + \frac{r}{n}$$

$$\left[\frac{[x]}{n}\right] = \left[q + \frac{r}{n}\right]$$

$$= q + \left[\frac{r}{n}\right]$$

$$= q + 0 \qquad \because \left[\frac{r}{n}\right] = 0$$

$$0 \le \left[\frac{r}{n}\right] < 1$$

$$\Rightarrow \left[\frac{[x]}{n}\right] = q \longrightarrow (3)$$

From (2) & (3) we get

$$\left[\frac{[x]}{n}\right] = \left[\frac{x}{n}\right].$$

Theorem:-

$$\left[\frac{[x/y]}{z}\right] = \left[\frac{x}{yz}\right]$$

NOTE: An even integer is perfect.
$\Leftrightarrow n = 2^{p-1}(2^p - 1)$ where $2^p - 1$ is prime.

→ Arithmetical function $f(n)$ is said to be multiplicative if $f(mn) = f(m)f(n)$ for all relatively prime integer m, n.

$n^2, n!$ A.F

→ The function which associates with each positive integer n, the number of its positive is arithmetical function which is denoted by $d(n)$ or $\tau(n)$.
for e.g. $d(16) = 5$.

$\sigma(n) =$ Sum of positive Divisor of n $= 2n$.

$\sigma(6) = 12 = 2(n)$.

Theorem: if $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ where p_i's are distinct primes.

$$d(n) = \prod_{i=1}^{r} (\alpha_i + 1).$$

$$\sigma(n) = \prod_{i=1}^{r} \frac{p_i^{\alpha_i+1}}{p_i - 1}.$$

2^4
$= 4+1$
$= 5$ ✓

Eul $\varphi(n) = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right)$.

A number $n \in \mathbb{Z}^+$ is perfect number.

$\sigma(n) = 2n$.

Sol All perfect number are even.

[redacted] A function 'f' is said to be arithmatic function if its domain is the set of integer.

A single valued airthmatic function is called regular or multiplicative i.e

$f(m \cdot n) = f(m) f(n)$.

Def:

(1) $d(n) = \tau(n)$ The number of +ve devizer of n.

$\tau(8) = 4$.

$S(n)$ = The sum of +ve divisor of 'n'.

A $S(8) = 1+2+4+8 = 15$.

Further the function

$d(n) = \tau(n)$ and $S(n)$ are multiplicative

$\tau(m \cdot n) = \tau(m) \tau(n)$.

$S(m \cdot n) = S(m) S(n)$. Such that

$\forall$ $(m, n) = 1$

— x —

[redacted]

let $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_r^{\alpha_r}$.
be the standes form of 'n' Then

i) $d(n) = \tau(n) = \prod_{i=1}^{n} (\alpha_i+1)$

ii) $S(n) = \prod_{i=1}^{r} \frac{p_i^{\alpha_i+1}-1}{p_i-1}$

Proof :- The divisor of $p_i^{\alpha_i}$

$1, p_i^1, p_i^2, \ldots, p_i^{\alpha_i}$

$\tau(p_i^{\alpha_i}) = \alpha_i+1$

$\tau(p_1^{\alpha_1})\cdot\tau(p_2^{\alpha_2})\cdot\tau(p_3^{\alpha_3})\cdots\tau(p_r^{\alpha_r})$

$\Rightarrow \tau(n) = (\alpha_1+1)\cdot(\alpha_2+1)\cdots(\alpha_r+1)$.

$= \prod_{i=1}^{r}(\alpha_i+1)$.

ii) Now $S(n) = S(p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot p_3^{\alpha_3}\cdots p_r^{\alpha_r})$

$= S(p_1^{\alpha_1})\cdot S(p_2^{\alpha_2})\cdot S(p_3^{\alpha_3})\cdots S(p_r^{\alpha_r})$

$S(p_1^{\alpha_1}) = 1+p_1^1+p_1^2+\cdots+p_1^{\alpha_1}$ — (1)

This is a geometric series with $r = p_1$, $a = 1$ and $n = \alpha_1 + 1$

$$S_n = \frac{a(r^n - 1)}{r - 1}$$

$$S_n = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1}$$

$$S(p_1^{\alpha_1}) = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1}$$

Similarly

$$S(p_2^{\alpha_2}) = \frac{p_2^{\alpha_2+1} - 1}{p_2 - 1}$$

$$S(p_3^{\alpha_3}) = \frac{p_3^{\alpha_3+1} - 1}{p_3 - 1}$$

$$\vdots$$

$$S(p_r^{\alpha_r}) = \frac{p_r^{\alpha_r+1} - 1}{p_r - 1}$$

So eqn (1)

$$\Rightarrow S(n) = \left(\frac{p_1^{\alpha_1+1} - 1}{p_1 - 1}\right)\left(\frac{p_2^{\alpha_2+1} - 1}{p_2 - 1}\right) \cdots \left(\frac{p_r^{\alpha_r+1}}{p_r - 1}\right)$$

$$S(n) = \prod_{i=1}^{r} \frac{p_i^{\alpha_i+1} - 1}{p_i - 1} \quad //.$$

[redacted]

Mobious function:-

let

$$m = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot p_3^{\alpha_3} \cdot \ldots \cdot p_r^{\alpha_r}$$

be the standared form of m and p_i for $i = 1, 2, 3, \ldots, r$ are distinct prime Then we take

$$\mu(m) = 0 \quad \text{if any } \alpha_i > 1$$

$$\mu(m) = (-1)^r \quad \text{if all } \alpha_i = 1$$

$$\mu(m) = 1 \quad \text{if all } \alpha_i = 0$$

So define $\mu(m)$ is called Mobious function of m.

e.g.

$$24 = 2^3 \cdot 3$$

$$\mu(24) = 0 \quad \because 3 > 1$$

Annual obj

$30 = 2 \cdot 3 \cdot 5$ → Total $r = 3$

$$\mu(30) = (-1)^3 = -1$$

$\alpha_i = 1$ of $2, 3, 5$

$$\mu(+1) = 1$$

$$\mu(1) = 1$$

$$\mu(-1) = 1$$

— x —

Ans Annual 2009 Paper

[redacted]

$$\left[\frac{[x/y]}{z}\right] = \left[\frac{x}{yz}\right]$$

L.H.S

Since $x = qy + r$; $0 \le r < y$.
Dividing both sides by 'y'

$$\frac{x}{y} = q + \frac{r}{y}$$

taking bracket ftn on both side

$$\left[\frac{x}{y}\right] = \left[q + \frac{r}{y}\right]$$

$$= q + \left[\frac{r}{y}\right] \quad \begin{array}{l} 0 \le r < y \\ 0 \le \frac{r}{y} < 1 \end{array}$$

$$\frac{[x/y]}{z} = \frac{\left[q + \frac{r}{y}\right]}{z}, \quad \left[\frac{r}{y}\right] = 0$$

$$\left[\frac{[x/y]}{z}\right] = \left[\frac{q}{z}\right] \ne 0$$

$$\left[\frac{[x/y]}{z}\right] = \frac{q}{z} \quad \text{--- (1)} \quad \text{As } q \,\&\, z \in Z. \quad q/z \in Z.$$

R.H.S

$$\left[\frac{x}{yz}\right].$$

$\because \quad x = qy + r \quad ; \quad 0 \le r < y$

$$\frac{x}{y} = q + \frac{r}{y}$$

$$\frac{x}{yz} = \frac{q}{z} + \frac{r}{yz}$$

$$\left[\frac{x}{yz}\right] = \left[\frac{q}{z} + \frac{r}{yz}\right]$$

$$\left[\frac{x}{yz}\right] = \left[\frac{q}{z}\right] + \left[\frac{r}{yz}\right] \quad \because 0 \le \frac{r}{yz} < 1$$

$$\left[\frac{x}{yz}\right] = \left[\frac{q}{z}\right] + 0$$

$$\left[\frac{x}{yz}\right] = \frac{q}{z} \text{ --- } (2) \quad \because \left[\frac{q}{z}\right] = \frac{q}{z} \text{ since } q/z \in \mathbb{Z}$$

From (1) & (2) we get

$$\left[\frac{\left[\frac{x}{y}\right]}{z}\right] = \left[\frac{x}{yz}\right]$$

—— x ——