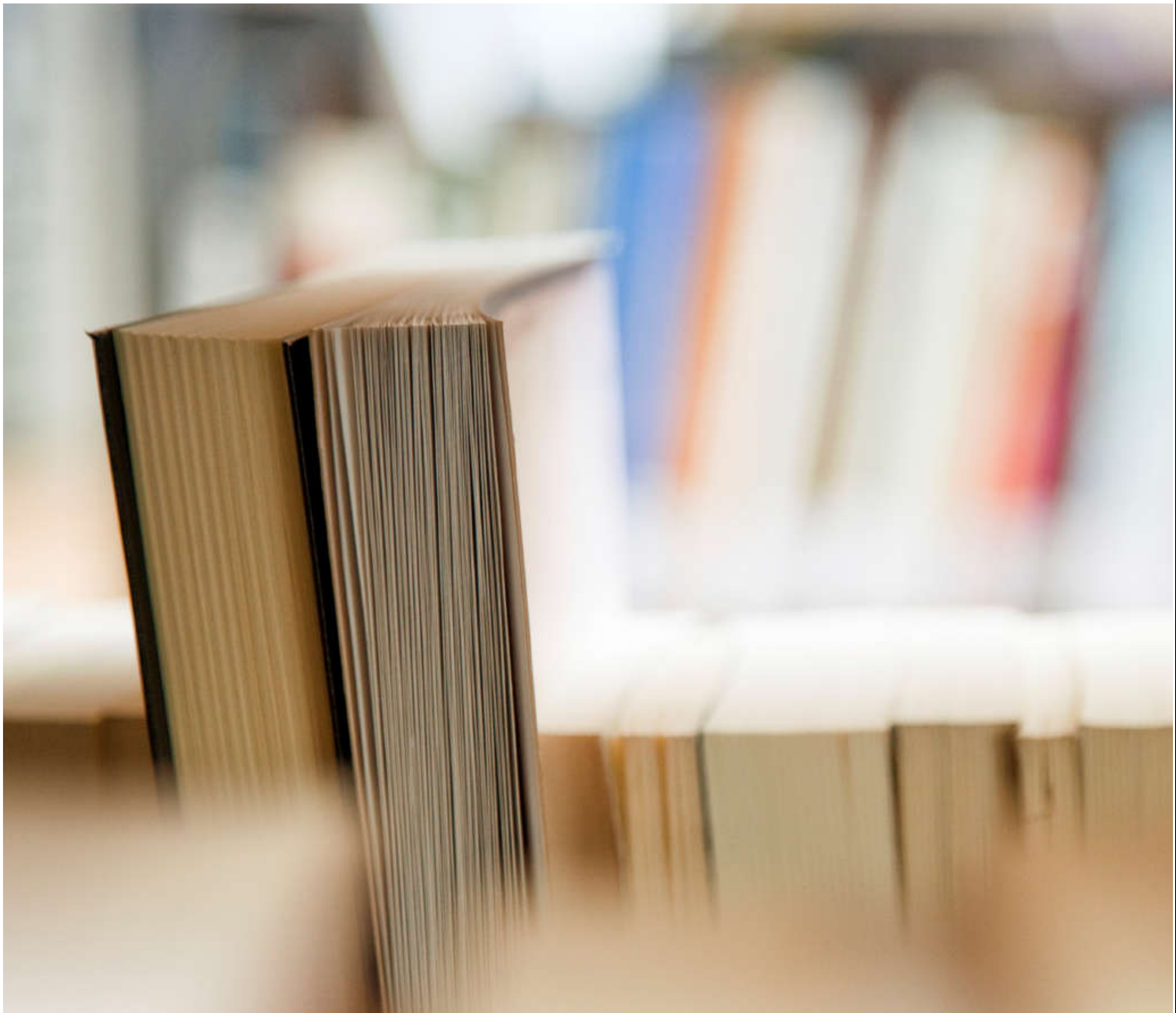

NUMBER THEORY

BY MUZAMMIL TANVEER

mtanveer8689@gmail.com

0316-7017457

Dedicated

To

My Honorable Teacher

Dr. Muhammad Umer Shuaib

&

My Parents

Lecture # 01

Integer:

The number which have no decimal no riven (بٹا) and no under root.

اعداد جس میں نہ اعشاریہ ہو نہ بٹا ہو اور نہ جذر ہو۔

Positive Integer:

The integer in which $x > 0$ i.e. $\{1,2,3,\ldots..\}$

Negative Integer:

The integer in which $x < 0$ i.e. $\{-1, -2, -3,\ldots..\}$

Non-negative Integer:

The integer in which $x \geq 0$ i.e. $\{0,1,2,3,\ldots..\}$

Non-positive Integer:

The integer in which $x \leq 0$ i.e. $\{0, -1, -2, -3,\ldots..\}$

Well Ordering Principle:

Let S be a non-empty set of non-negative integers. Then S contains a least (smallest) element.

Even Integer:

An integer 'n' is said to be even if $n = 2m$ where $m \in Z$

Odd Integer:

An integer 'n' is said to be odd if $n = 2m+1$ where $m \in Z$

Division Algorithm:

Let 'a' and 'b' be any two integers such that $b \neq 0$ then $\exists$ unique integers q and r s.t

$$a = qb+r \qquad ; \qquad 0 \leq r < |b|$$

e.g. a = 12 , b = 5 $\Rightarrow$ 12 = (5) + 2

& a = −36 , b = −7

−36 = 6(−7) + 6

Divisibility:

Let 'a' and 'b' be any two integers with b ≠ 0 we say that b divides a if ∃ an integer c such that

$$a = bc$$

In this case 'b' is called divisor or factor of 'a' and 'a' is called multiple of 'b' and is denoted by $b \mid a$

e.g $2 \mid 4$ & a = 6 , b = 2 $\Rightarrow$ 6 = 3(2)

Remark:

If there does not exist such integer 'c' we say be does not divide 'a' and is denoted by $b \nmid a$. e.g. $2 \nmid 5$

Remarks:

(i) Every integer a ≠ 0 divides 0 i.e $a \mid 0$
(ii) 1 divides every integer a i.e $1 \mid -5$ $\Rightarrow$ -5 = -5(1)
(iii) Every integer divide itself i.e $a \mid a$
(iv) If $a \mid b$ and $b \mid c$ then $a \mid c$ e.g. $2 \mid 4$ and $4 \mid 8$ then $2 \mid 8$
(v) If $a \mid b$ then $a \mid bx$ where $x \in Z$
(vi) If $a \mid b$ and $a \mid c$ the $a \mid bx+cy$
i.e. $a \mid b \Rightarrow a \mid bx$ and $a \mid c \Rightarrow a \mid cy$ then $a \mid bx+cy$
(vii) If $a \mid b$ and b≠ 0 then $|a| \leq |b|$ i.e. $2 \mid -6 \Rightarrow |2| \leq |-6|$

Common Divisor:

Let 'a' and 'b' be any two integers at least one of them is non-zero and integer 'c' is said to be common divisor of 'a' and 'b' if $c \mid a$ and $c \mid b$.

e.g. 4 is a common divisor of 8 and 12

Lecture # 02

Greatest Common Divisor:

Let ‘a’ and ‘b’ be any two integers at least one of them is non-zero. A positive integer ‘d’ is called Greatest Common Divisor (G.C.D) of ‘a’ and ‘b’ if

(i) $d \mid a$ and $d \mid b$
(ii) For any other common divisor (say) c of a and b the $c \mid d$

“It is also known as Highest Common Factor (H.C.F)

Notation:

The greatest common divisor of a and b is denoted by

G.C.D of a and b = (a,b) = d

Remark:

(i) If $a \mid b$ then (a,b) = a
e.g. (2,4) = 4
and (0,0) = not exist
(ii) $(a,b) = (|a|, |b|)$

Theorem:

Let ‘a’ and ‘b’ be any two integers at least one of them is non-zero. Then g.c.d of ‘a’ and ‘b’ exists and is unique.

Proof: Let S be a non-empty set of positive integers of the form ‘ma+nb’ where $m,n \in Z$.

$$S = \{ma+nb \; ; \; m,n \in Z\}$$

Then by Well ordering principle S contain a smallest element (say) ‘d’ where $d = ax + by \; ; \; x,y \in z$. Now we show that g.c.d of ‘a’ and ‘b’ = (a,b) = d

(i) Observed that d is positive because $d \in S$
(ii) Since $d \leq a$
then by division algorithm $\exists$ unique integers q and r such that
$a = qd+r \quad \ldots(1) \qquad$ where $\qquad 0 \leq r < d$
$\Rightarrow a = q(ax + by) + r$

$\Rightarrow a = aqx+bqy+r$

$\Rightarrow r = a-aqx-bqy$

$\Rightarrow r = a(1-qx)+(-qy)b$

$\Rightarrow r = pa+sb \quad$ where $p = 1-qx \quad , s = -qy$

$\Rightarrow r \in S$

For g.c.d

(i) $d \geq 0$

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

(iii) For any other common divisor c of a & b then $c|d$

Which is only possible if r = 0 put in (1)

$$a = qd$$

$$d|a$$

Similarly, $\quad d|b$

(iii) Let 'c' be any integer such that $c|a$ and $c|b$. Then
$c|ax$ and $c|by$
$\Rightarrow c|ax+by$
$\Rightarrow c|d \qquad \therefore d = ax+by$
Since d satisfy all conditions of definition of g.c.d. Therefore
$(a,b) = d$

Uniqueness:

Suppose that d_1 and d_2 (if possible) are g.c.d's of a and b.

If d_1 is g.c.d then by definition

$$d_2 | d_1$$

$$\Rightarrow \quad d_2 \leq d_1 \quad .....(ii)$$

Similarly, if d_2 is g.c.d then by definition

$$d_1 | d_2$$

$$\Rightarrow \quad d_1 \leq d_2 \quad ...(iii)$$

From (ii) and (iii)

$$d_1 = d_2$$

Which show the uniqueness

Lecture # 03

Remark:

If $(a,b) = d$ then $\exists$ integer x and y such that

$$ax+by = d$$

Co-prime integer or Relatively prime integer:

Two integers 'a' and 'b' are said to be co-prime integer if $(a,b) = 1$

Example: Find $(4,9) = ?$

Solution: 4 and 9 are relatively prime

$a = 9$, $b = 4$

$9 = 2(4) + 1$

$\Rightarrow (4,9) = 1$

$9x+4y = 1$ $\qquad\because ax+by=1$

$1 = 9 - 4(2)$

$1 = 9(1) + 4(-2)$

$\Rightarrow x = 1$ and $y = -2$

ان سوالات میں بڑے نمبر کو a اور چھوٹے نمبر کو b اور پھر division algorithm

لگانا ہے۔ $a=qb+r$; $1\le r\le |b|$

جو g.c.d آئے گا اس کو دیئے گئے اعداد کے linear combination میں لکھنا ہے

اور پھر x اور y کی قیمت معلوم کرنی ہے

Question: $(-9,4) = 4$

Solution: $a = 4$, $b = 4$

$9 = 2(4) + 1$

$\Rightarrow (-9,4) = 1$

In linear combination

$-9x+4y = 1$

$1 = -9(-1)+4(-2)$

$\Rightarrow x = -1$ and $y = -2$

Question: (5,12) = ?

Solution: a = 12 , b = 5

12 = 2(5) + 2 ____(i)

$$\begin{array}{r|l} & 2 \\ 5 & 12 \\ & \underline{10} \\ & 2 \end{array}$$

Here a = 5 , b =2

5 = 2(2) +1

i.e. (5,12) = 1

Now in linear combination

12x+5y = 1

1 = 5 – 2(2)

= 5–2[12–2(5)] from (i)

= 5 – 24 +4(5)

= 5(5) – 24

1 = 12(–2) + 5(5)

⇒ x = –2 and y = 5

Question: (13,6) = ?

Solution: a = 13 , b = 6

13 = 2(6) + 1

i.e (13 ,6) = 1

Now in linear combination

13x+6y = 1

1 = 13–6(2)

1 = 13(1)+6(–2)

⇒ x = 1 and y = –2

Question: (24,7) = ?

Solution: a = 24 , b = 7

$$\begin{array}{r|l} & 3 \\ 7 & 24 \\ & \underline{21} \\ & 3 \end{array}$$

24 = 3(7) + 3 ______(i)

7 = 2(3) +1

(24,7) = 1

Now in linear combination

24x+7y = 1

1 = 7 – 2(3)

= 7 – 2[24 – 3(7)] from (i)

= 7 – 2 (24) + 6(7)

1 = 24(–2) + 7(7)

$\Rightarrow$ x = –2 , y = 7

Question: (34,4) = ?

Solution: a = 34 , b = 4

جب g.c.d = zero آرہا ہو تو اس سے پہلے والا جواب اس کا g.c.d ہو گا۔

34 = 8(4) + 2

4 = 2(2) + 0

$\Rightarrow$ (34,4) = 2

Now in linear combination

34x + 4y = 2

2 = 34 – 8(4)

2 = 34(1) + 4(–8)

$\Rightarrow$ x = 1 and y = –8

Question: $(76,8) = ?$

Solution: $a = 76$, $b = 8$

$76 = 9(8) + 4$

$8 = 4(2) + 0$

$\Rightarrow (76,8) = 4$

Now in linear combination

$4 = 76 - 9(8)$

$4 = 76(1) + 8(-9)$

$\Rightarrow x = 1$ and $y = -9$

Question: $(59,11) = ?$

Solution: $a = 59$, $b = 11$

$59 = 5(11) + 4$ _______(i)

$11 = 2(4) + 3$ _______(ii)

$4 = 1(3) + 1$ _______(iii)

$\Rightarrow (59,11) = 1$

Now in linear combination

$1 = 4 - 3(1)$

$1 = 4 - (1)[11 - 2(4)]$ from (ii)

$1 = 4 - 11 + 2(4)$

$1 = -11 + 3(4)$

$1 = -11 + 3[59 - 5(11)]$ $\Rightarrow 1 = -11 + 3(59) - 15(11)$

$1 = -16(11) + 3(59)$ $\Rightarrow 1 = 59(3) - 11(16)$

$1 = 59(3) + 11(-16)$

$\Rightarrow x = 3$ and $y = -16$

Question: $(37,47) = ?$

Solution: $a = 47$ and $b = 37$

$47 = 1(37) + 10$ _____(i)

$37 = 3(10) + 7$ _____(ii)

$10 = 1(7) + 3$ _____(iii)

$7 = 2(3) + 1$ _____(iv)

$\Rightarrow (37,47) = 1$

Now in linear combination

$47x+37y = 1$

$1 = 7 - 3(2)$

$1 = 7 - 2[10 - 1(7)]$ from (iii)

$1 = 7 - 2(10) + 2(7)$

$1 = 3(7) - 2(10)$

$1 = -2(10) + 3[37-3(10)]$ from (ii)

$1 = -2(10) + 3(37) - 9(10)$

$1 = 3(37) - 11(10)$

$1 = 3(37) - 11[47-1(37)]$ from (i)

$1 = 3(37) - 11(47) + 11(37)$

$1 = 14(37) - 11(47)$

$1 = 47(-11) + 37(14)$

$\Rightarrow x = -11$ and $y = 14$

Example: Find $(256, 1166) = ?$

Solution: $a = 1166$, $b = 256$

$1166 = 4(256) + 142$ ____(i)

$256 = 1(142) + 114$ ___(ii)

$142 = 1(114) + 28$ ___(iii)

$114 = 4(28) + 2$ ___(iv)

$28 = 14(2) + 0$

$\Rightarrow \quad (256, 1166) = 2$

Now in linear combination

$1166x + 256y = 2$

$2 = 114 - 4(28)$

$2 = 114 - 4[142 - 1(114)]$ from (iii)

$2 = 114 - 4(142) + 4(114)$

$2 = -4(142) + 5(114)$

$2 = -4(142) + 5[256 - 1(142)]$ from (ii)

$2 = -4(142) + 5(256) - 5(142)$

$2 = 5(256) - 9(142)$

$2 = 5(256) - 9[1166 - 4(256)]$ from (i)

$2 = 5(256) - 9(1166) + 36(256)$

$2 = 1166(-9) + 41(256)$

$2 = 1166(-9) + 256(41)$

$\Rightarrow x = -9$ and $y = 41$

Lecture # 04

Theorem:

Let ‘a’ and ‘b’ be any two integers and ‘k’ be any integer then $(ka,kb) = k(a,b)$

Proof:

Let $(a,b) = d$

And $(ka,kb) = t$

Then we show that

$$kd = t$$

Since $(a,b) = d$

Then there exist integers u and v such that

$$au + bv = d$$

$\Rightarrow \quad u(ka) + v(kb) = kd \quad$ ____(i)

We suppose

$(ka,kb) = t$

$\Rightarrow \quad t|ka \quad , \quad t|kb$

$\Rightarrow \quad t|u(ka) \quad , \quad t|v(kb)$

$\Rightarrow \quad t|u(ka)+v(kb)$

By definition of divisibility

$\Rightarrow \quad u(ka)+v(kb) = tr$

Put in (i)

$$kd = tr$$

$\Rightarrow \quad t|kd \quad$ by def. of divisibility

$\Rightarrow \quad t \le kd \quad$ _____(ii)

Now as (a,b) = d

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

$\Rightarrow$ $kd|ka$ and $kd|kb$

$\Rightarrow$ $kd|(ka,kb)$

$\Rightarrow$ $kd|t$

$\Rightarrow$ $kd \leq t$ ______(iii)

From (ii) and (iii)

$kd = t$

or $t = kd$

$(ka,kb) = k(a,b)$ proved

Corollary:

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

Solution:

Given that (a,b) = d

$\Rightarrow$ $\left(\frac{ad}{d},\frac{bd}{d}\right) = d$

By using above theorem (ka,kb) = k(a,b)

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

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

Theorem: If $a|c$ and $b|c$ and (a,b) = 1 then show that $ab|c$

Proof: Since $a|c$ and $b|c$

So, by def. of divisibility $\exists$ integers x and y such that

$c = ax$ & $c = by$

Also given that (a,b) = 1 then $\exists$ integers u and v such that

$au + bv = 1$

$\Rightarrow \quad acu + bcv = c$

$a(by)\,u + b(ax)\,v = c$

$ab(yu+xv) = c$

$\Rightarrow \quad ab(z) = c \qquad \because\ z = yu + xv$ integer

Or $\quad c = ab(z)$

$\Rightarrow \quad ab\,|\,c \qquad \because$ *by def* .of divisibility

Proved.

Theorem: If $a\,|\,bc$ and $(a,b) = 1$ then $a\,|\,c$

Proof: Given that $(a,b) = 1$

Then $\exists$ integers x and y such that

$ax + by = 1$

$\Rightarrow \quad acx + bcy = c$

As $\quad a\,|\,a \quad \Rightarrow \quad a\,|\,acx$

$\Rightarrow \quad a\,|\,bc$ (given)

$\Rightarrow \quad a\,|\,bcy$

$\Rightarrow \quad a\,|\,acx+bcy$

$\Rightarrow \quad a\,|\,c \qquad$ Proved

Lecture # 05

Common Multiple:

Let 'a' and 'b' be any two integers at least one of them is non-zero. An integer (either positive or negative) 'm' is called common multiple of 'a' and 'b' if $a|m$ and $b|m$.

Least common multiple (LCM):

Let 'a' and 'b' be any two integers at least one of them is non-zero. A positive integer 'm' is called least common multiple of 'a' and 'b' if

(i) $a|m$ and $b|m$

(ii) If 'c' is any other common multiple of 'a' and 'b' i.e. $a|c$ & $b|c$ then $m|c$.

Notation:

If least common multiple of 'a' and 'b' is 'm' we denote it as [a,b] = m

Remark: If $a|b$ then [a,b] = b

$n = P_1^{x_1} \times P_2^{x_2} \times P_3^{x_3} \times ......P_r^{x_r}$ *where* P_i's are prime number and $x_i > 0$

$\because \quad 12 = 2\times 2\times 3$

$12 = (2)^2 \times (3)^1$

$\because \quad 72 = 2\times 2\times 2\times 3\times 3$

$= (2)^3 \times (3)^2$

$P_1 = 2, P_2 = 3$

$x_1 = 3, x_2 = 2$

$\because \quad 30 = 2\times 3\times 5$

$= (2)^1 \times (3)^1 \times (5)^1$

$P_1 = 2\ , P_2 = 3, P_3 = 5$

$x_1 = 1, x_2 = 1, x_3 = 1$

$n = P_1^{x_1} \times P_2^{x_2} \times P_3^{x_3} \times ......P_r^{x_r}$

$$n = \prod_{i=1}^{r} P_i^{x_i}$$

Theorem:

Let ‘a’ and ‘b’ be any two integers at least one of them is non-zero where $a = \prod_{i=1}^{r} P_i^{x_i}$, $b = \prod_{i=1}^{r} P_i^{y_i}$. Let $M_i = \max\{x_i, y_i\}$ then show that [a,b] = d where $d = \prod_{i=1}^{r} P_i^{M_i}$. Also show uniqueness of d.

Proof:

(i) Note that $d = \prod_{i=1}^{r} P_i^{M_i}$ is positive because all P_i are prime number and $M_i \geq 0$

(ii) Since $M_i = \max\{x_i, y_i\}$

$\Rightarrow x_i \leq M_i \quad and \quad y_i \leq M_i$

$\Rightarrow P^{x_i} \leq P^{M_i} \quad and \quad P^{y_i} \leq P^{M_i} \quad \forall\ i$

$\Rightarrow P^{x_i} \,\big|\, P^{M_i} \quad and \quad P^{y_i} \,\big|\, P^{M_i} \quad \forall\ i$

$\Rightarrow \prod_{i=1}^{r} P^{x_i} \,\Big|\, \prod_{i=1}^{r} P^{M_i} \quad and \quad \prod_{i=1}^{r} P^{y_i} \,\Big|\, \prod_{i=1}^{r} P^{M_i} \quad \forall\ i$

$\Rightarrow$ a|d and b|d

(iii) Let ‘c’ be any other common multiple of ‘a’ and ‘b’ where $c = \prod_{i=1}^{r} P_i^{t_i}$

Since a|c and b|c

i.e. $\prod_{i=1}^{r} P^{x_i} \,\Big|\, \prod_{i=1}^{r} P^{t_i} \quad and \quad \prod_{i=1}^{r} P^{y_i} \,\Big|\, \prod_{i=1}^{r} P^{t_i} \quad \forall\ i$

$\Rightarrow x_i \leq t_i \quad and \quad y_i \leq t_i$

$\Rightarrow \max\{x_i, y_i\} \leq t_i \quad \forall i$

$\Rightarrow M_i \leq t_i \quad \forall i$

$\Rightarrow P^{M_i} \leq P^{t_i} \quad \forall\ i$

$\Rightarrow \prod_{i=1}^{r} P^{M_i} \,\Big|\, \prod_{i=1}^{r} P^{t_i} \quad \forall\ i$

$\Rightarrow$ d|c Hence [a,b] = d

Three conditions for L.C.M

(i) d is +ve
(ii) a|d & b|d
(iii) any integer c then d|c

Uniqueness:

Suppose that d_1 and d_2 (if possible) are L.C.M's of a and b

If d_1 is L.C.M then by definition

$$d_2 | d_1$$

$$\Rightarrow \; d_2 \le d_1 \qquad \_\_\_\_\_\text{(i)}$$

If d_2 is L.C.M then by definition

$$d_1 | d_2$$

$$\Rightarrow \; d_1 \le d_2 \qquad \_\_\_\_\_\text{(ii)}$$

From (i) & (ii)

$d_1 = d_2$ which show the uniqueness

Theorem:

Let 'a' and 'b' be any two integers at least one of them is non-zero then

(a,b) . [a,b] = ab

Proof:

Let d = (a,b) and m = [a,b]

$\Rightarrow$ $\exists$ integers r,s and integers u,v such that

a = dr , b = ds (r,s) = 1 ____(i)

and d = au+bv

Also m = [a,b]

$\Rightarrow$ $\exists$ integers t and w such that

m = at & m = bw ______(ii)

d = au+bv

md = m(au+bv)

md = mau + mbv

= bwau + atbv

md = ab (uw + tv)

$\Rightarrow$ ab | md ______(iii)

Also $\frac{ab}{d} = \frac{drb}{d} = rb \quad \because by\ (i)$

$\frac{ab}{d} = \frac{ads}{d} = sa \quad \because by\ (i)$

$a\left|\frac{ab}{d}\right.$, $b\left|\frac{ab}{d}\right.$; $that\ \frac{ab}{d}$ is a common multiple of ‘a’ and ‘b’.

$\Rightarrow m\left|\frac{ab}{d}\right. \quad or \quad md|ab$ _____(iv)

From (iii) and (iv)

md = ab

(a,b).[a,b] = ab

Corollary:

If (a,b) = 1 then [a,b] = ab

Proof:

We know that from above theorem

(a,b).[a,b] = ab

Given that (a,b) = 1

1.[a,b] = ab

$\Rightarrow$ [a,b] = ab

(i) [6,14] = ?

$14 = 2(6) + 2$

$6 = 3\ (2) + 0$

$\Rightarrow (6,14) = 2$

Now $(6,14).[6,14] = 6\times14$

$2\ .\ [6,14] = 6\times14$

$[6,14] = 42$

If $[a,b,c]=\left[[a,b],c\right]$

(ii) [6,14,8] = ?

$[6,14,8]=\left[[6,14],8\right]$

First, we find [6,14]

$14 = 2(6) + 2$

$6 = 3\ (2) + 0$

$\Rightarrow (6,14) = 2$

Now $(6,14).[6,14] = 6\times14$

$2\ .\ [6,14] = 6\times14$

$[6,14] = 42$

$[6,14,8]=\left[[6,14],8\right]=[42,8]$

Now $42 = 5(8) + 2$

$8 = 4(2) + 0$ i.e. $(42,8) = 2$

$(42,8)\ .\ [42,8] = 42\times8$

$2\ .\ [42,8] = 42\times8 \quad\Rightarrow\quad [42,8]=\dfrac{42\times8}{2}=168$

$\Rightarrow [6,14,8] = 168$

Lecture # 06

Linear Indeterminate equations or Linear Diophantine equations:

An equation with two or more than two variables is called Linear indeterminate equations or Linear Diophantine equations.

e.g. $$ax + by = c$$

or $$\alpha x + \beta y + \gamma z = \delta$$

$x + 7y = 31$ is satisfied by $x = 21$, $y = 1$ also by $x = 3$, $y = 4$ and also by $x = 17$, $y = 2$ so we have infinite many solutions.

On the contrary the Diophantine equation $15x + 51y = 14$ or $2x + 4y = 5$ has no solutions. Thus, we may ask when can a given Diophantine have solutions? We give it in our next theorem.

Theorem: Let $a(\neq 0)$, $b(\neq 0)$ and 'c' be any integer then the equation

$$ax + by = c \qquad \_\_\_\_\text{(i)}$$

has a solution iff $d|c$ where $d = (a,b)$. If (x_0, y_0) is a solution of eq (i) then general solution of eq (i) is given by $x' = x_0 + \frac{b}{d}t$, $y' = y_0 - \frac{a}{d}t$ where $t \in Z$

Proof:

Suppose eq (i) has a solution (say) (x_0, y_0) then

$$ax_0 + by_0 = c \qquad \_\_\_\_\text{(ii)}$$

We are to show that $d|c$

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

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

$\Rightarrow$ $d|ax_0$ and $d|by_0$

$\Rightarrow$ $d|ax_0 + by_0$

$\Rightarrow$ $d|c$ by eq (ii)

Conversely:

Suppose d|c then by definition of divisibility there exist integer t such that

$$c = dt$$

Now as $d = (a,b)$

$\Rightarrow$ $\exists$ integers u and v such that

$$au + bv = d$$

$\Rightarrow$ $a(ut) + b(vt) = dt$ multiplying by t

$\Rightarrow$ $ax_0 + by_0 = c$

$where\ \ x_0 = ut\ \ ,\ y_0 = vt\ ,\ c = dt$

$\Rightarrow$ (x_0, y_0) is solution of eq (i)

Now suppose (x', y') is another solution of eq (i). Then

$$ax' + by' = c \qquad \text{\_\_\_\_\_(iii)}$$

Subtracting eq (ii) from eq (iii)

$$a(x' - x_0) + b(y' - y_0) = 0$$

$$\Rightarrow \qquad a(x' - x_0) = -b(y' - y_0) \qquad \text{\_\_\_\_\_(iv)}$$

As $d = (a,b)$

$\Rightarrow$ d|a and d|b

$\Rightarrow$ $\exists$ integers 'r' and 's' such that

$a = rd$, $b = sd$ where $(r,s) = 1$

Put the values of 'a' and 'b' in eq (iv)

$$rd(x' - x_0) = -sd(y' - y_0)$$

$$r(x' - x_0) = -s(y' - y_0) \qquad \text{\_\_\_\_\_\_(v)}$$

From (v) we have

$$s \mid r\left(x' - x_0\right)$$

But (r,s) = 1 (relatively prime) holds when

$$s \mid \left(x' - x_0\right)$$

$$\Rightarrow \quad x' - x_0 = st$$

$$\Rightarrow \quad x' = x_0 + st$$

$$\Rightarrow \quad x' = x_0 + \frac{b}{d}t \qquad \because b = sd \Rightarrow s = \frac{b}{d}$$

Again, from eq (v)

$$-r \mid s\left(y' - y_0\right)$$

But (r,s) = 1 holds when

$$r \mid -\left(y' - y_0\right)$$

$$\Rightarrow \quad -\left(y' - y_0\right) = rt$$

$$\Rightarrow \quad -y' + y_0 = rt$$

$$\Rightarrow \quad y' = y_0 - rt$$

$$\Rightarrow \quad y' = y_0 - \frac{a}{d}t \qquad \because a = rd \Rightarrow r = \frac{a}{d}$$ proved

Question: Find the general solution of 2x + 5y = 6

Solution:

Since (2,5) = 1 and 1 | 6

Solution of the given equation exists

Now $5 = 2(2) + 1$

$\Rightarrow \quad 1 = 5 - 2(2)$

Or $\quad 2(-2) + 5\ (1) = 1$

Multiplying by 6

$2(-12) + 5(6) = 6$

$$\Rightarrow \quad x_0 = -12\ ,\ y_0 = 6$$

Now for general solution

$$\Rightarrow \quad x' = x_0 + \frac{b}{d}t$$

$$x' = -12 + \frac{5}{1}t$$

$$x' = -12 + 5t$$

$$y' = y_0 - \frac{a}{d}t$$

$$y' = 6 - \frac{2}{1}t$$

$$y' = 6 - 2t$$

To check

When t = 1 $\Rightarrow \quad x' = -7\ ,\ y' = 4$

$2x + 5y = 6$

$2(-7) + 5(4) = -14+20 = 6$

Satisfied for all value of t.

Question: Find the general solution of $47x + 37y = 15$

Solution: Since $(47,37) = 1$ and $1 \mid 15$ so, solution of the given equation exists

Now
$$47 = 1(37) + 10 \quad \text{\_\_\_\_\_(i)}$$
$$37 = 3(10) + 7 \quad \text{\_\_\_\_\_(ii)}$$
$$10 = 1(7) + 3 \quad \text{\_\_\_\_\_(iii)}$$
$$7 = 2(3) + 1 \quad \text{\_\_\_\_\_(iv)}$$

Now
$$1 = 7 - 2(3)$$
$$1 = 7 - 2[10 - 1(7)] \quad \text{from (iii)}$$
$$1 = 7 - 2(10) + 2(7)$$
$$1 = 3(7) - 2(10)$$
$$1 = 3[37 - 3(10)] - 2(10) \quad \text{from (ii)}$$
$$1 = 3(37) - 9(10) - 2(10)$$
$$1 = 3(37) - 11(10)$$
$$1 = 3(37) - [47 - 1(37)] \quad \text{form (i)}$$
$$1 = 14(37) - 11(47)$$

Or
$$47(-11) + 37(14) = 1$$
$$47(-165) + 37(210) = 15$$
$$\Rightarrow \quad x_0 = -165 \ , \ y_0 = 210$$

For G.S
$$x' = x_0 + \frac{b}{d}t \quad , \quad y' = y_0 - \frac{a}{d}t$$
$$x' = -165 + 37t \quad , \quad y' = 210 - 47t$$

is the required general solution.

Question: Find the general solution of $85x + 60y = 20$

Solution: Since $(85, 60) = 1$ and $5 \mid 20$ so, solution of the given equation exists

Now

$$85 = 1(60) + 25 \qquad \text{\_\_\_\_\_(i)}$$

$$60 = 2(25) + 10 \qquad \text{\_\_\_\_\_(ii)}$$

$$25 = 2(10) + 5 \qquad \text{\_\_\_\_\_(iii)}$$

$$10 = 2(5) + 0$$

Now

$$\begin{aligned} 5 &= 25 - 2(10) \\ &= 25 - 2[60 - 2(25)] \qquad \text{from (ii)} \\ &= 25 - 2(60) + 4(25) \\ &= 5(25) - 2(60) \\ &= 5[85 - 1(60)] - 2(60) \qquad \text{from (i)} \\ &= 5(85) - 5(60) - 2(60) \end{aligned}$$

$$5 = 5(85) - 7(60)$$

Or $\quad 85(5) + 60(-7) = 5$

$$85(20) + 60(-28) = 20$$

$$\Rightarrow \quad x_0 = 20 \ , \ y_0 = -28$$

For G.S

$$x' = x_0 + \frac{b}{d}t \quad , \quad y' = y_0 - \frac{a}{d}t$$

$$x' = 20 + 12t \quad , \quad y' = -28 - 17t$$

is the required general solution.

For check t = 1

$$x' = 32 \ , \ y' = -45 \quad \Rightarrow \quad 85(32) + 60(-45) = 20$$

Question: Find the general solution of 34x + 7y = 2

Solution: Since (34, 7) = 1 and $1 \mid 2$ so, solution of the given equation exists

Now $34 = 4(7) + 6$ ______(i)

$7 = 1(6) + 1$ ______(ii)

Now $1 = 7 - 1(6)$

$= 7 - 1[34 - 4(7)]$ from (i)

$= 7 - 1(34) + 4(7)$

Or $34(-1) + 7(5) = 1$

$34(-2) + 7(10) = 2$

$\Rightarrow \quad x_0 = -2 \;,\; y_0 = 10$

For G.S

$$x' = x_0 + \frac{b}{d}t \quad , \quad y' = y_0 - \frac{a}{d}t$$

$$x' = -2 + 7t \quad , \quad y' = 10 - 34t$$

is the required general solution.

For check t = 1

$$x' = 5 \,,\; y' = -24 \quad \Rightarrow \quad 34(5) + 7(-24) = 2$$

Lecture # 07

Theorem: Let a(≠0) , b(≠0) and 'c' be any integer then the equation

$$ax-by = c \qquad \text{\_\_\_(i)}$$

has a solution iff d|c where d = (a,b). If (x_0, y_0) is a solution of eq (i) then general solution of equation is given by

$$x' = x_0 + \frac{b}{d}t \qquad and \qquad y' = y_0 + \frac{a}{d}t \qquad where\ t \in Z$$

Proof:

Suppose eq (i) has a solution (say) (x_0, y_0) then

$$ax_0 - by_0 = c \qquad \text{\_\_\_\_(ii)}$$

We are to show that d|c

Since (a,b) = d (given)

⇒ d | a and d|b

⇒ $d|ax_0$ and $d|by_0$

⇒ $d|ax_0 - by_0$

⇒ d|c by eq (ii)

Conversely:

Suppose d|c then by definition of divisibility there exist integer t such that

$$c = dt$$

Now as d = (a,b)

⇒ ∃ integers 'u' and 'v' such that

$$au + bv = d$$

⇒ a(ut) + b (vt) = dt multiplying by t

⇒ a(ut) – b(–vt) = dt

$$\Rightarrow \quad ax_0 - by_0 = c$$

$$where \;\; x_0 = ut \;,\; y_0 = vt \,,\; c = dt$$

$\Rightarrow \quad (x_0, y_0)$ is solution of eq (i)

Now suppose $\left(x', y'\right)$ is another solution of eq (i). Then

$$ax' - by' = c \qquad \_\_\_\_\_\text{(iii)}$$

Subtracting eq (ii) from eq (iii)

$$a\left(x' - x_0\right) - b\left(y' - y_0\right) = 0$$

$$\Rightarrow \quad a\left(x' - x_0\right) = b\left(y' - y_0\right) \qquad \_\_\_\_\_\text{(iv)}$$

As d = (a,b)

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

$\Rightarrow$ $\exists$ integers ‘r’ and ‘s’ such that

a = rd , b = sd where (r,s) = 1

Put the values of ‘a’ and ‘b’ in eq (iv)

$$rd\left(x' - x_0\right) = sd\left(y' - y_0\right)$$

$$r\left(x' - x_0\right) = s\left(y' - y_0\right) \qquad \_\_\_\_\_\_\text{(v)}$$

From (v) we have

$$s \,\big|\, r\left(x' - x_0\right)$$

But (r,s) = 1 (relatively prime) holds when

$$s \,\big|\, \left(x' - x_0\right)$$

$$\Rightarrow \quad x' - x_0 = st$$

$$\Rightarrow \quad x' = x_0 + st$$

$$\Rightarrow \qquad x' = x_0 + \frac{b}{d}t \qquad \because b = sd \Rightarrow s = \frac{b}{d}$$

Again, from eq (v)

$$r \mid s\left(y' - y_0\right)$$

But (r,s) = 1 holds when

$$r \mid \left(y' - y_0\right)$$

$$\Rightarrow \qquad \left(y' - y_0\right) = rt$$

$$\Rightarrow \qquad y' = y_0 + rt$$

$$\Rightarrow \qquad y' = y_0 + \frac{a}{d}t \qquad \because a = rd \Rightarrow r = \frac{a}{d} \quad \text{proved}$$

Question: Find the general solution of $8x - 15y = 20$

Solution: Since $(8, 15) = 1$ and $1 \mid 20$ so, solution of the given equation exists

Now $15 = 1(8) + 7$

$8 = 1(7) + 1$

And $1 = 8 - 1(7)$

$= 8 - 1[15 - 1(8)]$

$= 8 - 1(15) + 1(8)$

$= 2(8) - 1(15)$

$1 = 8(2) - 15(1)$

× by 20 $8(40) - 15(20) = 20$

$$\Rightarrow \qquad x_0 = 40 \;,\; y_0 = 20$$

For G.S $\quad x' = x_0 + \frac{b}{d}t \quad , \quad y' = y_0 + \frac{a}{d}t$

$$x' = 40 + 15t \quad , \quad y' = 20 + 8t$$

For check $\quad t = 1$

$$x' = 55 \quad , \quad y' = 28$$

$$8(55) - 15(28) = 20$$

Question: Find the general solution of $67x - 45y = 131$

Solution: Since $(67, 45) = 1$ and $1 \mid 131$ so, solution of the given equation exists

Now $\quad 67 = 1(45) + 22$

$$45 = 2(22) + 1$$

And $\quad 1 = 45 - 2(22)$

$$= 45 - 2[67 - 1(45)]$$

$$= 45 - 2(67) + 2(45)$$

$$1 = 3(45) - 2(67)$$

Or $\quad 67(-2) - 45(-3) = 1$

$\times$ by 131 $\quad 67(-262) - 45(-393) = 131$

$$\Rightarrow \quad x_0 = -262 \ , \ y_0 = -393$$

For G.S $\quad x' = x_0 + \frac{b}{d}t \quad , \quad y' = y_0 + \frac{a}{d}t$

$$x' = -262 + 45t \quad , \quad y' = -393 + 67t$$

For check $\quad t = 1$

$$x' = -217 \quad , \quad y' = -326$$

$$67(-217) - 45(-326) = 131$$

Question: If the cost of an apple is Rs.8 and cost of mango is Rs. 15 How many minimum (least) number of apples can bought from rupees 200.

Solution: Let x represent the number of apple and y represent the number of mangoes. Then

$$8x+15y = 200$$

Since $(8,15) = 1$ and $1|200$ so, solution of the given equation exists

Now $15 = 1(8) + 7$

$8 = 1(7) + 1$

And $1 = 8 - 1(7)$

$= 8 - 1[15 - 1(8)]$

$= 8 - 1(15) + 1(8)$

$1 = 2(8) - 1(15)$

Or $8(2) + 15(-1) = 1$

$\times$ by 200 $8(400) + 15(-200) = 200$

$\Rightarrow \quad x_0 = 400 \ , \ y_0 = -200$

For G.S $x' = x_0 + \frac{b}{d}t \quad , \quad y' = y_0 - \frac{a}{d}t$

$x' = 400 + 15t \quad , \quad y' = -200 - 8t$

Put $t = -26$ $\quad x' = 400 + 15(-26) \quad , \quad y' = -200 - 8(-26)$

$x' = 10 \quad , \quad y' = 8$

To check $8(10) + 15(8) = 80 + 120 = 200$

Hence, we bought 10 apples from 200 rupees.

Lecture # 08

$-13 \div 5 = 2 \quad \text{Re}\,mainder$

$$5\overline{\left)\begin{array}{r} 2 \\ -13 \\ \underline{10} \\ -3 \end{array}\right.} \qquad\qquad 5\overline{\left)\begin{array}{r} 3 \\ -16 \\ \underline{15} \\ -1 \end{array}\right.}$$

R = 5 – 3 = 2 R = 5 – 1 = 4

Remainder < Divisor

Congruence:

Let ‘a’ and ‘b’ be any two integers and ‘m’ be a fixed positive integer. We say that ‘a’ is congruent to ‘b’ modulo ‘m’ if ‘m’ divides a – b and is denoted by

$$a \equiv b \pmod{m} \quad \_\_\_\_(i)$$

The relation (i) is called congruence ‘m’ is called modulus value of congruence ‘b’ is called remainder/residue of the congruence. If ‘m’ does not divides a – b we say that ‘a’ is incongruent to ‘b’ modulo ‘m’ and denoted by

$$a \not\equiv b \pmod{m}$$

Examples:

(i) a = 8 , b = 5 , m = 3

$3|8-5 \quad \Rightarrow \quad 3|3$

‘a’ is congruent to 5(mod3) or $8 \equiv 5 \pmod{3}$

(ii) a = 8 , b = –5 , m = 3

$3|8-(-5) = 3|8+5 \quad \Rightarrow \quad 3|13$

$8 \not\equiv -5 \pmod{3}$

(iii) a = 8 , b = –10 , m = 2

$2|8-(-10) = 2 \quad \Rightarrow \quad 2|8+10 = 2|18 \quad \Rightarrow \quad 8 \equiv -10 \pmod{3}$

(iv) $a = 8$, $b = -6$, $m = 2$

$$2 \mid 8 - (-6) = 2 \mid 8+6 \quad \Rightarrow \quad 2 \mid 14$$

$$8 \equiv -6 \pmod{2}$$

Theorem: Show that the relation of congruence between integers is an equivalence relation.

Proof:

(i) Reflexive: Let 'a' be any integer and 'm' be fix (positive) integer

Since $\quad m \mid a$

$\Rightarrow \quad m \mid a - a$

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

It means that relation of congruence between integer is reflexive.

(ii). Symmetric: Let 'a' and 'b' be any two integers and 'm' be a fix (positive) integer.

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

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

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

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

It means that relation of congruence between integers is symmetric.

(iii) Transitive: Let 'a', 'b' and 'c' be any integers and 'm' be any fix (positive) integer.

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

And $\quad b \equiv c \pmod{m}$

$\Rightarrow \quad m \mid a - b$ and $m \mid b - c$

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

$$\Rightarrow \qquad m \mid a-c$$

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

It means that relation of congruence between integers is transitive. Since the relation is reflexive, symmetric and transitive. Therefore, the relation is equivalence.

Equivalence Class:

Since the relation of congruence between integer is an equivalence relation therefore it partitions set of integers into classes these classes are called Equivalence classes.

Example: $m = 2$

$$[0] = \{x \mid x = 0 \pmod 2\}$$

$$= \{x \mid x \ \ (\mathrm{mod}\, 2 \mid x-0)\}$$

$$\Rightarrow [0] = \{\pm 0, \pm 2, \pm 4, \ldots.\}$$

And $$[1] = \{x \mid x = 1 \pmod 2\}$$

$$= \{x \mid x \ \ (\mathrm{mod}\, 2 \mid x-1)\}$$

$$\Rightarrow [1] = \{\pm 1, \pm 3, \pm 5, \ldots.\}$$

We note that

$$[0] \cap [1] = 0$$

And $$[0] \cup [1] = \mathbb{Z}$$

Lecture # 9

Partition:

Let A = {1,2,3,4} A_1 *and* A_2 are partition of A if

(i) $A_1 \cup A_2 = A$

(ii) $A_1 \cap A_2 = \phi$

(i) m = 2

$[0],[1]$ *are classes* $\because$ Remainder 0,1

$$[0]=\{x \mid x \equiv 0 \pmod 2\}$$

$$[0]=\{x \mid 2 \mid x-0\}$$

$$[0]=\{0,\pm 2,\pm 4,\pm 6,......\}$$

$$[1]=\{x \mid x \equiv 1 \pmod 2\}$$

$$[1]=\{x \mid 2 \mid x-1\}$$

$$[1]=\{\pm 1,\pm 3,\pm 5,......\}$$

$$[0]\cup[1]=\mathbb{Z}$$

$$[0]\cap[1]=\phi$$

(ii) m = 3

$[0],[1],[2]$

$$[0]=\{x \mid x \equiv 0 \pmod 3\}$$

$$[0]=\{x \mid 3 \mid x-0\}$$

$$[0]=\{0,\pm 3,\pm 6 \pm 9,......\}$$

$$[1]=\{x \mid x \equiv 1 \pmod 3\}$$

$$[1]=\{x \mid 3 \mid x-1\}$$

$$[1]=\{1,4,7,10,....,-2,-5,-8,-11,...\}$$

$[2]=\{x \mid x\equiv 2(\text{mod}\,3)\}$

$[2]=\{x \mid 3|x-2\}$

$[2]=\{2,5,8,11,....,-1,-4,-7,-10,...\}$

$[0]\cup[1]\cup[2]=\mathbb{Z}$

$[0]\cap[1]\cap[2]=\phi$

(iii) **m = 4**

$[0],[1],[2],[3]$

$[0]=\{x \mid x\equiv 0(\text{mod}\,4)\}$

$[0]=\{x \mid 4|x-0\}$

$[0]=\{0,\pm 4,\pm 8\pm 12,......\}$

$[1]=\{x \mid x\equiv 1(\text{mod}\,4)\}$

$[1]=\{x \mid 4|x-1\}$

$[1]=\{1,5,9,13,17....,-3,-7,-11,-15,...\}$

$[2]=\{x \mid x\equiv 2(\text{mod}\,4)\}$

$[2]=\{x \mid 4|x-2\}$

$[2]=\{2,6,10,14,18....,-2,-6,-10,-14,-18...\}$

$[3]=\{x \mid x\equiv 3(\text{mod}\,4)\}$

$[3]=\{x \mid 4|x-3\}$

$[3]=\{3,7,11,15,19....,-1,-5,-9,-13,-17...\}$

$[0]\cup[1]\cup[2]\cup[3]=\mathbb{Z}$

$[0]\cap[1]\cap[2]\cap[3]=\phi$

(iv) **m = 5**

$[0],[1],[2],[3],[4]$

$[0]=\{x \mid x\equiv 0(\text{mod}\,5)\}$

$[0]=\{x \mid 5|x-0\}$

$[0]=\{0,\pm 5,\pm 10\pm 15,......\}$

$[1]=\{x \mid x\equiv 1(\text{mod}\,5)\}$

$$[1]=\{x \mid 5 \mid x-1\}$$
$$[1]=\{1,6,11,16,21....,-4,-9,-14,-19,...\}$$
$$[2]=\{x \mid x\equiv 2(\bmod 5)\}$$
$$[2]=\{x \mid 5 \mid x-2\}$$
$$[2]=\{2,7,12,17,22....,-3,-8,-13,-18,-23...\}$$
$$[3]=\{x \mid x\equiv 3(\bmod 5)\}$$
$$[3]=\{x \mid 5 \mid x-3\}$$
$$[3]=\{3,8,13,18,23....,-2,-7,-12,-17,-22...\}$$
$$[4]=\{x \mid x\equiv 4(\bmod 5)\}$$
$$[4]=\{x \mid 5 \mid x-4\}$$
$$[4]=\{4,9,14,19,24....,-1,-6,-11,-16,-21...\}$$
$$[0]\cup[1]\cup[2]\cup[3]\cup[4]=\mathbb{Z}$$
$$[0]\cap[1]\cap[2]\cap[3]\cap[4]=\phi$$

(v) **m = 6**

$$[0],[1],[2],[3],[4],[5]$$
$$[0]=\{x \mid x\equiv 0(\bmod 6)\}$$
$$[0]=\{x \mid 6 \mid x-0\}$$
$$[0]=\{0,\pm 6,\pm 12\pm 18,......\}$$
$$[1]=\{x \mid x\equiv 1(\bmod 6)\}$$
$$[1]=\{x \mid 6 \mid x-1\}$$
$$[1]=\{1,7,13,19,25....,-5,-11,-17,-23,...\}$$
$$[2]=\{x \mid x\equiv 2(\bmod 6)\}$$
$$[2]=\{x \mid 6 \mid x-2\}$$
$$[2]=\{2,8,14,20,26....,-4,-10,-16,-22,-28...\}$$
$$[3]=\{x \mid x\equiv 3(\bmod 6)\}$$
$$[3]=\{x \mid 6 \mid x-3\}$$

$[3]=\{3,9,15,21,27....,-3,-9,-15,-21,-27...\}$

$[4]=\{x|x\equiv 4(\text{mod}\,6)\}$

$[4]=\{x|\ 6|x-4\}$

$[4]=\{4,10,16,22,28....,-2,-8,-14,-20,-26...\}$

$[5]=\{x|x\equiv 5(\text{mod}\,6)\}$

$[5]=\{x|\ 6|x-5\}$

$[5]=\{5,11,17,23,29....,-1,-7,-13,-19,-25...\}$

$[0]\cup[1]\cup[2]\cup[3]\cup[4]\cup[5]=\mathbb{Z}$

$[0]\cap[1]\cap[2]\cap[3]\cap[4]\cap[5]=\phi$

(vi) **m = 7**

$[0],[1],[2],[3],[4],[5],[6]$

$[0]=\{x|x\equiv 0(\text{mod}\,7)\}$

$[0]=\{x|\ 7|x-0\}$

$[0]=\{0,\pm 7,\pm 14\pm 21,......\}$

$[1]=\{x|x\equiv 1(\text{mod}\,7)\}$

$[1]=\{x|\ 7|x-1\}$

$[1]=\{1,8,15,22,29....,-6,-13,-20,-27,...\}$

$[2]=\{x|x\equiv 2(\text{mod}\,7)\}$

$[2]=\{x|\ 7|x-2\}$

$[2]=\{2,9,16,23,30....,-5,-12,-19,-26,-33...\}$

$[3]=\{x|x\equiv 3(\text{mod}\,7)\}$

$[3]=\{x|\ 7|x-3\}$

$[3]=\{3,10,17,24,31....,-4,-11,-18,-25,-32...\}$

$[4]=\{x|x\equiv 4(\text{mod}\,7)\}$

$[4]=\{x|\ 7|x-4\}$

$[4]=\{4,11,18,25,32....,-3,-10,-17,-24,-31...\}$

$$[5]=\{x|x\equiv 5(\mathrm{mod}\,7)\}$$
$$[5]=\{x|\ 7|x-5\}$$
$$[5]=\{5,12,19,26,33....,-2,-9,-16,-23,-30...\}$$
$$[6]=\{x|x\equiv 6(\mathrm{mod}\,7)\}$$
$$[6]=\{x|\ 7|x-6\}$$
$$[6]=\{6,13,20,27,34....,-1,-8,-15,-22,-29...\}$$
$$[0]\cup[1]\cup[2]\cup[3]\cup[4]\cup[5]\cup[6]=\mathbb{Z}$$
$$[0]\cap[1]\cap[2]\cap[3]\cap[4]\cap[5]\cap[6]=\phi$$

(vii) **m = 8**

$$[0],[1],[2],[3],[4],[5],[6],[7]$$
$$[0]=\{x|x\equiv 0(\mathrm{mod}\,8)\}$$
$$[0]=\{x|\ 8|x-0\}$$
$$[0]=\{0,\pm 8,\pm 16\pm 24,......\}$$
$$[1]=\{x|x\equiv 1(\mathrm{mod}\,8)\}$$
$$[1]=\{x|\ 8|x-1\}$$
$$[1]=\{1,9,17,25,33....,-7,-15,-23,-31,...\}$$
$$[2]=\{x|x\equiv 2(\mathrm{mod}\,8)\}$$
$$[2]=\{x|\ 8|x-2\}$$
$$[2]=\{2,10,18,26,34....,-6,-14,-22,-30,-38...\}$$
$$[3]=\{x|x\equiv 3(\mathrm{mod}\,8)\}$$
$$[3]=\{x|\ 8|x-3\}$$
$$[3]=\{3,11,19,27,35....,-5,-13,-21,-29,-37...\}$$
$$[4]=\{x|x\equiv 4(\mathrm{mod}\,8)\}$$
$$[4]=\{x|\ 8|x-4\}$$
$$[4]=\{4,12,20,28,36....,-4,-12,-20,-28,-36...\}$$
$$[5]=\{x|x\equiv 5(\mathrm{mod}\,8)\}$$

$[5]=\{x|\ 8|x-5\}$

$[5]=\{5,13,21,29,37....,-3,-11,-19,-27,-35...\}$

$[6]=\{x|x\equiv 6(\mathrm{mod}\,8)\}$

$[6]=\{x|\ 8|x-6\}$

$[6]=\{6,14,22,30,38....,-2,-10,-18,-26,-34...\}$

$[7]=\{x|x\equiv 7(\mathrm{mod}\,8)\}$

$[7]=\{x|\ 8|x-7\}$

$[7]=\{7,15,23,31,39....,-1,-9,-17,-25,-33...\}$

$[0]\cup[1]\cup[2]\cup[3]\cup[4]\cup[5]\cup[6]\cup[7]=\mathbb{Z}$

$[0]\cap[1]\cap[2]\cap[3]\cap[4]\cap[5]\cap[6]\cap[7]=\phi$

(viii) **m = 9**

$[0],[1],[2],[3],[4],[5],[6],[7],[8]$

$[0]=\{x|x\equiv 0(\mathrm{mod}\,9)\}$

$[0]=\{x|\ 9|x-0\}$

$[0]=\{0,\pm 9,\pm 18\pm 27,......\}$

$[1]=\{x|x\equiv 1(\mathrm{mod}\,9)\}$

$[1]=\{x|\ 9|x-1\}$

$[1]=\{1,10,19,28,37....,-8,-17,-26,-35,...\}$

$[2]=\{x|x\equiv 2(\mathrm{mod}\,9)\}$

$[2]=\{x|\ 9|x-2\}$

$[2]=\{2,11,20,29,38....,-7,-16,-25,-34,-43...\}$

$[3]=\{x|x\equiv 3(\mathrm{mod}\,9)\}$

$[3]=\{x|\ 9|x-3\}$

$[3]=\{3,12,21,30,39....,-6,-15,-24,-33,-42...\}$

$[4]=\{x|x\equiv 4(\mathrm{mod}\,9)\}$

$[4]=\{x|\ 9|x-4\}$

$[4]=\{4,13,22,31,40....,-5,-14,-23,-32,-41...\}$

$[5]=\{x|x\equiv 5(\mathrm{mod}\,9)\}$

$[5]=\{x|\ 9|x-5\}$

$[5]=\{5,14,23,32,41....,-4,-13,-22,-31,-40...\}$

$[6]=\{x|x\equiv 6(\mathrm{mod}\,9)\}$

$[6]=\{x|\ 9|x-6\}$

$[6]=\{6,15,24,33,42....,-3,-12,-21,-30,-39...\}$

$[7]=\{x|x\equiv 7(\mathrm{mod}\,9)\}$

$[7]=\{x|\ 9|x-7\}$

$[7]=\{7,16,24,33,42....,-2,-11,-20,-29,-38...\}$

$[8]=\{x|x\equiv 8(\mathrm{mod}\,9)\}$

$[8]=\{x|\ 9|x-8\}$

$[8]=\{8,17,26,35,44....,-1,-10,-19,-28,-37...\}$

$[0]\cup[1]\cup[2]\cup[3]\cup[4]\cup[5]\cup[6]\cup[7]\cup[8]=\mathbb{Z}$

$[0]\cap[1]\cap[2]\cap[3]\cap[4]\cap[5]\cap[6]\cap[7]\cap[8]=\phi$

(ix) **m = 10**

$[0],[1],[2],[3],[4],[5],[6],[7],[8],[9]$

$[0]=\{x|x\equiv 0(\mathrm{mod}\,10)\}$

$[0]=\{x|\ 10|x-0\}$

$[0]=\{0,\pm 10,\pm 20\pm 30,......\}$

$[1]=\{x|x\equiv 1(\mathrm{mod}\,10)\}$

$[1]=\{x|\ 10|x-1\}$

$[1]=\{1,11,21,31,41....,-9,-19,-29,-39,...\}$

$[2]=\{x|x\equiv 2(\mathrm{mod}\,10)\}$

$[2]=\{x|\ 10|x-2\}$

$[2]=\{2,12,22,32,42....,-8,-18,-28,-38,-48...\}$

$$[3]=\{x \mid x\equiv 3(\text{mod}10)\}$$
$$[3]=\{x \mid 10|x-3\}$$
$$[3]=\{3,13,23,33,43....,-7,-17,-27,-37,-47...\}$$
$$[4]=\{x \mid x\equiv 4(\text{mod}10)\}$$
$$[4]=\{x \mid 10|x-4\}$$
$$[4]=\{4,14,24,34,44....,-6,-16,-26,-36,-46...\}$$
$$[5]=\{x \mid x\equiv 5(\text{mod}10)\}$$
$$[5]=\{x \mid 10|x-5\}$$
$$[5]=\{5,15,25,35,45....,-5,-15,-25,-35,-45...\}$$
$$[6]=\{x \mid x\equiv 6(\text{mod}10)\}$$
$$[6]=\{x \mid 10|x-6\}$$
$$[6]=\{6,16,26,36,46....,-4,-14,-24,-34,-44...\}$$
$$[7]=\{x \mid x\equiv 7(\text{mod}10)\}$$
$$[7]=\{x \mid 10|x-7\}$$
$$[7]=\{7,17,27,37,47....,-3,-13,-23,-33,-43...\}$$
$$[8]=\{x \mid x\equiv 8(\text{mod}10)\}$$
$$[8]=\{x \mid 10|x-8\}$$
$$[8]=\{8,18,28,38,48....,-2,-12,-22,-32,-42...\}$$
$$[9]=\{x \mid x\equiv 9(\text{mod}10)\}$$
$$[9]=\{x \mid 10|x-9\}$$
$$[9]=\{9,19,29,39,49....,-1,-11,-21,-31,-41...\}$$
$$[0]\cup[1]\cup[2]\cup[3]\cup[4]\cup[5]\cup[6]\cup[7]\cup[8]\cup[9]=\mathbb{Z}$$
$$[0]\cap[1]\cap[2]\cap[3]\cap[4]\cap[5]\cap[6]\cap[7]\cap[8]\cup[9]=\phi$$

Theorem: Let 'a', 'b', 'c' and 'd' be any integers and 'm' be fixed positive integer. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. Then

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

(ii) $a - c \equiv b - d \pmod{m}$

(iii) $ac \equiv bd \pmod{m}$

Proof: (i) Given

$$a \equiv b \pmod{m} \quad , \quad c \equiv d \pmod{m}$$

By definition of congruence

$$\Rightarrow \quad m \mid a - b \quad and \quad m \mid c - d$$

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

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

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

(ii). Given

$$a \equiv b \pmod{m} \quad , \quad c \equiv d \pmod{m}$$

By definition of congruence

$$\Rightarrow \quad m \mid a - b \quad and \quad m \mid c - d$$

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

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

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

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

(iii). Given

$$a \equiv b \pmod{m} \quad , \quad c \equiv d \pmod{m}$$

By definition of congruence

$$\Rightarrow \quad m|a-b \quad and \quad m|c-d$$

$$\Rightarrow \quad m|(a-b)c \quad and \quad m|(c-d)b$$

$$\Rightarrow \quad m|ac-bc \quad , \quad m|bc-bd$$

$$\Rightarrow \quad m|ac-bc+bc+bd$$

$$\Rightarrow \quad m|ac-bd$$

$$\Rightarrow \quad ac \equiv bd \pmod m$$

Theorem: If $a \equiv b \pmod m$ then show that $a^n \equiv b^n \pmod m$

Proof: Given

$$a \equiv b \pmod m$$

By definition of congruence

$$\Rightarrow \quad m|a-b$$

$$\Rightarrow \quad m|(a-b)\left(a^{n-1}+a^{n-2}b+....+b^{n-1}\right)$$

$$\Rightarrow \quad m|a^n-b^n$$

$$\Rightarrow \quad a^n \equiv b^n \pmod m$$

Remark: The converse of above theorem is not true in general.

e.g. a = 8 , b = 4 , m = 3 , n = 2

$$\Rightarrow \quad 8^2 \equiv 4^2 \pmod 3 \quad \text{But} \quad \Rightarrow \quad 8 \not\equiv 4 \pmod 3$$

Some formula's $a^2-b^2=(a-b)(a+b)$, $a^3-b^3=(a-b)\left(a^2+ab+b^2\right)$

$a^4-b^4=(a-b)\left(a^3+a^2b+ab^2+b^3\right)$, $a^5-b^5=(a-b)\left(a^4+a^3b+a^2b^2+ab^3+b^4\right)$,

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

Lecture # 10

Question: Find remainder when 2^{57} is divisible by 13

Solution: Since $64 \equiv -1 \pmod{13}$

$\Rightarrow 2^6 \equiv -1 \pmod{13}$

$\Rightarrow (2^6)^9 \equiv (-1)^9 \pmod{13}$

$\Rightarrow 2^{54} \equiv -1 \pmod{13}$

$\Rightarrow 2^3.2^{54} \equiv -1.2^3 \pmod{13}$

$\Rightarrow 2^{57} \equiv -8 \pmod{13}$

$\Rightarrow 2^{57} \equiv 5 \pmod{13} \qquad \because -8+13=5$

$\Rightarrow$ Remainder = 5

Question: Find remainder when 5^{48} is divisible by 12

Solution: Since $25 \equiv 1 \pmod{12}$

$\Rightarrow 5^2 \equiv 1 \pmod{12}$

$\Rightarrow (5^2)^{24} \equiv (1)^{24} \pmod{12}$

$\Rightarrow 5^{48} \equiv 1 \pmod{12}$

$\Rightarrow$ Remainder = 1

Question: Find remainder when 3^{101} is divisible by 10

Solution: Since $81 \equiv 1 \pmod{10}$

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

$\Rightarrow (3^4)^{25} \equiv (1)^{25} \pmod{10}$

$\Rightarrow 3^{100} \equiv 1 \pmod{10}$

$$\Rightarrow \quad 3.3^{100} \equiv 1.3(\bmod 10)$$

$$\Rightarrow \quad 3^{101} \equiv 3(\bmod 10)$$

$$\Rightarrow \text{Remainder} = 3$$

Question: Find remainder when 2^{47} is divisible by 3

Solution: Since $\quad 4 \equiv 1(\bmod 3)$

$$\Rightarrow \quad 2^2 \equiv 1(\bmod 3)$$

$$\Rightarrow \quad \left(2^2\right)^{23} \equiv (1)^{23}(\bmod 3)$$

$$\Rightarrow \quad 2^{46} \equiv 1(\bmod 3)$$

$$\Rightarrow \quad 2.2^{46} \equiv 1.2(\bmod 3)$$

$$\Rightarrow \quad 2^{47} \equiv 2(\bmod 3)$$

$$\Rightarrow \quad \text{Remainder} = 2$$

Question: Find the remainder when sum of the given series is divisible by 4

$$1!+2!+3!+\ldots+100!$$

Solution: Since $\quad 4! \equiv 0(\bmod 4)$

$$\Rightarrow \quad 4!+5!+6!+\ldots+100! \equiv 0(\bmod 4)$$

$$\Rightarrow \quad 1!+2!+3!+4!+\ldots+100! \equiv 1!+2!+3!(\bmod 4)$$

$$\Rightarrow \quad 1!+2!+3!+4!+\ldots+100! \equiv 9(\bmod 4)$$

$$\Rightarrow \quad 1!+2!+3!+4!+\ldots+100! \equiv 1(\bmod 4)$$

Question: Find the remainder when sum of the given series is divisible by 15

$$1!+2!+3!+\ldots+1000!$$

Solution: Since $5!\equiv 0\pmod{15}$

$$\Rightarrow\quad 5!+6!+....+1000!\equiv 0\pmod{15}$$

$$\Rightarrow\quad 1!+2!+3!+4!+5!+6!+....+1000!\equiv 1!+2!+3!+4!\pmod{15}$$

$$\Rightarrow\quad 1!+2!+3!+....+1000!\equiv 33\pmod{15}$$

$$\Rightarrow\quad 1!+2!+3!+....+1000!\equiv 3\pmod{15}$$

Remainder = 3

Lecture # 11

Theorem: If $a \equiv b \pmod{m}$ then show that $f(a) \equiv f(b) \pmod{m}$

Proof: Given that $a \equiv b \pmod{m}$ ___(i)

$$\Rightarrow ax \equiv bx \pmod{m} \quad \_\_\_(ii)$$

$$\Rightarrow ax^2 \equiv bx^2 \pmod{m} \quad \_\_\_(iii)$$

. .

. .

. .

$$\Rightarrow ax^{n-1} \equiv bx^{n-1} \pmod{m} \quad \_\_\_(iv)$$

From (i) , (ii) , (iii) and (iv) we have

$$a + ax + ax^2 + \ldots + ax^{n-1} \equiv b + bx + bx^2 + \ldots + bx^{n-1}$$

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

$$\because f(a) = a_0 + a_1x + a_2x^2 + \ldots. + a_{n-1}x^{n-1}$$

Theorem: If $a \equiv b \pmod{m_1}$ *and* $a \equiv b \pmod{m_2}$ then show that $a \equiv b \pmod{< m_1, m_2 >}$ where $< m_1, m_2 >$ is called L.C.M of x_1, x_2

Proof: Since $a \equiv b \pmod{m_1}$ *and* $a \equiv b \pmod{m_2}$

$$\Rightarrow m_1 | a - b \quad , \quad m_2 | a - b$$

Multiplying by m_2

$$\Rightarrow m_1 m_2 | m_2 (a - b)$$

$$\Rightarrow < m_1, m_2 > | (a - b)$$

$$\Rightarrow a \equiv b \pmod{< m_1, m_2 >}$$

Complete Residue System (CRS)

Let $\{a_1, a_2, ..., a_k\}$ be a set of integers and m be a fixed positive integer we say that the set $\{a_1, a_2, ..., a_k\}$ forms a complete Residue system modulo m (denoted by CRS (mod m)) if

(i) $\Rightarrow \quad a_i \not\equiv a_j \pmod{m} \quad \forall\ i \neq j$

(ii) For any integer n there exist a unique a_i such that $n \equiv a_i \pmod{m}$

Example: Check the set forms CRS $\{11,12,13\}$, m = 3

Solution: (i) Condition

$$11 \not\equiv 12 \pmod{3} \qquad \because 3 \nmid 11-12$$

$$12 \not\equiv 13 \pmod{3} \qquad \because 3 \nmid 12-13$$

$$11 \not\equiv 13 \pmod{3} \qquad \because 3 \nmid 11-13$$

1st condition satisfied

(ii). For 2nd condition for any other integer

$$25 \equiv 13 \pmod{3} \qquad \because 3 \mid 25-13$$

Example: Show that the set $\{6,7,8,9\}$, m = 4 from CRS.

Solution: (i) 1st condition

$$6 \not\equiv 7 \pmod{4}$$

$$6 \not\equiv 8 \pmod{4}$$

$$6 \not\equiv 9 \pmod{4}$$

$$7 \not\equiv 8 \pmod{4}$$

$$7 \not\equiv 9 \pmod{4}$$

$$8 \not\equiv 9 \pmod{4}$$

(ii). 2^{nd} condition

For any other integer

$$10 \equiv 6 \pmod 4$$

Example: Show that the set {6,7,10,9} , m = 4 forms CRS.

Solution: 1^{st} condition

$$6 \not\equiv 7 \pmod 4$$

$$6 \equiv 10 \pmod 4$$

Which is not true. The given set not forms CRS.

Theorem: Let A = $\{a_1, a_2, \ldots, a_k\}$ be a set of integers then 'A' forms CRS (mod m) if k = m.

Proof: We know {0,1,2,….,m–1} forms a CRS (mod m) hence for each j , $1 \le j \le k$ $\exists$ unique i such that $0 \le i \le m-1$ and

$$a_j \equiv i \pmod m$$

Thus $k \le m$. But then $\{a_1, a_2, \ldots, a_k\}$ is also a CRS (mod m). Hence $\forall$ i $0 \le i \le m-1$, $\exists$ unique j $1 \le j \le k$ such that

$$i \equiv a_j \pmod m$$

$$\Rightarrow \quad m \le k$$

By combining the above result i.e. $k \le m$ & $m \le k$

$$\Rightarrow \quad m = k$$

Alternate definition:

The set A = $\{a_1, a_2, \ldots, a_k\}$ forms a CRS (mod m) if

(i) A contain exactly m elements

(ii) $a_i \not\equiv a_j \pmod m \quad \forall\ i \ne j$

Example: Show that the set {81,82,83,84} , m = 4 forms CRS.

Solution: (i) Observe that A contains exactly 4 elements. Condition (i) satisfied.

(ii).
$$81 \not\equiv 82 \pmod 4$$
$$81 \not\equiv 83 \pmod 4$$
$$81 \not\equiv 84 \pmod 4$$
$$82 \not\equiv 83 \pmod 4$$
$$82 \not\equiv 84 \pmod 4$$
$$83 \not\equiv 84 \pmod 4$$

Condition (ii) satisfied. Hence the given set forms CRS.

Exercise: Let $\{x_1, x_2, ...x_m\}$ be a CRS (mod m) and a,b ∈ Z such that (a,m) = 1 then show that the set $A = \{ax_1 + b, ax_2 + \text{b}, ...\text{a}\, x_m + b\}$ forms CRS (mod m)

Solution: (i) Observe that A contain exactly m elements.

(ii). Now we show

$$ax_i + b \not\equiv ax_j + b \pmod m \quad \forall\ i \neq j$$

Suppose $\quad ax_i + b \equiv ax_j + b \pmod m \quad \forall\ i \neq j$

$$\Rightarrow \quad ax_i \equiv ax_j \pmod m \quad \forall\ i \neq j$$

Since (a,m) = 1 then

$$x_i \equiv x_j \pmod m \quad \forall\ i \neq j$$

A contradiction against the fact that the given set $\{x_1, x_2, ...x_m\}$ forms a CRS (mod m). So our supposition is wrong. Thus

$$ax_i + b \not\equiv ax_j + b \pmod m \quad \forall\ i \neq j$$

Hence set A forms CRS (mod m)

Remark: The set {0,1,2,…, n – 1} always form a CRS (mod n)

Example: A = {81,82,83,84} , m = 4

The least residues of A (mod 4) are {1,2,3,0}

By using remark, the given set forms CRS (mod 4)

Example: A = {81,82,84,88} , m = 4

Solution: The least residues of A (mod 4) are {1,2,0,0} which are not remainder of 4 i.e {0,1,2,3}. Hence the given set not forms CRS (mod 4).

Lecture # 12

Reduced Residue System (RRS)

A set of integers $\{a_1, a_2, ..., a_k\}$ forms a Residue system modulo 'm' (denoted by RRS (mod m)) if

(i) $(a_i, m) = 1 \quad \forall i$

(ii) $a_i \not\equiv a_j \pmod{m} \quad \forall\ i \neq j$

(iii) For any integer n where (n,m) = 1 there exist a unique a_i such that

$n \equiv a_i \pmod{m}$

Example: Check the set forms RRS $\{1,3,5,7\}$, m = 8

Solution: (i) Since (1,8) = (3,8) = (5,8) = (7,8) = 1

(ii).

$$1 \not\equiv 3 \pmod{8}$$

$$1 \not\equiv 5 \pmod{8}$$

$$1 \not\equiv 7 \pmod{8}$$

$$3 \not\equiv 5 \pmod{8}$$

$$3 \not\equiv 7 \pmod{8}$$

$$5 \not\equiv 7 \pmod{8}$$

(iii). n = 15 $\Rightarrow$ (15,8) = 1

And $15 \equiv 7 \pmod{8}$

Hence the given set makes RRS.

Euler ϕ function:

Let n be a +ve integer ($n \geq 1$) we define Euler ϕ function as follows

$$\phi(n) = \begin{cases} n & \text{if } n = 1 \\ \text{The number of } +ve \text{ integers less than} \\ \text{and co} - \text{prime to } n \text{ if } n > 1 \end{cases}$$

e.g. If n = 1 then $\phi(1) = 1$

If n = 2

(0,2) = 2 , (1,2) = 1

1 & 2 are co-prime

$\phi(2) = 1$

If n = 3

(0,3) = 3 , (1,3) = 1 , (2,3) = 1

1 & 3 and 2 & 3 are relatively prime

$\phi(3) = 2$

If n = 4

$\phi(4) = 2$

If n = 5

$\phi(5) = 4$

If n = 13

$\phi(13) = 12$

Remark : (i) If P is prime number then $\phi(P) = P-1$

(ii). The set $\{1,2,3,..,P-1\}$ always forms a Reduced Residue system (mod P) where P is a prime number.

Theorem: If $\{a_1, a_2, ..., a_k\}$ is a Reduced Residue system (mod m) then k = ϕ(m).

Proof: $t_1, t_2, ..., t_{\phi(m)}$ be the ϕ(m) integers that are less than m and co-prime to m. We show $\{t_1, t_2, ..., t_{\phi(m)}\}$ is a RRS (mod m)

Suppose $t_i \equiv t_j (\bmod m) \quad 1 \le t_i, t_j < m$

$\because \quad m | t_i - t_j \quad$ ___(1)

But $\quad 1 \le t_i \ , \ t_j < m$

$\Rightarrow \quad t_i - t_j < m \qquad$ hence (i) cannot be possible unless $t_i - t_j = 0$

Next, let 'b' be an integer such that (n,m) = 1. By division algorithm

$$n = qm + r \quad ; \qquad 0 \le r < m$$

And the quotient q = 0 if n < m and q ≥ 1 if n > m. Also (r,m) = 1. Hence $r = t_i$ for some i $1 \le i \le \phi(m)$ and $n \equiv r \equiv t_i (\bmod m)$

Since $\forall$ i $\quad 1 \le i \le k \qquad (a_i, m) = 1$ $\exists$ a unique $\ell \quad 1 \le \ell \le \phi(m) \ni a_i \equiv t_i (\bmod m)$

$$\therefore \ k \le \phi(m)$$

Similarly, $\qquad \phi(m) \le k$

$\Rightarrow \quad k = \phi(m)$

Alternative definition:

A set $\{a_1, a_2, ..., a_k\}$ forms Reduced Residue system (mod m) if

(i) $\quad k = \phi(m)$

(ii) $\quad (a_i, m) = 1 \quad \forall i$

(iii) $\quad a_i \not\equiv a_j (\bmod m) \quad \forall \ i \ne j$

Example: Check the set forms RRS $\{1,3,5,7\}$, m = 8

Solution: (i) Since ϕ(m) = 4

(ii). $1 \not\equiv 3 \pmod{8}$

$1 \not\equiv 5 \pmod{8}$

$1 \not\equiv 7 \pmod{8}$

$3 \not\equiv 5 \pmod{8}$

$3 \not\equiv 7 \pmod{8}$

$5 \not\equiv 7 \pmod{8}$

Hence the given set form RRS.

Exercise: If $\{x_1, x_2, \ldots\ldots x_{\phi(m)}\}$ is a RRS (mod m) and a $\in$ Z such that (a,m) = 1.

Then show that the set A = $\{ax_1, a\,x_2, \ldots\ldots a\,x_{\phi(m)}\}$ forms RRS (mod m)

Solution: (i) Observe that the given set has exactly ϕ(m) elements

(ii). Since $\{x_1, x_2, \ldots\ldots x_{\phi(m)}\}$ forms RRS (modm)

So $(x_1, m) = (x_2, m) = \ldots., (x_{\phi(m)}, m) = 1$

Then $(ax_1, m) = (ax_2, m) = \ldots., (ax_{\phi(m)}, m) = 1 \quad \because (a, m) = 1$

(iii). Since $\{x_1, x_2, \ldots\ldots x_{\phi(m)}\}$ forms RRS (mod m)

So $x_1 \not\equiv x_2 \pmod{m}$

$x_2 \not\equiv x_3 \pmod{m}$

.

.

$x_{\phi(m)-1} \not\equiv x_{\phi(m)} \pmod{m}$

Then $ax_1 \not\equiv ax_2 \pmod{m}$

$$ax_2 \not\equiv ax_3 \pmod{m}$$

.

.

$$ax_{\phi(m)-1} \not\equiv ax_{\phi(m)} \pmod{m}$$

Since all conditions are satisfied. Hence the given set forms RRS (mod m)

Prime Number:

A positive integer n > 1 is called prime if 'n' has exactly two integer divisors namely 1 and 'n' itself otherwise 'n' is called composite number.

Composite Number:

A positive number n > 1 is called composite if 'n' has at least three positive divisors.

Perfect Number:

A positive integer 'n' is called perfect if the sum of its positive divisor is twice of the number 'n'.

Examples n = 6

Divisor of 6 = 1,2,3,6

Sum of divisor = 1+2+3+6 = 12 = 2(6)

$\Rightarrow$ 6 is perfect number

n = 28

divisor of 28 = 1,2,4,7,14,28

Sum of divisor = 1+2+4+7+14+28 = 56 = 2 (28)

$\Rightarrow$ 28 is perfect number.

Twin Primes:

Let ‘n’ be a positive integer , if $n-1$ and $n+1$ are prime number then these prime number are called twin primes.

$n = 4$

$n-1 = 3$ is prime number

$n+1 = 5$ is prime number

$\Rightarrow$ 3 and 5 are twin primes.

Prime Triplet:

Let ‘P’ be a prime number if P+2 and P+4 are prime then the triplet (P,P+2,P+4) is called Prime Triplet

e.g. $P = 3$

$P+2 = 5$

$P+4 = 7$

(3,5,7) is called Prime Triplet.

Powerful integer:

A positive integer ‘n’ is powerful if whenever a prime ‘P’ divides ‘n’. P^2 also divides ‘n’.

e.g. $n = 8$

$P = 2 \quad , \quad 2|8$

$P^2 = 4 \quad , \quad 4|8 \qquad \Rightarrow$ 8 is powerful.

Exercise: The smallest divisor of an integer is prime.

Solution: Let $d > 1$ be the smallest divisor of an integer ‘n’.

Let d_1 be any divisor of ‘d’. Then $1 \le d_1 \le d$. Suppose $d_1 \ne 1$. Then $d_1|d$ and $d|n$ $\Rightarrow d_1|n$ but $d_1 \le d \Rightarrow d_1 = d$. Hence only divisors of ‘d’ are 1 and ‘d’ itself.

$\Rightarrow$ ‘d’ is prime. Hence the smallest divisor of an integer is prime.

Exercise: Let P be a prime and 'a' be any integer then show that either $P|a$ or $(a,P) = 1$.

Solution: If $P|$ a we have nothing to prove. But if $P \nmid a$ then we show that $(a,P) = 1$

Let $d = (a,P)$ $\Rightarrow d|a$ and $d|P$

Since P is prime $d = 1$ or $d = P$. If $d = P$ then $P|a$, not possible. Hence $d = 1$

$\Rightarrow (a,P) = 1$

Exercise: Fundamental theorem of Arithmetic

OR

"Every integer can be decomposed as a product of prime number."

Proof: Suppose there exist an integer $n > 1$ which is not a product of primes. Let 'm' be the smallest then 'm' is not a prime and hence $m = ab$; $1 < a , b < m$. But then by choice of 'm' both 'a' and 'b' are products of primes. So, 'm' is a product pf primes. A contradiction, hence every integer can be decomposed as a product of prime number.

Lecture # 13

Question: Let 'm' be a positive integer, 'a' and 'b' any integers. The Linear congruence $ax \equiv b \pmod{m}$ has a solution if and only if $d | b$, $d = (a,m)$.

Solution: Suppose the linear congruence $ax \equiv b \pmod{m}$ has solution exist

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

$$\Rightarrow \quad m | ax - b \qquad \because \text{ by definition of congruence}$$

$$\Rightarrow \quad ax - b = my$$

$$\Rightarrow \quad ax + my = b$$

If $(a,m) = d$ then $d | b$

Conversely: If $d | b$ then we show $ax \equiv b \pmod{m}$ has solution exist

Let x_0 be the solution of $ax \equiv b \pmod{m}$ then

$$ax_0 \equiv b \pmod{m} \quad \_\_\_\_(i)$$

Let x' be another solution of $ax \equiv b \pmod{m}$ then

$$ax' \equiv b \pmod{m} \quad \_\_\_\_(ii)$$

From (i) and (ii)

$$ax' \equiv ax_0 \pmod{m} \quad \_\_\_\_(iii)$$

Since $(a,m) = d$

$$\Rightarrow \quad d | a \quad \text{and} \quad d | m$$

$$\Rightarrow \quad a = dr \quad \text{and} \quad m = ds \quad \text{where}(r,s) = 1$$

Put in (iii) $\Rightarrow \quad drx' \equiv drx_0 \pmod{ds}$

$$\Rightarrow \quad ds | drx' - drx_0$$

$$\Rightarrow \qquad ds \mid dr\left(x' - x_0\right)$$

$$\Rightarrow \qquad s \mid r\left(x' - x_0\right)$$

Since (r,s) =1 only possible if

$$s \mid x' - x_0$$

$$\Rightarrow \qquad x' - x_0 = hs$$

$$\Rightarrow \qquad x' = x_0 + hs \qquad \_\_\_\_(iv)$$

By Division Algorithm

$$h = dq + t \quad ; \qquad 0 \le t < d$$

$$(iv) \Rightarrow \qquad x' = x_0 + dqs + ts$$

$$x' = x_0 + mq + \frac{tm}{d} \qquad \because ds = m \ , \ s = \frac{m}{d}$$

$$x' = x_0 + t.\frac{m}{d}$$

Therefore, the congruence $ax \equiv b(\bmod m)$ has solution x_0. Hence solution exist.

Question: Under what conditions solution the system of linear congruence having monic leading coefficients. Justify your answer?

Solution: A general system of simultaneous linear congruences

$$a_1 x \equiv b_1 \left(\bmod n_1\right)$$

$$a_2 x \equiv b_2 \left(\bmod n_2\right)$$

$$\vdots \qquad \vdots$$

$$a_r x \equiv b_r \left(\bmod n_r\right)$$

can be simplified to form
$$x \equiv c_1 \pmod{m_1}$$
$$x \equiv c_2 \pmod{m_2}$$
$$\vdots$$
$$x \equiv c_r \pmod{m_r}$$

by dividing each congruence through by (a_i, n_i) then multiplying by the inverse mod $m_i = \dfrac{n_i}{(a_i, n_i)}$ of the coefficient $\dfrac{a_i}{(a_i, n_i)}$. The simplified system may or may not be solvable but in any case, it must have the same set of solution as the original system. Hence, the linear congruence having monic leading coefficients.

Example: The system $x \equiv 8 \pmod{12}, x \equiv 6 \pmod 9$ has no solutions. Since, the first congruence implies that $x \equiv 8 \equiv 2 \pmod 3$ but the second implies that $x \equiv 6 \equiv 0 \pmod 3$ and these are incompatible with each other.

Question: Solve the system of linear congruence
$$x \equiv 2 \pmod 3$$
$$x \equiv 4 \pmod 5$$
$$x \equiv 5 \pmod 6$$

Solution: Gcd (5,3) = 1 | 5 – 3 = 1 | 2

Gcd (6,5) = 1 | 6 – 5 = 1 | 1

Gcd (6,3) = 3 | 6 – 3 = 3 | 3

$$x \equiv 2 \pmod 3$$

$\Rightarrow$ $3 \mid x - 2$

$\Rightarrow \quad x - 2 = 3k \quad$ where k is integer

$\Rightarrow \quad x = 2 + 3k \quad$ ____(i)

$x \equiv 4 \pmod 5$

$2 + 3k \equiv 4 \pmod 5$

$3k \equiv 4 - 2 \pmod 5$

$3k \equiv 2 \pmod 5$

$-2k \equiv 2 \pmod 5$

$k \equiv -1 \pmod 5$

$k \equiv 4 \pmod 5$

$\Rightarrow \quad 5 \mid k - 4$

$\Rightarrow \quad k - 4 \equiv 5k' \quad$ where k' is any integer

$k \equiv 4 + 5k' \quad put\ in\ (i)$

$x \equiv 2 + 3(4 + 5k')$

$x \equiv 2 + 12 + 15k'$

$x \equiv 14 + 15k' \quad$ ___(ii)

$x \equiv 5 \pmod 6$

$14 + 15k' \equiv 5 \pmod 6$

$15k' \equiv -9 \pmod 6$

$15k' \equiv 3 \pmod 6$

$3k' \equiv 3 \pmod 6$

$k' \equiv 1 \pmod 6$

$\Rightarrow \quad 6 | k' - 1$

$\Rightarrow \quad k' - 1 = 6k''$

$\Rightarrow \quad k' = 1 + 6k'' \quad put\ in\ (ii)$

$x = 14 + 15(1 + 6k'')$

$x = 14 + 15 + 90k''$

$x = 29 + 90k''$

$x - 29 = 90k''$

$\Rightarrow \quad 90 | x - 29$

$\Rightarrow \quad x \equiv 29 \pmod{90}$

Question: Solve the system of linear congruence

$x \equiv 5 \pmod 6$

$x \equiv 4 \pmod{11}$

$x \equiv 3 \pmod{17}$

Solution: Gcd (6,11) = 1 | 11 – 6 = 1 | 5

Gcd (11,17) = 1 | 17 – 11 = 1 | 6

Gcd (6,17) = 1 | 17 – 6 = 1 | 11

$x \equiv 5 \pmod 6$

$\Rightarrow \quad 6 \mid x - 5$

$\Rightarrow \quad x - 5 = 6k$ where k is integer

$\Rightarrow \quad x = 5 + 6k$ ____(i)

$x \equiv 4 \pmod{11}$

$5 + 6k \equiv 4 \pmod{11}$

$$6k \equiv 4-5 \pmod{11}$$

$$6k \equiv -1 \pmod{11}$$

$$6k \equiv 10 \pmod{11}$$

$$-5k \equiv 10 \pmod{11}$$

$$k \equiv -2 \pmod{11}$$

$$k \equiv 9 \pmod{11}$$

$\Rightarrow \quad 11 \mid k-9$

$\Rightarrow \quad k-9 \equiv 11k'$ where k' is any integer

$$k \equiv 9+11k' \quad put\ in\ (i)$$

$$x \equiv 5+6\left(9+11k'\right)$$

$$x \equiv 5+54+66k'$$

$$x \equiv 59+66k' \quad \_\_\_(ii)$$

$$x \equiv 3 \pmod{17}$$

$$59+66k' \equiv 3 \pmod{17}$$

$$66k' \equiv 3-59 \pmod{17}$$

$$66k' \equiv -56 \pmod{17}$$

$$66k' \equiv 12 \pmod{17}$$

$$15k' \equiv 12 \pmod{17}$$

$$-2k' \equiv 12 \pmod{17}$$

$$k' \equiv -6 \pmod{17}$$

$$k' \equiv 11 \pmod{17}$$

$$\Rightarrow \quad 17 | k' - 11$$

$$\Rightarrow \quad k' - 11 = 17k''$$

$$\Rightarrow \quad k' = 11 + 17k'' \quad \text{put in } (ii)$$

$$x \equiv 59 + 66(11 + 17k'')$$

$$x = 59 + 726 + 1122k''$$

$$x = 785 + 1122k''$$

$$x - 785 = 1122k''$$

$$\Rightarrow \quad 1122 | x - 785$$

$$\Rightarrow \quad x \equiv 785 (\text{mod} 1122)$$

Question: State and prove Wilson's theorem.

Statement: An integer P is prime if and only if $(P-1)! \equiv -1(\text{mod}\, P)$

Proof: Suppose P is prime. Let 'a' be an integer such that 1≤ a ≤ P−1. Then (a,p)=1 . Hence the congruence $ax \equiv 1(\text{mod}\, P)$ has a unique solution (mod P) (say) b

$$\because \quad ab \equiv 1(\text{mod}\, P)$$

Also, if $\quad b \equiv a(\text{mod}\, P)$ *then*

$$a^2 \equiv 1(\text{mod}\, P)$$

$$\Rightarrow P | a^2 - 1 \qquad P | a - 1 \quad or \quad P | a + 1$$

Thus for each integer b ∈ { 2,3,….,P−2} such that $bc \equiv 1(\text{mod}\, P)$

Therefore, by pairing bs 1< b < P−1 with cs 1< c < P−1 ∍ $bc \equiv 1(\text{mod}\, P)$ we get

$$1.2.3......(P-1) \equiv 1.(P-1)(\text{mod}\, P)$$

$$1.2.3......(P-1) \equiv -1(\text{mod}\, P)$$

$$\Rightarrow \quad (P-1)! \equiv -1 \pmod P$$

Conversely: Suppose that $\Rightarrow \quad (P-1)! \equiv -1 \pmod P$ and $d \mid P \qquad 1 \le d < P$

Clearly d is a factor of $(P-1)!$

$$\Rightarrow d \mid (P-1)!$$

As $\qquad (P-1)! \equiv -1 \pmod P$

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

$$\Rightarrow \quad d \mid (P-1)! + 1$$

$$\Rightarrow \quad d \mid 1$$

$\Rightarrow \quad d = 1 \qquad$ Hence P is prime

Question: State and prove Chinese Remainder theorem?

Statement: The linear system of congruence $x \equiv a_i \pmod{m_i}$ where the moduli are pair wise relatively prime and $1 \le i \le k$ has unique solution $m_1, m_2, \ldots m_k$

Proof: The proof consists of two parts. First, we will construct a solution and then show that it is unique modulo $m_1, m_2, \ldots m_k$

(i) Let $M = m_1, m_2, \ldots m_k$ and $M_i = M \mid m_i \quad where \ 1 \le i \le k$

Since $\quad$ Gcd $\quad (M_i, m_i) = 1 \quad \forall i$

Also $\quad M_i \equiv 0 \pmod j \quad where \ \ i \ne j$

Since $\quad (M_i, \mathrm{m}_i) = 1$

So $\quad M_i y_i \equiv 1 \pmod{m_i}$

has a unique solution say y_i (y_i is in fact the inverse of M_i modulo m_i)

Let $x = a_1 M_i y_1 + a_2 M_2 y_2 + \ldots . + a_k M_k y_k$

To show M is a solution of linear system we have

$$x = \sum_{\substack{i=1 \\ i \neq j}}^{k} a_i M_i y_i + a_j M_j y_j$$

$$x = \sum_{i \neq j}^{k} a_i \ .0 + a_j \ .1 \qquad (\text{mod } j)$$

$$x = 0 + a_j \quad \text{mod } j$$

$$x = a_j \quad (\text{mod } j) \quad 1 \leq j \leq k$$

(ii) To show that solution is unique.

Let $x_0 \ and \ x_1$ be two solutions of the system. We shall show that

$$x_0 \equiv x_1 (Mod\ M)$$

Since $\quad x_0 \equiv a_j (mod\ m_j)$

And $\quad x_1 \equiv a_j (mod\ m_j) \quad for\ 1 \leq j \leq k$

$$x_1 - x_0 \equiv a_j - a_j \quad (\text{mod}\, m_j)$$

$$x_1 - x_0 \equiv 0 \quad (\text{mod}\, m_j)$$

$$m_j \left| (x_1 - x_0) - 0 \right.$$

$$m_j \left| x_1 - x_0 \right. \qquad for\ 1 \leq j \leq k$$

$$m_1, m_2, \ldots m_k \left| x_1 - x_0 \right.$$

$$where \quad M = m_1, m_2, \ldots m_k$$

$$\Rightarrow \quad M \left| x_1 - x_0 \right.$$

$$\Rightarrow \quad x_1 - x_0 \equiv 0 \quad (Mod\ M)$$

$$\Rightarrow \quad x_1 \equiv x_0 (Mod\ M)$$

Thus any two solution of linear system are congruent modulo M , so the solution is unique modulo M.

Question: Let ‘a’ and ‘b’ be any two integers and ‘m’ be a positive integer show that of $n\,a \equiv nb(\text{mod}\, m)$ then $a \equiv b(\text{mod}\, m)$ where gcd (m,n) = 1

Solution: Given that $\quad n\,a \equiv nb(\text{mod}\, m)$

$$\Rightarrow \qquad m | na - nb \qquad \because \text{ by definition of congruence}$$

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

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

$$\Rightarrow \quad a \equiv b \pmod m$$

Question: Let 'a' and 'b' be any two integers and 'm' be a positive integer. Show that if $a \equiv b \pmod m$ then $a^n \equiv b^n \pmod m$

Solution: Given that $a \equiv b \pmod m$

By definition of congruence

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

$$\Rightarrow \quad m \mid (a-b)\left(a^{n-1}+a^{n-2}b+....+b^{n-1}\right)$$

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

$$\Rightarrow \quad a^n \equiv b^n \pmod m$$

Question: Define Fermat numbers and show that any two Fermat numbers are relatively primes.

Fermat numbers: The number of the form 2^{k+1} is a prime then $k=2^m$ for some integer m; so that $2^{k+1}=2^{2^m}+1=F_m$ the number of this form is called Fermat number.

Take any two distinct Fermat numbers, say $F_a < F_b$

Let $d=\gcd(F_a,F_b)$. We know $F_a \mid F_b-2$

Using the definition of d, $d \mid F_a$ and hence $d \mid F_b-2$

Since we also know that $d \mid F_b$ it follows that $d \mid F_b-(F_b-2)$

$$\Rightarrow \mathrm{d} \mid 2$$

But all Fermat number are odd and therefore d cannot be 2. So, d = 1 and the numbers F_a *and* F_b are relatively prime.

Question: State and prove Unique Factorization theorem.

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

Proof: We prove the theorem by induction on 'n'

For n =2 $\Rightarrow$ 2 = 2 (true)

Let us suppose that the statement is true for n = 2 ,3 , 4 ,…,k

Now prove it for n = k+1

If k+1 is prime. Then the induction is complete. If k+1 is composite. 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, induction is complete and theorem is true i.e. $n = P_1 P_2 P_3, ...P_r$ where P_i for i = 1,2,3,….,r are primes

For uniqueness

Let $n = P_1 P_2 P_3, ...P_r$ where i = 1,2,3,….,r

And $n = q_1 q_2 q_3, ...\mathrm{q}_s$ where j = 1,2,3,….,s

Then $q_1 q_2 q_3, ...\mathrm{q}_s = P_1 P_2 P_3, ...P_r$ ______(1)

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

$$q_1 q_2 q_3, ...\mathrm{q}_i = P_1 P_2 P_3, ...P_j \qquad \_\_\_(2)$$

Then by result, If $P \mid P_1 P_2 P_3, ...P_k \quad where \;\; P_i \;\; for \;\; i = 1, 2, 3, ...\mathrm{k}$ are the primes then $P = P_i \quad for \;\; i = 1, 2, 3, ...\mathrm{k} \quad \because \;\; q_1 \mid q_1 q_2 q_3, ...\mathrm{q}_i$

Therefor $q_1 \mid P_1 P_2 P_3, ...\mathrm{P}_j \qquad \because by(2)$

Then by above result $q_1 = P_j \quad for \;\; i = 1, 2, 3, ...\mathrm{j}$ which is contradiction. Hence this prove the uniqueness theorem.