Analytic Number Theory

DIVISIBILITY:-

Suppose $a, b \in Z$, then we say that a divides b if b is a multiple of a. If a divides b then a is also called the divisor of b.

We know that b is a multiple of a if

$$b = (some\ other\ integer) \times a$$

If we name that "some other integer" to be c, then the definition of divisibility is

a divides b if there exist an integer c such that

$$b = c.a$$

Notation:

If a divides b then we use the notation a/b. If a does not divide b then we use the notation

Theorem 1: show that $a/0$.

Proof:

As we know

$$0 = a.0$$

$$a/0 \qquad \forall\ 0 \in Z$$

Theorem 2: show that $1/a$ and $-1/a$.

Proof:

As by simple multiplication, we know that

$$a = 1.a$$

$$\Longrightarrow\ 1/a \qquad \forall\ a \in Z$$

Similarly, by using simple multiplication

$$a = (-1).(-a)$$

$$\Longrightarrow\ -1/a \qquad \forall\ -a \in Z$$

Theorem 3: ifa/b, then show that $a/b\ c$.

Proof:

If a/b, then ∃ a point $c_1 \in Z$ such that

$$b = a.c_1 \qquad (i)$$

Multiplying both sides by c, we have

$$bc = a.c_1.c$$

Umer Asghar (umermth2016@gmail.com) **For Online Skype Tuition (Skype ID): sp15mmth06678**

Since $\forall\, c, c_1 \in Z \qquad c.c_1 = c_2 (we\ say) \in Z$

Therefore,

$$bc = a.c_2$$

$$\Longrightarrow a/b\, c \quad \forall c_2 \in Z$$

This completes the proof.

Theorem 4: if a/b and b/a ,then show that $a = \pm b$.

Proof:

If a/b *and* b/a, *then there exists two integers* c_1, c_2 *such that*

$$b = a.c_1 \ldots\ldots (i)$$

$$a = b.c_2 \ldots\ldots (ii)$$

Using $(i) in\ (ii)$, we have

$$a = (a.c_1).c_2$$

$$\Longrightarrow a = a.c_1c_2$$

$$\Longrightarrow c_1c_2 = 1$$

This will be hold only if

$$c_1 = \pm 1\ \&\ c_2 = \pm 1$$

Using $c_2 = \pm 1\ in\ (ii)$, we have

$$a = b.(\pm 1)$$

$$\Longrightarrow a = \pm b$$

This completes the proof.

Theorem 5: if a/b and b/c ,then show that a/c.

Proof:

If a/b *and* b/c, *then by definition of divisibility, there exists two integers* c_1 & c_2 *such that*

$$b = a.c_1 \ldots\ldots (i)$$

$$c = b.c_2 \ldots\ldots (ii)$$

Using (i) in (ii), we have

$$c = (a.c_1).c_2$$

$$\Longrightarrow\ c = a.c_1.c_2$$

since $\forall\ c_1, c_2 \in Z, \qquad c_1.c_2 = c_3 (we\ say) \in Z$

Therefore,

$$c = a.c_3$$

$$\Longrightarrow a/c \quad \forall c_3 \in Z$$

This completes the proof.

Umer Asghar (umermth2016@gmail.com) **For Online Skype Tuition (Skype ID): sp15mmth06678**

Theorem 6: if a/b and a/c ,then $a/bx+cy$ for any integers x and y.

Proof:

If a/b and a/c, then by definition of divisibility, there exists two integers c_1 & c_2 such that

$$b = a.c_1 \ldots\ldots (i)$$

$$c = a.c_2 \ldots\ldots (ii)$$

Now consider

$$bx + cy = (a.c_1)x + (a.c_2)y$$

$$\Longrightarrow bx + cy = a.c_1x + a.c_2y$$

$$\Longrightarrow bx + cy = a(c_1x + c_2y)$$

Since $c_1, c_2, x, y \in Z$, $c_1x + c_2y = c_3 \in Z$

Therefore,

$$bx + cy = ac_3$$

$$\Longrightarrow a/bx + cy \qquad \forall c_3 \in Z$$

This completes the proof.

Theorem 7: if $a/b_1 + b_2$ and a/b_1 ,then a/b_2 .

Proof:

If $a/b_1 + b_2$ and a/b_1, then by definition of divisibility, there exists two integers c_1 & c_2 such that

$$b_1 + b_2 = a.c_1 \ldots\ldots\ldots (i)$$

$$b_1 = a.c_2 \ldots\ldots\ldots (ii)$$

Using $b_1 = a.c_2$ in (i), we have

$$a.c_2 + b_2 = a.c_1$$

$$\Longrightarrow b_2 = a.c_1 - a.c_2$$

$$\Longrightarrow b_2 = a.(c_1 - c_2)$$

Put $c_1 - c_2 = c_3 \in Z$ *where c_1 & c_2 both are the integers*. So that

$$b_2 = a.c_3$$

$$\Longrightarrow a/b_2 \qquad \forall\, c_3 \in Z$$

This completes the proof of the theorem.

Theorem 8:(DIVISION ALGORITHM OR EUCLIDE THEOREM)

If a and b are integers such that $b > 0$, then there exist unique integers q and r such that

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

Proof:

Consider that

$$A = \{a - bx \geq 0 : x \in Z\}$$

Note that A is non-empty.

If $0 \in A$, then by well ordering property 0 is least element of A. If $0 \notin A$, then A be the set that must have least element.

Let $r \in A$ be the least element. Then,

$$r = a - bx \quad where\ r \geq 0$$

Replace x by q, we have

$$r = a - bq \quad where\ r \geq 0$$

$$\Longrightarrow a = bq + r \quad where\ r \geq 0 \ldots\ldots (a)$$

Now, we have to prove $r < b$. For this, we suppose on contrary that

$$r \geq b \implies r - b \geq 0 \implies r - b \in A$$

But $r - b < r$

This is contradiction to our supposition. So our supposition is wrong and therefore

$$r < b \ldots\ldots (b)$$

Combining (a)& (b), we have

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

UNIQUENESS:

To prove uniqueness, we suppose that "If a and b are integers such that $b > 0$, then there exist unique integers q_1 and r_1 such that

$$a = bq_1 + r_1 \quad where \quad 0 \leq r_1 < b$$

$$\Longrightarrow bq + r = +r_1 \quad using\ (A)$$

$$\Longrightarrow bq - bq_1 = r_1 - r$$

$$\Longrightarrow b(q - q_1) = r_1 - r$$

Taking modulus on both sides, we have

$$|b(q - q_1)| = |r_1 - r|$$

$$\Longrightarrow b|(q - q_1)| = |r_1 - r| \ldots\ldots\ldots (1)$$

Since $r_1 < b$ & $r < b$. Then $|r_1 - r| < b$, so the equation (1) will become

$$b|(q-q_1)| < b$$

$$\Rightarrow |q-q_1| < 1$$

$$\Rightarrow |q-q_1| = 0$$

$$\Rightarrow q = q_1$$

Using $q = q_1$ in equation (1), we have

$$r = r_1$$

Hence $q = q_1$ and $r = r_1$ implies that both q and r are unique. This completes the proof of division algorithm.

APPLICATION OF DIVISION ALGORITHM:

Theorem 9: Every integer can be written in the form of $3n, 3n+1$ & $3n-1$.

Proof:

Let "a" be any integer. Then for $b = 3 > 0$, the euclide theorem will be

$$a = 3q + r \quad where \;\; 0 \leq r < 3$$

Here $0 \leq r < 3$ *implies that* $r = 0,1,2$

Case-1: when $r = 0$

Then,

$$a = 3q + 0$$

$$\Rightarrow a = 3q$$

$$\Rightarrow a = 3n \qquad by\ replacing\ q\ by\ n$$

Case-2: when $r = 1$

Then,

$$a = 3q + 1$$

$$\Rightarrow a = 3n + 1 \qquad by\ replacing\ q\ by\ n$$

Case-3: when $r = 2$

Then,

$$a = 3q + 2$$

$$\Rightarrow a = 3q + 3 - 1 \qquad since\ 2 = 3 - 1$$

$$\Rightarrow a = 3(q+1) - 1$$

$$\Rightarrow a = 3n - 1 \qquad by\ replacing\ q+1\ by\ n$$

This completes the proof.

Theorem 10: Every odd integer can be written in the form of $4n+1$ & $4n-1$.

Proof:

Let "a" be any odd integer. Then for $b=4>0$, the euclide theorem will be

$$a = 4q + r \quad where \;\; 0 \leq r < 4$$

Here $0 \leq r < 4$ *implies for odd integer that* $r = 1,3$

Case-1: when $r=1$

Then,

$$a = 4q + 1$$

$$\Longrightarrow a = 4n + 1 \qquad by\ replacing\ q\ by\ n$$

Case-2: when $r=3$

Then,

$$a = 4q + 3$$

$$\Longrightarrow a = 4q + 4 - 1 \qquad since\ \ 3 = 4 - 1$$

$$\Longrightarrow a = 4(q+1) - 1$$

$$\Longrightarrow a = 4n - 1 \qquad by\ replacing\ q+1\ by\ n$$

This completes the proof.

COMMON DIVISOR:

Suppose a and b be any two integers then a number "c" is called common divisor of a and b if

$$c/a \ \& \ c/b$$

EXAMPLE:-

2 is common divisor of the set $\{4,8\}$ *because*

$$2/4 \ \& \ 2/8$$

MATHEMATICAL INDUCTION:

It is a method which is often used to prove the divisibility based result. It is most powerful tool to prove the result in exponent form. To prove the result with the help of mathematical induction, we have to follow the following steps

- *First, we will check the result at n=1*
- *In the second step, we suppose that the result is true for n=k-1*
- *Now with the help of above supposition, we have to prove the result is true for n=k*

Remark:

If a result fulfilled the above three steps, then that result is true mathematically.

Theorem 11: If n is odd then $a+b/a^n+b^n$.

Proof:-

We use mathematical induction in order to prove the result.

- *When* $n=1$

$$a+b/a^1+b^1$$

$$\Longrightarrow a+b/a+b$$

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

- *Now, we suppose that the result is true for n=k. That is,*

$$a+b/a^k+b^k \qquad (\mathbf{1})$$

- *Now, we have to prove that the result is true for* $n=k+2$. *That is,*

$$a+b/a^{k+2}+b^{k+2} \qquad (to\ prove)$$

Consider that

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

$$a^{k+2}+b^{k+2}=a^k.a^2+a^kb^2-a^kb^2+b^k.b^2 \qquad (by\ adding\ and\ subtracting\ a^kb^2)$$

$$\Longrightarrow a^{k+2}+b^{k+2}=a^k(a^2-b^2)+b^2(a^k+b^k) \qquad (\mathbf{2})$$

Since $a+b/a^2-b^2 \quad (by\ division),\ and\ a+b/a^k+b^k \quad (by\ 1)$

Therefore,

$$a+b/a^k(a^2-b^2)+b^2(a^k+b^k) \qquad (by\ a\ result)$$

$$\Longrightarrow a+b/a^{k+2}+b^{k+2} \qquad (by\ \mathbf{2})$$

It follows that the result is true for $n=k+2$.

Hence, by principle of mathematical induction, it is proved that $a+b/a^n+b^n$.

Theorem 12: If n is odd then prove that $8/n^2-1$. .

Proof:

Since n is an odd number. Then, we have

$$n=2k+1 \qquad \forall\ k\in Z$$

$$\Longrightarrow n^2=(2k+1\ )^2 \qquad \forall\ k\in Z$$

$$\Longrightarrow n^2=4k^2+1+4k$$

$$\Longrightarrow n^2-1=4k(k+1) \qquad \forall\ k\in Z$$

Case -1:- When k is even. That is, $k=2k_1 \quad \forall\ k_1\in Z$

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

$$\Longrightarrow n^2-1=8.k_1(2k_1+1)$$

$$\Longrightarrow 8/n^2-1 \qquad \forall\ k_1(2k_1+1)\in Z$$

Case -2:- When k is odd. That is, $k = 2k_2 + 1 \quad \forall\, k_2 \in Z$

$$n^2 - 1 = 4(2k_2 + 1)(2k_2 + 1 + 1)$$
$$\Longrightarrow n^2 - 1 = 4(2k_2 + 1)(2k_2 + 2)$$
$$\Longrightarrow n^2 - 1 = 8.(2k_2 + 1)(k_2 + 1)$$
$$\Longrightarrow 8/n^2 - 1 \qquad \forall (2k_2 + 1)(k_2 + 1) \in Z$$

Hence in both above cases

$$8/n^2 - 1$$

This completes the proof.

Theorem 13: Show that the product of three consecutive natural number is divisible by 6.

Proof:-

Assume that n,n+1 and n+2 be three consecutive natural numbers.

We claim that

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

We use induction method in order to prove our claim

- *When n=1*

$$6/1(1 + 1)(1 + 2)$$
$$\Longrightarrow 6/1(2)(3)$$
$$\Longrightarrow 6/6$$

This implies that the result is true for n=1

- *Now, we suppose that the result is true for n=k. That is,*

$$6/k(k + 1)(k + 2)$$

- *Now, we have to prove that the result is true for n=k+1. That is,*

$$6/(k + 1)(k + 1 + 1)(k + 1 + 2)$$
$$= 6/(k + 1)(k + 2)(k + 3)$$
$$= 6/(k + 1)(k + 2)k + 3(k + 1)(k + 2)$$
$$\Longrightarrow 6/(k + 1)(k + 2)(k + 3) = 6/(k + 1)(k + 2)k + 6/3(k + 1)(k + 2)$$

Since $6/(k + 1)(k + 2)k$ is true by supposition.

Now, we prove that

$$6/3(k + 1)(k + 2) \ \ is\ true.$$

Case -1:- When k is even. That is, $k = 2k_1 \quad \forall\, k_1 \in Z$

$$6/3(k + 1)(k + 2) = 6/3(2k_1 + 1)(2k_1 + 2)$$
$$\Longrightarrow 6/3(k + 1)(k + 2) = 6/6(2k_1 + 1)(k_1 + 1)$$

The right hand side of above equation is true by division. Hence $6/3(k + 1)(k + 2)$ is true.

Case -2:- When k is odd. That is, $k = 2k_2 + 1 \quad \forall\ k_2 \in Z$

$$6/3(k+1)(k+2) = 6/3(2k_2+1+1)(2k_2+1+2)$$

$$\Longrightarrow 6/3(k+1)(k+2) = 6/3(2k_2+2)(2k_2+3)$$

$$\Longrightarrow 6/3(k+1)(k+2) = 6/6(k_2+1)(2k_2+3)$$

The right hand side of above equation is true obviously. Hence $6/3(k+1)(k+2)$ is true.

Thus in both above cases, we proved

$6/3(k+1)(k+2)$ *is true*

This implies that $6/(k+1)(k+2)(k+3)$.

It follows that the result is true for n=k+1.

Hence by principle of mathematical induction, it is proved that

" Product of three consecutive natural numbers is divisible by 6".

Theorem 14: Show that $14/3^{4n+2} + 5^{2n+1}$.

Proof:-

We use induction method in order to prove our result.

- *When $n = 1$. Then,*

  $14/3^{4(1)+2} + 5^{2(1)+1}$

  $\Longrightarrow 14/3^6 + 5^3$

  $\Longrightarrow 14/729 + 125$

  $\Longrightarrow 14/854$

  The result is true for $n = 1$.

- *Now, we suppose that the result is true for $n = k$. That is,*

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

- Now, we have to prove that the result is true for $n = k + 1$. That is,

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

  $= 14/3^{4k+6} + 5^{2k+3}$

  $= 14/3^{4k+2+4} + 5^{2k+1+2}$

  $= 14/3^{4k+2}.3^4 + 5^{2k+1}.5^2$

  $= 14/3^{4k+2}.81 + 5^{2k+1}.25$

  $= 14/3^{4k+2}.(56+25) + 5^{2k+1}.25$

  $= 14/56.3^{4k+2} + 25.3^{4k+2} + 5^{2k+1}.25$

  $= 14/56.3^{4k+2} + 25(3^{4k+2} + 5^{2k+1})$

Here

$14/56.3^{4k+2}$ *since by simple division*

$14/25(3^{4k+2}+5^{2k+1})$ *since by supposition*

Therefore,

$14/56.3^{4k+2}+25(3^{4k+2}+5^{2k+1})$ *is true*

This implies that the result is true for $n=k+1$.

Hence by principle of mathematical induction, it is proved that

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

Theorem 15: Show that $9/10^n+3.4^{n+2}+5$.

Proof:-

We use induction method in order to prove our result.

- *When* $n=1$. *Then,*

$9/10^1+3.4^{1+2}+5$

$\Longrightarrow 9/10+3.4^3+5$

$\Longrightarrow 9/10+3.64+5$

$\Longrightarrow 9/10+192+5$

$\Longrightarrow 9/207$

This implies that the result is true for n=1.

- *Now, we suppose that the result is true for* $n=k$. *That is,*

$9/10^k+3.4^{k+2}+5$

- Now, we have to prove that the result is true for $n=k+1$. That is,

$9/10^{k+1}+3.4^{k+1+2}+5$

$=9/10^{k+1}+3.4^{k+3}+5$

$=9/10^k.10^1+3.4^{k+2}.4+5$

$=9/10^k.10+12.4^{k+2}+5$

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

$=9/10^k.1+9.10^k+3.4^{k+2}+9.4^{k+2}+5$

$=9/(10^k+3.4^{k+2}+5)+9(10^k+4^{k+2})$

Here

$9/10^k+3.4^{k+2}+5$ *since by supposition*

$9/9(10^k+4^{k+2})$ *since by simple division*

Therefore,

$9/(10^k+3.4^{k+2}+5)+9(10^k+4^{k+2})$ *is true*

Umer Asghar (umermth2016@gmail.com) **For Online Skype Tuition (Skype ID): sp15mmth06678**

$\Longrightarrow 9/10^{k+1} + 3.4^{k+1+2} + 5$

That is, the result is true for $n = k + 1$.

Hence by principle of mathematical induction, it is proved that

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

Theorem 16: Show that $\mathbf{24/2.7^{n} + 3.5^{n} - 5}$.

Proof:-

We use induction method in order to prove our result.

- *When* $n = 1$. *Then,*

  $24/2.7^{1} + 3.5^{1} - 5$

  $\Longrightarrow 24/14 + 15 - 5$

  $\Longrightarrow 24/24$

  This implies that the result is true for $n = 1$

- *Now, we suppose that the result is true for* $n = k$. *That is*

  $24/2.7^{k} + 3.5^{k} - 5$

- Now, we have to prove that the result is true for $n = k + 1$. That is,

  $24/2.7^{k+1} + 3.5^{k+1} - 5$

  $= 24/2.7^{k}.7^{1} + 3.5^{k}.5^{1} - 5$

  $= 24/14.7^{k} + 15.5^{k} - 5$

  $= 24/(2 + 12).7^{k} + (3 + 12).5^{k} - 5$

  $= 24/2.7^{k} + 12.7^{k} + 3.5^{k} + 12.5^{k} - 5$

  $= 24/(2.7^{k} + 3.5^{k} - 5) + 12(7^{k} + 5^{k})$

  Here

  $24/2.7^{k} + 3.5^{k} - 5$ $\quad since\ by\ supposition$

  $24/2.12(7^{k} + 5^{k})$ $\quad since\ by\ division$

Therefore,

$24/(2.7^{k} + 3.5^{k} - 5) + 12(7^{k} + 5^{k})$ $\ is\ true.$

This implies that the result is true for $n = k + 1$.

Hence by principle of mathematical induction, it is proved that

$24/2.7^{n} + 3.5^{n} - 5$

Theorem 17: Show that $64/7^{2n} + 16n - 1$.

Proof:-

We use induction method in order to prove our result.

- *When* $n = 1$. *Then,*

  $64/7^{2(1)} + 16(1) - 1$

  $\Longrightarrow 64/49 + 16 - 1$

  $\Longrightarrow 64/64$

  This implies that the result is true for $n = 1$.

- *Now, we suppose that the result is true for* $n = k$. *That is*

  $64/7^{2k} + 16k - 1$

- Now, we have to prove that the result is true for $n = k + 1$. That is,

  $$64/7^{2(k+1)} + 16(k+1) - 1$$
  $$= 64/7^{2(k+1)} + 16(k+1) - 1$$
  $$= 64/7^{2k+2} + 16k + 16 - 1$$
  $$= 64/7^{2k}.7^2 + 16k + 16 - 1$$
  $$= 64/7^{2k}.49 + 16k(49 - 48) + 16 - (49 - 48)$$
  $$= 64/7^{2k}.49 + 49.16k - 48.16k + 16 - 49 + 48$$
  $$= 64/49(7^{2k} + 16k - 1) - 768k + 64$$
  $$= 64/49(7^{2k} + 16k - 1) + 64(1 - 12k)$$

Here

$64/49(7^{2k} + 16k - 1)$ $since\ by\ supposition$

$64/64(1 - 12k)$ $since\ by\ division$

Therefore,

$64/49(7^{2k} + 16k - 1) + 64(1 - 12k)\ is\ true$

This implies that the result is true for $n = k + 1$.

Hence by principle of mathematical induction, it is proved that

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

GREATEST COMMON DIVISOR:

The largest positive integer that divides both a and b is called greatest common divisor of a and b. it is denoted as (a, b).

EXAMPLE:-

Let us calculate the g.c.d of 42 and 48

Divisor of 42$= \{1,2,3,6,7,14,21,42\}$

Divisor of 48$= \{1,2,3,4,6,8,12,16,24,48\}$

Common Divisor of 42 & 48$= \{1,2,3,6\}$

Therefore,

$$(42,48) = 6$$

LINEAR COMBINITION:-

Suppose a and b be any two integer then "m" is called linear combination of a and b if $\forall\ x, y \in Z$, *we have*

$$m = ax + by$$

Remark:

The greatest common divisor of two numbers a and b is the smallest positive linear combination of a and b. that is,

$$(a, b) = ax + by$$

RELATIVELY PRIME:

The integers a and b is called relatively prime if $(a, b) = 1$. *More generally, it is defined as*

"The integers$m_1, m_2, \ldots\ldots, m_n$ *are relatively prime if every pair of* m_i *is relatively prime i.e.*

$$(m_i, m_j) = 1, \text{ whenever } \neq j \text{ ".}$$

Remark: *Any two consecutive numbers are relatively prime.*

Proof:

Assume that n and n+1 are two consecutive integers. Then for all$x, y \in Z$, *we have*

$$(n, n+1) = nx + (n+1)y$$

Take$x = -1\ \&\ y = 1$, *then we have*

$$(n, n+1) = n(-1) + (n+1)1$$

$$\Longrightarrow (n, n+1) = 1$$

This completes the proof.

Theorem18: If c is any common divisor of a and b, then c divides (a, b).

Proof:

Suppose c is common divisor of a and b. Then by definition

$$c/a \ \& \ c/b$$

Then by a result, we have

$$c/ax + by$$

$$\Longrightarrow c/(a,b) \quad Because\ (a,b) = ax + by$$

This proves the result.

Alternative Definition of G.C.D

In view of the previous result we can reformulate the definition of g.c.d.

Definition: A positive integer d is called g.c.d of a and b if

I. $d \geq 0$

II. $d|a$ *and* $d|b$

III. If some other integer $e|a$ *and* $e|b$*, then* $e|d$.

Theorem 19: The greatest common divisor of a & b is unique.

Proof:-

Suppose $(a,b) = d_1 \ \& (a,b) = d_2$

Then, we have to show that

$$d_1 = d_2$$

If "d_2" is G.C.D of a & b and "d_1" is common divisor of a & b. Then, by definition of G.C.D, we have

$$d_1/d_2 \qquad (A)$$

If "d_1" is G.C.D of a & b and "d_2" is common divisor of a & b. Then, by definition of G.C.D, we have

$$d_2/d_1 \qquad (B)$$

From (A) & (B)*, we have*

$$d_1 = \pm d_2$$

Since d_1 & d_2 *are non-negative. Therefore.*

$$d_1 = d_2$$

Theorem 20: If $(a,b)=1$ then show that $(a-b,a+b)=1$ or 2.

Proof:-

Suppose that

$$(a-b,a+b)=d \qquad (A)$$

This implies by alternative definition of G.C.D, we have

$$d/a-b\ ,d/a+b$$
$$\Rightarrow d/a-b+a+b\ \ \&\ \ d/a-b-a-b$$
$$\Rightarrow d/2a\ \ \&\ \ d/-2b$$
$$\Rightarrow d/2a\ldots..(a)\ \ \&\ \ d/2b\ldots..(b)$$

Since it is given that $(a,b)=1$

$\Rightarrow \exists$ *Two integers* x *&* y *such that*

$$ax+by=1$$
$$\Rightarrow 2ax+2by=2\ldots\ldots(i)$$

From (a)*&* (b)*, we have*

$$d/2a\ \&\ d/2b$$
$$\Rightarrow d/2ax\ \&\ d/2by$$
$$\Rightarrow d/2ax+2by$$
$$\Rightarrow d/2 \qquad from\ (i)$$

Since 2 is a prime number. Therefore,

$$d=1\ or\ 2$$

Using $d=1$ *or* 2 *in equation (A), we have*

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

This completes the proof.

Theorem 21: Let a and b be integers. Then

(I) $(ca.cb)=c(a,b)$ ***for any positive integer c;***

(II) $\left(\frac{a}{d},\frac{b}{d}\right)=1$ ***if*** $d=(a,b)$***.***

Proof:-

I. $(ca.cb)=c(a,b)$ ***for any positive integer c;***

As we know "The greatest common divisor of two numbers a and b is the smallest positive linear combination of a and b". Therefore,

$$(ca.cb)=ca(x)+cb(y) \qquad \forall\ x,y\in Z$$
$$(ca.cb)=c(ax+by) \qquad \forall\ x,y\in Z$$

Umer Asghar (umermth2016@gmail.com) **For Online Skype Tuition (Skype ID): sp15mmth06678**

Here $ax + by$ is the smallest linear combination of a and b. therefore,

$$ax + by = (a, b)$$

It follows that,

$$(ca.cb) = c(a, b) \quad for\ any\ integer\ c$$

II. $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$ ***if*** $\boldsymbol{d = (a, b)}$.

Since $d = (a, b)$. Then, $\frac{a}{d}$ & $\frac{b}{d}$ both are integers.

Now consider that,

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

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

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

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

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

This completes the proof.

Theorem 22: If $\boldsymbol{(a, b) = d}$ ***then*** $\boldsymbol{(ma.mb) = md.}$

Proof:-

Since it is given that $(a, b) = 1$

$\Longrightarrow$ *∃ Two integers x & y such that*

$$ax + by = d$$

$$\Longrightarrow max + mby = md \ldots\ldots. (i)$$

Let $(ma.mb) = d_1 \ldots\ldots\ldots. (A)$. Then, we have to show that $d_1 = md$

$$\Longrightarrow d_1/ma \ \ \& \ \ d_1/mb$$

$$\Longrightarrow d_1/max \ \ \& \ \ d_1/mby$$

$$\Longrightarrow d_1/max + mby$$

$$\Longrightarrow d_1/md \ldots\ldots\ldots\ldots\ldots (*)$$

As $(a, b) = d$. This implies by definition

$$d/a \ \ \& \ \ d/b$$

$$\Longrightarrow md/ma \ \ \& \ \ md/mb$$

The above shows that "md" is common divisor of ma and mb. But from (A), d_1 is G.C.D of ma and mb. Then by definition of G.C.D, we have

$$md/d_1 \dots\dots\dots\dots\dots (**)$$

Now from $(*)$ & $(**)$, we have

$$d_1 = md$$

It follows that

$$(ma.mb) = md$$

This completes the proof.

Theorem 23: If a/bc and $(a,b) = 1$, then a/c.

Proof:-

Since it is given $(a,b) = 1$

$\Longrightarrow$ *∃ Two integers x & y such that*

$$ax + by = 1$$

$$\Longrightarrow cax + cby = c \quad (by\ multiplying\ c\ on\ both\ sides)$$

Since

$$a/cax \quad (by\ division)$$

$$a/bcy \quad (\ by\ supposition)$$

$Therefore,$

$$a/cax + cby$$

$$\Longrightarrow a/c \quad (by\ 1)$$

This completes the proof.

Theorem 24: Let a, b and c be integers.

(I) If $(a,b) = (a,c) = 1$, then $(a,bc) = 1$

(II) If $a|c$, $b|c$ and $(a,b) = 1$, then $ab|c$.

Proof:-

I. $(a,b) = (a,c) = 1$, then $(a,bc) = 1$

Since $(a,b) = (a,c) = 1$. Then, there exists the integers s,t,x & y such that

$$as + bt = 1 \quad \Longrightarrow bt = 1 - as \quad (i)$$

$$ax + cy = 1 \quad \Longrightarrow cy = 1 - ax \quad (ii)$$

Multiplying (i) & (ii), we have

$$(bt)(cy) = (1 - as)(1 - ax)$$

$$\Longrightarrow bc(ty) = 1 - ax - as + a^2sx$$

Umer Asghar (umermth2016@gmail.com) **For Online Skype Tuition (Skype ID): sp15mmth06678**

$$\Longrightarrow bc(ty) = 1 - a(x + s - asx)$$

$$\Longrightarrow a(x + s - asx) + bc(ty) = 1$$

$$\Longrightarrow (a, bc) = 1 \quad (by\ definition)$$

II. $\boldsymbol{a|c,\ b|c\ and\ (a,b) = 1,\ then\ ab|c}$.

Since $a|c$ & $b|c$. *This implies that there exists two integers* c_1 & c_2 *such that*

$$c = ac_1 \qquad (i)$$

$$c = bc_2 \qquad (ii)$$

Also it is given that $(a, b) = 1$

$\Longrightarrow \exists$ *Two integers* x & y *such that*

$$ax + by = 1$$

$$\Longrightarrow cax + cby = c \quad (by\ multiplying\ c\ on\ both\ sides)$$

$$\Longrightarrow (bc_2)ax + (ac_1)by = c \qquad (by\ using\ (i)\ \&\ (ii))$$

$$\Longrightarrow abc_2x + abc_1y = c$$

$$\Longrightarrow ab(c_2x + c_1y) = c$$

$$\Longrightarrow c = ab(c_2x + c_1y)$$

$$\Longrightarrow ab/c \quad \forall\ c_2x + c_1y \in Z$$

This completes the proof

Theorem 25: If $\boldsymbol{(d_1, d_2) = 1, d_1/a\ \&\ d_2/a}$ ***then*** $\boldsymbol{d_1d_2/a.}$

Proof:

Since $d_1|a$ & $d_2|a$. *This implies that there exists two integers* c_1 & c_2 *such that*

$$a = d_1c_1 \qquad (i)$$

$$a = d_2c_2 \qquad (ii)$$

Also it is given that $(d_1, d_2) = 1$

$\Longrightarrow \exists$ *Two integers* x & y *such that*

$$d_1x + d_2y = 1$$

$$\Longrightarrow ad_1x + ad_2y = a \quad (by\ multiplying\ c\ on\ both\ sides)$$

$$\Longrightarrow (d_2c_2)d_1x + (d_1c_1)d_2y = a \qquad (by\ using\ (i)\ \&\ (ii))$$

$$\Longrightarrow d_1d_2c_2x + d_1d_2c_1y = a$$

$$\Longrightarrow d_1d_2(c_2x + c_1y) = a$$

$$\Longrightarrow a = d_1d_2(c_2x + c_1y)$$

$$\Longrightarrow d_1d_2/a \quad \forall\ c_2x + c_1y \in Z$$

This completes the proof

Theorem 26: If $(b,c)=1$ & a/c ***, then*** $(a,b)=1$.

Proof:-

If a/c *, then there exist an integer* c_1 *such that*

$$c = a\,c_1 \ \ldots\ldots\ldots\ (a)$$

Also it is given that $(b,c)=1$

$\Longrightarrow \exists\ Two\ integers\ x\ \&\ y\ such\ that$

$$bx + cy = 1$$

$$\Longrightarrow bx + a\,c_1 y = 1 \ldots\ldots (b) \qquad since\ c = a\,c_1$$

Let $(a,b)=d \ldots\ldots\ldots (c)$

Then we have to show that $d=1$.

As $(a,b)=d$. Then, by definition of G.C.D, we have

$$d/a \ \ \&\ \ d/b$$

$$\Longrightarrow d/ac_1y \ \ \&\ \ d/bx$$

$$\Longrightarrow d/ac_1y + bx$$

$$\Longrightarrow d/1 \qquad from\ (b)$$

$\Longrightarrow d=1$ *put in* (c)*, we have*

$$(a,b)=1$$

This completes the proof.

Theorem 27: If $(a,c)=1$ ***then*** $(a,bc)=(a,b)$.

Proof:-

Suppose that

$$(a,bc)=d_1 \qquad (i)$$

$$(a,b)=d_2 \qquad (ii)$$

Then, we have to show that $d_1=d_2$.

From (ii), we have

$$(a,b)=d_2$$

$$\Longrightarrow d_2/a \ \ \&\ \ d_2/b$$

$$\Longrightarrow d_2/a \ \ \&\ \ d_2/b\,c$$

Which shows that "d_2" is common divisor of a & bc. But from (i), it is clear that "d_1" is G.C.D of a & bc. This implies by the definition

$$d_2/d_1 \ldots\ldots\ldots\ldots\ldots (A)$$

Since $(a,c)=1$

$\Longrightarrow$ $\exists$ Two integers x & y such that

$$ax + cy = 1$$

$$\Rightarrow bax + bcy = b \qquad (iii)$$

Now from (i), we have

$$(a, bc) = d_1$$

$$\Rightarrow d_1/a \ \ \& \ \ d_1/bc$$

$$\Rightarrow d_1/bax \ \ \& \ \ d_1/b\,cy$$

$$\Rightarrow d_1/bax + bcy$$

$$\Rightarrow d_1/b \qquad from\ (iii)$$

$d_1/a \ \& \ d_1/b$ Implies that "d_1" is common divisor of a & b. But from (ii), G.C.D of a & b is "d_2".

Then by definition of G.C.D, we have

$$d_1/d_2 \ldots\ldots\ldots\ldots\ldots (B)$$

From (A)& (B), we have

$$d_1 = d_2.$$

Therefore,

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

This completes the proof.

Theorem 28: If $a = bq + r$ then show that $(a, b) = (b, r)$.

Proof:-

Suppose that

$$(a, b) = d_1 - - - - - (i)$$

$$(b, r) = d_2 - - - - - (ii)$$

$$a = bq + r - - - - - (iii)$$

From (ii), we have

$$(b, r) = d_2$$

$$\Rightarrow d_2/b \ \ \& \ \ d_2/r$$

$$\Rightarrow d_2/bq \ \ \& \ \ d_2/r$$

$$\Rightarrow d_2/bq + r$$

$$\Rightarrow d_2/a \qquad from\ (iii)$$

$d_2/a \ and \ d_2/b$ Shows that "d_2" is common divisor of a & b. But from (i), G.C.D of a & b is "d_1".

Then by definition of G.C.D, we have

$$d_2/d_1 - - - - - - - - - (A)$$

From (i), we have

$$(a,b) = d_1$$
$$\Rightarrow d_1/a \ \ \& \ \ d_1/b$$
$$\Rightarrow d_1/a \ \ \& \ \ d_1/bq$$
$$\Rightarrow d_1/a - bq$$
$$\Rightarrow d_1/r \qquad since \ \ r = a - bq \ \ from \ (iii)$$

$d_1/b \ \& \ d_1/r$ Shows that "d_1" is common divisor of b & r. But from (ii), G.C.D of b & r is "d_2". Then by definition of G.C.D, we have

$$d_1/d_2 - - - - - - - - - - (B)$$

From (A)& (B), we have

$$d_1 = d_2$$

Therefore,

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

This completes the proof.

Theorem 29: If $(b,c) = 1$ then show that $(a,bc) = (a,b)(a,c)$.

Proof:-

Suppose that

$$(a,b) = d_1 - - - - - (i)$$
$$(a,c) = d_2 - - - - - (ii)$$
$$(a,bc) = d_3 - - - - - (iii)$$

From (i), we have

$$(a,b) = d_1$$
$$\Rightarrow d_1/a \ \ \& \ \ d_1/b$$
$$\Rightarrow d_1/a \ \ \& \ \ d_1/bc$$

This Shows that "d_1" is common divisor of a & bc. But from (iii), G.C.D of a & bc is "d_3". Then by definition of G.C.D, we have

$$d_1/d_3 - - - - - - - - - - (A)$$

From (ii), we have

$$(a,c) = d_2$$
$$\Rightarrow d_2/a \ \ \& \ \ d_2/c$$
$$\Rightarrow d_2/a \ \ \& \ \ d_2/bc$$

This Shows that "d_2" is common divisor of a & bc. But from (iii), G.C.D of a & bc is "d_3". Then by definition of G.C.D, we have

$$d_2/d_3 - - - - - - - - - - (B)$$

Since it is given that $(b,c) = 1$

$\Longrightarrow$ $\exists$ *Two integer* x & y *such that*

$$bx + cy = 1 - - - - (iv)$$

From (i) & (ii)*, we have*

$$d_1/b \quad \& \quad d_2/c$$

$\Longrightarrow$ $\exists$ *The integers* m & n *such that* $b = d_1 m \ \& \ c = d_2 n$

Put in (iv)*, we have*

$$d_1 mx + d_2 ny = 1$$

$$\Longrightarrow (d_1, d_2) = 1 \ldots\ldots (v) \qquad \forall\, m,n,x,y \in Z$$

From (A) & (B)*, we have*

$$d_3 = d_1 f - - - (vi) \ \&$$

$$d_3 = d_2 g - - - (vii) \quad \forall\, f,g \in Z$$

From (v)*, we have*

$$(d_1, d_2) = 1$$

$$\Longrightarrow d_1 x + d_2 y = 1 \quad \forall\, x,y \in Z$$

$$\Longrightarrow d_3 d_1 x + d_3 d_2 y = d_3 \ \ multiplying\ with\ d_3$$

$$\Longrightarrow (d_2 g) d_1 x + (d_1 f) d_2 y = d_3$$

$$\Longrightarrow d_1 d_2 (gx + fy) = d_3$$

$$\Longrightarrow d_1 d_2 / d_3 - - - - (C)$$

From(i) $\quad ax_1 + by_1 = d_1 - - - (viii)$

From(i) $\quad ax_2 + cy_2 = d_2 - - - (ix)$

Multiplying $(viii)$& (ix)*, we have*

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

$$\Longrightarrow ax_1 x_2 a + ax_1 cy_2 + ax_2 by_1 + bcy_1 y_2 = d_1 d_2$$

$$\Longrightarrow a(x_1 x_2 a + x_1 cy_2 + x_2 by_1) + bc(y_1 y_2) = d_1 d_2$$

$$\Longrightarrow (a, bc) = d_1 d_2$$

$$\Longrightarrow (a, bc) = (a, b)(a, c).$$

This completes the proof.

Least Common Multiple

Definition(l.c.m):-

The smallest positive integer which is multiple of two numbers a and b is called the lease common multiple of a and b and is denoted by $< a, b >$.

Alternative definition of L.C.M:-

An integer "m" is called L.C.M of a & b if it satisfies the following axioms:

- $m > 0$
- a/m , b/m
- *If* a/c , b/c *then* m/c

Theorem 30: L.C.M of two numbers a & b is unique.

Proof:-

Suppose that $m_1 =< a, b >$ & $m_2 =< a, b >$.

- *If "m_1" is L.C.M of a, b then m_2 is common multiple of a, b. Then by definition of L.C.M, we have*

$$m_1/m_2 - - - - - (*)$$

- *If "m_2" is L.C.M of a, b then m_1 is common multiple of a, b. Then by definition of L.C.M, we have*

$$m_2/m_1 - - - - - (**)$$

From $(*)$& $(**)$*, we have*

$$m_1 = m_2$$

This proves the uniqueness of the L.C.M.

Theorem 31: If $(a, b) = d$ then show that $m =< a, b >= \frac{|ab|}{d}$.

Proof:-

To prove "m" is L.C.M of a, b we shall prove that "m" satisfies all the axioms of L.C.M

- *As "d" is greatest common divisor of a & b. Then, $d > 0$*

Also, $|ab| > 0$

$$\Longrightarrow m = \frac{|ab|}{d} > 0.$$

$$\Longrightarrow m > 0$$

This is the 1st axiom of L.C.M

- *Since it is given* $(a, b) = d$

$$d/a \ \& \ d/b$$

If d/a*, then* $\exists$ *a point* $a_1 \in Z$ *such that*

Umer Asghar (umermth2016@gmail.com) For Online Skype Tuition (Skype ID): sp15mmth06678

$$a = d.a_1$$

If d/b, *then* $\exists$ *a point* $b_1 \in Z$ *such that*

$$b = d.b_1$$

Therefore,

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

$$= \frac{|da_1.db_1|}{d}$$

$$m = |a_1 b_1 d|$$

$$\Longrightarrow m = |ab_1|\ , m = |a_1 b|$$

$$\Longrightarrow a/m\ , b/m$$

This is the 2^{nd} *axiom of L.C.M.*

- *Let* $a/c\ \&\ b/c$. *Then* $\exists$ *two integers* $d_1\ \&\ d_2$ *such that*

$$c = ad_1\ \&\ c = bd_2$$

Since $(a, b) = d$ *implies that*

$$a = d.a_1\ \&\quad b = d.b_1$$

Therefore, $c = a_1 dd_1 - - - (i)\ \&\ c = b_1 dd_2 - - - (ii)$

Comparing (i) & (ii), we have

$$a_1 dd_1 = b_1 dd_2$$

$$\Longrightarrow a_1 d_1 = b_1 d_2$$

$$\Longrightarrow b_1 d_2 = a_1.d_1$$

$$\Longrightarrow a_1/b_1 d_2$$

$$\Longrightarrow a_1/d_2$$

The above last expression implies that $\exists\ t \in Z$ *such that*

$$d_2 = a_1.t$$

Substituting $d_2 = a_1.t$ *in* (ii), *we have*

$$c = b_1 d(a_1.t)$$

$$\Longrightarrow c = a_1 b_1 d.t$$

$$\Longrightarrow c = m.t \quad since\ m = |a_1 b_1 d|$$

$$\Longrightarrow\ m/c$$

This is the 3^{rd} *axiom of L.C.M.*

Since "m" satisfies all the axiom of L.C.M. So "m" is L.C.M of a, b *and therefore,*

$$\boldsymbol{m =< a, b >= \frac{|ab|}{d}}$$