be. Superior College

B.Sc Math

Numbr Theory

M.TANVEER

M.Sc Math

Punjab University

Contacts Number

03009602869

The Superior

Book Shop

NUMBER THEORY

M. TANVEER
SUPERIOR GROUP OF COLLEGES
: 0300-9602869

Divisibility:

Let $a, b \in z$ we say 'a' divides 'b' if $\exists\ c \in z$ s.t $b = ac$

'a' is called divisor or factor of 'b' and 'b' is called multiple of 'a'

Symbolically, we write it as $a \mid b$ which is read as 'a divides b'

Show that

i) $a \mid 0$, $a \in z, a \neq 0$

$\because 0 = a.0 \Rightarrow a \mid 0$

(ii) $-1 \mid a$, $1 \mid a$

$\because a = (-1)(-a) \Rightarrow -1 \mid a$

$a = 1(a) \Rightarrow 1 \mid a$

ii) **if $a \mid b$ and $c \in z$ then $a \mid bc$**

as $a \mid b \Rightarrow b = ac_1$ $\because c_1 \in z$

Now $bc = ac_1c$ $c_1c = c_3 \in z$

$bc = ac_3$

$\Rightarrow a \mid bc$

iv) **$a \mid b$ and $b \mid a$ then $a = \pm b$**

$a \mid b \Rightarrow b = ac$ $\quad b \mid a \Rightarrow a = bc_1$

as $b = ac$

$b = bc_1c$

$b - bc_1c = 0 \Rightarrow b(1 - cc_1) = 0$

$\because b \neq 0 \Rightarrow 1 - cc_1 = 0$

$cc_1 = 1$

which is possible when

$c = \pm 1$; $c_1 = \pm 1$

Then in both cases $a = \pm b$

v) **if $a \mid b$ and $a \mid c \Rightarrow a \mid bx + cy$**

$a \mid b \Rightarrow b = ad_1$ where $d_1 \in z$;

$\Rightarrow bx = ad_1x$;

$\Rightarrow bx = ad_3$ put $d_3 = d_1x$;

$a \mid c \Rightarrow c = ad_2$ where $d_2 \in z$

$\Rightarrow cy = ad_2y$

$\Rightarrow cy = ad_4$ put $d_4 = d_2y$

adding:

$bx+cy = ad_3 + ad_4 = a(d_3+d_4)$ put $d_3+d_4=d$

$bx+cy = ad$

$\Rightarrow a \mid bx+cy$

(vi) $a \mid b$; $a \mid b+b_2 \Rightarrow a \mid b_2$

$a \mid b$; $a \mid b+b_2$

$\Rightarrow b = ac_1$; $b+b_2 = ac_2$

$ac_1+b_2 = ac_2$ Put value of b

$b_2 = ac_2 - ac_1$

$b_2 = a(c_2-c_1)$ put $c_2-c_1=c$

$b_2 = ac$

$\Rightarrow a \mid b_2$

(vii) if $a \mid b$; $b \mid c \Rightarrow a \mid c$

$a \mid b$ $\quad$ $b \mid c$

$\Rightarrow b = ac_1$ $\quad$ $\Rightarrow c = bc_2$

$c = ac_1c_2$ put value of b

$c = ac_3$

$\Rightarrow a \mid c$

Common Divisor:

Let $a,b \in z$ then $c \in z$ is called common divisor of 'a' & 'b' if $c \mid a$ & $c \mid b$

Greatest Common divisor:

Let $a,b \in z$ then $d \in z$ is called G.C.D of 'a' & 'b' if

(i) $d > 0$ (ii) $d \mid a$ & $d \mid b$

(iii) if $c \mid a$ and $c \mid b$ then $c \mid d$

& we write $(a,b) = d$

Euclide Theorem:-

If $a,b \in z$ and $b > 0$ then ∃ a unique integers 'q' & 'r' such that

$a = bq + r$ $\quad$ $0 \le r < b$

Proof:

Let $A = \{a - bx \ge 0 \; ; x \in z\}$

then $A \neq \emptyset$ $\quad$ $\because a - b(-|a|) \in A$

If $0 \in A$ then 0 is least element of A.
If $0 \notin A$ then 'A' being set (of (non-empty) +ve integers) has a least element.
Let 'r' be the least element then

$$r = a - bx \quad \text{for some } x \in z$$
$$a = bx + r$$
$$\Rightarrow \quad a = bq + r \quad \text{for } r \geq 0, x = q.$$

r<b

Suppose contrary let $r \geq b \Rightarrow r - b \geq 0$
Also

$$r - b = a - bq - b$$
$$r - b = a - b(q+1) \geq 0 \qquad \because a - b(1-x1)$$
$$r - b \in A$$

But $r - b < r$
It is a contradiction to the fact that 'r' is least element of A. hence $r < b$.

Uniqueness:

Let $a = bq_1 + r_1 \qquad 0 \leq r_1 < b$

$$bq + r = bq_1 + r_1$$
$$|bq - bq_1| = |r_1 - r|$$
$$b|q - q_1| = |r_1 - r| \rightarrow (1)$$

Now $0 < r, \; r_1 < b$

$$r_1 - r < b$$

$(1) \Rightarrow \quad b|q - q_1| < b$

$$q - q_1 < 1$$
$$q - q_1 = 0 \Rightarrow q = q_1$$

Again (1) $\quad 0 = |r_1 - r|$

$$r_1 = r$$

Hence q & r are unique.

Prove that G.C.D of two integers is unique.

Let $(a,b) = d$ is not unique
Let $(a,b) = d$ & $(a,b) = c$

$\because$ d is g.c.d of a,b $\Rightarrow c|d \rightarrow (1)$

$\because$ c is g.c.d of a & b $\Rightarrow d|c \rightarrow (2)$

from (1) & (2) $c = \pm d$

as g.c.d > 0
$\Rightarrow c = d$

Find G.C.D of any two integers by using Euclidean Algorithm.

Let $a, b \in z$ such that both a, b are non-zero. By Euclidean Theorem, we can find unique integers q_1, r_1 s.t

$$a = bq_1 + r_1 \qquad 0 \le r_1 < b \longrightarrow (1)$$

If $r_1 \neq 0$, we divide b by r_1

$$b = r_1 q_2 + r_2 \qquad 0 \le r_2 < r_1 \longrightarrow (2)$$

If $r_2 \neq 0$, we divide r_1 by r_2

$$r_1 = r_2 q_3 + r_3 \qquad 0 \le r_3 < r_2 \longrightarrow (3)$$

Continuing the process till the remainder r_{k+1} is obtained which is zero.

$$r_2 = r_3 q_4 + r_4 \qquad 0 \le r_4 < r_3 \longrightarrow (4)$$

$$\vdots$$

$$r_{k-2} = r_{k-1} q_k + r_k \qquad 0 \le r_k < r_{k-1} \longrightarrow (k)$$

$$r_{k-1} = r_k q_{k+1} + r_{k+1} \longrightarrow (k+1)$$

we note the following properties of r_k

(i) $r_k > 0$

(ii) eq $(k+1) \Rightarrow r_k \mid r_{k+1}$ eq $(k) \Rightarrow r_k \mid r_{k-2}$ and so on

thus $r_k \mid b$ & $r_k \mid a$

$\Rightarrow r_k$ is common divisor of 'a' & 'b'.

(iii) if $c \mid a$ & $c \mid b$ the

eq $(1) \Rightarrow c \mid r_1$ eq $(2) \Rightarrow c \mid r_2$ and so on.

eq $(k+1) \Rightarrow c \mid r_k$

$\Rightarrow r_k$ satisfies conditions of G.C.D.

$\Rightarrow (a, b) = r_k$

If $a, b \in z$ where a, b both are non-zero and $(a, b) = d$ then prove $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$

given $(a, b) = d$

$\Rightarrow d \mid a$; $d \mid b$

$\Rightarrow a = a_1 d \rightarrow (1)$; $b = b_1 d \rightarrow (2)$

Let $\left(\frac{a}{d}, \frac{b}{d}\right) = (a_1, b_1) = c$

$(a_1, b_1) = c$

$\Rightarrow c \mid a_1$ & $c \mid b_1$

$\Rightarrow \frac{a_1}{c} = b_2$; $\frac{b_1}{c} = b_3$

$\Rightarrow a_1 = cb_2 \rightarrow ③$; $b_1 = cb_3$ ④

using (i) & ③ using ② & ④

$a = cb_2 d$; $b = cb_3 d$

$\Rightarrow a = b_2(cd)$; $\Rightarrow b = b_3(cd)$

$\Rightarrow cd \mid a$; $\Rightarrow cd \mid b$

$\Rightarrow$ cd is common divisor of a & b.

But $(a, b) = d$

$\Rightarrow d \mid cd$

$\Rightarrow \frac{cd}{d} \Rightarrow c = \pm 1$ ∵ we are dealing with +ve integers!

$c = 1$

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

Least Common Multiple: (L.C.M)

Let $a, b \in z$ s.t both 'a' and 'b' are non-zero, then an integer 'm' with the following properties is called L.C.M of a & b if

(i) $m > 0$ (ii) $a \mid m$, $b \mid m$

(iii) if $c \in z$ is a comon multiple of a & b then $m \mid c$.

It is written as $\langle a, b \rangle = m$.

Prove that if 'n' is odd integer then $8 \mid n^2 - 1$

Let $n = 2k+1$

$n^2 = (2k+1)^2 = 4k^2 + 4k + 1$

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

Case (i)
if k is even
$\Rightarrow$ 2 is factor of k
$\Rightarrow$ 4k contains 8 as factor
$\Rightarrow$ 4k(k+1) is divisible by 8
Hence $8 \mid n^2 - 1$

Case (ii)
if k is odd
$\Rightarrow$ 2 is factor of k+1
$\Rightarrow$ 8 is factor of 4(k+1)
$\Rightarrow$ 8 is factor of 4k(k+1)
Hence $8 \mid n^2 - 1$

Prove that product of any three consequtive numbers is divisible by 6.

Let $n, n+1, n+2$ be three consecutive numbers
we are to show $6 \mid n(n+1)(n+2)$
we'll prove this by Mathematical Induction.

C-I: Put $n=1$

$n(n+1)(n+2) = 1(1+1)(1+2) = 6$

$\Rightarrow 6 \mid 6$ C-I Satisfied.

C.II suppose this is true for $n=k$ where $k \in z^+$
i.e $6 \mid k(k+1)(k+2)$

C.III Now we prove this true for $n=k+1$ i.e
$6 \mid (k+1)(k+2)(k+3)$

$\because (k+1)(k+2)(k+3) = k(k+1)(k+2) + 3(k+2)(k+1)$

Simply; we show $6 \mid 3(k+2)(k+1)$

Case 1
When k is even
$\Rightarrow 2$ is factor of $k+2$
$\Rightarrow 6$ is factor of $2(k+2)$
$\Rightarrow 6$ is factor of $3(k+1)(k+2)$
$\rightarrow 6 \mid 3(k+1)(k+2)$

Case II
When k is odd, $k+1$ is even
$\Rightarrow 2$ is factor of $k+1$
$\Rightarrow 6$ is factor of $3(k+1)$
$\Rightarrow 6$ is factor of $3(k+1)(k+2)$
$\Rightarrow 6 \mid 3(k+1)(k+2)$

$\Rightarrow 6 \mid (k+1)(k+2)(k+2)$
Condition-3 satisfied

Hence 6 divides product of 3 consecutive integers.

Prove that any odd integer is of form $4n-1$ or $4n+1$.

By Euclidean Theorem;
Any number $a = 4n+r$ $\quad 0 \le r < 4$
$\because a = 4n, 4n+1, 4n+2, 4n+3$
Now $4n, 4n+2$ are even
& all odd number (integers) must be either of form $4n+1$ or $4n+3$ i.e $4n-1$

If a and b are two integers and $(a,b)=d$ then $\langle a,b\rangle = \frac{|ab|}{d}$

Let $m = \frac{|ab|}{d}$

we have to prove 3 properties of L.C.M

(i) M_1: $m>0$ because of absolute value of ab and $d>0$.

$\because \frac{|ab|}{d} > 0$

(ii) M_2: $a \backslash m$ and $b \backslash m$

$\because (a,b) = d$

$d \backslash a \Rightarrow a = a_1 d$ $\quad d \backslash b \Rightarrow b = b_1 d$

Now $m = \frac{|ab|}{d}$

$m = \frac{|a_1 d b|}{d}$ $\qquad m = \frac{|a b_1 d|}{d}$

$\Rightarrow m = a_1 b$ $\qquad \Rightarrow m = b_1 a$

$\Rightarrow b \backslash m$ $\qquad \Rightarrow a \backslash m$

(iii) M_3: Let c is integer such that $a \backslash c$ & $b \backslash c$

$\Rightarrow c = ad_1$; $\Rightarrow c = bd_2$

$\Rightarrow ad_1 = bd_2 = c$

$\Rightarrow a_1 d d_1 = b_1 d d_2 = c$ $\quad \because a = a_1 d, b = b_1 d$

$\Rightarrow a_1 d_1 = b_1 d_2$ $\quad \because c = b_1 d d_2 \rightarrow (3)$

$\Rightarrow a_1 \backslash b_1 d_2$ $\quad \because (a_1, b_1) = 1$

$\Rightarrow a_1 \backslash d_2$

Now $a_1 \backslash d_2$

$\Rightarrow d_2 = a_1 t$ $\quad t \in z$

Put in (3)

$c = b_1 d (a_1 t)$

$c = (b_1 d a_1) t \Rightarrow b_1 d a_1 \backslash c \rightarrow (iv)$

$m = \frac{|ab|}{d} = \frac{|abd|}{d \cdot d}$

$m = \frac{a}{d} \cdot \frac{b}{d} d \Rightarrow m = a_1 b_1 d$

Put in (iv)

$\Rightarrow m \backslash c$

Hence $m = \langle a, b \rangle$

If 'n' is any positive odd integer, then prove that $a+b \mid a^n+b^n$

Let n is +ve odd integer say $n=2m+1$
we have to prove $a+b \mid a^{2m+1}+b^{2m+1}$
we'll prove this by M.I.

C.I put $m=1$

$a^{2+1}+b^{2+1} = a^3+b^3 = (a+b)(a^2-ab+b^2)$

$\Rightarrow a+b \mid (a+b)(a^2-ba+b^2) \Rightarrow a+b \mid a^3+b^3$

C-I satisfied.

C.II Suppose this is true for $m=k$ where $k \in z^+$
i.e $a+b \mid a^{2k+1}+b^{2k+1}$

C.III Now we prove this true for $m=k+1$
i.e $a+b \mid a^{2k+3}+b^{2k+3}$

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

$\Rightarrow a^{2k+1}(a^2-b^2)$ is divisible by $a+b$ $\because (a-b)(a+b) = a^2-b^2$
& $(a^{2k+1}+b^{2k+1})$ is divisible by $a+b$ (C-II)
So $a+b \mid a^n+b^n$

When 'n' is even integer then prove that $a+b \mid a^n-b^n$

Let n is even integer say $n=2m$
we have to show $a+b \mid a^{2m}-b^{2m}$ $\because m \in z$

C.I put $m=1$

$a^2-b^2 = (a+b)(a+b)$ Hence $a+b \mid a^2-b^2$.

C.II Suppose this is true for $m=k$ where $k \in z^+$
i.e $a+b \mid a^{2k}-b^{2k}$

C.III Now we prove this true for $m=k+1$
i.e $a+b \mid a^{2k+2}-b^{2k+2}$

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

$\Rightarrow a^{2k}(a^2-b^2)$ is divisible by $a+b$ $\because a^2-b^2 = (a+b)(a-b)$
$\Rightarrow (a^{2k}-b^{2k})b^2$ is divisible by $a+b$ (C-II)
Hence $a+b \mid a^n-b^n$

$9 \mid 10^n + 3.4^{n+2} + 5$

We'll prove this by M.I.

C-I: put $n=1$

$10+3.4^3+5 = 207$

$9 \mid 207 = 23$ C-I satisfied.

C-II Suppose this is true for $n=k$ where $k \in z^+$

i.e $9 \mid 10^k + 3.4^{k+2} + 5$

C-III Now we prove this true for $n=k+1$

i.e $9 \mid 10^{k+1} + 3.4^{k+3} + 5$

$$10^{k+1} + 3.4^{k+3} + 5 = 10^k.10 + 3.4^{k+2}.4 + 5$$
$$= 10^k(9+1) + 3.4^{k+2}(1+3) + 5$$
$$= 9.10^k + 10^k + 3.4^{k+2} + 9.4^{k+2} + 5$$
$$= 9(10^k + 4^{k+2}) + (10^k + 3.4^{k+2} + 5)$$

$\Rightarrow$ $9 \mid 9(10^k + 4^{k+2})$ & $9 \mid 10^k + 3.4^{k+2} + 5$ (Supposition)

All conditions satisfied.

Hence $9 \mid 10^n + 3.4^{n+2} + 5$

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

We'll prove this by M.I.

C-I put $n=1$

$3^6 + 5^3 = 854$

$\Rightarrow 14 \mid 854 = 16$ (C-I satisfied)

C-II Suppose this is true for $n=k$; $k \in z^+$

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

C-III Now we prove this true for $n=k+1$

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

$$3^{4k+6} + 5^{2k+3} = 3^{4k+2}.3^4 - 3^{4k+2}5^2 + 3^{4k+2}5^2 + 5^{2k+1}5^2$$
$$= 3^{4k+2}(3^4 - 5^2) + 5^2(3^{4k+2} + 5^{2k+1})$$
$$= 56.3^{4k+2} + 5^2(3^{4k+2} + 5^{2k+1})$$

$\Rightarrow$ $14 \mid 56(3^{4k+2})$ $\because 14 \mid 56 = 4$

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

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

$64 \mid 7^{2n}+16n-1$

We'll prove this by M.I.

put $n=1$

$64 \mid 7^2+16-1 \Rightarrow 64 \mid 64 = 1$ C-I Satisfied

Suppose this is true for $n=k$ where $k \in z^+$

i.e $64 \mid 7^{2k}+16k-1$

Now we prove this true for $n=k+1$

i.e $64 \mid 7^{2k+2}+16(k+1)-1$

$$7^{2k+2}+16(k+1)-1 = 7^{2k}.7^2+16k+16-1$$
$$= 7^{2k}(49)+16k(49-48)+16-(49-48)$$
$$= 7^{2k}(49)+16k(49)-48.16k-49+48+16$$
$$= 49(7^{2k}+16k-1)-16k(48)+64$$
$$= 49(7^{2k}+16k-1)+64(1-12k)$$

$\Rightarrow 64 \mid 49(7^{2k}+16k-1)$ our supposition.

& $64 \mid 64(1-12k)$

Hence $64 \mid 7^{2n}+16n-1$

Show that if $(b,c)=1$ & $a \mid c$ then $(a,b)=1$

$a \mid c \Rightarrow \frac{c}{a} = p \quad \because p \in z$

$\Rightarrow c = ap$

$\because (b,c) = 1$

$\Rightarrow (b, ap) = 1$

Let $(a,b) = d$

$d \mid a$ & $d \mid b$ $\quad a_1, b_1 \in z$

$\Rightarrow a = a_1 d$ & $b = b_1 d$ & $(a_1, b_1) = 1$

then

$$(b,c) = (b, ap) = (b_1 d, a_1 dp)$$
$$(b,c) = d(b_1, a_1 p)$$

Show that if $(a,b) = 1$ then

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

(ii) $(a+b, a-b, ab) = 1$

(i) $(a,b) = 1$ (given)

Let $(a-b, a+b) = d$

$\Rightarrow d \mid a-b \rightarrow$(i) ; $d \mid a+b \rightarrow$(ii)

from (i) & (ii) $d \mid a-b+a+b$

$\Rightarrow d \mid 2a \rightarrow$(iii)

from (i) & (ii) $d \mid a+b-a+b$

$\Rightarrow d \mid 2b \rightarrow$(iv)

from (iii) & (iv) $d \mid 2a+2b$

$\Rightarrow d \mid 2(a+b)$

$\Rightarrow d \mid 2$ or $d \mid a+b$

$d \mid 2 \Rightarrow d = 1$ or $d = 2$

So $(a-b, a+b) = 1$ or 2.

(ii) $(a+b, a-b, ab) = 1$

Two possibilities

(i) 'a' is even, b is odd

(ii) both 'a' & 'b' are odd

∵ if both a, b even ⇒ g.c.d must be 2 (atleast)

Case I:

If a is even and b is odd (vice versa) then $a+b, a-b$ are odd and ab is even

$\Rightarrow (a+b, a-b, ab) = 1$ ∵ $(a,b) = 1$

Case II

If both 'a' and 'b' are odd then $(a+b), (a-b)$ are even and ab is odd

$\Rightarrow (a+b, a-b, ab) = 1$ ∵ $(a,b) = 1$

Show that $(ma, mb) = m(a,b)$ where m is +ve integer.

Let $(a,b) = d$

$\Rightarrow d \mid a$ & $d \mid b$ ∵ $a_1, b_1 \in z$

$\Rightarrow a = a_1 d$ & $b = b_1 d$ & $(a_1, b_1) = 1$

Reason:

$(a+b, a-b, ab) = d$

$d \mid a+b$, $d \mid a-b$, $d \mid ab$

$\Downarrow$

$d \mid a$ & $d \mid b$

$\Rightarrow$ d is common divisor of a, b

But $(a, b) = 1$

$\Rightarrow$ $d = 1$

$(a+b, a-b, ab) = 1$

Now $ma = ma_1 d$ & $mb = mb_1 d$

$(ma, mb) = (ma_1 d, mb_1 d) = md(a_1, b_1)$

$= md(1)$

$= md = m(a,b)$

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

If $a = bq + r$ then show that $(a,b) = (b,r)$

Let $(a,b) = d \Rightarrow d \mid r$ $\because a - bq = r$

$(b,r) = d_1 \Rightarrow d_1 \mid a$ $\because a = bq + r$

Let $(a,b,r) = (d,r) = d_1$ $\because d \mid r$

$(a,b,r) = (a,d_1) = d_1$ $\because d_1 \mid a$

$\Rightarrow d = (a,d,r) = d_1$

$\Rightarrow d = d_1$

$\Rightarrow (a,b) = (b,r)$

Prove that if $(c,b) = 1$ then $(ac,b) = (a,b)$

Let $(ac,b) = d$

$\Rightarrow d \mid ac$ and $d \mid b$

$\because d \mid b$ and $(c,b) = 1$

$\Rightarrow d \nmid c$ and $d \mid a$

$\because d \mid a$ and $d \mid b$

$\Rightarrow (a,b) = d$

$\because (ac,d) = d = (a,b)$

$\Rightarrow (ac,d) = (a,b)$

Show that if $b \mid a$ and $c \mid a$ and $(b,c) = 1$ then $bc \mid a$.

$b \mid a \Rightarrow \frac{a}{b} = d_1 \Rightarrow a = bd_1 \rightarrow (i)$

$c \mid a \Rightarrow \frac{a}{c} = d_2 \Rightarrow a = cd_2 \rightarrow (ii)$

from (i) & (ii)

$\Rightarrow bd_1 = cd_2$

$\Rightarrow c \mid bd_1$

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

$\Rightarrow \frac{d_1}{c} = t \Rightarrow d_1 = ct$

$a = bd_1 = b(ct)$

$a = (bc)t$

$\Rightarrow bc \mid a$ Proved.

Show that if $(b,c) = 1$ then $(a,bc) = (a,b)(a,c)$

Let $(a,b) = d_1 \rightarrow ①$

$(a,c) = d_2 \rightarrow ②$

$(a,bc) = d_3 \rightarrow ③$

$① \Rightarrow b = md_1$

$② \Rightarrow c = nd_2$

$\Rightarrow bx + cy = mxd_1 + nyd_2$

$1 = mxd_1 + nyd_2$ $\because bx+cy=1$ $\because (b,c)=1$

$\Rightarrow (d_1, d_2) = 1 \rightarrow ④$

$① \& ③ \Rightarrow d_1 \mid d_3 \rightarrow ⑤$

$② \& ③ \Rightarrow d_2 \mid d_3 \rightarrow ⑥$

$④, ⑤ \& ⑥ \Rightarrow d_1 d_2 \mid d_3 \rightarrow Ⓐ$

Now $① \Rightarrow ax_1 + by_1 = d_1$

$② \Rightarrow ax_2 + cy_2 = d_2$

Multiplying the two equations.

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

$ax_1x_2a + ax_1y_2c + by_1ax_2 + by_1y_2c = d_1d_2$

$a(ax_1x_2 + cx_1y_2 + by_1x_2) + bc(y_1y_2) = d_1d_2 \rightarrow ⑦$

from ③ & ⑦ $\Rightarrow d_3 \mid d_1d_2 \rightarrow Ⓑ$

OR $(a,bc) = d_1d_2$

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

from Ⓐ & Ⓑ

$d_1 d_2 = d_3$.

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

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

Using Theorem:

If $(a,b) = 1$ then there exist $x,y \in z$ such that $ax + by = 1$

If $a_1, a_2, a_3, \ldots, a_k$ are non-zero integers show that

$$\langle a_1, a_2, a_3, \ldots, a_k \rangle = \langle \langle a_1, a_2, a_3, \ldots, a_{k-1} \rangle, a_k \rangle$$

Let

$m_1 = \langle a_1, a_2 \rangle$, $m_2 = \langle m_1, a_3 \rangle$, $m_3 = \langle m_2, a_4 \rangle$

$\ldots\ldots$ $m_{k-1} = \langle m_{k-2}, a_k \rangle$

then

$$m_{k-1} = \langle a_1, a_2, a_3, \ldots, a_k \rangle$$

we'll prove this by M.I.

C-I: Let it is true for $k=2$

$m_k = \langle a_1, a_2 \rangle$

Condition-I satisfied.

C-II: Let Suppose, this is true for $k=n$

$m_{n-1} = \langle a_1, a_2, a_3, \ldots, a_n \rangle \rightarrow (1)$

C-III: Now prove This true for $k=n+2$.

$m_{n+1} = \langle a_1, a_2, a_3, \ldots, a_{n+1} \rangle \rightarrow (2)$

$\because$ given. $m_n = \langle m_{n-1}, a_{n+1} \rangle \rightarrow (3)$

Now **Properties:**

(i) $m_n > 0$

(ii) $(1) \Rightarrow a_i \mid m_{n-1} \rightarrow (a)$ $\forall$ $i = 1, 2, 3, \ldots n$

$(3) \Rightarrow m_{n-1} \mid m_n \rightarrow (b)$ & $a_{n+1} \mid m_n \rightarrow (c)$

from (a) & (b)

$a_i \mid m_n \rightarrow (d)$ $\forall$ $i = 1, 2, 3, \ldots, n$

from (c) & (d)

$a_i \mid m_n$ $\forall$ $i = 1, 2, 3, \ldots, n, n+1$

(iii) Let 'c' be an integer s.t

$a_i \mid c$ $\forall$ $i = 1, 2, 3, \ldots, n, n+1$

$\Rightarrow a_i \mid c \rightarrow (e)$ $\forall$ $i = 1, 2, 3, \ldots, n$ & $a_{n+1} \mid m_n \rightarrow (f)$

from (1) & (e)

$m_{n-1} \mid c \rightarrow (g)$

from (f), (g) & (3)

$m_n \mid c$

If $a_1, a_2, a_3 \ldots\ldots a_m$ be integers not all zero and if

$d_1 = (a_1, a_2)$, $d_2 = (d_1, a_3)$, $d_3 = (d_2, a_4) \ldots\ldots$

$\ldots\ldots$ $d_{m-1} = (d_{m-2}, a_m)$

then $d_{m-1} = (a_1, a_2, a_3, \ldots\ldots, a_m)$

We'll prove this by M-I.

C-I: put $m=2$

$d_{2-1} = (a_1, a_2) \Rightarrow d_1 = (a_1, a_2)$ Satisfied.

C-II Let its true for $m=k$

i.e $d_{k-1} = (a_1, a_2, a_3, \ldots\ldots, a_k) \rightarrow (1)$

Now we prove this true for $m=k+1$

i.e $d_k = (a_1, a_2, a_3, \ldots\ldots, a_{k+1}) \rightarrow (2)$

we have $d_k = (d_{k-1}, a_{k+1}) \rightarrow (3)$

(i) $d_k > 0$ $\because$ d_k is g.c.d of d_{k-1} & a_{k+1}

(ii) $(3) \Rightarrow d_k \mid d_{k-1} \rightarrow (a)$ & $d_k \mid a_{k+1} \rightarrow (b)$

$(1) \Rightarrow d_{k-1} \mid (a_1, a_2, a_3 \ldots a_k) \rightarrow (c)$

from (a) & (c) $d_k \mid a_1, a_2, a_3, \ldots, a_k \rightarrow (d)$

from (b) & (d)

$d_k \mid a_i$ $\quad i = 1, 2, 3, \ldots, k, k+1$

Hence d_k is common divisor of a_i.

(iii) Let 'c' be an integer such that $c \mid a_i$

$i = 1, 2, 3, \ldots, k, k+1$

$c \mid a_i \Rightarrow c \mid a_1, a_2, a_3, \ldots, a_k \rightarrow (e)$ & $c \mid a_{k+1} \rightarrow (f)$

from (e) & (1)

$c \mid d_{k-1} \rightarrow (g)$

from (f) & (g) & (3)

$c \mid d_k$

Hence any comon divisor of $a_1, a_2, a_3, \ldots, a_k, a_{k+1}$ also divide d_k.

$\Rightarrow d_k$ is g.c.d of $a_1, a_2, a_3, \ldots, a_{k+1}$