Number Theory: Handwritten Notes

by

Atiq ur Rehman

http://www.MathCity.org/atiq

Partial Contents

0937PST
Thursday
14-10-04

"Number Theorey"

Divisibility:-

Let $a, b \in \mathbb{Z}$, we say 'a' divide b if $\exists\ c \in \mathbb{Z}$ such that $b = ac$.

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

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

If 'a' does not divide b, we write $a \nmid b$.

Theorem:-

i) $a \mid 0$, $a \in \mathbb{Z}$ $(a \neq 0)$

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

iii) If $a \mid b$ and $c \in \mathbb{Z}$, then $a \mid bc$.

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

v) If $a \mid b$ and $b \mid c$ then $a \mid c$.

vi) $a \mid a$ for every $a \in \mathbb{Z}$.

vii) If $a \mid b$ and $a \mid c$ then $a \mid bx + cy$ $\forall\ x, y \in \mathbb{Z}$.

viii) If $a \mid b_1 + b_2$ and $a \mid b_1$ then $a \mid b_2$.

Proof:-

i) $a \mid 0$, $a \in \mathbb{Z}$

Since $0 = a \cdot 0 \Rightarrow a \mid 0$

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

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

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

iii) If $a \mid b$ and $c \in \mathbb{Z}$ then $a \mid bc$.

$a \mid b \Rightarrow \exists\ c_1 \in \mathbb{Z}$ such that $b = ac_1$

$bc = ac_1c$, $c_1c \in \mathbb{Z}$

Let $c_1c = c_2$

$\Rightarrow bc = ac_2 \Rightarrow a \mid bc$.

iv) If $a \mid b$ and $b \mid a$ then $a = \pm b$.

$a \mid b \Rightarrow b = ac$ for $c \in \mathbb{Z}$

and $b \mid a \Rightarrow a = bc_1$ for $c_1 \in \mathbb{Z}$

$\Rightarrow b = bc_1c$

$\Rightarrow b - bc_1c = 0$

$\Rightarrow b(1 - c_1c) = 0$

$\Rightarrow |b|\,|1 - c_1c| = 0$ *

* $\Rightarrow c_1c = 1$

$\Rightarrow$ either $c = 1$ and $c_1 = 1$

or $c = -1$ and $c_1 = -1$

in both cases

$a = \pm b$

(v) If $a \mid b$ and $b \mid c$ then $a \mid c$

$a \mid b \Rightarrow \exists\ c_1 \in Z$ such that $b = ac_1$

and $b \mid c \Rightarrow \exists\ c_2 \in Z$ such that $c = bc_2$

we have to show that $a \mid c$.

then

$c = ac_1c_2$

Now $c_1c_2 \in Z \Rightarrow c_1c_2 = c_3 \in Z$

$\Rightarrow c = ac_3 \Rightarrow a \mid c$.

vi) Since $a = a \cdot 1 \Rightarrow a \mid a$.

vii) If $a \mid b$ and $a \mid c$ then $a \mid bx + cy\ \ \forall\ x, y \in Z$.

$a \mid b \Rightarrow \exists\ c_1 \in Z$ such that $b = ac_1 \Rightarrow bx = ac_1x$

$a \mid c \Rightarrow \exists\ c_2 \in Z$ such that $c = ac_2 \Rightarrow cy = ac_2y$

$\Rightarrow bx + cy = ac_1x + ac_2y = a(c_1x + c_2y) = ac_3$

$\Rightarrow a \mid bx + cy$.

viii) $a \mid b_1 + b_2 \Rightarrow b_1 + b_2 = ac$ for $c \in Z$.

and $a \mid b_1 \Rightarrow b_1 = ac_1$ for $c_1 \in Z$

then $b_1 + b_2 = ac \Rightarrow ac_1 + b_2 = ac$

$\Rightarrow b_2 = ac - ac_1$

$= a(c - c_1)$

$= ac_2 \quad , c_2 \in Z$

$\Rightarrow a \mid b_2$.

Division Algorithm:-

If $P_1(x), P_2(x) \in R[x]$ and $P_2(x) \neq 0$, then $\exists$ $q(x)$ and $r(x)$ in $R[x]$ such that

$$P_1(x) = q(x)P_2(x) + r(x) \quad ; \deg r(x) < \deg P_2(x) \text{ or } r(x) = 0$$

Greatest Common Divisor:-

The greatest common divisor $d(x)$ of $P_1(x)$ and $P_2(x)$ is defined as:

i) If $d(x) \mid P_1(x)$ and $d(x) \mid P_2(x)$; $d(x) \in R[x]$
ii) If $d_1(x) \mid P_1(x)$ and $d_1(x) \mid P_2(x)$ then $d_1(x) \mid d(x)$

Remarks:

If $(P_1(x), P_2(x)) = d(x)$, then there are $q_1(x)$, $q_2(x)$ in $R[x]$ such that

$$d(x) = P_1(x)q_1(x) + P_2(x)q_2(x)$$

Algebraic Numbers:

If α is a root (zero) of polynomial equation $P(x) = x^n + r_1 x^{n-1} + \cdots + r_n = 0$ where $P(x) \in R[x]$, and $n > 0$, then α is called an algebraic number.

Degree of Algebraic Number:-

If $p(x)$ is irreducible polynomial then α is ~~called~~ said to be of degree n.

e.g $\sqrt{2}$ is of degree 2 (x^2-2 is irreducible)
$\sqrt[3]{2}$ is of degree 3.

All the rational number are algebraic number of degree 1

Minimal or defining polynomial:-

A polynomial $P(x) \in R[x]$ is called the minimal or defining polynomial for an algebraic number α if $p(x)$ is unique irreducible; monic polynomial, otherwise α would satisfy a polynomial of lower degree.

e.g x^2-5 is ~~are~~ minimal polynomial of $\sqrt{5}$

$\frac{1}{5}x^2-1$, x^3-5x are not minimal polynomials of $\sqrt{5}$.

Conjugates of algebraic number: α :-

If $p(x)$ is a minimal polynomial of α, then for $p(x) = a_0 + a_1 x + \cdots + a_n x^n$ has n zero's $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_n$ are called conjugate of α.

e.g $\sqrt[3]{2}$ being a root of polynomial x^3-2 is an algebraic number of degree 3.

its conjugates are $\sqrt[3]{2}$, $\sqrt[3]{2}\,\omega$ and $\sqrt[3]{2}\,\omega^2$

where $\omega = \frac{1}{2}(-1+\sqrt{3}\,i)$

End of Lesson at 1033 PST

0938 PS

Friday

15 - - 04

Review (The Theorem of Euclid)

Let $a, b \in \mathbb{Z}$, $b > 0$ then $\exists$ unique q and r such that $a = bq + r$, $0 \leq r < b$.

Remarks:-

i) In this theorem "a" divided by b, q is called quotient and r is called the remainder.

ii) If $r = 0$, we say b divides a, conversely if $b \mid a$ then $r = 0$.

iii). If $b = 2$, then $r = 0$ or $r = 1$.

It means every integer is either of the form $2k$ or $2k+1$.

If it is of the form $2k$, it is called even.

If it is of the form $2k+1$, it is called odd.

Example:-

Every integer can be written in one of the three forms $3n$, $3n+1$, $3n-1$,

Proof:

Let a be any integer then by Euclid theorem $a = 3k + r$, $0 \leq r < 3$ i.e $r = 0, 1, 2$

If $r = 0$ and $k = n$ $\Rightarrow$ $a = 3n$

If $r = 1$ and $k = n$ $\Rightarrow$ $a = 3n + 1$

If $r = 2$ $\Rightarrow$ $a = 3k + 2$

$= 3k + 3 - 1 = 3(k+1) - 1$

$= 3n - 1$ if $n = k + 1$

Hence every integer can be written in the form of $3n$, $3n+1$ or $3n-1$ where $n \in \mathbb{Z}$.

Example:-

Every odd integer can be written in the form of $4k+1$ or $4k-1$, $k \in \mathbb{Z}$

Do yourself.

Hint: Take $2k+1$ as odd intege.

iii) If n is odd, $a+b \mid a^n+b^n$

we prove this assertion by induction on n.

C-I For $n=1$, result is true

C-II Let $a+b \mid a^k+b^k$, we prove $a+b \mid a^{k+2}+b^{k+2}$

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

$\because a+b \mid a^k+b^k$ and $a+b \mid a^2-b^2$.

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

The induction is complete.

Problem:-

If n is odd, then $8 \mid n^2-1$

Solution:-

Let $n = 2k+1$, $k \in \mathbb{Z}$

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

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

Now k is either even or odd

If k is even, $k = 2k_1$ for $k_1 \in \mathbb{Z}$, then

$n^2-1 = 8k_1(2k_1+1) \rightarrow 8 \mid n^2-1$

If k is odd i.e $k = 2k_2+1$ for $k_2 \in \mathbb{Z}$ then

$$n^2-1 = 4(2k_2+1)(2k_2+1+1)$$
$$= 4(2k_2+1)(2k_2+2) = 8(2k_2+1)(k_2+1)$$

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

Exercise:-

Show that the product of any three consective integers is divisible by 6.

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

$= 8(2k_2+1)(k_2+1) \Rightarrow 8 \mid n^2-1$.

Example:- Show that the product of any three consecutive integers is divisible by 6.

Sol:- Suppose that the three consecutive numbers are $n, (n+1), (n+2)$. We prove this theorem by M.I.

C-1 For $n=1$ $6 \mid (1)(1+1)(1+2) \Rightarrow 6 \mid 6 \Rightarrow$ The result is true for $n=1$

C-2 For $n=k$ $6 \mid k(k+1)(k+2) \longrightarrow (A)$

We have to prove for $n=k+1 \Rightarrow 6 \mid (k+1)(k+2)(k+3)$.

$$6 \mid \underset{(\text{I})}{k(k+1)(k+2)} + 6 \mid \underset{(\text{II})}{3(k+1)(k+2)}$$

$(k+1)(k+2)(k+3)$

(I) is proved by (A). Now we check (II)

Now k is either even or odd. If k is even, $k=2k_1$, $k_1 \in Z$ then $6 \mid 3(2k_1+1)(2k_1+2) \Rightarrow 6 \mid 6(2k_1+1)(k_1+1)$

If k is odd i.e. $k = 2k_2+1$ for $k_2 \in Z$ Then

$6 \mid 3(2k_2+1+1)(2k_2+1+2)$.

$\Rightarrow 6 \mid 3(2k_2+2)(2k_2+3)$

$\Rightarrow 6 \mid 6(k_2+1)(2k_2+3)$

Hence $6 \mid (k+1)(k+2)(k+3)$

The induction is complete.

Base and Radix Representation:-

:- Every +ive integer can be written as

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

where $0 < r_n < 10$ and $0 \le r_i < 10$, $i = 0, 1, 2, \ldots, n-1$

This representation is called representation of 'a' in scale of ten and 10 is called base or radix.

Infact every fix integer $g > 1$ can serve as a base or radix.

Theorem:-

Let $g > 1$, then every +ive integer "a" can be written uniquely as

$$(1) \left\{ \begin{array}{l} a = r_n g^n + r_{n-1} g^{n-1} + \cdots + r_1 g + r_0 \\ 0 < r_n < g \quad \text{and} \quad 0 \le r_i < g \ ; \ i = 0, 1, 2, 3, \ldots, n-1 \end{array} \right.$$

Proof: If $a < g$, then we have the desired result.

$a = r_0$ for $n = 0$

If $a > g$, then by Euclid theorem, $\exists$ a unique integers q_0 and r_0 such that

$$a = q_0 g + r_0$$

$$q_0 > 0, \quad 0 \le r_0 < g, \quad \cancel{a > g}$$

If $q_0 < g$ then by taking $q_0 = r_1$, we have the desired form. $a = r_1 g + r_0$ for $n = 1$

If $q_0 \ge g$ then again by Euclid's theorem $\exists$ unique integers q_1 and r_1 such that

$$q_0 = q_1 g + r_1, \quad q_1 > 0 \ ; \ 0 \le r_1 < g$$

If $q_1 < g$, we have $a = q_1 g^2 + r_1 g + r_0$ then for $q_1 = r_2$ we have desire form

$$a = r_2 g^2 + r_1 g + r_0 \quad \text{for } n = 2$$

If $q_1 \ge g$, we repeat the process untill we obtain a quotient q_{n-1} such that

The proof is complete.

Note:-

In abbreviated form, we write

$$a = (r_n r_{n-1} r_{n-2} \cdots r_1 r_0)_g$$

The base is specified at right end. If no base is specified the integer is written in scale of 10.

Exercise:-

$$(123\alpha 4)_{12} \times (45\beta 9)_{12} = ?$$
$$(123\alpha 4)_{12} - (45\beta 9)_{12} = ?$$

Exercise:-

Show that $14 \mid 3^{4n+2} + 5^{2n+1}$, $n \geq 0$, $n \in \mathbb{Z}$.

Theorem:-

The G.C.D of a and b is unique, a and b are non-negative integers.

Proof.

Let $(a,b) = d_1$ and $(a,b) = d_2$

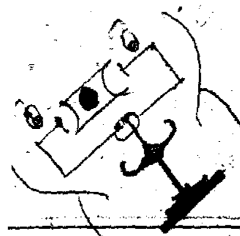
Now d_1 is common divisor of a and b, and d_2 is ~~common~~ G.C.D ~~divisor~~ of a and b, then $d_1 \mid d_2$.

Similarly if d_1 is G.C.D and d_2 is common divisor of a & b then $d_2 \mid d_1$

$\Rightarrow d_1 = \pm d_2$ but $d_1, d_2 > 0 \Rightarrow d_1 = d_2$.

This proves the uniqueness.

End of Lesson at 1107 PST.



Method of finding the G.C.D.

We suppose $a > b > 0$, then by Euclid's theorem $\exists$ unique integers q_1 and r_1 such that $a = bq_1 + r_1$ ——— (1) $0 \le r_1 < b$.
Then b is G.C.D of a and b, if $r_1 = 0$
If $r_1 \neq 0$, then $\exists$ unique integers q_2 and r_2 such that $b = q_2 r_1 + r_2$, $0 \le r_2 < r_1$ ——— (2)
If $r_2 \neq 0$, $\exists$ unique integers q_3 and r_3 such that

$$r_1 = q_3 r_2 + r_3 \quad ; \quad 0 \le r_3 < r_2 \quad \text{——— (3)}$$

We repeat this process until we obtain a remainder r_{k+1}, which is zero.

Then $r_{k-3} = q_{k-1} r_{k-2} + r_{k-1}$; $0 \le r_{k-1} < r_{k-2}$ ——— (k-1)

$$r_{k-2} = q_k r_{k-1} + r_k \quad , \quad 0 \le r_k < r_{k-1} \quad \text{——— (k)}$$

$$r_{k-1} = q_{k+1} r_k \quad \text{——— (k+1)}$$

~~Then r_k is the G.C.D of~~

We note the following properties of r_k.

i) $r_k > 0$
ii) $r_k \mid a$ and $r_k \mid b$
iii) From equation (1) to (k+1), we see that if $c \mid a$ and $c \mid b$ then $c \mid r_k$.

Hence r_k is the greatest common divisor of a and b.

Definition:-

An integer n is called linear combination of $a, b \in \mathbb{Z}$ if $\exists$ $x, y \in \mathbb{Z}$ such that

$$n = ax + by$$

Theorem:-

If $(a,b) = d$, then d can be expressed as a linear combination of a and b.

Proof. The method used above in finding the G.C.D is called Euclidean Algorithm. In the above process, we see

$$d = r_k = r_{k-2} - q_k r_{k-1}$$
$$= r_{k-2} - q_k(r_{k-3} - q_{k-1} r_{k-2})$$
$$= (1 + q_k q_{k-1}) r_{k-2} - q_k r_{k-3}$$

Proceeding in this way, we altemately obtain a relation $d = ax + by$

where x and y are polynomials in

$$q_k, q_{k-1}, q_{k-2}, \ldots, q_1$$

Exercise:-

Find the G.C.D of 105 and 275 and express it as a linear combination of 105 and 275.

Corollaries:-

i) If $(a,b) = 1$, then $\exists\ x, y \in \mathbb{Z}$ such that $ax + by = 1$

ii) If $c \mid ab$ and $(c, b) = 1$, then $c \mid a$.

Proof.

$(c, b) = 1 \Rightarrow \exists\ x, y \in \mathbb{Z}$ such that $cx + by = 1$

$\Rightarrow acx + aby = a$ ——— (1)

Now $c \mid acx$, and $c \mid aby$ (by hypothesis)

then c divides a, by (i) i.e $c \mid a$.

G.C.D of more than two integers:-

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

if i) $d > 0$

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

iii) If $c \mid a_i$; $i = 1, 2, \ldots, n$ then $c \mid d$.

then we write $(a_1, a_2, \ldots, a_n) = d$

Method of finding:-

Let $d_1 = (a_1, a_2)$, $d_2 = (d_1, a_3)$, ——
$d_{n-1} = (d_{n-2}, a_n)$ then
$d_{n-1} = (a_1, a_2, \ldots, a_n)$.

Exercise:-

Let $d = (a, b, c)$, then $d = ma + nb + kc$
where $m, n, k \in Z$.

Problem:-

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

Solution:

Let $(a-b, a+b) = d$, then $d \mid a-b$ and $d \mid a+b$
$\Rightarrow d \mid (a-b)+(a+b)$ i.e $d \mid 2a$
and $d \mid (a-b)-(a+b)$ i.e $d \mid -2b$

Now a and b are relatively prime
$\Rightarrow \exists\ x, y \in z$ such that $ax + by = 1$
$\Rightarrow 2ax + 2by = 2$ —— (i).
Now $d \mid 2a$ and $d \mid 2b$ $\Rightarrow d \mid$ (L.H.S of (i))
$\Rightarrow d \mid 2$ $\Rightarrow$ $d = 1$ or 2.

Exercise:-

If $(a, b) = 1$, then $(a-b, a+b, ab) = 1$.

Exercise:-

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

Exercise:-

If $(a, b) = d$ then $(ma, mb) = md$; $m > 0$.

Problem:-

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

Solution:-

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

$(a,c)=d_2$, we prove $d=d_1d_2$

Now $(b,c)=1$ and $d_1|b$, $d_2|c \Rightarrow (d_1,d_2)=1$

then $d_1|a$ and $d_2|a \Rightarrow d_1d_2|a$.

Next, $d_1d_2|a$ and $d_1d_2|bc$

$\Rightarrow d_1d_2$ is a common divisor of a and bc

but d is the greatest common divisor of a and bc.

$\Rightarrow d_1d_2|d$ ——— (i)

On the other hand $(a,b)=d_1$ and $(a,c)=d_2$

$\Rightarrow \exists\, x_1,y_1 \in Z$ and $x_2,y_2 \in Z$

such that $ax_1+by_1=d_1$.

and $ax_2+cy_2=d_2$

Multiplying these two equations, we obtain

$a^2x_1x_2+abx_2y_1+acx_1y_2+bcy_1y_2=d_1d_2$ ——— (ii)

Since $d|a$ and $d|bc$.

therefore $d|$ (L.H.S of (ii))

so this implies $d|d_1d_2$ ——— (ii)

By (i) and (ii), we have

$d=d_1d_2$

End of Lesson.

Theorem:- If $(a,b)=d$ then d can be expressed as linear combination of 'a' & 'b'.

Proof:- The method used in above theorem in finding the G.C.D is called Euclidean Algorithm. In the above process we see

$$d = r_k = r_{k-2} - q_k r_{k-1}$$

$$= r_{k-2} - q_k\left(r_{k-3} - q_{k-1} r_{k-2}\right)$$

$$= (1 + q_k q_{k-1}) r_{k-2} - q_k r_{k-3}$$

Proceeding in this way, we ultimately obtain a relation $d = ax + by$.
where a & b are polynomials in $q_k, q_{k-1}, q_{k-2}, \ldots, q_1$.
$\quad x \quad y$

Exercise:- Find the G.C.D of 105 and 275 and express it as a linear combination of 105 & 275.

Sol:-

$105 \,\big|\, 275 \;(2)$, 210

$65 \,\big|\, 105 \;(1)$, 65

$40 \,\big|\, 65 \;(1)$, 40

$25 \,\big|\, 40 \;(1)$, 25

$15 \,\big|\, 25 \;(1)$, 15

$10 \,\big|\, 15 \;(1)$, 10

$5 \,\big|\, 10 \;(2)$, 10, x

Hence
$(105, 275) = 5$
$275x + 105y = 5$

Rabi → Rabbit

Example:- Let $d = (a, b, c)$ then $d = ma + nb + kc$ where $m, n, k \in \mathbb{Z}$.

Sol:-

Problem:- If $(a, b) = 1$, then $(a-b, a+b) = 1$ or 2.

Sol:- Let $(a-b, a+b) = d$ then $d \mid a-b$ and $d \mid a+b$.

$\Rightarrow d \mid (a-b)+(a+b)$ i.e. $d \mid 2a$ and $d \mid (a-b)-(a+b)$

$\Rightarrow d \mid -2b \Rightarrow d \mid 2b$. Now a & b are relatively prime $\Rightarrow \exists\ x, y \in \mathbb{Z}$ s.t. $ax + by = 1 \Rightarrow 2ax + 2by = 2$. $\rightarrow$ (A)

Now $d \mid 2a$ & $d \mid 2b$ $\Rightarrow d \mid$ (L.H.S. of (A)) $\Rightarrow d \mid 2$

$\Rightarrow d = 1$ or 2.

Example:- If $(a, b) = 1$ then $(a-b, a+b, ab) = 1$.

Sol:-

Given that $(a, b) = 1$ & we already proved $(a-b, a+b) = 1$ or 2

$(1, ab) = 1$ & $(2, ab) = 1$

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

Exercise: If $(b,c)=1$ and $a|c$ then $(a,b)=1$.

Sol:

$(b,c)=1$ & $a|c \Rightarrow \exists\ c_1 \in Z$ s.t. $c = ac_1$

Let $(a,b)=d \Rightarrow d|a \Rightarrow d|a$ & $d|b \Rightarrow \exists\ a_1, b_1 \in Z$ s.t. $a = a_1 d$ & $b = b_1 d$, $(a_1, b_1)=1$

then $c = a_1 c_1 d \Rightarrow d|c$ & $d|b \Rightarrow d$ is the common divisor of b & c but 1 is the G.C.D. of c & $b \Rightarrow d|1 \Rightarrow d=1$.

Exercise:- If $(a,b)=d$ then $(ma, mb) = md$, $m>0$.

Sol:- $(a,b)=d \Rightarrow \exists\ x, y \in Z$ s.t. $ax+by=d \rightarrow (1)$

Suppose $(ma, mb) = d_1$. Multiplying (1) by m we have $max + mby = md \rightarrow (2)$

Now $d_1|ma$ & $d_1|mb \Rightarrow d_1|$ L.H.S of (2) $\Rightarrow d_1|md \rightarrow (3)$

Now $d|a$ & $d|b \Rightarrow md|ma$ & $md|mb \Rightarrow md$ is a common divisor of ma & mb. Hence by def. of G.C.D $md|d_1 \rightarrow (4)$

by (3) & (4) we have

$d_1 = md$. Q.E.D.

Problem:- If $(b,c)=1 \Rightarrow (a,bc) = (a,b)\cdot(a,c)$

Solution:- Let $(a,bc)=d$ and $(a,b)=d_1$, $(a,c)=d_2$ we prove $d = d_1 d_2$. Now $(b,c)=1$ and $d_1|b$, $d_2|c \Rightarrow (d_1, d_2)=1$. then $d_1|a$ & $d_2|a \Rightarrow d_1 d_2|a$.

Next $d_1 d_2|a$ & $d_1 d_2|bc \Rightarrow d_1 d_2$ is a common divisor of a & bc but d is the g.c.d of 'a' & 'bc' $\Rightarrow d_1 d_2|d \rightarrow (1)$

On the other hand $(a,b)=d_1$ & $(a,c)=d_2 \Rightarrow$

$\exists\ x_1, y_1 \in Z$ & $x_2, y_2 \in Z$ s.t. $ax_1 + by_1 = d_1$ and $ax_2 + cy_2 = d_2$. Multiplying these two eqs. we obtain

$$a^2 x_1 x_2 + ab\, x_2 y_1 + ac\, x_1 y_2 + bc\, y_1 y_2 = d_1 d_2 \rightarrow (2)$$

Since $d|a$ & $d|bc$ therefore $d|$ (L.H.S) of (2) so this implies $d|d_1 d_2 \rightarrow (3)$

by (1) & (3) we have $d = d_1 d_2$.

Hence proved.

Example:- Show that $14 | 3^{4n+2} + 5^{2n+1}$, $n \geq 0$, $n \in Z$

Sol:- We prove this by Mathematical Induction

C-I when $n = 1$

$$14 | 3^6 + 5^3 \Rightarrow 14 | 854.$$

The result is true for $n = 1$.

C-II when $n = k$.

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

we prove, this is true for $n = k+1$

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

we can write

$$\begin{aligned}
3^{4k+6} + 5^{2k+3} &= 3^{4k+4+2} + 5^{2k+1+2} \\
&= 3^{4k+2} \cdot 3^4 + 5^{2k+1} \cdot 5^2 \\
&= 3^{4k+2} \cdot 3^4 + 5^{2k+1} \cdot 5^2 + 3^{4k+2} \cdot 5^2 - 3^{4k+2} \cdot 5^2 \\
&= 3^{4k+2} \cdot 3^4 - 3^{4k+2}\, 5^2 + 3^{4k+2} \cdot 5^2 + 5^{2k+1} \cdot 5^2 \\
&= 3^{4k+2}(3^4 - 5^2) + (3^{4k+2} + 5^{2k+1}) 5^2 \\
&= 3^{4k+2} \cdot 56 + 5^2 (3^{4k+2} + 5^{2k+1})
\end{aligned}$$

Now $14 | 3^{4k+2} + 5^{2k+1}$ by hypothesis and also $14 | 56$.

$\Rightarrow \quad 14 | 5^2 (3^{4k+2} + 5^{2k+1}) + 56 \cdot 3^{4k+2}$

$\Rightarrow \quad 14 | 3^{4k+6} + 5^{2k+3}$. Hence it is true for $n = k+1$.

The induction is complete.

Example (i) $(2\alpha 34)_{12} \times (\beta 934)_{12}$ $\qquad \alpha = 10$

(ii) $(\alpha\alpha)_{12} + (\beta\beta)_{12}$ $\qquad \beta = 11$

Sol:- (i) $(\overset{3}{2}(10)\overset{1}{3}4)_{12}$

$((11)\,9\,3\,4)_{12}$

$$
\begin{array}{rrrrrrrr}
 & & & & (11) & 5 & 1 & 4 \\
 & & & 8 & 6 & (10) & 0 & \times \\
 & 2 & 1 & 8 & 6 & 0 & \times & \times \\
2 & 7 & 5 & 0 & 8 & \times & \times & \times \\
\hline
2 & 9 & 7 & 6 & 8 & 3 & 1 & 4
\end{array}
$$

(ii):-

$$
\begin{array}{r}
((10)(10))_{12} \\
+\ ((11)(11))_{12} \\
\hline
(1(10)9)_{12}
\end{array}
\Rightarrow (1\alpha 9)_{12}
$$

$4 = 1, 2, 4$
$8 = 1, 2, 4, 8$
$1, 2, 4$
G.C.D = 4

0943 PST
Tuesday
19-10-04

Problem:-

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

Solution:-

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

We prove $d_1 \mid a$ and $d_1 \mid b \Rightarrow d_1 \mid bc$

Now $d_1 \mid a$ and $d_1 \mid b \Rightarrow \boxed{d_1 \mid bc}^{*}$

$\Rightarrow d_1$ is a common divisor of a & bc.

then $d_1 \mid d$. ——— (1)

Next, $(a, c) = 1 \Rightarrow \exists\ x, y \in \mathbb{Z}$

such that $ax + cy = 1$

$\Rightarrow abx + bcy = b$ ——— (2)

Now $d \mid a$ and $d \mid bc \Rightarrow d \mid (\text{L.H.S of } (2))$

hence $d \mid b$

Then d is common divisor of a and b.

then by definition of G.C.D

$d \mid d_1$ ——— (3)

By (1) & (3), we have $d = d_1$.

Problem:-

If $(d_1, d_2) = 1$ and $d_1 \mid a$, $d_2 \mid a$

then $d_1 d_2 \mid a$.

Solution:-

$d_1 \mid a \Rightarrow \exists\ a_1 \in \mathbb{Z}$ such that $a = a_1 d_1$

and $d_2 \mid a \Rightarrow \exists\ a_2 \in \mathbb{Z}$ such that $a = a_2 d_2$

Now $(d_1, d_2) = 1 \Rightarrow \exists\ x, y \in \mathbb{Z}$ such that

$d_1 x + d_2 y = 1$

$\Rightarrow a d_1 x + a d_2 y = a$

$\cancel{\Rightarrow a_2 d_2 d_1 x + a_1}$

$\Rightarrow a_2 d_2 d_1 x + a_1 d_1 d_2 y = a$

Now $d_1 d_2$ divides the L.H.S of above

hence $d_1 d_2$ will also divide R.H.S i.e $d_1 d_2 \mid a$.

Problem:-

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

Solution:

Let $(a, b) = d$ and $(b, r) = d_1$

we prove $d = d_1$.

Now $a - bq = r$

then $d \mid a$ and $d \mid b$

$\Rightarrow$ d divides the R.H.S of above i.e $d \mid r$.

Hence d is a common divisor of b and r.

then by definition of G.C.D, $d \mid d_1$ —— (1)

Next,

$$a = bq + r \qquad \text{—— (2)}$$

then $d_1 \mid b$ and $d_1 \mid r$

$\Rightarrow$ d_1 divides the R.H.S of (2)

then $d_1 \mid a$

Hence d_1 is a common divisor of a and b.

Then by definition of G.C.D

$$d_1 \mid d \qquad \text{—— (3)}$$

By (1) and (3), we get

$$d = d_1$$

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

A integer 'm' is called the least common multiple of a and b (integers) if

i) $m > 0$

ii) $a \mid m$, $b \mid m$

iii) If $a \mid c$, $b \mid c$, then $m \mid c$.

The L.C.M of a and b will be denoted by $m = \langle a, b \rangle$.

Exercise:-

L.C.M of a and b is unique.

Do yourself.

Theorem:-

If $(a,b)=d$, ~~then~~ then $m=\langle a,b\rangle=\dfrac{|ab|}{d}$

Proof:-

We prove that m satisfies all the three properties of L.C.M.

i) Since $d>0$, $|ab|>0$ so $m>0$

ii) Since $(a,b)=d$, $\exists\ a_1, b_1 \in Z$ such that

$$a=a_1d\ ,\quad b=b_1d\ .$$

then $m=\dfrac{|a_1d\cdot b_1d|}{d} = |a_1b_1d|$ —— ①

$= |a\cdot b_1|$ $\quad\because a=a_1d$

$\Rightarrow$ ~~a|m~~ $= |a_1 b|$ $\quad\because b_1d=b$

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

iii)

Let $a\mid c$ and $b\mid c$

$\Rightarrow \exists\ d_1, d_2 \in Z$ such that $c=ad_1=bd_2$

Now $(a,b)=d \Rightarrow \exists\ a_1, b_1 \in Z$ such that

$a=a_1d$, $b=b_1d$, $(a_1, b_1)=1$

then $c=a_1dd_1=b_1dd_2$ —— (2)

Now $m=|a_1b_1d|$ by (1)

From (2) we see

$a_1d_1=b_1d_2 \Rightarrow a_1\mid b_1d_2$

Since $(a_1, b_1)=1 \Rightarrow a_1\mid d_2$

$\Rightarrow \exists\ t\in Z$ such that $d_2=a_1t$

then $c=b_1da_1t$

then $m\mid c$ $\quad\because m=|a_1b_1d|$

End of Lesson at 1027 PST

$a|b$ $\quad a|m,\ b|m$
$b=ac$ $\quad a|c$

$a = 12 = 1, 2, 3, 4, 6, 12$
$b = 24 = 1, 2, 3, 4, 6, 8, 12, 24$
Common divisors $= 1 \times 2 \times 3 \times 4 \times 6 \times 12 = 1728 = C$

Least Common Multiple:- (See previous page)

An integer m is called least common multiple of a & b (integers) if

(i) $m > 0$ $\qquad \langle a, b\rangle = m$

(ii) $a|m$, $b|m$ $\qquad \langle 12, 24\rangle = 24$

(iii) If $a|c$, $b|c$ then $m|c$. $\qquad \langle 6, 9\rangle = 18$

Example:- L.C.M of a and b is Unique.

L.C.M. of a and b will be denoted by $m = \langle a, b\rangle$

Sol:- Suppose $a, b \in Z$ Let $\langle a, b\rangle = m_1$, $\langle a, b\rangle = m_2$

(i) $m_1, m_2 > 0$

(ii) $a|m_1$, $b|m_1$

(iii) If $a|c$, $b|c$ then $m_1|c$ also $a|m_2$ & $b|m_2$ then m_2 is a common multiple of a & b then $m_1|m_2$. $\because m_1$ is a least common multiple of a & b. Similarly $m_2|m_1$. $\Rightarrow m_1 = m_2$.

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

Theorem:- If $(a, b) = d$ then $m = \langle a, b\rangle = \frac{|ab|}{d}$

Proof:- We prove that 'm' satisfies all the three conditions of L.C.M.

(i) Since by def. of G.C.D. $d > 0$
$|ab| > 0$, so $m > 0$.

(ii) Since $(a, b) = d$, $\exists\ a_1, b_1 \in Z$ s.t $a = a_1 d$, $b = b_1 d$ then $m = \frac{|a_1 d \cdot b_1 d|}{d} = |a_1 b_1 d| = |a b_1|$ or $|a_1 b| \rightarrow (1)$

The Linear Diophantine Equation:-

Theorem:-

$ax+by=c$, $a,b,c\in Z$ has an integral solution iff $(a,b)\mid c$. If (x_0,y_0) is a solution of equation, the solution set is

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

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

Proof:-

Suppose $ax+by=c$ has a solution,

Since $(a,b)=d$

i.e $d\mid a$, $d\mid b$ $\Rightarrow d\mid ax+by \Rightarrow d\mid c$.

i.e $(a,b)\mid c$.

Conversely,

If $d\mid c$, then $\exists\ c_1\in Z$ such that $c=c_1d$.

and since $(a,b)=d$, $\exists\ a_1,b_1\in Z$ such that $a=a_1d$ and $b=b_1d$, $(a_1,b_1)=1$

Now $(a,b)=d \Rightarrow \exists\ x_0,y_0\in Z$ such that $ax_0+by_0=d$

$$\Rightarrow ac_1x_0+bc_1y_0=c_1d=c$$

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

This completes the first part of the theorem

Now suppose (x_0,y_0) and (x_1,y_1) be two solution, then

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

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

Subtracting (ii) from (i), we have

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

$$\Rightarrow a_1(x_0-x_1)+b_1(y_0-y_1)=0 \qquad \text{using } a=a_1d,\ b=b_1d$$

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

$$\Rightarrow a_1\mid b_1(y_1-y_0)$$

Now $(a_1,b_1)=1 \Rightarrow a_1\mid(y_1-y_0) \Rightarrow \exists\ t\in Z$

such that $y_1-y_0=a_1t$

$$\Rightarrow y_1=a_1t+y_0$$

$$\Rightarrow y_1=y_0+\frac{at}{d} \qquad \because a=a_1d$$

substituting the value of $y_1 - y_0$ in (3) we have

$$a_1(x_0 - x_1) = b_1(y_1 - y_0)$$

$$\Rightarrow a_1(x_0 - x_1) = a_1 b_1 t \quad \Rightarrow \quad x_0 - x_1 = b_1 t$$

$$\Rightarrow \quad x_1 = x_0 - b_1 t$$

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

Next, for any $t \in Z$, we have

$$ax_1 + by_1 = c$$

$$\Rightarrow a\left(x_0 - \frac{b}{d} t\right) + b\left(y_0 + \frac{a}{d} t\right) = ax_0 + by_0 = c$$

hence the solution set is

$$\left\{ \left(x_0 - \frac{b}{d} t,\ y_0 + \frac{a}{d} t\right) : t \in Z \right\}.$$

Example:-

Find all the integral solution of

$$69x + 111y = 9000.$$

Solution:-

$(69, 111) = 3$ and $3 \mid 9000$

hence the equation has integral solution.

We divide the equation by 3.

we obtain $23x + 37y = 3000$

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

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

$$\Rightarrow 23z + 14y = 10 \qquad \text{where } z = x + y - 130$$

$$\Rightarrow (14 + 9)z + 14y = 10$$

$$\Rightarrow 14v + 9z = 9 + 1 \qquad \text{where } z + y = v$$

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

$$\Rightarrow 5v + 9w = 1 \qquad \text{where } v + z - 1 = w$$

$$\Rightarrow v = 2, \quad w = -1$$

$$\because v + z - 1 = w$$

$$\Rightarrow 2 + z - 1 = -1 \quad \Rightarrow \quad z = -2$$

Also ~~xxxx~~ $z + y = v \Rightarrow -2 + y = 2 \Rightarrow y = 4$

Now $z = x + y - 130$

$\Rightarrow -2 = x + 4 - 130 \Rightarrow x = -2 - 4 + 130$

$\Rightarrow x = 124$

Hence $x_0 = 124$, $y_0 = 4$

So

$S.Set = \left\{ \left(x_0 - \frac{111}{3} t , y_0 + \frac{69}{3} t \right) ; t \in Z \right\}$

For integral solution

$124 - 37t > 0 \Rightarrow -37t > -124$

$\Rightarrow 37t < 124$

$\Rightarrow t < \frac{124}{37}$

& $4 + 23t > 0 \Rightarrow 23t > -4$

$\Rightarrow t > \frac{-4}{23}$

So $\frac{124}{37} > t > -4/23$

i.e $t = \{3, 2, 1, 0\}$

~~28z + 14y ≤ 80~~

End of Lesson at 1032 PST

Exercise:-

i) $5x + 22y = 18$

ii) $46x + 74y = 8000$

iii) $2072x + 1813y = 2849$.

Prime Number:-

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

e.g. 2, 3, 5, 7, 11, ...

A number m which is not prime is called composite, it can be written as $m = d_1 d_2$ where $1 < d_1, d_2 < m$.

Note: i) 1 is neither prime nor composite.

ii) 2 is only even prime number.

Theorem:-

Every integer m has a prime divisor.

Proof:

If m is prime, then m is a prime divisor of m.

If m is composite, then m can be written as $m = d_1 d_2$ such that $1 < d_1, d_2 < m$

Let $d_1 < d_2$.

If d_1 is prime, then d_1 is a prime divisor of m.

If d_1 is composite, we can write

$$d_1 = d_3 d_4 \quad \text{where} \quad 1 < d_3, d_4 < d_1$$

Let $d_3 < d_4$

If d_3 is prime, then d_3 is a prime divisor of d_1.

i.e d_3 is a prime divisor of m.

If d_3 is composite, we proceed in the same manner, ultimately we arrive at an integer

$1 < d_k, d_{k-1} < m$ such that d_k can not be factored more.

then d_k will be prime divisor of m.

Theorem:

If p is a prime divisor and $p \mid ab$, then either $p \mid a$ or $p \mid b$.

Proof:-

Suppose $p \nmid a$ $\because$ p is prime ~~(p,q)=1~~

then $(p, a) = 1$

then $\exists$ $x, y \in \mathbb{Z}$ such that $px + \cancel{q}^{a} y = 1$

$\Rightarrow pbx + aby = b$

Now $p \mid pbx$, $p \mid aby$ $\Rightarrow$ $p \mid pbx + aby$.

$\Rightarrow$ $p \mid b$.

The theorem is complete.

Corollary :-

i) If p is prime and $p \mid a_1 a_2 \cdots a_K$ then $p \mid a_i$ for some $i = 1, 2, 3, \cdots, K$.

ii) If $p \mid P_1 P_2 \cdots P_K$, where P_i ; $i = 1, 2, \cdots, K$ are primes. $p = P_j$ for some $j = 1, 2, \cdots, K$.

~~Statem~~ The Fundamental theorem of Arithmetic (Unique Factorization theorem).

-: 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.

The theorem is true for $n = 2$

Now we prove for $n = K+1$.

Next suppose the theorem is true for $n = 2, 3, 4, \cdots, K$

If $K+1$ is prime, induction is complete

If $K+1$ is composite, then it can be written as $K+1 = K_1 K_2$; $1 < K_1, K_2 < K+1$

then by inductive hypothesis, K_1 and K_2 can be expressed as a product of primes

The induction is complete and theorem is true for every $n > 1$.

i.e $n = P_1 P_2 P_3 \cdots P_r$ where P_i, $i = 1, 2, \cdots, r$ are primes

continue →

→ for uniqueness;

Let $n = p_1 p_2 \cdots p_r$; p_i ; $i = 1, 2, \ldots, r$ are primes and $n = q_1 q_2 q_3 \cdots q_s$, q_j $(j = 1, 2, \ldots, s)$ are all primes then

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

We cancel common factors on both sides of the equation and let we obtain $q_1 q_2 \cdots q_j = p_1 p_2 \cdots p_i$ such that no factor is common on both sides

Now q_1 divides the L.H.S of this equation. Hence it must be divide the R.H.S. Then by the theorem

" If $p \mid p_1 p_2 \cdots p_k$, where p_i $(i = 1, 2, \ldots, k)$ all are primes, then $p = p_j$ for some $j = 1, 2, \ldots, k$".

so $q_1 = p_t$ for some $t = 1, 2, 3, \ldots, i$

This is a contradition.

hence this proves the uniqueness.

Note: i) If $n = p_1 p_2 \cdots p_s$ is the prime factorization of n, then it is not necessary that all the factors are distinct.

Let they appear $\alpha_1, \alpha_2, \ldots, \alpha_r$ times respectively. then we write

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r} = \prod_{i=1}^{r} p_i^{\alpha_i}$$

This form of n is called standard form of n, where $p_1 < p_2 < \cdots < p_r$

i.e p_i's are written in assending order

e.g $2700 = 2^2 \cdot 3^3 \cdot 5^2$.

Problem:

Show that the following $n-1$ consective integers are not prime.

$$n! + 2, \; n! + 3, \ldots, n! + n$$

Solution:

2 divides $(n! + 2)$, $3 \mid (n! + 3), \ldots, n \mid (n! + n)$

hence they are not prime.

We conclude that we find n consective ~~integers~~ composite integers for any given n i.e $(n+1)!+2$, $(n+1)!+3, \ldots, (n+1)!+(n+1)$ are n consective composite numbers.

Exercise :-

If p is a prime and $p \mid a^2+b^2$, $p \mid a$ then $p \mid b$.

Exercise :

Show that every prime is either of the form $4n+1$ or of the form $4n-1$.

Problem :-

An integer n is a perfect square iff the exponent of every prime in the standard form is even.

Solution :-

Let $p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ be the standard form of n.

i.e

$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_r^{\alpha_r}$. Suppose each α_i; $i = 1, 2, \ldots r$ is even then

$$n = p_1^{2\left(\frac{\alpha_1}{2}\right)} \cdot p_2^{2\left(\frac{\alpha_2}{2}\right)} \cdots p_r^{2\left(\frac{\alpha_r}{2}\right)} = \left(p_1^{\frac{\alpha_1}{2}}\right)^2 \cdot \left(p_2^{\frac{\alpha_2}{2}}\right)^2 \cdots \left(p_r^{\frac{\alpha_r}{2}}\right)^2$$

$$= \left(p_1^{\alpha_1/2} \cdot p_2^{\alpha_2/2} \cdots p_r^{\alpha_r/2}\right)^2$$

Hence n is a perfect square.

Conversely, suppose n is a perfect square and let $n = m^2$ and $m = q_1^{\beta_1} \cdot q_2^{\beta_2} \cdots q_s^{\beta_s}$ be the standard form of m.

Then $n = m^2 = \left(q_1^{\beta_1} \cdot q_2^{\beta_2} \cdots q_s^{\beta_s}\right)^2 = q_1^{2\beta_1} \cdot q_2^{2\beta_2} \cdots q_s^{2\beta_s}$

Since $q_1, q_2, \ldots, q_s$ are primes, therefore $q_1^{2\beta_1} \cdot q_2^{2\beta_2} \cdots q_s^{2\beta_s}$ is the standard form of n and we see that each exponent is even.

Problem:-

If $(b,c)=1$ and bc is a perfect square, then both b and c are perfect square

Solution:

Let $b = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ and $c = q_1^{\beta_1} q_2^{\beta_2} \cdots q_t^{\beta_t}$ be the standard form of b and c respectively.

Since $(b,c)=1$, $q_i \neq p_j$ for any $i \in \{1,2,3,\ldots,t\}$ and $j \in \{1,2,3,\ldots,r\}$.

Then $bc = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot p_2^{\beta_2} \cdots p_r^{\alpha_r} \cdot q_1^{\beta_1} q_2^{\beta_2} \cdots q_t^{\beta_t}$ is the standard form of bc.

Since bc is a perfect square, every exponent is even

Then

$$bc = p_1^{2(\frac{\alpha_1}{2})} \cdot p_2^{2(\frac{\alpha_2}{2})} \cdots p_r^{2(\frac{\alpha_r}{2})} \cdot q_1^{2(\frac{\beta_1}{2})} \cdots q_t^{2(\frac{\beta_t}{2})}$$

$$= \left(p_1^{\frac{\alpha_1}{2}} \cdot p_2^{\frac{\alpha_2}{2}} \cdots p_r^{\frac{\alpha_r}{2}}\right)^2 \cdot \left(q_1^{\beta_1/2} q_2^{\beta_2/2} \cdots q_t^{\beta_t/2}\right)^2$$

we see that b and c are perfect square.

Problem:-

Show that if x and y are odd integers, then there does not exist an integer z such that $x^2+y^2=z^2$.

Solution:

Since x and y are odd, $\exists$ $k_1, k_2 \in \mathbb{Z}$ such that $x = 2k_1+1$, $y = 2k_2+1$. Then

$$x^2+y^2 = 4k_1^2 + 4k_1 + 1 + 4k_2^2 + 4k_2 + 1$$

$$= 2\left(2k_1^2 + 2k_1 + 2k_2^2 + 2k_2 + 1\right)$$

$$= 2(2k+1) \quad \text{where } k = k_1^2 + k_1 + k_2^2 + k_2$$

Since $2k+1$ is odd, it can not have 2 as a ~~perfect~~ factor then $2(2k+1)$ has a factor 2, whose exponent of 2 is odd and the standard form of $2(2k+1)$ contains 2, whose exponent is odd (i.e. 1). Hence $2(2k+1)$ can not be perfect square, so x^2+y^2 can not be equal to z^2

Exercise:-

Show that $a^2 = 2b^2$ does not hold for any $a, b \in \mathbb{Z}$.

Exercise:-

Show that an integer of the form $3n+2$ has a prime divisor of the form $3n+2$.

Theorem:-

A composite n has a prime divisor $\leq \sqrt{n}$.

Proof:

Let p be the least prime which divides n.
and $n = n_1 p$.
Suppose $p > \sqrt{n}$ then $n_1 < \sqrt{n}$
then $n_1 < \sqrt{n} < p$, so we have prime less than p which divides n.
This is a contradiction.
hence $p \leq \sqrt{n}$.

Corollary:-

An integer n is a prime if it has no prime divisor $\leq n$.

$$\begin{array}{r} 34 \\ 4\overline{)137} \\ 12 \\ \hline 17 \\ 16 \\ \hline 1 \end{array}$$

Exercise:-

137 is a prime or not $4n+1$
$4(34)+1$

Theorem:-

The number of prime is infinite.

Proof:

Let $2, 3, 5, \ldots, p$ be the only primes then consider the number $P = 4(2 \cdot 3 \cdot 5 \cdots p) + 1$
we note that no number $2, 3, 5, \ldots, p$ divides P.
But we know that every integer has a prime divisor therefore our assumption that $2, 3, 5, \ldots p$ are the

only prime is wrong
and numbers of primes is infinite.

Theorem:-
The number of primes of the form $4n-1$ is infinite.

Proof:-
Suppose the number of primes of the form $4n-1$ is finite and $3, 7, 11, \dots, p$ (p being the least) be the primes of the form $4n-1$.
Consider the number
$$P = 4(3\cdot 7\cdot 11 \cdots p) - 1$$
Now none of the number $3, 7, 11, \dots, p$ divides P.
Hence p has no prime factors of the form $4n-1$.
Then p has all prime factor of the form $4n+1$. is a number not of the form $4n-1$.
But p is of the form $4n-1$.
This is a contradiction. Hence number of primes of the form $4n-1$ is infinite.

End of Lesson at 1045 PST

~~# Fermat~~

Fermat Numbers :-

The numbers of the form $F_n = 2^{2^n}+1,\ n\in\mathbb{N}$, are called Fermat Number, Fermat conjectured that F_n are prime $\forall\ n\in\mathbb{N}$ and proved his ~~conjured~~ conjuctured for $n=1,2,3,4$ i.e. he proved that F_1, F_2, F_3 and F_4 are primes. But later Euler proved that F_5 is divisible by 641.

Theorem :-

Any two Fermat numbers are relatively prime.

Proof:-

Let $F_m = 2^{2^m}+1$ and $F_n = 2^{2^n}+1$ be two Fermat numbers such that

$$(F_n, F_m) = d.$$

Let $m = n+r$, then

$$\frac{F_m-2}{F_n} = \frac{2^{2^m}+1-2}{2^{2^n}+1} = \frac{2^{2^{n+r}}-1}{2^{2^n}+1} = \frac{2^{2^n\cdot 2^r}-1}{2^{2^n}+1}$$

$$= \frac{\left(2^{2^n}\right)^{2^r}-1}{\left(2^{2^n}+1\right)}$$

put $a = 2^{2^n}$

$$\Rightarrow \frac{F_m-2}{F_n} = \frac{a^{2^r}-1}{a+1}$$

$$= a^{2^r-1} - a^{2^r-2} + a^{2^r-3} - \cdots\cdots - 1$$

$\Rightarrow F_n \mid F_m - 2$.

But $d \mid F_n \Rightarrow d \mid F_m - 2$

also $d \mid F_m \Rightarrow d \mid -2 \Rightarrow d = 1$ or 2.

Since F_n and F_m are odd, therefore $d=1$.

This complete the proof.

Mersenne Numbers :-

The numbers of the form $M_n = 2^n - 1$, $n > 0$ are called Mersenne numbers.

If M_n is prime then M_n is called Mersenne ~~numbers~~ prime.

Theorem :-

If M_n is prime then n is prime.

Proof:

Suppose n is composite, then $n = n_1 n_2$, $1 < n_1, n_2 < n$

$$\Rightarrow M_n = 2^n - 1 = 2^{n_1 n_2} - 1 = \left((2^{n_1})^{n_2} - 1\right)$$
$$= (2^{n_1} - 1)(2^{n_1 n_2 - n_1} + 2^{n_1 n_2 - 2n_1} + \cdots + 1)$$

This is a contradiction. ~~If n is composite then M_n is not Mersenne~~ prime

Note:

The converse of the theorem is not true i.e if n is prime, then M_n is not neceessarity prime.

Problem :-

Show that number of primes of the form $6n - 1$ is infinite.

Arithmetic Function :-

A function of variables x_i, where $i = 1, 2, \cdots, r$ is called an arithmetic function if it assumes only integral values for the sets of integral values of x_i

e.g. Integral polynomial.

A single valued Arithmetic function is called regular or multiplicative.

An arithmetic function f is called multiplicative if $f(mn) = f(m)f(n) \quad \forall\, m, n \;, (m,n)=1$

Examples:-
Function $d(n) = \tau(n)$ is the number of +tive divisor of n, is arithmetic
e.g $\sigma(6) = 1+2+3+6 = 12$
$\sigma(4) = 1+2+4 = 7$

Theorem:-
The functions $d(n) = \tau(n)$ and $\sigma(n)$ are multiplicative.

Proof.
Let $(m,n)=1$, we prove
$d(mn) = d(m)\cdot d(n)$ and $\sigma(mn) = \sigma(m)\sigma(n)$
Let $d_1, d_2, d_3, \ldots, d_k$ be the +tive divisors of m and $d_1', d_2', \ldots, d_t'$ be of n.
Consider the identity

$$(d_1+d_2+\cdots+d_k)(d_1'+d_2'+\cdots+d_t') = \sum_{i=1}^{k}\sum_{j=1}^{t} d_i d_j'$$

Now
$d_i d_j' \mid mn$ for $i=1,2,\ldots,k$ and $j=1,2,\ldots,t$
i.e every term of R.H.S is a divisor of mn.
We prove these are only divisor of mn.
For if d is divisor of mn, then either $d \mid m$ or $d \mid n$, Since $(m,n)=1$ or $d = \bar{d}_1\bar{d}_2$ such that $\bar{d}_1 \mid m$, $\bar{d}_2 \mid n$, in either case $\bar{d}_1\bar{d}_2$ is a term on R.H.S.
Now $d(m) = K$, $d(n) = t$
~~R.H.S~~ so L.H.S $=$ (K terms)(t terms) $= d(m)\,d(n)$
Since on the R.H.S, there are kt terms
~~Moreover L.H.S = σ(m)~~ $\Rightarrow d(m)\,d(n) = d(mn)$

Moreover L.H.S $= \sigma(m)\,\sigma(n) = \sigma(mn)$

Theorem:

Let $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots\cdots p_r^{\alpha_r}$ be the standard form of n, then

i) $d(n) = \tau(n) = \prod_{i=1}^{r} (\alpha_i + 1)$

ii) $\sigma(n) = \prod_{i=1}^{r} \dfrac{p_i^{\alpha_i+1} - 1}{p_i - 1}$

Proof:

The divisors of $p_i^{\alpha_i}$ are $1, p_i, p_i^2, \ldots, p_i^{\alpha_i}$ then

$$\tau(p_i^{\alpha_i}) = \alpha_i + 1 \quad \text{——— (1)}$$

Now

$$\tau(n) = d(n) = \tau(p_1^{\alpha_1} p_2^{\alpha_2} \cdots\cdots p_r^{\alpha_r})$$

$$= \tau(p_1^{\alpha_1})\,\tau(p_2^{\alpha_2}) \cdots\cdots \tau(p_r^{\alpha_r})$$

$$= (\alpha_1+1)(\alpha_2+1) \cdots\cdots (\alpha_r+1) \quad \text{using (i)}$$

$$= \prod_{i=1}^{r} (\alpha_i + 1)$$

ii) $\sigma(n) = \sigma(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots\cdots p_r^{\alpha_r})$

$$= \sigma(p_1^{\alpha_1})\,\sigma(p_2^{\alpha_2}) \cdots\cdots \sigma(p_r^{\alpha_r})$$

Now

$$\sigma(p_i^{\alpha_i}) = 1 + p_i + p_i^2 + \cdots\cdots + p_i^{\alpha_i}$$

$$S_n = \frac{a(r^n - 1)}{r - 1} = \frac{(p_i^{\alpha_i+1} - 1)}{p_i - 1}$$

then $\sigma(n) = \dfrac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdot \dfrac{p_2^{\alpha_2+1} - 1}{p_2 - 1} \cdots\cdots \dfrac{p_r^{\alpha_r+1} - 1}{p_r - 1}$

$$= \prod_{i=1}^{r} \frac{p_i^{\alpha_i+1} - 1}{p_i - 1}$$

Learning notes:

Problem:

Show that $\tau(n)$ is odd iff n is a perfect square.

Solution:-

Let $n = 2^m . p_1^{\alpha_1} . \cdots p_r^{\alpha_r}$ be the standard form of n and suppose n is a perfect square, then all the exponents $m, \alpha_1, \alpha_2, \cdots, \alpha_r$ are even.

Then $(m+1), (\alpha_1+1), \cdots, (\alpha_r+1)$ will be odd.

so $\tau(n) = \prod_{i=1}^{r} (m+1)(\alpha_i+1)$ will be odd.

Conversely, suppose that $\tau(n)$ is odd

i.e $\tau(n) = (m+1)(\alpha_1+1) \cdots (\alpha_r+1)$ is odd.

then all the factors on R.H.S are odd,

Consequently $m, \alpha_1, \cdots, \alpha_r$ all are even

Accordingly.

$n = 2^m p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ is a perfect square

End of Lesson at 1057 PST

(38)

Problem:-

If $\sigma(n)$ is odd then n is a perfect square and conversely.

Solution:-

Let $n = 2^m p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots\cdots p_r^{\alpha_r}$, $m \geq 0$, $\alpha_i \geq 1$ be the standard form of n.

Suppose $\sigma(n)$ is odd, then

$$\sigma(n) = \left(\frac{2^{m+1}-1}{2-1}\right) \prod_{i=1}^{r} \left(\frac{p_i^{\alpha_i+1}-1}{p_i - 1}\right)$$

$$= (2^{m+1}-1)(p_1^{\alpha_1} + p_1^{\alpha_1-1} + \cdots + p_1+1) \cdot$$

$$(p_2^{\alpha_2} + p_2^{\alpha_2-1} + \cdots + p_2+1) \cdots\cdots (p_r^{\alpha_r} + p_r^{\alpha_r-1} + \cdots + p_r+1)$$

Since $\sigma(n)$ is odd,

$\Rightarrow$ each factor on R.H.S must be odd.

they will be odd if each α_i is even, $(i = 1, 2, \cdots, r)$

If m is odd, $2^m = 2 \cdot 2^{m-1}$, $m-1$ is even,

then $n = 2 \cdot 2^{m-1} \cdot p_1^{\alpha_1} \cdots\cdots p_r^{\alpha_r}$

where $m-1, \alpha_1, \cdots\cdots, \alpha_r$ all are even.

then n is a double of square

If m is even then n is a perfect square.

Conversely,

Suppose n is a perfect square, then every exponent in the standard form of n is even.

then

$$(2^{m+1}-1), (p_1^{\alpha_1} + p_1^{\alpha_1-1} + \cdots + p_1+1), \cdots\cdots\cdots,$$
$$(p_r^{\alpha_r} + p_r^{\alpha_r-1} + \cdots + p_r+1)$$

all are odd, ~~Conseq~~

Consequently, their product is odd

i.e $\sigma(n) = (2^{m+1}-1) \prod_{i=1}^{r} \left(\frac{p_i^{\alpha_i+1}-1}{p_i - 1}\right)$ is odd.

End of Lesson at 1018 PST

Ex: Solve the integral solution of $92x + 158y = 16000$.

Sol:- $(92, 158) = 2$, $2 \mid 16000$ hence the eq. has integral solution. We divide the eq. by 2 to obtain

$46x + 79y = 8000$

$46x + 46y + 33y = 46 \times 170 + 180$

$46(x + y - 170) + 33y = 180$

$46z + 33y = 180$

$33z + 13z + 33y = 33 \times 5 + 15$

$33(z + y - 5) + 13z = 15$

$33w + 13z = 15$

$13w + 20w + 13z = 13 + 2$

$13(w + z - 1) + 20w = 2$

$13v + 20w = 2$

$13v + 13w + 7w = 2$

$13(v + w) + 7w = 2$

$13u + 7w = 2$

$7u + 6u + 7w = 2$

$7(u + w) + 6u = 2$

$7t + 6u = 2$

$6t + t + 6u = 2$

$6(t + u) + t = 2$

$6s + t = 2$

$6(1) + -4 = 2$

$x + y - 170 = z$

$x - 28 - 170 = 24$

$x - 198 = 24$

$x = 24 + 198$

$\boxed{x = 222}$

$z + y - 5 = w$

$24 + y - 5 = -9$

$y = -9 - 19$

$\boxed{y = -28}$

$w + z - 1 = v$

$-9 + z - 1 = 14$

$z - 10 = 14$

$\boxed{z = 24}$

$v + w = u$

$v - 9 = 5$

$\boxed{v = 14}$

$u + w = t$

$5 + w = -4$

$\boxed{w = -9}$

$t + u = s$

$-4 + u = 1$

$\boxed{u = 5}$

$s = 1,\ t = -4$

$x_0 = 222$

$y_0 = -28$

$S = \left\{ \left(x_0 - \frac{158}{2} t\right), \left(y_0 + \frac{92}{2} t\right), t \in \mathbb{Z} \right\}$

$222 - 79t > 0$

$\frac{222}{79} > t$

$2.810 > t$

$-28 + 46t > 0$

$t > 28/46$

~~$t > 0.06$~~

$2.810 > t > 0.06$

$t = \{2, 1, 0\}$

1003 PST
Wednesday
27-10-04

Perfect Numbers:-

A positive integer n is called perfect number if $\sigma(n) = 2n$. i.e the sum of its +ive divisor is double itself.

e.g, 6, 28, 496, 8128, are the first four perfect numbers.

Theorem:

An even integer n is perfect iff $n = 2^{p-1}(2^p - 1)$, where $2^p - 1$ is prime.

Proof:

Suppose n is perfect number

$\because$ n is even, we can write $n = 2^{k-1} \cdot n'$

where $k \geq 2$ and n' is odd.

Now by assumption that n is perfect

$$\sigma(n) = 2n$$

$$\Rightarrow \sigma(n) = \sigma(2^{k-1} \cdot n')$$

$$= \sigma(2^{k-1}) \cdot \sigma(n') \qquad \because (2^{k-1}, n') = 1$$

$$= (2^k - 1) \cdot \sigma(n') \qquad \prod_{i=1}^{r} \frac{P_i^{\alpha+1} - 1}{P_i - 1}$$

$$\Rightarrow 2n = (2^k - 1) \cdot \sigma(n')$$

$$\Rightarrow 2(2^{k-1} \cdot n') = (2^k - 1)\, \sigma(n') \qquad \because n = 2^{k-1} \cdot n'$$

$$\Rightarrow 2^k \cdot n' = (2^k - 1)\, \sigma(n') \quad \text{——— (i)}$$

$$\Rightarrow 2^k - 1 \mid 2^k \cdot n' \text{ and}$$

$$\because (2^k - 1, 2^k) = 1$$

$$\Rightarrow 2^k - 1 \mid n'$$

$\Rightarrow \exists$ an integer n'' such that $n' = (2^k - 1) \cdot n''$ ——— (2)

$$\Rightarrow n' + n'' = (2^k - 1)\, n'' + n''$$

$$= 2^k \cdot n'' \quad \text{——— (3)}$$

Using (2) in (i)

$$2^k(2^k-1)\cdot 2n'' = (2^k-1)\cdot \sigma(n')$$

$\Rightarrow \quad 2^k\cdot n'' = \sigma(n')$

$\Rightarrow \quad n'+n'' = \sigma(n') \qquad$ by (3)

$\Rightarrow \quad n'$ and n'' are the divisor of n'

$\Rightarrow \quad n'' = 1$

this ~~shows~~ also shows that n' is a prime number.

Then from (2)

$n' = (2^k-1)(1) = 2^k-1$ is a prime number

and $\quad n = 2^{k-1}\cdot n' = 2^{k-1}\cdot(2^k-1)$.

Conversely,

Suppose $n = 2^{p-1}(2^p-1)$ and 2^p-1 is prime number,

Now $(2^{p-1}, 2^p-1) = 1$

Then $\sigma(n) = \sigma(2^{p-1})\cdot\sigma(2^p-1)$

$= (2^p-1)(1+2^p-1)$

$= 2^p(2^p-1)$

$= 2\cdot 2^{p-1}(2^p-1)$

$= 2n$

$$\prod_{i=1}^{r}\frac{p_i^{a+1}-1}{p_i-1}$$

$\Rightarrow \quad n$ is a perfect number

End of Lesson,

Using (2) in (1)

$$2^k(\cancel{2^k-1})\, n'' = (\cancel{2^k-1})\,\sigma(n')$$

$$2^k n'' = \sigma(n')$$

Using ③ $\quad 2^k n'' = \sigma(n')$

$$n' + n'' = \sigma(n')$$

$\Rightarrow$ n' & n'' are the divisors of n'.

$\Rightarrow$ $n'' = 1$. This also shows that n' is a prime number then from (2)

$n' = (2^k-1)(1) = 2^k-1$ is a prime and $n = 2^{k-1} n' = 2^{k-1}(2^k-1)$

The Bracket Function :-

Let $x \in \mathbb{R}$, then we denote $[x]$, the greatest integer, not (greater than) exceeding x, $[x]$ is called bracket fn. $[-5\frac{1}{2}] = -6$ $\quad -6, -5, -4, -3, -2, -1, 0$ ($-5\frac{1}{2}$)

e.g. $[5\frac{1}{2}] = 5$, $[5] = 5$ $\quad [-5] = -5$ $\quad [\frac{7}{3}] = 2$ $\quad [\frac{-7}{3}] = -3$

$[x]$ is called the integral part of x.

Theorems:- (i) $x = [x] + \theta \qquad 0 \le \theta < 1$

(ii) $[x+n] = [x] + n \qquad n \in \mathbb{Z},\ x \in \mathbb{R}$

(iii) If $x, y \in \mathbb{R}$, $y \neq 0$ and $x = qy + r$, $0 \le r < y$ then $\left[\frac{x}{y}\right] = q$.

(iv) $\left[\frac{x}{n}\right] = \left[\frac{[x]}{n}\right]$

Proof:- (i) This is obvious by def. that

$x = [x] + \theta \qquad 0 \le \theta < 1$ $\qquad$ θ is fractional part

(ii) $[x+n] = [x] + n$

We have $\quad x = [x] + \theta \qquad 0 \le \theta < 1$

$[x] = x - \theta$

$[x] + n = n + x - \theta$

$[x] + n = [x+n] + \theta_1 - \theta \Rightarrow (1), \quad 0 \le \theta_1 < 1$

Now $[x]$, n, $[x+n]$ all are integers

$\Rightarrow \theta_1 - \theta$ is an integer s.t. $0 \le |\theta_1 - \theta| < 1$

$\Rightarrow |\theta_1 - \theta| = 0$

$\Rightarrow \theta_1 = \theta$

$(1) \Rightarrow [x] + n = [x+n] + \cancel{\theta} - \cancel{\theta}$

$\Rightarrow [x+n] = [x] + n$ as required.

(iii) If $x, y \in \mathbb{R}, y \ne 0$ and $x = qy + r$, $0 < r < y$ Then $\left[\frac{x}{y}\right] = q$

Proof: $x = qy + r \Rightarrow \frac{x}{y} = q + \frac{r}{y}$

$\Rightarrow \left[\frac{x}{y}\right] = \left[q + \frac{r}{y}\right]$

$= q + \left[\frac{r}{y}\right]$ by (ii)

Now $\left[\frac{r}{y}\right] < \left[y/y\right] = 1 \Rightarrow \frac{r}{y} = 0$

$\Rightarrow \left[\frac{x}{y}\right] = q + 0 = q$

(iv) $\left[\frac{x}{n}\right] = \left[\frac{[x]}{n}\right]$

$[x] = nq + r \;-(1), \quad 0 \le r \le n-1 < n$

$\Rightarrow x = [x] + \theta \Rightarrow (2), \quad 0 \le \theta < 1$ (by def. of bracket fn.)

Using (2) in (1)

$x - \theta = nq + r$

$\Rightarrow x = nq + r + \theta$

$\frac{x}{n} = q + \frac{r+\theta}{n}$

$\left[\frac{x}{n}\right] = \left[q + \frac{r+\theta}{n}\right]$ By (ii) $\left[\frac{x}{n}\right] = q + \left[\frac{r+\theta}{n}\right]$

& again $\left[\frac{r+\theta}{n}\right] < \left[\frac{n-1+1}{n}\right] = 1$

$\Rightarrow \frac{r+\theta}{n} = 0$

$\Rightarrow \left[\frac{x}{n}\right] = q \quad -(3)$

$\because \frac{r}{n} < 1$, $\frac{r}{n} = 0$

$(1) \Rightarrow \frac{[x]}{n} = q + \frac{r}{n} \Rightarrow \left[\frac{[x]}{n}\right] = \left[q + \frac{r}{n}\right] = q + \left[\frac{r}{n}\right] = q \Rightarrow (4)$ by (ii)

$0 \le \frac{r}{n} < 1$

$(3) \& (4) \Rightarrow \left[\frac{x}{n}\right] = \left[\frac{[x]}{n}\right]$ Q.E.D.

Ex:- Solve the integral Solution

(i) $5x + 22y = 18$

$(5,22) = 1 \qquad 1 \mid 18$

$5x + 5y + 17y = 5 \times 3 + 3$ $\qquad x + y - 3 = z$

$5(x+y-3) + 17y = 3$ $\qquad x + 4 - 3 = -13$

$\qquad x + 1 = -13$

$5z + 17y = 3$ $\qquad \boxed{x = -14}$

$5z + 5y + 12y = 3$ $\qquad z + y = s$

$5(z+y) + 12y = 3$ $\qquad z + 4 = -9$

$5s + 12y = 3$ $\qquad \boxed{z = -13}$

$5s + 5y + 7y = 3$

$5(s+y) + 7y = 3$ $\qquad s + y = t$

$\qquad s + 4 = -5$

$5t + 7y = 3$ $\qquad \boxed{s = -9}$

$5t + 5y + 2y = 3$

$5(t+y) + 2y = 3$ $\qquad t + y = u$

$\qquad t + 4 = -1$

$5u + 2y = 3$ $\qquad \boxed{t = -5}$

$2u + 3u + 2y = 2 + 1$

$2(u+y-1) + 3u = 1$ $\qquad u + y - 1 = v$

$2v + 3u = 1$ $\qquad -1 + y - 1 = 2$

$3u + 2v = 1$

$\cancel{2v + 2u + u} = 1$ $\qquad \boxed{y = 4}$

$\cancel{2(v+u) + u} = 1$ $\qquad v + u = w$

$\qquad v - 1 = 1$

$\cancel{2w + u} = 1$ $\qquad \boxed{v = 2}$

$\cancel{2(1) - 1} = 1$ $\qquad w = 1,\ u = -1$

Ex:- Solve the integral solution for

i) $5x + 22y = 18$

$(5, 22) = 1 \quad 1 \mid 18$

$5x + 5y + 17y = 5 \times 3 + 3$

$5x + 5y - 5\times 3 + 17y = 3$ $\qquad x + y - 3 = z$

$5(x + y - 3) + 17y = 3$ $\qquad x - 1 - 3 = 4$

$5z + 17y = 3$ $\qquad x - 4 = 4$, $\boxed{x = 8}$

$5z + 5y + 12y = 3$

$5(z + y) + 12y = 3$ $\qquad z + y = w$

$5w + 12y = 3$ $\qquad z - 1 = 3$, $\boxed{z = 4}$

$5(w + 5y + 7y = 3$

$5(w + y) + 7y = 3$ $\qquad w + y = t$, $w - 1 = 2$

$5t + 7y = 3$ $\qquad \boxed{w = 3}$

$5(t + y) + 2y = 3$ $\qquad t + y = s$

$5s + 2y = 3$ $\qquad t - 1 = 1$

$3s + 2s + 2y = 2 + 1$ $\qquad \boxed{t = 2}$

$2(s + y - 1) + 3s = 1$ $\qquad s + y - 1 = u$

$2u + 3s = 1$ $\qquad 1 + y - 1$

$3s + 2u = 1$ $\qquad \boxed{y}$

$3(1) + 2(-1) = 1$ $\qquad \boxed{s = 1}, \boxed{u}$

$x_0 = 8,$

$S = \{(x_0 - \frac{22}{1}t, \; y_0 + \frac{5}{1}t), \; t \in z\}$

For integral Solution

$8 - 22t > 0$ $\qquad -1 + 5t > 0$

$8 > 22t$ $\qquad 5t > 1$

$\frac{8}{22} > t$ $\qquad t > 1/5$

$0.364 > t$ $\qquad t > 0.2$

$0.364 > t > 0.2$

$t = \{ \cdot \}$

$23\times 173 + 21$
$= 21$
$z + 14y$
$z = x + 84 - 173$

(ii) $46x + 74y = 8000$

$(46, 74) = 2 \quad \& \quad 2 \mid 8000$

$46x + 74y = 8000$

$23x + 37y = 4000$

$23x + 23y + 14y = 23\times 170 + 90$ $\qquad x + y - 170 = z$

$23x + 23y - 23\times 170 + 14y = 90$ $\qquad x - 10 - 170 = 10$

$23(x + y - 170) + 14y = 90$ $\qquad \boxed{x = 190}$

$23z + 14y = 90$

$14z + 9z + 14y = 14\times 6 + 6$

$14z + 14y - 14\times 6 + 9z = 6$ $\qquad z + y - 6 = w$

$14(z + y - 6) + 9z = 6$ $\qquad 10 + y - 6 = -6$

$14w + 9z = 6$ $\qquad \boxed{y = -10}$

$9w + 5w + 9z = 6$

$9(w + z) + 5w = 6$ $\qquad w + z = t$

$9t + 5w = 6$ $\qquad -6 + z = 4$

$\qquad \boxed{z = 10}$

$5t + 4t + 5w = 5 + 1$

$5(t + w - 1) + 4t = 1$ $\qquad t + w - 1 = u$

$5u + 4t = 1$ $\qquad 4 + w - 1 = -3$

$\qquad \boxed{w = -6}$

$4u + u + 4t = 1$

$4(u + t) + u = 1$ $\qquad u + t = v$

$4v + u = 1$ $\qquad -3 + t = 1 \Rightarrow \boxed{t = 4}$

$4(1) - 3 = 1$ $\qquad v = 1, \; u = -3$

$S = \left\{ \left(x_0 - \frac{74}{2}t, \; y_0 + \frac{46}{2}t\right); \; t \in \mathbb{Z} \right\}$ $\qquad x_0 = 190$, $y_0 = -10$

For Integral Solution

$190 - 37t > 0 \quad , \quad -10 + 23t > 0$

$\frac{190}{37} > t \qquad\qquad t > \frac{10}{23} \Rightarrow t > 0.4348$

$5.135 > t$

$5.135 > t > 0.4348$

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

(47)

(iii) $2072x + 1813y = 2849$

$(2072, 1813) = 259 \quad \& \quad 259 \mid 2849.$

$2072x + 1813y = 2849$

$8x + 7y = 11$

$7x + 7y + x = 7 + 4$

$7x + 7y - 7 + x = 4$

$7(x + y - 1) + x = 4$

$7z + x = 4$

$x + y - 1 = z$

$-3 + y - 1 = 1$

$y = 1 + 4$

$\boxed{y = 5}$

$\boxed{z = 1}$

$\boxed{x = -3}$

$S = \left\{ x_0 - \frac{1813}{259} t, \; y_0 + \frac{2072}{259} t \right\}, t \in Z \}$

$-3 - \frac{1813}{259} t > 0 \qquad 5 + \frac{2072}{259} t > 0$

$-3 - 7t > 0 \qquad 5 + 8t > 0$

$\frac{-3}{7} > t \qquad 8t > -5$

$-0.4286 > t \qquad t > \frac{-5}{8}$

$t > -0.625$

$-0.4286 > t > -0.625$

$t = \{ \quad \}$

28.10.04 Thursday.

Theorem:-

(i) If $x_1, x_2 \in \mathbb{R}$, then $[x_1 + x_2] \geq [x_1] + [x_2]$

(ii) If $x \in \mathbb{R}$ then the number of multiples of $n, \leq x$ is $\left[\frac{x}{n}\right]$

Proof:-

(i) $x_1 = [x_1] + \theta_1 \quad , \quad 0 \leq \theta_1 < 1$ &

$x_2 = [x_2] + \theta_2 \qquad 0 \leq \theta_2 < 1$.

$[x_1 + x_2] = \left[[x_1] + [x_2] + (\theta_1 + \theta_2)\right]$

$= [x_1] + [x_2] + [\theta_1 + \theta_2]$

$\Rightarrow [x_1 + x_2] = [x_1] + [x_2] \quad$ if $\theta_1 + \theta_2 < 1$.

$[x_1 + x_2] > [x_1] + [x_2] \quad$ if $\theta_1 + \theta_2 \geq 1$.

(ii) The ~~number~~ of multiples of $n \leq x$ are $1 \cdot n, 2 \cdot n, \ldots n_1 n$, $n_1 n$ being the last multiple of $n \leq x$ then $n_1 n \leq x < (n_1+1)n$ $\qquad 0 \leq \frac{x}{n} - n_1 < 1$

29.10.04 Friday

$\Rightarrow n_1 \leq \frac{x}{n} < n_1 + 1 \Rightarrow \left[\frac{x}{n}\right] = n_1$

Hence the numbers of multiples of $n \leq x$ is $n_1 = \left[\frac{x}{n}\right]$

Theorem:

The exponent of a highest power of a prime p, which divides $n!$ is $\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \ldots$

Proof:-

The number of multiples of $p \leq n$ is $\left[\frac{n}{p}\right]$. and they are $p, 2p, 3p, \ldots, \left[\frac{n}{p}\right]p$ then the exponent of the highest power of p which divides $n!$ is infact the exponent of the highest power of p which divides the product $p \cdot 2p \cdot 3p \cdots \left[\frac{n}{p}\right]p =$

$\left(1 \cdot 2 \cdot 3 \cdots \left[\frac{n}{p}\right]\right) p^{\left[\frac{n}{p}\right]}$

Let $K(n!)$ be the exponent of the highest power of p which divides $n!$ then $K(n!) = \left[\frac{n}{p}\right] +$ the exponent of the highest power of p which divides $1 \cdot 2 \cdot 3 \cdots \left[\frac{n}{p}\right]$ i.e. $K(n!) = \left[\frac{n}{p}\right] + K\left(\left[\frac{n}{p}\right]!\right)$ ...... (1)

Now replacing n by $\left[\frac{n}{p}\right]$ in (1) we obtain

$$K\left(\left[\frac{n}{p}\right]!\right) = \left[\frac{n/p}{p}\right] + K\left(\left[\frac{[n/p]}{p}\right]!\right)$$

$$K\left(\left[\frac{n}{p}\right]!\right) = \left[\frac{n}{p^2}\right] + K\left(\left[\frac{n}{p^2}\right]!\right)$$ then putting in (1), we get

$$K(n!) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + K\left(\left[\frac{n}{p^2}\right]!\right)$$

Proceeding in this way we ultimately obtain

$$K(n!) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \cdots\cdots$$ & the theorem is proved.

Theorem:-

Let $n = \sum_{i=1}^{m} a_i$, a_i are +ve integers, then $\frac{n!}{a_1!\,a_2!\cdots a_m!}$ is an integer.

Proof:-

It is sufficient to prove that the exponent of the highest power of any prime p which divides the numerator is greater than or equal to the highest power of that prime p which divides the denominator i.e. using the notation of the above theorem

$$K(n!) \geq K(a_1!) + K(a_2!) + \cdots + K(a_m!)$$

Now $K(a_1!) = \left[\frac{a_1}{p}\right] + \left[\frac{a_1}{p^2}\right] + \left[\frac{a_1}{p^3}\right] + \cdots\cdots$

$$K(a_2!) = \left[\frac{a_2}{p}\right] + \left[\frac{a_2}{p^2}\right] + \left[\frac{a_2}{p^3}\right] + \cdots$$

$$K(a_m!) = \left[\frac{a_m}{p}\right] + \left[\frac{a_m}{p^2}\right] + \left[\frac{a_m}{p^3}\right] + \cdots$$

$[x_1+x_2] \geq [x_1]+[x_2]$

i.e. $K(a_1!)+K(a_2!)+\dots+K(a_m!) = \left[\frac{a_1}{p}\right]+\left[\frac{a_2}{p}\right]+\left[\frac{a_3}{p}\right]+\dots+\left[\frac{a_m}{p}\right]+\left[\frac{a_1}{p^2}\right]+\left[\frac{a_2}{p^2}\right]+\dots+\left[\frac{a_m}{p^2}\right]+\left[\frac{a_1}{p^3}\right]+\left[\frac{a_2}{p^3}\right]+\dots+\left[\frac{a_m}{p^3}\right]+\dots \leq$

$\left[\frac{a_1+a_2+\dots+a_m}{p}\right]+\left[\frac{a_1+a_2+\dots+a_m}{p^2}\right]+\dots = \left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\dots$

$= K(n!)$

theorem is proved. $*\ 8=3+5$ so $\frac{8!}{3!5!}$

ple:-

$^nC_r^* = \binom{n}{r}$ is an integer $\quad {}^nC_r = \frac{n!}{r!(n-r)!}$

:-

we have $n = r+(n-r)$, then using the above theorem $\frac{n!}{r!(n-r)!}$ is an integer.

It is sufficient to prove that the exponent the highest power of any prime p which divides the numerator is greater than or equal to the highest power of that prime p which divides the denominator i.e. ~~using the notation of~~ Let $K(n!)$ be the exponent of the highest power of p which divides $n!$

$K(n!) \geq K(r!) + K((n-r)!)$

$K(r!) = \left[\frac{r}{p}\right]+\left[\frac{r}{p^2}\right]+\left[\frac{r}{p^3}\right]+\dots$

$K((n-r)!) = \left[\frac{n-r}{p}\right]+\left[\frac{n-r}{p^2}\right]+\left[\frac{n-r}{p^3}\right]+\dots$

$K(r!)+K(n-r)! = \left[\frac{r}{p}\right]+\left[\frac{n-r}{p}\right]+\left[\frac{r}{p^2}\right]+\left[\frac{n-r}{p^2}\right]$

$\leq \left[\frac{r+(n-r)}{p}\right]+\left[\frac{r+(n-r)}{p^2}\right]+\dots$

$= \left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\dots$

$= K(n!)$

Example:-

Show that the product of any r consecutive integers is divisible by $r!$

Sol:-

We know that $^nC_r = \frac{n!}{r!(n-r)!}$ is an integer

then

$$\frac{n!}{r!(n-r)!} = \frac{n(n-1)(n-2)\cdots(n-r+1)(n-r)!}{r!\,(n-r)!}$$

$$= \frac{n(n-1)(n-2)\cdots(n-r+1)}{r!}$$

is an integer

$\Rightarrow$ The product of any r consecutive integers is divisible by $r!$

Ex:- $[x]+[-x]=0$ if x is an integer &

$[x]+[-x]=-1$ otherwise

Sol:-

If x is an integer then $[x]=x$ & $[-x]=-x$

then $[x]+[-x]= x-x=0$

If x is not an integer then

$x = [x]+\theta \Rightarrow [x]=x-\theta$ $\quad 0<\theta<1$

$-x = [-x]+(1-\theta) \Rightarrow [-x]=-x+\theta-1$

$[x]+[-x] = \cancel{x}-\cancel{\theta}-\cancel{x}-1+\cancel{\theta} = -1$

$1\cdot 2\cdot 3\cdots m\cdot\boxed{m+1\cdot m+2\cdots m+n-1}$

$m!\,n!$

30·10·04 Saturday

Problem:-

If $(m,n)=1$ then $\dfrac{(m+n-1)!}{m!\,n!}$ is an integer.

Sol:

Now by the theorem "Let $n=\sum_{i=1}^{m} a_i$, a_i are integers then $\dfrac{n!}{a_1!\,a_2!\cdots a_m!}$ is an integer".

$\dfrac{(m+n)!}{m!\,n!}$ is an integer.

Now $\dfrac{(m+n)!}{m!\,n!} = \dfrac{(m+n-1)!\,(m+n)}{m!\,n!}$

$$= \frac{(m+1)(m+2)\cdots(m+n-1)(m+n)}{n!}$$

$$= \frac{(m+1)(m+2)\cdots(m+n-1)}{(n-1)!}\cdot\frac{(m+n)}{n}$$

Now $\dfrac{(m+1)(m+2)\cdots(m+n-1)}{(n-1)!} = n_1$ is an integer, since product of $(n-1)$ consecutive integers is divisible by $(n-1)!$

So $\dfrac{(m+n)!}{m!\,n!} = \dfrac{(m+n-1)!\,(m+n)}{m!\,n!}$

$$= n_1\,\frac{(m+n)}{n} \text{ is an integer.}$$

Now $(m,n)=1 \Rightarrow (m+n,\,n)=1$

$\Rightarrow^{*}$ $n\mid n_1 \Rightarrow \dfrac{(m+1)(m+2)\cdots(m+n-1)}{n(n-1)!}$ is an integer.

$\Rightarrow \dfrac{1\cdot 2\cdot 3\cdots m(m+1)\cdots(m+n-1)}{m!\,n!} = \dfrac{(m+n-1)!}{m!\,n!}$ is an integer.

Problem:-

If $x, y, z \in Z$, $x, y, z > 0$ then

$$\left[\frac{[\frac{x}{y}]}{z}\right] = \left[\frac{x}{yz}\right]$$

Sol:- Let $\left[\frac{x}{y}\right] = \alpha$, $\left[\frac{\alpha}{z}\right] = \beta$ then

$x = \alpha y + r_1 \qquad 0 \leq r_1 < y$

$\alpha = \beta z + r_2 \qquad 0 \leq r_2 < z$

So $x = \beta yz + y r_2 + r_1 \Rightarrow \frac{x}{yz} = \beta + \frac{r_2}{z} + \frac{r_1}{yz}$

Now r_1 can be atmost $y-1$

" r_2 " " " $z-1$

$$\Rightarrow \left[\frac{x}{yz}\right] = \beta + \left[\frac{r_2}{z} + \frac{r_1}{yz}\right] \to (1)$$

$$\text{Now} \left[\frac{r_2}{z} + \frac{r_1}{yz}\right] = \left[\frac{r_2 y + r_1}{yz}\right] \leq \left[\frac{yz - y + y - 1}{yz}\right]$$

$$= \left[\frac{yz-1}{yz}\right]$$

$$= 0$$

$$(1) \Rightarrow \left[\frac{x}{yz}\right] = \beta = \left[\frac{\alpha}{z}\right] = \left[\frac{[\frac{x}{y}]}{z}\right].$$

Ex:- (1) If $n > 0$, $T(1) + T(2) + \cdots + T(n) = \left[\frac{n}{1}\right] + \left[\frac{n}{2}\right] + \cdots + \left[\frac{n}{n}\right]$.

(2) $\sigma(1) + \sigma(2) + \cdots + \sigma(n) = \left[\frac{n}{1}\right] + 2\left[\frac{n}{2}\right] + 3\left[\frac{n}{3}\right] + \cdots + n\left[\frac{n}{n}\right]$

(3) Find the exponent of highest powers of 7 which divides 500!

(1) On the L.H.S all the divisors are $1, 2, 3, \ldots n$. 'n' being the greatest divisor, n will be counted only once. i.e for $[n/n]$ times. Every divisor will be counted as many times as are its multiples $\leq n$. If 'd' is a divisor it will be counted $[n/d]$ times. Then C[illegible]

$T(1) + T(2) + \cdots + T(n)$ [illegible]

Sol:- The exponent of a highest power of a prime p, which divides $n!$ is

$$\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\left[\frac{n}{p^3}\right]+\left[\frac{n}{p^4}\right]$$

Here $n = 500$, $p = 7$

$$\left[\frac{500}{7}\right]+\left[\frac{500}{7^2}\right]+\left[\frac{500}{7^3}\right]+\left[\frac{500}{7^4}\right]$$

$$\left[\frac{500}{7}\right]+\left[\frac{500}{49}\right]+\left[\frac{500}{343}\right]+\left[\frac{500}{2401}\right]$$

$$\left[71\frac{3}{7}\right]+\left[10\frac{10}{49}\right]+\left[1\frac{157}{343}\right]+\left[0\right]$$

$$71+10+1+0 = 82 \quad \text{Ans.}$$

The Möbius Function:-

Let $m = \pm p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ be the standard form of m i.e. p_i $(i = 1, 2, 3, \ldots, r)$ are disjoint primes. we take

$\mu(m) = 0$ if any $\alpha_i > 1$;

$\mu(m) = (-1)^r$ if all $\alpha_i = 1$;

$\mu(m) = 1$ if all $\alpha_i = 0$ i.e. $\mu(\pm 1) = 1$; so defined $\mu(m)$ is called "The Möbius Function" of m.

If $n = 117 = 3^2 \cdot 13$ so $\mu(117) = 0$ $\because$ any $\alpha_i > 1 \Rightarrow 2 > 1$ $n = 30 = 2 \cdot 3 \cdot 5$ $\mu(30) = (-1)^3 = -1$ If $\alpha_1 = \alpha_2 \cdots \alpha_r = 1$

Theorem :-

The Möbius function is multiplicative.

Proof:-

Let $(a, b) = 1$ and $a = \pm p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$; & $b = \pm q_1^{t_1} q_2^{t_2} \cdots q_s^{t_s}$ be the standard forms of a & b. If any $\alpha_i > 1$ or $t_j > 1$ then $\mu(a) = 0$ or $\mu(b) = 0 \Rightarrow \mu(a)\mu(b) = 0$, But Then $\mu(ab) = 0$

$\Rightarrow \mu(ab) = \mu(a)\mu(b)$

If all $\alpha_i = 1$ & all $t_j = 1$ then $\mu(a) = (-1)^r$ & $\mu(b) = (-1)^s$ & $\mu(ab) = (-1)^{r+s}$ then

$$\mu(a)\mu(b) = (-1)^r(-1)^s = (-1)^{r+s} = \mu(ab)$$

If all $\alpha_i = 0$ & all $t_j = 0$ $i = 1, 2, 3, \ldots, r$; $j = 1, 2, \ldots, s$

then $\mu(a) = \mu(\pm 1) = 1$

& $\mu(b) = \mu(\pm 1) = 1$ $\mu(ab) = \mu(\pm 1) = 1$

$\mu(a)\mu(b) = \mu(ab)$.

$\Rightarrow$ The proof is complete.

Theorem:-

$\sum_{d|m} \mu(d)$ is 0 or 1 according as $|m|$ is greater than or equal to 1.

Proof:-

If $m=1$, $d=1$ then $\sum_{d|m} \mu(d) = \mu(1) = 1$

Let $m = \pm p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$ where p_i; $i = 1, 2, \dots, r$ are distinct primes.

If any divisor d of m contains a factor p_i^2 ($i = 1, 2, \dots, r$) then $\mu(d) = 0$ so we need to consider only the divisors of $\pm p_1 p_2 \dots p_r$. These divisors are obtained by combining the primes p_i in all possible combinations.

First, we have $\mu(1) = {}^rC_0 = 1$.

$\sum_{i=1}^{r} \mu(p_i) = (-1)^1\, {}^rC_1$, $\sum_{\substack{i=1 \\ j=1 \\ j>i}} \mu(p_i p_j) = (-1)^2\, {}^rC_2$

$(\mu(p_1) + \mu(p_2) + \dots + \mu(p_r))$

$(-1)^1 + (-1)^1 + \dots + (-1)^1 = (-1)^1 r = (-1)^1\, {}^rC_1)$

$\mu(p_1 p_2 \dots p_r) = (-1)^r\, {}^rC_r$

$\Rightarrow \sum_{d|m} \mu(d) = {}^rC_0 + {}^rC_1(-1) + {}^rC_2(-1)^2 + \dots + {}^rC_r(-1)^r$

$= (1-1)^r = 0$

The proof is complete

$\mu(2) = (-1)^1 = -1$

Theorem :-

If m is a positive integer, then
$\sum_{n=1}^{m} \mu(n) \cdot \left[\frac{m}{n}\right] = 1$

Proof:-

From the above theorem $\sum_{d|m} \mu(d)$ is 0 or 1 according as $|m|$ is greater than or equal to 1.

$$* \Rightarrow \sum_{d_1|1} \mu(d_1) + \sum_{d_2|2} \mu(d_2) + \cdots + \sum_{d_m|m} \mu(d_m) = 1 \rightarrow (*)$$

$1 + 0 + \cdots + 0 = 1$

Now 1 is a divisor of all integers from 1 through m; so $\mu(1)$ will occur $\left[\frac{m}{1}\right]$ times in the sum. (**)

2 is a divisor of $\left[\frac{m}{2}\right]$ integers from 1 through m, therefore $\mu(2)$ will occur $\left[\frac{m}{2}\right]$ times in the sum $(*)$.

Generally d is a divisor of $\left[\frac{m}{d}\right]$ integers in the set $\{1, 2, \ldots, m\}$. Hence $\mu(d)$ will occur $\left[\frac{m}{d}\right]$ times in the sum $(*)$

Accordingly

$$\sum_{n=1}^{m} \sum_{d|n} \mu(d) = \mu(1)\left[\frac{m}{1}\right] + \mu(2)\left[\frac{m}{2}\right] + \cdots + \mu(d)\left[\frac{m}{d}\right] + \cdots + \mu(m)\left[\frac{m}{m}\right]$$

$$= \sum_{n=1}^{m} \mu(n)\left[\frac{m}{n}\right]$$

$$\Rightarrow \sum_{n=1}^{m} \mu(n)\left[\frac{m}{n}\right] = 1 \quad \text{as required.}$$

2.11.04 Tuesday (58)

The Möbius Inversion Formula:-

If $m > 0$ and $f(m)$ is an arithematic fn. & a fn. $g(m)$ is so defined that $g(m) = \sum_{d|m} f(d)$. then $f(m) = \sum_{d|m} \mu(d) \cdot g\left(\frac{m}{d}\right)$

Proof:-

As d ranges over all +ive divisors of m, $\frac{m}{d}$ does ~~not~~ also likewise, then by hypothesis

$$g\left(\frac{m}{d}\right) = \sum_{a|\frac{m}{d}} f(a) \Rightarrow \mu(d) \cdot g\left(\frac{m}{d}\right) = \mu(d) \cdot \sum_{a|\frac{m}{d}} f(a)$$

$$\Rightarrow \sum_{d|m} \mu(d) \cdot g\left(\frac{m}{d}\right) = \sum_{d|m} \mu(d) \sum_{a|\frac{m}{d}} f(a) = \sum_{d|m} \sum_{a|\frac{m}{d}} \mu(d) \cdot f(a).$$

Now d divides m and a divides $\frac{m}{d}$ is the same as saying a divides m and d divides $\frac{m}{a}$

$$\Rightarrow \sum_{d|m} \mu(d) \cdot g\left(\frac{m}{d}\right) = \sum_{a|m} \sum_{d|\frac{m}{a}} \mu(d) \cdot f(a)$$

$$= \sum_{d|\frac{m}{a}} \mu(d) \cdot \sum_{a|m} f(a)$$

Now $\sum_{d|\frac{m}{a}} \mu(d) = 1$ if $a = m$ $\left(\frac{m}{a} = 1\right)$

$= 0$ otherwise

then we get

$$\sum_{d|m} \mu(d) \cdot g\left(\frac{m}{d}\right) = \sum_{m|m} f(m) = f(m).$$

Hence Proved.

$\mu(p_1 p_2) = (-1)^2$
$\tau(p_1 p_2) = 4 = 2^2$
$1, p_1, p_2, p_1 p_2$

Problem: (p_i are distinct odd primes)

If $1 < n = \prod_{i=1}^{k} p_i^{n_i}$ then $\sum_{d|n} \mu(d)\,\tau(d) = (-1)^k$

Sol:-

Since $\mu(d) = 0$, if d contains any factor p_i^2 $(i = 1, 2, \ldots, k)$, so we need to consider only divisors of $p_1 p_2 \ldots p_k$. But these divisors are obtained by combining the p_i's in all possible ways. 1 is a divisor, so $\mu(1)\tau(1) = {}^kC_0 = 1$

$$\sum_{i=1}^{k} \mu(p_i)\,\tau(p_i) = (-1)^1 (2)\, {}^kC_1$$

$$\left(\mu(p_1)\tau(p_1) + \mu(p_2)\tau(p_2) + \ldots + \mu(p_k)\tau(p_k)\right)$$

$$\sum_{\substack{i=1 \\ j>i}}^{k} \mu(p_i p_j)\,\tau(p_i p_j) = (-1)^2\, 2^2\, {}^kC_2$$

$$\sum \mu(p_1 p_2 \ldots p_k)\,\tau(p_1 p_2 \ldots p_k) = (-1)^k\, 2^k\, {}^kC_k$$

then

$$\begin{aligned}
\sum_{d|n} \mu(d)\,\tau(d) &= {}^kC_0 + (-1)2\,{}^kC_1 + \ldots + (-1)^k 2^k\, {}^kC_k \\
&= {}^kC_0 + (-2)\,{}^kC_1 + \ldots + (-2)^k\, {}^kC_k \\
&= (1-2)^k \qquad \text{by using binomial theorem} \\
&= (-1)^k
\end{aligned}$$

Problem:- If $1 < n = \prod_{i=1}^{k} p_i^{n_i}$ Then $\sum_{d|n} \mu(d)\,\sigma(d) = (-1)^k p_1 p_2 \ldots p_k$

Sol:- Since $\mu(d) = 0$ for any divisor d of n which has factor p_i^2, $i = 1, 2, \ldots, k$. So we need to consider only divisors of $p_1 p_2 \ldots p_k$. But these divisors are obtained by combining the p_i's in all possible way. 1 is a divisor, so $\mu(1)\,\sigma(1) = {}^kC_0 = 1$