Thursday
18/07/2019

* Unit I: Divisibility Theory In The Integers *

* Principle of Well ording -:

Every non-empty set 's' of non-negative integers has a least element

i.e. There is some integer a ∈ s such that $a \leq b$ ∀ b ∈ s.

* Theorem [Division Algorithm] -:

* Statement:

Given integers 'a' and 'b' with $b > 0$ there exist unique integers 'q' and 'r' (are called respectively quotient and remainder in the division of a|b) satisfying $a = bq + r$; $0 \leq r < b$.

Proof:

Let us consider the set

$S = \{a - xb \mid x \text{ is integer}, a - xb \geq 0\}$

Claim - S is non-empty.

consider, $x = -|a|$

Then $a - xb = a + |a|b$

$\geq a + |a|$

≥ 0

Thus, S is non-empty.

Thus by well ordering principle has a least element say r.

Clearly, $0 \leq r$.

Claim - $r < b$.

Suppose on the contrary that $r \geq b$

Since $r \in S$ ∃ an integer 'q' such that

$r = a - qb$

Consider, $a - (q+1)b = a - qb - b$

$= r - b \geq 0$

$\Rightarrow r - b \in S$.

Which contradicts minimality of 'r'

Thus, $r < b$.

Thus, $0 \leq r < b$

Uniqueness -

Let if possible there be integers q' and r' such that,

$$a = bq' + r' \quad ; \quad 0 \leq r' < b$$

$\therefore$ We have,

$$bq' + r' = bq + r$$

$$\Rightarrow b|q' - q| = |r - r'| \quad \text{——} (1)$$

Now, $0 \leq r' < b$

$$-b < -r' \leq 0$$

$$\Rightarrow -b < r - r' < b$$

$$\Rightarrow |r - r'| < b$$

$\therefore$ Eq^n (1) becomes,

$$b|q' - q| < b$$

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

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

$$\Rightarrow q' - q = 0$$

$$\Rightarrow q' = q \quad \text{——} (*)$$

and hence $|r - r'| = b|q' - q|$

$$\Rightarrow |r - r'| = b|q - q| \quad (\text{by } *)$$

$$\Rightarrow |r - r'| = b|0|$$

$$\Rightarrow |r - r'| = 0$$

$$\Rightarrow r - r' = 0$$

$$\Rightarrow r = r'$$

This proves the uniqueness of q and r.

Hence the uniqueness.

Hence the proof.

* Corollary -:

If 'a' and 'b' are integers with $b \neq 0$ then there exist unique integers 'q' and 'r' such that $a = bq + r$; $0 \leq r < |b|$.

Proof:

Suppose $b < 0$.

$\therefore |b| > 0$

Now by Division algorithm theorem we get unique integers q' and r.

$\therefore a = q' \cdot |b| + r$; $0 \leq r < |b|$

since $b < 0$, $|b| = -b$

$\therefore a = -q' \cdot b + r$; $0 \leq r < |b|$

If we take $q = -q'$ then,

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

Hence the proof.

Que. Show that square of any integer is of the form $4k$ or $4k+1$.

→ Any integer is of the form $2k$ or $2k+1$

$\therefore$ Square of an integer is of the form

$(2k)^2 = 4k^2 = 4k'$; $k' = k^2$

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

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

$= 4k' + 1$; $k' = k^2 + k$.

Which is precisely $4k$ or $4k+1$.

* Note -:

No integer is of the form $4k+2$ or $4k+3$ can never be a perfect square.

Que. The square of any integer is of the for $3k$ or $3k+1$.

→ Let n be any integer.

Suppose $a=n$ and $b=3$.

Then by Division algorithm $\exists$ unique integers q and r such that,

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

$$\therefore n = 3k + r \quad ; \quad 0 \leq r < 3.$$

i.e. n is of the form $3k, 3k+1, 3k+2$.

suppose, $n = 3k$ then

$$\therefore n^2 = (3k)^2$$
$$= 9k^2$$
$$= 3(3k^2)$$
$$= 3k \quad ; \; k = 3k^2$$

suppose, $n = 3k+1$ then

$$\therefore n^2 = (3k+1)^2$$
$$= 9k^2 + 6k + 1$$
$$= 3(3k^2 + 2k) + 1$$
$$= 3k+1 \quad ; \; k = 3k^2 + 2k$$

suppose, $n = 3k+2$ then

$$\therefore n^2 = (3k+2)^2$$
$$= 9k^2 + 12k + 4$$
$$= 9k^2 + 12k + 3 + 1$$
$$= 3(3k^2 + 4k + 1) + 1$$
$$= 3k+1 \quad ; \; k = 3k^2 + 4k + 1$$

This proves that square of any integer is of the form $3k$ or $3k+1$.

Que. Prove that $3a^2 - 1$ is never a perfect square.

→ On the contrary suppose that $3a^2 - 1$ is a perfect square.

(We know that the square of any integer is of the form 3k or 3k+1)

Then by previous example it must be of the form $3k$ or $3k+1$

i.e. $3a^2-1 = 3k$ or $3a^2-1 = 3k+1$

i.e. $3a^2-3k = 1$ or $3a^2-3k = 2$

i.e. $3(a^2-k) = 1$ or $3(a^2-k) = 2$

i.e. $3m = 1$ or $3m = 2$.

Where, $a^2-k = m$.

But clearly this is not possible for any $m \in \mathbb{Z}$

∴ We must have $3a^2-1$ is never a perfect square.

Que. Show that square of odd integer is of the form $8k+1$.

→ Any integer has one of the form $4k+1$, $4k+3$

∴ Square of integer is of the form.

i) $(4k+1)^2 = 16k^2+8k+1$

$= 8(2k^2+k)+1$

$= 8k'+1$; $k' = 2k^2+k$.

ii) $(4k+3)^2 = 16k^2+24k+9$

$= 16k^2+24k+8+1$

$= 8(2k^2+3k+1)+1$

$= 8k'+1$; $k' = 2k^2+3k+1$

Which is precisely $(8k+1)$.

OR

Any integer is one of the form $2k$ or $2k+1$

∴ Square of integer is of the form

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

$= 4k(k+1)+1$ ——— (*)

We know $k(k+1)$ = even no $= 2k$

That means $k(k+1) = 2k$ ——— put in (*)

∴ $(2k+1)^2 = 4(2k)+1 = 8k+1$

Friday
19/07/2019

Que. Show that expression $\frac{a(a^2+2)}{3}$ is an integer for all $a \geq 1$.

→ Any integer $a \geq 1$ has one of the form $3k$, $3k+1$, $3k+2$.

i) a is of the form $3k$.

$$\therefore \frac{a(a^2+2)}{3} = \frac{(3k)(9k^2+2)}{3} = k(9k^2+2)$$

Which is an integer.

ii) a is of the form $3k+1$.

$$\therefore \frac{a(a^2+2)}{3} = \frac{(3k+1)(9k^2+6k+1+2)}{3}$$

$$= \frac{(3k+1)\,3(3k^2+2k+1)}{3}$$

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

Which is an integer.

iii) a is of the form $3k+2$

$$\therefore \frac{a(a^2+2)}{3} = \frac{(3k+2)(9k^2+12k+4+2)}{3}$$

$$= \frac{(3k+2)\,3(3k^2+4k+2)}{3}$$

$$= (3k+2)(3k^2+4k+2)$$

Which is an integer.

Que. Show that the cube of any integer has one of the form $9k$, $9k+1$, $9k+8$

→ Any integer has one of the form $3k$, $3k+1$ or $3k+2$.

i) $(3k)^3 = 27k^3 = 9(3k^3) = 9k^1$; $k^1 = 3k^3$

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

ii) $(3k+1)^3 = 27k^3 + (3 \times 9k^2) + (3 \times 3k \times 1) + 1$

$= 27k^3 + 27k^2 + 9k + 1$

$= 9(3k^3 + 3k^2 + 1) + 1$

$= 9k' + 1$; $k' = 3k^3 + 3k^2 + 1$.

iii) $(3k+2)^3 = 27k^3 + (3 \times 9k^2 \times 2) + (3 \times 3k \times 4) + 8$

$= 27k^3 + 54k^2 + 36k + 8$

$= 9(3k^3 + 6k^2 + 4k) + 8$

$= 9k' + 8$; $k' = 3k^3 + 6k^2 + 4k$.

Que. Show that any fourth power of integer has one of the forms $5k$ or $5k+1$.

→ Any integer has one of the form $5k$, $5k+1$, $5k+2$, $5k+3$ or $5k+4$. $(a+b)^4 = a^4 + 4a^3b + 6a^2b^2 + b^4$

i) $(5k)^4 = 625k^4$

$= 5(125k^4)$

$= 5k'$; $k' = 125k^4$

ii) $(5k+1)^4 = 625k^4 + (4 \times 125k^3 \times 1) + (6 \times 25k^2 \times 1) + (4 \times 5k \times 1) + 1$

$= 625k^4 + 500k^3 + 150k^2 + 20k + 1$

$= 5(125k^4 + 100k^3 + 30k^2 + 4k) + 1$

$= 5k' + 1$; $k' = 125k^4 + 100k^3 + 30k^2 + 4k$

iii) $(5k+2)^4 = 625k^4 + (4 \times 125k^3 \times 2) + (6 \times 25k^2 \times 4) + (4 \times 5k \times 8) + 16$

$= 625k^4 + 1000k^3 + 600k^2 + 160k + 15 + 1$

$= 5(125k^4 + 200k^3 + 120k^2 + 32k + 3) + 1$

$= 5k' + 1$; $k' = 125k^4 + 200k^3 + 120k^2 + 32k + 3$

iv) $(5k+3)^4 = 625k^4 + (4 \times 125k^3 \times 3) + (6 \times 25k^2 \times 9) + (4 \times 5k \times 9) + 81$

$= 625k^4 + 1500k^3 + 1350k^2 + 180k + 80 + 1$

$= 5(125k^4 + 300k^3 + 270k^2 + 36k + 16) + 1.$

$= 5k' + 1$; $k' = 125k^4 + 300k^3 + 270k^2 + 36k + 16$

v) $(5K+4)^4 = 625K^4 + (4\times125K^3\times4) + (6\times25K^2\times16) + (4\times5K\times64) + 256$

$= 625K^4 + 2000K^3 + 2400K^2 + 1280K + 256$

$= 5(125K^4 + 400K^3 + 480K^2 + 256K + 51) + 1$

$= 5K' + 1 \quad ; \quad K' = 125K^4 + 400K^3 + 480K^2 + 256K + 51$

Que For $n \geq 1$, prove that $\frac{n(n+1)(2n+1)}{6}$ is an integer.

→ Any integer has one of the ~~form~~ $6K, 6K+1, 6K+2, 6K+3, 6K+4, 6K+5$.

i) n is of the $6K$.

$\therefore \frac{n(n+1)(2n+1)}{6} = \frac{6K(6K+1)(12K+1)}{6}$

$= K(6K+1)(12K+1)$

Which is an integer.

ii) n is of the ~~form~~ $6K+1$

$\therefore \frac{n(n+1)(2n+1)}{6} = \frac{(6K+1)(6K+2)(12K+2+1)}{6}$

$= \frac{(6K+1)(6K+2)(12K+3)}{6}$

$= \frac{(6K+1)\,2(3K+1)\,3(4K+1)}{6}$

$= (6K+1)(3K+1)(4K+1)$

Which is an integer.

iii) n is of the ~~form~~ $6K+2$.

$\therefore \frac{n(n+1)(2n+1)}{6} = \frac{(6K+2)(6K+3)(12K+4+1)}{6}$

$= \frac{2(3K+1)\,3(2K+1)(12K+5)}{6}$

$= (3K+1)(2K+1)(12K+5)$

Which is an integer.

iv) n is of the form 6K+3.

$$\therefore \frac{n(n+1)(2n+1)}{6} = \frac{(6K+3)(6K+4)(12K+6+1)}{6}$$

$$= \frac{3(2K+1)\,2(3K+2)(12K+7)}{6}$$

$$= (2K+1)(3K+2)(12K+7)$$

Which is an integer.

v) n is of the form 6K+4.

$$\therefore \frac{n(n+1)(2n+1)}{6} = \frac{(6K+4)(6K+5)(12K+8+1)}{6}$$

$$= \frac{2(3K+4)(6K+5)\,3(4K+3)}{6}$$

$$= (3K+2)(6K+5)(4K+3)$$

Which is an integer.

vi) n is of the form 6K+5.

$$\therefore \frac{n(n+1)(2n+1)}{6} = \frac{(6K+5)(6K+6)(12K+10+1)}{6}$$

$$= \frac{(6K+5)\,6(K+1)(12K+11)}{6}$$

$$= (6K+5)(K+1)(12K+11)$$

Which is an integer.

Que For $n \geq 1$, prove that $\frac{n(n+1)(n+2)}{6}$ is an integer

→ Any integer is of the form 6K, 6K+1, 6K+2, 6K+3, 6K+4, 6K+5.

i) n is of the form 6K.

$$\therefore \frac{n(n+1)(n+2)}{6} = \frac{6K(6K+1)(6K+2)}{6}$$

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

Which is an integer.

ii) n is of the form 6k+1

$\therefore \frac{n(n+1)(n+2)}{6} = \frac{(6k+1)(6k+2)(6k+3)}{6}$

$= \frac{(6k+1)\,2(3k+1)\,3(2k+1)}{6}$

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

Which is an integer.

iii) n is of the form 6k+2.

$\therefore \frac{n(n+1)(n+2)}{6} = \frac{(6k+2)(6k+3)(6k+4)}{6}$

$= \frac{2(3k+1)\,3(2k+1)(6k+4)}{6}$

$= (3k+1)(2k+1)(6k+4)$

Which is an integer.

iv) n is of the form 6k+3.

$\therefore \frac{n(n+1)(n+2)}{6} = \frac{(6k+3)(6k+4)(6k+5)}{6}$

$= \frac{3(2k+1)2(3k+2)(6k+5)}{6}$

$= (2k+1)(3k+2)(6k+5)$

Which is an integer.

v) n is of the form 6k+4.

$\therefore \frac{n(n+1)(n+2)}{6} = \frac{(6k+4)(6k+5)(6k+6)}{6}$

$= \frac{(6k+4)(6k+5)6(k+1)}{6}$

$= (6k+4)(6k+5)(k+1)$

Which is an integer

vi) n is of the form 6k+5.

$$\therefore \frac{n(n+1)(n+2)}{6} = \frac{(6k+5)(6k+6)(6k+7)}{6}$$

$$= \frac{(6k+5)\,6(k+1)(6k+7)}{6}$$

$$= (6k+5)(k+1)(6k+7)$$

Which is an integer.

* Definition of Divisibility -:

Let 'a' and 'b' be integers then we say that a divides b (b is divisible by a) if there is an integer 'c' such that $b = ac$.

In this case we write $a|b$.

* Theorem -:

For integers a, b, c following holds,

a) $a|0$, $1|a$, $a|a$.

b) $a|1$ iff $a = \pm 1$

c) If $a|b$ and $c|d$ then $ac|bd$.

d) If $a|b$ and $b|c$ then $a|c$.

e) $a|b$ and $b|a$ iff $a = \pm b$.

f) If $a|b$ and $b \neq 0$ then $|a| \leq |b|$

g) If $a|b$ and $a|c$ then $a|bx+cy$ for arbitary integers x and y.

Proof:

a) Here we have,

$0 = a \cdot 0$

$\therefore$ By definition of divisibility $a|0$.

similary, by definition of divisibility we can prove following,

$1|a$ and $a|a$

b) If $a|1$

$\Rightarrow 1 = a \cdot 1$

It is possible only when,

$1 = 1 \cdot 1$

$\Rightarrow a = 1$.

Now, $1 = a \cdot (-1)$

$\Rightarrow 1 = (-1)(-1)$

$\Rightarrow a = -1$

$\therefore a = \pm 1$.

Conversely, $a = \pm 1$

Now $1 = 1 \cdot 1$

$\Rightarrow 1 = a \cdot 1$

By definition of divisibility,

$a|1$

Also, $1 = (-1) \cdot (-1)$

$\Rightarrow 1 = a \cdot (-1)$

By definition of divisibility;

$a|1$.

c) If $a|b$ and $c|d$

$\Rightarrow b = a \cdot e$ and $d = c \cdot f$, for some $e, f \in z$

$\Rightarrow bd = ac \cdot ef$

$\Rightarrow bd = ac \cdot g$ ($\because g = ef$; g, e, f are integers)

By definition of divisibility,

$ac|bd$.

d) If $a|b$ and $b|c$ then

By definition of divisibility,

$\exists$ $e, f > 0$ such that

$b = ae$; $e = bf$

$\Rightarrow bc = abef$

$\Rightarrow c = a \cdot ef$

$\Rightarrow c = a \cdot g$ ($\because g = ef$; g is an integer)

$\Rightarrow a \mid c$.

e) If $a \mid b$ and $b \mid a$

$\therefore a = bc$ and $b = ad$, for some $c, d \in \mathbb{Z}$

$\therefore a = bc$

$\Rightarrow a = ad \cdot c$

$\Rightarrow cd = 1$

$\therefore c = 1, d = 1$ or $c = -1, d = -1$

$\Rightarrow a = b$ or $a = -b$

i.e. $a = \pm b$

Conversely,

Let $a = \pm b$

If $a = b$ or $a = -b$

If $a = b$ then $a \mid b$ and $b \mid a$.

If $a = -b$ then $a = b \cdot (-1) \Rightarrow b \mid a$.

and $b = -a$ then $b = a \cdot (-1) \Rightarrow a \mid b$

f) Let $a \mid b$

$\Rightarrow b = ac$, for some $c \in \mathbb{Z}$

$\Rightarrow |b| = |ac|$

$= |a| \cdot |c|$

But $b \neq 0 \Rightarrow c \neq 0$

$\Rightarrow c \geq |1|$

since $|b| = |a||c|$

$\Rightarrow |b| \geq |a|$

$\therefore |a| \leq |b|$

g) Let $a|b$ and $a|c$

$\Rightarrow b = ak$ and $c = al$, for some $k, l \in z$

$\therefore bx = akx$ and $cy = aly$.

$\therefore bx + cy = akx + aly$.

$= a(kx + ly)$

$\Rightarrow a | bx + cy$; where $x, y \in z$.

Hence the proof.

Thursday
25/07/2019

Que If x and y be two odd integers then one of the two numbers $\frac{x+y}{2}$ and $\frac{x-y}{2}$ is odd and the other even.

→ Any integer is of the form $2n+1$.

Let $x = 2n+1$ and $y = 2m+1$

$$\frac{x+y}{2} = \frac{2n+1+2m+1}{2}$$

$$= \frac{2n+2m+2}{2}$$

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

$$= n+m+1$$

and

$$\frac{x-y}{2} = \frac{2n+1-2m-1}{2}$$

$$= \frac{2n-2m}{2}$$

$$= n-m$$

Case I: When 'n' and 'm' both are odd numbers then $n+m+1$ = odd number.

$\therefore \frac{x+y}{2}$ is odd number.

and for $n-m$ = even number.

$\therefore \frac{x-y}{2}$ is even number.

Case II: When 'n' and 'm' both are even numbers.

For $n+m+1$ = odd number.

$\therefore \frac{x+y}{2}$ is odd number.

and for $n-m$ = even number.

$\therefore \frac{x-y}{2}$ is even number.

Case III: When 'm' is odd and 'n' is even.

For $n+m+1$ = even number.

$\therefore \frac{x+y}{2}$ is even number.

and for $n-m$ = odd number.

$\therefore \frac{x-y}{2}$ is odd number.

Case IV: When 'm' is even and 'n' is odd.

For $n+m+1$ = even number.

$\therefore \frac{x+y}{2}$ is even number.

and for $n-m$ = odd number.

$\therefore \frac{x-y}{2}$ is odd number.

Que. One of every three consecutive integers is divisible by 3.

→ Let $a, a+1, a+2$ be any three consecutive integers.

We know that,
Any integer can be represented in the form of $3k$, $3k+1$, $3k+2$.

i) If $a = 3k$ then theorem holds trivially.

ii) If $a = 3k+1$ then

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

Which is in multiple of three.

iii) If $a = 3k+2$ then

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

Which is in multiple of three.

∴ One of every three consecutive integers is divisible by 3.

Que The product of any three consecutive integers is divisible by 3!

→ Let a, $a+1$ and $a+2$ be any three consecutive integers.

Step I: Let $a = 1$ (By Mathematical induction)

then $(a)\cdot(a+1)\cdot(a+2)$

$$= 1 \cdot 2 \cdot 3$$
$$= 6$$
$$= 3!$$

∴ For $a = 1$

which is divisible by 3!

Step II: Let $a = k$ (Assume that result holds for $a=k$)

then $(a).(a+1).(a+2) = k(k+1)(k+2)$

∴ Result holds trivially.

Step III: Let $a = k+1$

then $(a)\cdot(a+1)(a+2)$

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

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

In the step III we have the term $k(k+1)(k+2)$ is divisible by 3! also in the second term the product $(k+1)(k+2)$ is in the multiple of 2 therefore the term $3(k+1)(k+2)$ is multiple of 3!.

∴ By mathematical induction is true for all integers $a \in \mathbb{Z}$

Saturday 27/07/2019

* Common Divisors :-

Let 'a' and 'b' be two integers, atleast one of which is non-zero then an integer 'c' is a common divisor if $c|a$ and $c|b$.

* Greatest Common Divisor [g.c.d] :-

Let 'a' and 'b' be two integers, atleast one of which is non-zero then a positive integer 'd' is g.c.d of 'a' and 'b' if

i) $d|a$ and $d|b$

ii) If 'c' is positive integer such that $c|a$ and $c|b$ then $c \leq d$ ($c|d$)

Ex. Find the g.c.d (-16, 40)

→ Here $a = -16$ and $b = 40$.

∴ positive divisor of $a = -16$ are 1, 2, 4, 8, 16 and positive divisors of $b = 40$ are 1, 2, 4, 5, 8, 10, 20, 40.

∴ g.c.d (a,b) = g.c.d $(-16, 40)$

$= 8$.

Now, common divisors are 1, 2, 4, 8.

* Theorem -:

* **Statement:**

Given integers 'a' and 'b' not both of which are zero. There exist integers 'x' and 'y' such that $g.c.d(a,b) = ax+by$.

Proof:

Let $S = \{au+bv \mid au+bv>0;\ u,v \text{ are integers}\}$

For $a \neq 0$,

$|a| = au+0.v$, where $u = 1$ or -1 according as $a>0$ or $a<0$

Thus, S is non-empty.

Thus, S is non-empty set of positive integers.

Hence by principle of well ordering set 'S' has least positive integer $d \in S$.

Hence $\exists$ integers 'x' and 'y' such that

$d = ax+by$. ——— (1)

By division algorithm,

$\exists$ integers 'q' and 'r' such that

$a = dq+r$; $0 \leq r < d$.

Thus, $r = a - dq$

$= a - (ax+by)q$

$= a - aqx - bqy$.

$= a(1-qx) + b(-qy)$

Hence $r \in S$.

But this contradicts minimality of d.

Hence we must have $r=0$.

$\therefore$ For $r=0$ we have $a = dq$.

$\Rightarrow d \mid a$

similary, we can prove that $d \mid b$.

$\therefore$ 'd' is common divisor of 'a' and 'b' ——— (2)

Now, we have to prove that 'd' is greatest

among all the common divisors of 'a' and 'b'.

Let $c \in \mathbb{Z}$ such that,

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

$\Rightarrow c \mid ax+by$ (By prev. theorem).

$\Rightarrow c \mid d$ ($\because d = ax+by$)

Here $d \neq 0$ and $c \mid d$

$\Rightarrow |c| \leq |d|$

$\Rightarrow c \leq d$ — (3)

Hence from (2) and (3),

$d = g.c.d\,(a,b)$

$\therefore g.c.d\,(a,b) = ax+by$.

Hence the proof.

Wednesday 31/07/2019

* Corollary -:

If 'a' and 'b' are given integers not both are zero then the set $T = \{ax+by \mid x, y \in \mathbb{Z}\}$ is precisely the set of all multiples of d. [where 'd' is $g.c.d\,(a,b)$]

Proof: We have,

$d = g.c.d.\,(a,b)$

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

$\Rightarrow d \mid ax+by$, for some integers 'x' and 'y'.

$\therefore ax+by = d.n$, for some $n \in \mathbb{Z}$.

$\therefore$ Every member of set T is in multiple of d.

Conversely,

Let $n.d$ be any multiple of d.

As $d = g.c.d\,(a,b)$

$\therefore \exists$ integers 'x' and 'y' such that,

$d = ax+by$

$\Rightarrow nd = a(nx)+b(ny)$

$\Rightarrow nd = ax'+by'$; $x' = nx$ and $y' = ny$

$\Rightarrow nd \in T$.

Hence the proof.

Ex. Show that any integer of the form $6k+5$ is also of the form $3j+2$ but not conversely.

→ An integer is of the form $6k+5$.

i.e. $n = 6k+5$

$\therefore n = 6k+5$

$= 6k+3+2$

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

$= 3j+2 \quad ; j = 2k+1$

Conversely,

$3j+2 = 6k+5$

$\Rightarrow 3j = 6k+3$

$\Rightarrow j = 2k+1$

$\Rightarrow 2k = j-1$

For 'j' is even we get $(j-1)$ is odd integer.

But L.H.S. cleary shows that even integer.

Hence for even j, $2k \neq j-1$

Hence, our assumption is wrong.

Thus an integer $3j+2$ cannot be written as of the form $6k+5$.

Ex. Prove that any positive integer n and any positive integer a, $g.c.d(a, a+n) | n$ and hence $g.c.d(a, a+1) = 1$.

→ Let $d = g.c.d(a, a+n)$

$\Rightarrow d | a$ and $d | a+n$

$\Rightarrow d | ax + (a+n)y$. ; for $x, y \in z$.

Take $x = -1$ and $y = 1$

$\therefore d | -a+a+n$

$\Rightarrow d | n$.

Hence $g.c.d(a, a+n) | n$

Now take $n = 1$

We have,

$gcd(a, a+1) \mid 1$

$\Rightarrow gcd(a, a+1) = \pm 1$

But since g.c.d is possitive we get,

$gcd(a, a+1) = 1$.

Ex. For any integer $a \in \mathbb{Z}$ show the following

i) $gcd(2a+1, 9a+4) = 1$

ii) $gcd(5a+2, 7a+3) = 1$

iii) If 'a' is odd then $gcd(3a, 3a+2) = 1$.

→ i) Let $d = gcd(2a+1, 9a+4)$

$\Rightarrow d \mid 2a+1$ and $d \mid 9a+4$

$\Rightarrow d \mid (2a+1)x + (9a+4)y$; for $x, y \in \mathbb{Z}$

Take $x = -9$ and $y = 2$

$\therefore d \mid (2a+1)(-9) + (9a+4)(2)$

$\Rightarrow d \mid -18a - 9 + 18a + 8$

$\Rightarrow d \mid -1$

$\therefore gcd(2a+1, 9a+4) \mid -1$

$\Rightarrow gcd(2a+1, 9a+4) = \pm 1$

But since gcd is positive we get,

$gcd(2a+1, 9a+4) = 1$

ii) Let $d = gcd(5a+2, 7a+3)$

$\Rightarrow d \mid 5a+2$ and $d \mid 7a+3$

$\Rightarrow d \mid (5a+2)x + (7a+3)y$; for $x, y \in \mathbb{Z}$.

Take $x = -7$ and $y = 5$

$\therefore d \mid (5a+2)(-7) + (7a+3)(5)$

$\therefore d \mid -35a - 14 + 35a + 15$

$\therefore d \mid 1$

$\Rightarrow gcd(5a+2, 7a+3) \mid 1$

$\Rightarrow gcd(5a+2, 7a+3) = \pm 1$

But since g.c.d is positive then we get,

$gcd(5a+2, 7a+3) = 1$.

iii) Let $d = g.c.d(3a, 3a+2)$

$\Rightarrow d \mid 3a$ and $d \mid 3a+2$

$\Rightarrow d \mid 3ax + (3a+2)y$; for $x, y \in \mathbb{Z}$.

Take $x = 1$ and $y = -1$

$\therefore d \mid 3a - 3a - 2$

$\therefore d \mid -2$

$\Rightarrow d \mid \pm 1$ and $d \mid \pm 2$.

Suppose $d = 2$.

Now since 'd' divides $3a$

$\therefore 2 \mid 3a$

But $3a$ is odd. ($\because a$ is odd)

$2 \nmid 3a \Rightarrow d \neq 2$

$\Rightarrow d = 1$

$\therefore g.c.d(3a, 3a+2) = 1.$

Ex. If a and b are integers not both are zero then prove that $g.c.d(2a-3b, 4a-5b) \mid b$ and hence $g.c.d(2a-3b, 4a+5) = 1$.

→ Let $d = g.c.d(2a-3b, 4a-5b)$

$\Rightarrow d \mid 2a-3b$ and $d \mid 4a-5b$

$\Rightarrow d \mid (2a-3b)x + (4a-5b)y$; for $x, y \in \mathbb{Z}$.

Taking $x = 2$ and $y = -1$

$\therefore d \mid (2a-3b)(2) + (4a-5b)(-1)$

$\therefore d \mid 4a - 6b - 4a + 5b$

$\therefore d \mid b$

$\Rightarrow d = \pm b$

Since g.c.d is positive,

$\therefore d \mid b$

$\Rightarrow g.c.d(2a-3b, 4a-5b) \mid b.$

Now,

Let $d = g.c.d(2a+3, 4a+5)$

$\Rightarrow d \mid 2a+3$ and $d \mid 4a+5$

$\Rightarrow d \mid (2a+3)x + (4a+5)y$; for $x, y \in \mathbb{Z}$

Take $x = -2$ and $y = 1$

$\therefore d \mid (2a+3)(-2) + (4a+5)(1)$

$\Rightarrow d \mid -4a-6+4a+5$

$\Rightarrow d \mid -1$

$\Rightarrow d = \pm 1$

But g.c.d must be positive

$\therefore d = 1$

$\therefore$ g.c.d $(2a+3, 4a+5) = 1$

Que Use mathematical induction to prove that

(a) $8 \mid 5^{2n}+7$.

→ **Step I:** First we prove result for $n=1$.

$\therefore 5^{2n}+7 = 5^{2\cdot 1}+7$

$= 5^2+7$

$= 25+7$

$= 32$.

since $8 \mid 32$.

$\therefore$ Result is true for $n=1$.

Step II: Assume that result is true for $n=k$.

i.e. $8 \mid 5^{2k}+7$.

Step III: For $n=k+1$

$\therefore 5^{2n}+7 = 5^{2(k+1)}+7$

$= 5^{2k+2}+7$

$= 5^{2k} \cdot 5^2 + 7$

$= 5^{2k} 5^2 + 5^2 7 - 5^2 7 + 7$

$= 5^2 (5^{2k}+7) + 7(-25+1)$

$= 5^2 (5^{2k}+7) + 7(-24)$

$\Rightarrow d \mid 5^{2(k+1)}+7$.

$\therefore$ Result is true for $n = k+1$.

(b) $15 \mid 2^{4n}-1$

→ **Step I:** First we prove the result for $n=1$

$\therefore 2^{4n}-1 = 2^{4(1)}-1$

$= 2^4-1$

$= 16+1$

$= 15$

since $15 \mid 15$

$\therefore$ Result is true for $n=1$

Step II: Assume that result is true for $n=k$.

i.e $15 \mid 2^{4k}-1$

Step III: For $n=k+1$

$\therefore 2^{4n}-1 = 2^{4(k+1)}-1$

$= 2^{4k+4}-1$

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

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

$= 2^4[2^{4k}-1] + 1[2^4-1]$

$= 2^4[2^{4k}-1] + 1[15]$

$\Rightarrow 15 \mid 2^{4(k+1)}-1$

$\therefore$ Result is true for $n=k+1$

(c) $5 \mid 3^{3n+1} + 2^{n+1}$

→ Result holds for $n=1$

Suppose result is true for any integer k.

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

$\therefore \exists$ integer m such that $3^{3k+1} + 2^{k+1} = 5m$ — (1)

($\because$ by def^n of divisibility)

Now to prove $n=k+1$.

Consider,

$3^{(3k+1)+1} + 2^{(k+1)+1} = 3^{3k+4} + 2^{k+2}$

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

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

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

$= 3^3 (5m) + 2^{k+1} (-25)$ —— by (1)

$= 3^3 (5m) - 25 (2^{k+1})$

$= 5 (3^3 m - 5 \cdot 2^{k+1})$

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

∴ Result holds for $k+1$.

(d) $24 \mid 2 \cdot 7^n + 3 \cdot 5^n - 5$

→ Result holds for $n = 1$

Suppose it is true for any integer k.

$\therefore 24 \mid 2 \cdot 7^k + 3 \cdot 5^k - 5$

$\Rightarrow \exists$ integer q such that

$2 \cdot 7^k + 3 \cdot 5^k - 5 = 24q$ —— (1)

(by def^n of divisibility)

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

$2 \cdot 7^{k+1} + 3 \cdot 5^{k+1} - 5$

$= 2 \cdot 7 \cdot 7^k + 3 \cdot 5 \cdot 5^k - 5$

$= 7(2 \cdot 7^k) + 5(3 \cdot 5^k) - 5$

$= 2(2 \cdot 7^k) + 5(2 \cdot 7^k) + 5(3 \cdot 5^k) - 5$

$= 2(2 \cdot 7^k) + 5(2 \cdot 7^k) + 5(3 \cdot 5^k) - 5 + 5 \cdot 5 - 5 \cdot 5$

$= 2(2 \cdot 7^k) + 5[(2 \cdot 7^k) + (3 \cdot 5^k) - 5] - 5 + 5 \cdot 5$

$= 2(2 \cdot 7^k) + 5(24 \cdot q) - 5 + 5 \cdot 5$ —— by (1)

$= 5(24q) + 2(2 \cdot 7^k) - 5 + 5 \cdot 5$

$= 24(5q) + 4 \cdot 7^k + 20$ —— (2)

But we have,

$24 \mid 4 \cdot 7^k + 20$

Then eq^n (2) becomes,

$24(5q) + 24\alpha = 24(5q + \alpha)$

$\Rightarrow 24 \mid 2 \cdot 7^{k+1} + 3 \cdot 5^{k+1} - 5$

∴ Result is true for $n = k+1$.

(e) $21 \mid 4^{n+1} + 5^{2n-1}$

→ Result holds for $n = 1$

Suppose it is true for any integer k.

$\therefore 21 \mid 4^{k+1} + 5^{2k-1}$

$\Rightarrow \exists$ integer p such that

$4^{k+1} + 5^{2k-1} = 21p$ —— ① (by def° of divisibility)

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

$\therefore 4^{(k+1)+1} + 5^{2(k+1)-1}$

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

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

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

$= 5^2 (4^{k+1} + 5^{2k-1}) + 4^{k+1} (4 - 5^2)$

$= 5^2 (21p) + 4^{k+1} (-21)$ —— by ①

$= 5^2 (21p) - 21 (4^{k+1})$

$= 21 (5^2 p - 4^{k+1})$

$\Rightarrow 21 \mid 4^{(k+1)+1} + 5^{2(k+1)-1}$

$\therefore$ Result is true for $n = k+1$.

Saturday
24/05/2019

* Relatively Prime integers -:

Two integers 'a' and 'b' are relatively prime if $g.c.d\,(a,b) = 1$

* Theorem -:

Let 'a' and 'b' be the integers not both zero. Then 'a' and 'b' are relatively prime if and only if there exist integers 'x' and 'y' such that $ax + by = 1$.

Proof:

Suppose 'a' and 'b' are relatively prime then $g.c.d.(a,b) = 1$.

$\therefore \exists$ integers 'x' and 'y' such that,

$ax + by = 1$.

Conversely,

Suppose that $ax+by=1$, for some integers 'x' and 'y'

Let $d = g.c.d(a,b)$

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

$\Rightarrow d \mid ax+by$

$\Rightarrow d \mid 1$

$\Rightarrow d = 1$

Hence "a" and 'b' are relatively prime.

Ex. Show that if $g.c.d(a,b) = d$ then $g.c.d(a/d, b/d) = 1$.

→ Suppose $d = g.c.d(a,b)$ then $d \mid a$, $d \mid b$.

$\therefore \frac{a}{d}, \frac{b}{d}$ are Integers.

since $d = g.c.d(a,b)$, $\exists$ integers 'x' and 'y' such that $ax+by=d$ (by above theorem)

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

$\therefore g.c.d\left(\frac{a}{d}, \frac{b}{d}\right) = 1.$

* Theorem -:

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

Proof:

Let $a \mid c$ then their exists integer 'r' such that $c = ar$. —— ①

and Let $b \mid c$ then their exist integer 's' such that $c = bs$. —— ②

We know, $g.c.d(a,b) = 1$ then their exist integers 'x' and 'y' such that

$ax + by = 1$

$\Rightarrow acx + bcy = 1$

$\Rightarrow abrx + abry = 1$; from ① and ②

$\Rightarrow ab(sx + ry) = 1$; 'r' and 's' are integers.

$\Rightarrow abk = c$

$\Rightarrow ab \mid c$

* Remark -:

If $g.c.d(a,b) \neq 1$ then above may or may not be hold.

e.g. i) $a=2,\ b=4,\ c=8$

$g.c.d(a,b) = 2$

$\Rightarrow 2 \mid 8$ and $4 \mid 8$

$\Rightarrow 2 \cdot 4 \mid 8$

$\Rightarrow 8 \mid 8$

ii) $a=2,\ b=4,\ c=12$.

$g.c.d(a,b) = 12$

$\Rightarrow 2 \mid 12$ and $4 \mid 12$

$\Rightarrow 2 \cdot 4 \nmid 12$

$\Rightarrow 8 \nmid 12$

* Theorem [Euclid's Lemma] -:

If $a \mid bc$ with $g.c.d(a,b) = 1$ then $a \mid c$.

Proof:

Suppose $g.c.d(a,b) = 1$ then $\exists$ integers 'x' and 'y' such that,

$ax + by = 1$ —— ①

Multiply eqⁿ ① by 'c' we obtain,

$acx + bcy = c$ —— ②

and

let $a|bc$ and $a|ac$ then $\exists$ any integers 'x' and 'y' such that

$a| acx + bcy$

$\Rightarrow a|c$; from (2).

* Remark-:

If $gcd(a,b) \neq 1$ then above result may or may not hold.

e.g. i) $a=2, b=4, c=2$ with $g.c.d(a,b)=2$ but $a|c$ hold. $\Rightarrow 2|2$

ii) $a=3, b=9, c=2$ with $g.c.d(a,b)=9$ but $a \nmid c$ not hold $\Rightarrow 3 \nmid 2$.

Que. Given integers a, b, c, d verify the following.

a) $a|b$ then $a|bc$

b) If $a|b$ and $a|c$ then $a^2|bc$.

c) $a|b$ iff $ac|bc$ $(c \neq 0)$

d) If $a|b$ and $c|d$ then $ac|bd$.

→ For given integers a, b, c, d

a) Here $a|b$

$\therefore \exists$ an integer 'r' such that,

$b = ar$

$\Rightarrow bc = arc$

$bc = ka$ $(\because k = rc)$

$\Rightarrow a|bc$

b) If $a|b$ and $a|c$ then

$\exists$ an integer 'r' such that,

$b = ar$ —— (1)

Ily, $\exists$ an integer 's' such that,

$c = as$ —— (2)

From ① and ② we have,

$bc = a^2rs$

$\Rightarrow a^2 | bc$

c) Let $a|b$

$\therefore \exists$ an integer 'r' such that,

$b = ar$

$\Rightarrow bc = arc$

$\therefore ac | bc \quad (\because c \neq 0)$

conversely,

$ac | bc$

$\therefore \exists$ an integer 'r' such that

$bc = acr$

Here $c \neq 0$

$\therefore b = ar$

$\Rightarrow a | b.$

d) Let $a|b$ and $c|d$.

$\therefore \exists$ an integer 'r' such that,

$b = ar \quad —①$

Ily, $\exists$ an integer 's' such that,

$d = cs \quad —②$

From ① and ② we have,

$bd = acrs.$

$\Rightarrow ac | bd$

Ex. Establish that the difference between two consecutive cube is never divisible by 2.

→ Let 'a' and 'a+1' be two consecutive cubes

$\therefore (a+1)^3 - a^3 = a^3 + 3a^2 - 3a + 1 - a^3$

$= 3a^2 - 3a + 1$

$= 3a(a+1)+1$

Since $a(a+1)$ is always divisible by 2.

We have $a(a+1) = 2k$; for some k

$\therefore 3a(a+1)+1 = 3(2k)+1$

$= 6k+1$

$= 2(3k)+1.$

Which is always an odd integer.

Hence $(a+1)^3 - a^3$ is never divisible by 2

Hence, the difference between two consecutive cube is never divisible by 2.

Ex. Prove that for a possitive integer n, and any integer a, g.c.d $(a, a+n)$ divides n hence $gcd(a, a+1) = 1$.

→ Let $d = g.c.d\,(a, a+n)$

$\Rightarrow d \mid a$ and $d \mid a+n$

$\Rightarrow d \mid ax + (a+n)y$; for $x, y \in \mathbb{Z}$

Take $x = -1$ and $y = 1$

$\therefore d \mid -a + a + n$

$\Rightarrow d \mid n$

Hence $g.c.d\,(a, a+n) \mid n$.

Now take $n = 1$.

We have $gcd\,(a, a+1) \mid 1$

$\Rightarrow gcd\,(a, a+1) = \pm 1$

But since g.c.d is possitive we get,

$g.c.d\,(a, a+1) \mid n.$

Ex. Assuming that $gcd\,(a,b) = 1$. Prove that g.c.d $(a+b, a-b) = 1$ or 2

→ Let $gcd\,(a,b) = 1$

Suppose $d = gcd\,(a+b, a-b)$

$\therefore d \mid a+b$ and $d \mid a-b$

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

$\Rightarrow d \mid 2a$ and $d \mid 2b$

$\Rightarrow d \mid g.c.d(2a, 2b)$

$\Rightarrow d \mid 2\,gcd(a,b)$

$\therefore d \mid 2 \cdot 1$ as $gcd(a,b) = 1$

$\Rightarrow d \mid 2$ and $d \mid 1$

Thus $g.c.d(a+b, a-b) = 1$ or 2.

Ex. If 'a' and 'b' both are odd integers then $16 \mid a^4+b^4-2$.

→ Consider,

$a = 2k+1$ and $b = 2j+1$

Now,

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

$\therefore a^2 = 8k+1$

and

$$b^2 = (2j+1)^2$$
$$= 4j^2 + 4j + 1$$
$$= 4j(j+1) + 1$$
$$= 4(2j) + 1$$

$\therefore b^2 = 8j+1$

Now,

$$a^4+b^4-2 = (a^2)^2 + (b^2)^2 - 2$$
$$= (8k+1)^2 + (8j+1)^2 - 2$$
$$= 64k^2+16k+1 + 64j^2+16j+1-2$$
$$= 16k(4k+1) + 16j(4j+1)$$

$\therefore 16 \mid 16k(4k+1) + 16j(4j+1)$

$\Rightarrow 16 \mid a^4+b^4-2$.

* Least Common Multiple [L.C.M] -:

Let 'a' and 'b' be integers, not both zero then a positive integer 'm' is said to be least common multiple of 'a' and 'b' if,

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

ii) If 'c' is any positive integer such that $a|c$ and $b|c \Rightarrow m|c$ or $m \leq c$.

Vimp * Theorem -:

Let a, b be integers, not both zero then $lcm(a,b) \cdot gcd(a,b) = a \cdot b$.

Proof:

Let $d = gcd(a,b)$ and $m = \frac{ab}{d}$ then

we have to show that $lcm(a,b) = m$.

Here, $d = gcd(a,b)$ then

$d|a$ and $d|b$.

$\therefore$ $\exists$ an integers 'x' and 'y' such that

$a = dx$ and $b = dy$

$\therefore$ $m = \frac{ab}{d}$ becomes,

$m = \frac{dx \cdot b}{d}$ and $m = \frac{a \cdot dy}{d}$

$\Rightarrow$ $m = bx$ and $m = ay$

$\Rightarrow$ $b|m$ and $a|m$

Hence, first condition is satisfied.

Let 'c' be common multiple of 'a' and 'b' then $\exists$ an integers 'r' and 's' such that,

$ar = c$ and $bs = c$

since, $d = gcd(a,b)$

Then $\exists$ integers 'p' and 'q' such that,

$d = ap + bq$.

Consider,

$$\frac{c}{m} = \frac{cd}{ab} = \frac{c}{ab}(ap + bq)$$

$$= \frac{cap}{ab} + \frac{cbq}{ab}$$

$$= \frac{cp}{b} + \frac{cq}{a}$$

Since, 'c' is common multiple of 'a' and 'b'

$\therefore$ $\frac{c}{a}$ and $\frac{c}{b}$ are integers.

$\therefore$ $m \mid c$ i.e. $m \leq c$.

Hence 'm' is lcm(a,b)

$\therefore$ $m = \frac{ab}{d}$ gives,

$$lcm(ab) = \frac{ab}{gcd(a,b)}$$

i.e. $lcm(a,b) \cdot gcd(a,b) = a \cdot b$.

Hence the proof.

* Remark -:

If $gcd(a,b) = 1$ then $lcm(a,b) = a \cdot b$.

Wednesday 04/09/2019

* The Euclidean Algorithm -:

* **Theorem:**

Apply the division algorithm repeatedly for any two possitive integers 'a' and 'b', $a > b$. To obtain a set of remainder then the last non-zero remainder in the process of division is the gcd (a,b).

Proof:

By division algorithm we have,

$a = bq_1 + r_1 \; ; \; 0 \leq r_1 < b$.

If it happens that $r_1 = 0$, then $b \mid a$ and $\gcd(a, b) = b$.

When $r_1 \neq 0$;

divide 'b' by 'r_1' to produce the integers 'q_1' and 'r_1' satisfying,

$$b = r_1 q_2 + r_2 \quad ; \quad 0 \leq r_2 < r_1$$

If $r_2 = 0$ then we stop otherwise, proceed as before to obtain

$$r_1 = r_2 q_3 + r_3 \quad ; \quad 0 \leq r_3 < r_2$$

This division process continues until some zero remainder appears, say, at $(n+1)^{th}$ stage where 'r_{n-1}' is divided by 'r_n'.

The result is the following system of equations,

$$a = bq_1 + r_1 \quad ; \quad 0 \leq r_1 < b$$
$$b = r_1 q_2 + r_2 \quad ; \quad 0 \leq r_2 < r_1$$
$$r_1 = r_2 q_3 + r_3 \quad ; \quad 0 \leq r_3 < r_2$$
$$\vdots \qquad \vdots \qquad \vdots$$
$$r_{n-1} = r_n q_{n+1} + r_{n+1} \quad ; \quad 0 \leq r_{n+1} < r_n$$
$$r_n = r_{n+1} q_{n+2} + 0$$

We argue that the last non-zero remainder that appears in this manner, is equal to $\gcd(a, b)$. Our proof is based on the lemma below.

* Lemma –:

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

Proof:

Here given that,

$$a = bq + r \quad ; \quad 0 \leq r < b \quad \text{—— (1)}$$

Let us suppose that,
$\gcd(a,b) = d_1$ and $\gcd(b,r) = d_2$.
Now,
$\gcd(a,b) = d_1$
$\Rightarrow d_1 | a$ and $d_1 | b$
$\Rightarrow d_1 | a$ and $d_1 | bq$
$\Rightarrow d_1 | a - bq$ ... ($\because$ by (1))
$\Rightarrow d_1 | r$ ... ($\because$ by (1))
$\Rightarrow d_1 | b$ and $d_1 | r$
$\therefore d_1 \leq d_2$ —— (I)
and
$\gcd(b,r) = d_2$
$\Rightarrow d_2 | b$ and $d_2 | r$
$\Rightarrow d_2 | bq$ and $d_2 | r$
$\Rightarrow d_2 | bq + r$
$\Rightarrow d_2 | a$ ($\because$ by (1))
$\Rightarrow d_2 | a$ and $d_2 | b$
$\therefore d_2 \leq d_1$ —— (II)
From (I) and (II) we have,
$d_1 = d_2$.
$\therefore \gcd(a,b) = \gcd(b,r)$
Hence the proof.

* Examples -:

(1) Find gcd (12378, 3054) by using Euclidean algorithm and express it as linear combination of 12378, 3054.

→ Let, $12378 = (4)\,3054 + 162$
$3054 = (18)\,162 + 138$
$162 = (1)\,138 + 24$
$138 = (5)\,24 + 18$
$24 = (1)\,18 + \boxed{6}$

$18 = (3)6 + 0$

$\therefore$ gcd $(12378, 3054) = 6$

Now,

$6 = (1)24 - (1)18$

$= (1)24 - [(1)138 - (5)24]$

$= (6)24 - (1)138$

$= (6)[(1)162 - (1)138] - (1)138$

$= (6)162 - (7)138$

$= (6)162 - (7)[(1)3054 - (18)162]$

$= (6)162 - (7)3054 + (126)162$

$= (132)162 - (7)3054$

$= (132)[(1)12378 - (4)3054] - (7)3054$

$= (132)12378 - (528)3054 - (7)3054$

$\therefore \quad 6 = (132)12378 - (595)3054$

② Find gcd $(143, 227)$ and express it as $143x + 227y$.

→ Let $227 = (1)143 + 84$

$143 = (1)84 + 59$

$84 = (1)59 + 25$

$59 = (2)25 + 9$

$25 = (2)9 + 7$

$9 = (1)7 + 2$

$7 = (3)2 + \boxed{1}$

$2 = (1)2 + 0$

Now,

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

$= (1)7 - (3)[(1)9 - (1)7]$

$= (4)7 - (3)9$

$= (4)[(1)25 - (2)9] - (3)9$

$= (4)25 - (8)9 - (3)9$

$= (4)25 - (11)9$

$= (4)25 - (11)[(1)59 - (2)25]$

$= (4)25 - (11)59 + (22)(25)$

$= (26)25 - (11)59$

$= (26)[(1)84 - (1)59] - (11)59$

$= (26)84 - (26)59 - (11)59$

$= (26)84 - (37)59$

$= (26)84 - (37)[(1)143 - (1)84]$

$= (26)84 - (37)143 + (37)84$

$= (63)84 - (37)143$

$= (63)[(1)227 - (1)143] - (37)143$

$= (63)(227) - (63)143 - (37)143$

$\therefore 1 = (63)(227) - (100)143$

$\Rightarrow 1 = (-100)143 + (63)227$

$\therefore x = -100$ and $y = 63$

③ Find gcd (56, 72) and express it as $56x + 72y$

→ Let $72 = (1)56 + 16$

$56 = (3)16 + 8$

$16 = (2)8 + 0$

$\therefore$ gcd $(56, 72) = 8$.

Now,

$8 = (1)56 - (3)16$

$= (1)56 - (3)[(1)72 - (1)56]$

$= (1)56 - (3)72 + (3)56$

$\therefore 8 = (4)56 - (3)72$

Here $x = 4$ and $y = -3$

④ Find gcd (723, 24).

→ Let $723 = (30)24 + 3$

and $24 = (8)3 + 0$

$\therefore$ gcd $(723, 24) = 3$.

⑤ Find gcd (426, 246) and express it as. $426x + 246y$.

→ Let $426 = (1)246 + 180$

$246 = (1)180 + 66$

$180 = (2)66 + 48$

$66 = (1)48 + 18$

$48 = (2)18 + 12$

$18 = (1)12 + 6$

$12 = (2)6 + 0$

$\therefore$ gcd (426, 246) = 6.

Now,

$6 = (1)18 - (1)12)$

$= (1)18 - (1)[48 - (2)18]$

$= (3)18 - (1)48$

$= (3)[(1)66 - (1)48] - (1)48$

$= (3)66 - (4)48$

$= (3)66 - (4)[(1)180 - (2)66]$

$= (3)66 - (4)180 + (8)66$

$= (11)66 - (4)180$

$= (11)[(1)246 - (1)180] - (4)180$

$= (11)246 - (15)180$

$= (11)246 - (15)[(1)426 - (1)246]$

$= (11)246 - (15)426 + (15)246$

$= (26)246 - (15)426$

$\therefore 6 = (-15)2426 + (26)246$

Here $x = -15$ and $y = 26$.

Tuesday 17/09/2019

* Theorem -:

If $k > 0$ then gcd $(ka, kb) = k \cdot$ gcd (a, b)

Proof:

Let $d =$ gcd (a, b) then $d|a$ and $d|b$.

$\therefore$ for any $k > 0$, $kd > 0$

$\therefore kd \mid a$ and $kd \mid b$ — ①

Let 'c' be a positive integer such that

$c \mid ka$ and $c \mid kb$

since $d = gcd(a,b)$

$\therefore \exists$ integers 'x' and 'y' such that $d = ax + by$ — *

$c \mid kax + kby \Rightarrow c \mid k(ax+by)$

$\Rightarrow c \mid k \cdot d$ — ② ; by *

From ① and ②,

$gcd(ka, kb) = k \cdot gcd(a,b)$.

* Note -:

If $k \neq 0$ then $gcd(ka, kb) = 1 \cdot k \mid gcd(a,b)$.

* Diophantine Equation -:

In general any equation in one or more unknowns which is to be solved in integers is Diophantine equation. The name honours the Greek mathematician Diophantus.

There is an intresting problems something about how did Diophantus lived.

Ex. His boyhood lasted $(1/6)^{th}$ of his life; His beared grew after $(1/12)^{th}$ more; After $(1/7)^{th}$ more he married and his son was borned 5 years after. The son lived to $(1/2)^{th}$ his father age and the father died after 4 years after his son.

→ Let x be the age of Diophantes when he died.

$\therefore$ From given information.

$$\frac{1}{6}x + \frac{1}{12}x + \frac{1}{7}x + 5 + \frac{x}{2} + 4 = x$$

$\therefore \frac{18x}{72} + \frac{9}{14}x + 9 = x$

$\therefore \frac{1}{4}x + \frac{9}{14}x + 9 = x$

$\frac{14x + 36x}{56} + 9 = x$

$\Rightarrow \frac{50}{56}x + 9 = x \Rightarrow 9 = x - \frac{50}{56}x$

$\Rightarrow 9 = x - \frac{25}{28}x$

$\Rightarrow 9 = \frac{3x}{28}$

$\Rightarrow \frac{9 \times 28}{3} = x$

$\Rightarrow \boxed{x = 84 \text{ years.}}$

Diophantine equation may be of any degree and in any number of unknowns, however we are intrested in linear Diophantine equation of the form $ax + by = c$.

A Diophantine equation may have a number of solution.

e.g. $3x + 6y = 18$

$3 \cdot 0 + 6 \cdot 3 = 18$

$3 \cdot 6 + 6 \cdot 0 = 18$

$3 \cdot 2 + 6 \cdot 2 = 18$

$3 \cdot (-2) + 6(4) = 18$

$3 \cdot (8) + 6(-1) = 18$

i.e. $(0, 3), (6, 0), (2, 2), (-2, 4), (8, -1)$ are all solutions of eqn $3x + 6y = 18$.

VImp

* Theorem -:

The linear Diophantine equation $ax+by=c$ has a solution if and only if $d|c$ where $d=\gcd(a,b)$. If x_0, y_0 is any particular solution of this equation then all other solutions are given by, $x = x_0 + \left(\frac{b}{d}\right)t$ and $y = y_0 - \left(\frac{a}{d}\right)t$.

Proof:

Let $d=\gcd(a,b)$ then $d|a$ and $d|b$.
suppose $ax+by=c$ has a solution that is there exist integers 'x_0' and 'y_0' such that,

$$ax_0 + by_0 = c.$$

since $d|a$ and $d|b$ we have,

$$d \mid ax_0 + by_0 = c.$$

Thus $d|c$

Conversely,

suppose that $d|c$.

since $d=\gcd(a,b)$ there exists integers 'x_0' and 'y_0' such that,

$$d = ax_0 + by_0$$

since $d|c$ there exists an integer 'r' such that $dr = c$

Thus $c = dr$

$$= r(ax_0+by_0)$$
$$= a(rx_0) + b(ry_0)$$

Hence $x = rx_0$ and $y = ry_0$ is a solution of $ax+by=c$.

Suppose that $ax+by=c$ has a solution (x_0, y_0) then $ax_0+by_0=c$.

Let (x, y) be any solution of $ax+by=c$ then $ax+by = ax_0+by_0$

$$\Rightarrow a(x-x_0) = b(y_0-y) \quad \text{——①}$$

since $d = \gcd(a,b)$ there exist relatively prime integers 'r' and 's' such that,

$$a = dr \quad \text{and} \quad b = ds \quad \text{—— ②}$$

∴ Eqⁿ ① becomes,

$$dr(x - x_0) = ds(y_0 - y)$$

$$\Rightarrow r(x - x_0) = s(y_0 - y)$$

since $r \mid r(x - x_0) = s(y_0 - y)$

but $\gcd(r, s) = 1$

∴ By Euclid's Lemma,

$$r \mid (y_0 - y)$$

Therefore, there is an integer 't' such that

$$y_0 - y = rt$$

$$\Rightarrow y = y_0 - rt$$

$$\Rightarrow \boxed{y = y_0 - \frac{a}{d}t} \quad \text{— from ②.}$$

Further,

$$x - x_0 = st$$

$$\Rightarrow x = x_0 + st$$

$$\Rightarrow \boxed{x = x_0 + \frac{b}{d}t} \quad \text{— from ②}$$

Let

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

Then,

$$ax' + by' = a\left(x_0 + \frac{b}{d}t\right) + b\left(y_0 - \frac{a}{d}t\right)$$

$$= ax_0 + \frac{ab}{d}t + by_0 - \frac{ab}{d}t$$

$$= ax_0 + by_0$$

$$= c.$$

['x_0' and 'y_0' be the particular solution of $ax + by = c$.]

Thus every other solution of $ax+by=c$ is of the form,

$$x = x_0 + \frac{b}{d}t \quad \text{and} \quad y = y_0 - \frac{a}{d}t.$$

Where 't' is arbitary integer.

Thus there are infinitely many solutions for given equation, one for each value of t.

Ex. Solve the linear Diophantine equation

$172x + 20y = 1000$

→ Here,

$\gcd(172, 20) = 4$

$4 \mid 1000$

∴ Given Diophantine eqⁿ has a solution

Consider,

$172 = (8)20 + 12$

$20 = (1)12 + 8$

$12 = (1)8 + 4$

$8 = (2)4 + 0$

Thus,

$\gcd(172, 20) = 4.$

Now,

$4 = (1)12 - (1)8$

$= (1)12 - (1)[(1)20 - (1)12]$

$= (1)12 + (1)20 + (1)12$

$= (2)12 - (1)20$

$= (2)[(1)172 - (8)20] - (1)20$

$= (2)172 - (16)20 - (1)20$

∴ $4 = (2)172 + (-17)20$

∴ $1000 = 172(500) + 20(-4250)$

∴ $(x_0, y_0) = (500, -4250)$ be the solution of $172x + 20y = 1000$

∴ General solutions of given eqⁿ are,

$x = x_0 + \frac{b}{d}t$ and $y = y_0 - \frac{a}{d}t$

i.e. $x = 500 + \frac{20}{4}t$ and $y = -4250 - \frac{172}{4}t$

i.e. $\boxed{x = 500 + 5t, \quad y = -4250 - 43t}$

for some positive integer t.

For positive solution,

$500 + 5t > 0$ and $-4250 - 43t > 0$

i.e. $5t > -500$ and $-4250 > 43t$

i.e. $t > -500$ and $-98.83 > t$

∴ $t = -99$

∴ For $t = -99$ eqⁿ ① becomes,

$x = 5, \quad y = 7$

$(x, y) = (5, 7)$ is the positive solution of given equation.

Ex. Determine all solutions in the integers of the following Diophantine equations.

a) $56x + 72y = 40$

b) $24x + 138y = 18$

c) $221x + 35y = 11$

→ a) $56x + 72y = 40$

Here $\gcd(56, 72) = 8$

∴ $8 \mid 40$

∴ Given Diophantine eqⁿ has a solution.

Consider,

$72 = (1)56 + 16$

$56 = (3)16 + 8$

$16 = (2)8 + 0$

∴ $\gcd(56, 72) = 8$

Now,

$8 = 56 - (3)16$

$= 56 - (3)[72 - (1)56]$

$= 56 - (3)72 + (3)56$

$= (4)56 + (-3)72$

$\boxed{8 = 56(4) + 72(-3)}$

$\therefore 40 = 56(20) + 72(-15)$

$\therefore \boxed{(x_0, y_0) = (20, -15)}$ be the solution of $56x + 72y = 40$.

$\therefore$ General solution of given eqⁿ are,

$x = x_0 + \frac{b}{d}t$ and $y = y_0 - \frac{a}{d}t$

i.e $x = 20 + \frac{72}{8}t$ and $y = -15 - \frac{56}{8}t$.

$\therefore \boxed{x = 20 + 9t \text{ and } y = -15 - 7t}$

for some positive integer t.

b) $24x + 138y = 18$

Here $\gcd(24, 138) = 6$

$\therefore 6 | 18$

$\therefore$ Given Diophantine eqⁿ has a solution.

consider,

$138 = (5)24 + 18$

$24 = (1)18 + 6$

$18 = (3)6 + 0$

$\therefore \gcd(24, 138) = 6$

Now,

$6 = 24 - (1)18$

$= 24 - (1)[138 - (5)24]$

$= 24 - (1)138 + (5)24$

$= (6)24 + (-1)138$

$\therefore \boxed{6 = 24(6) + 138(-1)}$

$\therefore 18 = 24(18) + 138(-3)$

$\therefore \boxed{(x_0, y_0) = (18, -3)}$ be the solution of

$24x + 138y = 18$

$\therefore$ General solution of given eqⁿ are,

$x = x_0 + \frac{b}{d}t$ and $y = y_0 - \frac{a}{d}t$

i.e $x = 18 + \frac{138}{6}t$ and $y = -3 - \frac{24}{6}t$.

$\therefore \boxed{x = 18 + 23t \text{ and } y = -3 - 4t.}$

for some positive integer t.

c) $221x + 35y = 11$

Here $\gcd(221, 35) = 1$

$\therefore 1 \mid 11$

$\therefore$ Given Diophantine eqⁿ has solution.

consider,

$221 = (6)35 + 11$

$35 = (3)11 + 2$

$11 = (5)2 + 1$

$2 = (1)2 + 0$

$\therefore \gcd(221, 35) = 1$

Now,

$1 = 11 - (5)2$

$= 11 - (5)[35 - (3)11]$

$= 11 - (5)35 + (15)11$

$= (16)11 - (5)35$

$= (16)[221 - (6)35] - (5)35$

$= (16)221 - (96)35 - (5)35$

$= (16)221 - (101)35$

$\boxed{1 = 221(16) + 35(-101)}$

$\therefore 11 = 221(176) + 35(-1111)$

$\therefore \boxed{(x_0, y_0) = (176, -1111)}$ be the solution of

$221x + 35y = 11$

∴ General solution of given eqⁿ are,

$x = x_0 + \frac{b}{d}t$ and $y = y_0 - \frac{a}{d}t$.

i.e $x = 176 + \frac{85}{1}t$ and $y = -1111 - \frac{221}{1}t$.

∴ $\boxed{x = 176 + 85t \text{ and } y = -1111 - 221t}$

for some positive integer t.

Ex. Which of the following Diophantine equation cannot be solved.

a) $8x + 51y = 22$

b) $33x + 14y = 115$

c) $14x + 35y = 93$.

→ a) $6x + 51y = 22$.

Now,

$51 = (8)6 + 3$

$6 = (2)3 + 0$

$\gcd(6, 51) = 3$

and $3 \nmid 22$.

∴ Given Diophantine eqⁿ has no solution.

b) $33x + 14y = 115$

Now,

$33 = (2)14 + 5$

$14 = (2)5 + 4$

$5 = (1)4 + 1$

$4 = (1)4 + 0$

∴ $\gcd(33, 14) = 1$.

and $1 | 115$.

∴ Given Diophantine eqⁿ has a solution.

c) $14x + 35y = 93$

Now,

$35 = (2)14 + 7$

$14 = (2)7 + 0$

$\therefore \gcd(14, 35) = 7$

and $7 \nmid 93$.

$\therefore$ Given Diophantine eqⁿ has no solution.

Tuesday
24/09/2019

Ex. If a cock is worth 5 coins, a hen 3 coins and three chicks together 1 coin. How many cocks, hens and chicks totalling 100 can be brought for 100 coins.

→ Let x be the no. of cocks, y be the no. of hens and z be the no. of chicks. then from given condition we have,

$$5x + 3y + \frac{z}{3} = 100$$

i.e. $15x + 9y + z = 300$ — ①

and $x + y + z = 100$ — ②

From ① and ② we get,

$z = 100 - x - y$. — ③

put the value of eqⁿ ③ in eqⁿ ①,

$15x + 9y + 100 - x - y = 300$

$\therefore 14x + 8y = 200$

$\therefore 7x + 4y = 100$ — ④

$\gcd(7, 4) = 1$

$\Rightarrow 1 \mid 100$

Now,

$1 = 4 - (1)3$

$= 4 - (1)[7 - (1)4]$

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

$= (2)4 - (1)7$

$\therefore$ $\boxed{1 = 7(-1) + 4(2)}$

$\Rightarrow 100 = 7(-100) + 4(200)$

$\therefore$ $\boxed{(x_0, y_0) = (-100, 200)}$ be the solution of

$7x + 4y = 100$

$\therefore$ General solution is given by,

$x = x_0 + \frac{b}{d}t$ and $y = y_0 - \frac{a}{d}t$

i.e. $\boxed{x = -100 + 4t \text{ and } y = 200 - 7t}$

for some positive integer t.

For positive solution,

$-100 + 4t > 0$ and $200 - 7t > 0$

i.e $4t > 100$ and $200 > 7t$

i.e $t \geq 25$ and $28.5 \geq t$

$\therefore$ Possible values of 't' are 26, 27, 28.

t	x	y	z
26	4	18	78
27	8	11	81
28	12	4	84

$\therefore$ 4 cocks, 18 hens and 78 chicks are brought together ~~for~~ 100 coins.

Ex. A Customer brought a dozen pieces of fruits, apples and oranges ~~for~~ 132. If an apple costs 3 Rs more than an oranges and more apples than oranges are purchased. How many pieces of each kind were brought.

→ Let 'x' be the no. of apples and 'y' be the no. of oranges.

Let 'z' be the cost of oranges then

$x + y = 12$ ——①

$\therefore (z+3)x + zy = 132$

$\therefore zx + 3x + zy = 132.$

$\therefore x(x+y) + 3x = 132$

$\therefore 12x + 3x = 132$

$\therefore 4x + x = 44$

$\therefore \gcd(1, 4) = 1$

$\Rightarrow 1 \mid 44.$

Now,

$1 = (1)4 - (3)1$

$\therefore \boxed{44 = (44)4 - (132)1}$

$\Rightarrow 44 = 1(-132) + 4(44)$

$\therefore \boxed{(x_0, y_0) = (-132, 44)}$ be the solution of $4x + x = 44$.

$\therefore$ General solution is given by,

$x = x_0 + \frac{b}{d}t$ and $y = y_0 - \frac{a}{d}t$

i.e. $\boxed{x = -132 + 4t \text{ and } y = 44 - t}$

for some positive integer t.

For positive solution,

$-132 + 4t > 0$ and $44 - t > 0$

i.e. $4t > 132$ and $44 > t$

i.e. $t > 33$ and $44 > t$

$\therefore$ Possible values of t are 34, 35, 36, 37, 38, 39, 40, 41, 42, 43.

t	x	y	z
34	4	8	10
35	8	4	9
36	12	0	8
37	16	-4	7
38	20	-8	6
39	24	-12	5
40	28	-16	4
41	32	-20	3
42	36	-24	2
43	40	-28	1

Wednesday
26/09/2019

* The Fundamental Theorem of Arithmetic -:

* Prime Numbers -:

An integer $p > 1$ is called a prime number or simply a prime, if its only positive divisors are '1' and 'p'. An integer greater than 1 that is not a prime the term as composite.

* Theorem -:

If p is prime and $p \mid ab$ then $p \mid a$ or $p \mid b$

Proof:

If $p \mid a$ then there is nothing to prove suppose that $p \nmid a$, then p being a prime its only divisors are 1 and p.

$\therefore \gcd(p, a) = 1$ or p.

If $\gcd(p, a) = p$ then $p \mid a$.

Which is contradiction.

Hence $\gcd(p, a) = 1$.

Then by Euclid's Lemma,

$p \mid ab$ and $\gcd(p, a) = 1$ we get,

$p \mid b$.

Hence the proof.

* Corollary -:

If p is prime and $p \mid a_1 a_2 a_3 \cdots a_n$ then $p \mid a_k$ for some $1 \leq k \leq n$.

Proof:

We proceed by induction on n, the no. of factors.

Case I) $n = 1$.

For $n = 1$, the stated conclusion obviously hold

case II) $n = 2$.

From above theorem result is true for $n=2$.

case III) Suppose the result hold for $n = m$.

i.e $p \mid a_1 a_2 a_3 \cdots a_m$ then $p \mid a_k$; $1 \le k \le m$

case IV) Consider,

$p \mid a_1 a_2 a_3 \cdots a_m \cdot a_{m+1}$

$\Rightarrow p \mid (a_1 a_2 a_3 \cdots a_m) \cdot a_{m+1}$

$\Rightarrow p \mid a_1 a_2 a_3 \cdots a_m$ or $p \mid a_{m+1}$

$\Rightarrow p \mid a_k$; $1 \le k \le m$ or $p \mid a_{m+1}$

(from case III)

$\Rightarrow p \mid a_k$; $1 \le k \le m$.

Hence the result hold for $n = m+1$ whenever it hold for $n = m$.

∴ By principle of mathematical induction.

i.e hold for any n.

* Theorem -:

If $p, q_1, q_2, \cdots, q_n$ are all primes and $p \mid q_1, q_2, q_3, \cdots, q_n$, then $p = q_k$ for some k, where $1 \le k \le n$.

Proof:

Let $p, q_1, q_2, q_3, \cdots, q_n$ are all primes and $p \mid q_1 q_2 q_3 \cdots q_k$. then,

$p \mid q_k$; $1 \le k \le n$.

∴ By using previous theorem,

'p' and 'q_k' both are primes.

∴ $p \mid q_k$ iff $p = q_k$.

Hence the proof.

* Theorem [Fundamental Theorem of Arithmetic]:-

* **Statement:**

Every positive integer $n>1$, can be expressed as a product of primes; this representation is unique, apart from the order in which the factors occur.

Proof:

If 'n' is prime then there is nothing to prove

Suppose 'n' is composite then there exist an integer $d>1$ such that $d|n$ with $1<d<n$. Thus there is set of divisors of n such that $1<d<n$.

$\therefore S = \{d / d|n : 1<d<n\}$

$\Rightarrow$ There is smallest integer p_1 such that $1<p_1<n$ and $p_1|n$.

Claim: p_1 is prime.

suppose on contrary that p_1 is composite integer then there is a divisor q $(1<q<p_1)$ of p_1 which ultimately a divisor of n. which contradicts minimality of p_1.

Hence p_1 is prime.

Thus we have $n = p_1 \cdot n_1$, where p_1 is prime.

If 'n_1' is prime then we are done, otherwise there is prime p_2 dividing n_1.

Let $n_1 = p_2 n_2$; $n > n_1 > n_2$.

If 'n_2' is prime then we stop here, otherwise there is prime p_3 and

$n_2 = p_3 \cdot n_3$; $n > n_1 > n_2 > n_3$.

Since 'n' is finite, the above process can not be continued, there is postive integer 'k' such that,

$n_{i-1} = p_i \cdot q_i$ where q_i and p_i are primes.

Thus,

$n = p_1 p_2 p_3 \cdots p_r q_r$ is the prime factorisation of $n > 1$.

Uniqueness :

Let $q_1 q_2 q_3 \cdots q_s$ be primes such that

$n = p_1 p_2 p_3 \cdots p_r = q_1 q_2 q_3 \cdots q_s$ —— ⊛

where $p_1 p_2 p_3 \cdots p_r$ and $q_1 q_2 q_3 \cdots q_s$ are primes written in ascending order $p_1 \leq p_2 \leq \cdots \leq p_r$ and $q_1 \leq q_2 \leq q_3 \leq \cdots \leq q_s$.

Now,

$p_1 \mid p_1 p_2 p_3 \cdots p_r$

$\therefore$ from ⊛ we have,

$p_1 \mid q_1 q_2 q_3 \cdots q_s$

$\Rightarrow p_1 \mid q_k$ for some k ; $1 \leq k \leq s$

$\Rightarrow p_1 = q_k \geq q_1$

$\Rightarrow p_1 \geq q_1$

Now starting with q_1 instead of p_1 we get,

$q_1 \leq p_1$

$\therefore$ We have $p_1 = q_1$

$\therefore$ Eqⁿ ⊛ becomes,

$p_2 p_3 \cdots p_r = q_2 q_3 \cdots q_s$

Repeating the above process we get,

$1 = q_{r+1} q_{r+2} \cdots q_s$

This is possible only when $r = s$.

Hence the uniqueness.

* **Corollary :-**

Any positive integer $n > 1$ can be written uniquely in the canonical form $n = p_1^{k_1} \cdot p_2^{k_2} \cdots p_r^{k_r}$ where each k_i is positive; $i = 1, 2, 3, \cdots, r$ and each p_i is prime with $p_1 < p_2 < p_3 < \cdots < p_n$.

Friday
27/09/2019

Ex: Find prime factorisation of i) 4725
ii) 17460.

→ i) $4725 = 5 \times 945$
$= 5 \times 5 \times 189$
$= 5 \times 5 \times 3 \times 63$
$= 5 \times 5 \times 3 \times 3 \times 21$
$= 5 \times 5 \times 3 \times 3 \times 3 \times 7.$
$\therefore 4275 = 5^2 \times 3^3 \times 7.$

ii) $17460 = 2 \times 8730$
$= 2 \times 2 \times 4365$
$= 2 \times 2 \times 3 \times 1455$
$= 2 \times 2 \times 3 \times 3 \times 485$
$= 2 \times 2 \times 3 \times 3 \times 5 \times 97$
$\therefore 17460 = 2^2 \cdot 3^2 \cdot 5 \cdot 97$

* Theorem [Pythagoras] -:
* Statement:
The number $\sqrt{2}$ is irrational.

Proof.
We have to prove that $\sqrt{2}$ is irrational number.
On contrary suppose that $\sqrt{2}$ is rational number.
$\therefore$ It can be written in the form of $\frac{p}{q}$

$\therefore \sqrt{2} = \frac{a}{b}$; a, b are integers, $\gcd(a, b) = 1$ and $b \neq 0$.
squaring on both sides,
$2 = \frac{a^2}{b^2}$
$\therefore 2b^2 = a^2 \Rightarrow a^2 = b(2b)$
$\Rightarrow b \mid a^2$.

∴ By fundamental theorem of arithmetic
∃ a prime 'p' such that, $p|b$

But $b|a^2 \Rightarrow p|a^2$

$\Rightarrow p|a \cdot a$

$\Rightarrow p|a$

$\Rightarrow p|\gcd(a,b)$

$\Rightarrow p|1$

But 'p' is prime.

∴ This is contradiction.

∴ Our assumption is wrong.

Hence $\sqrt{2}$ is irrational.

Hence the proof.

* Euclid's Theorem-:

* Statement:

There are an infinite number of primes.

Proof:

Let $P_1=2$, $P_2=3$, $P_3=5$, $P_4=7$, --- be primes in natural order. If possible there be last prime P_n.

i.e. $P_1 P_2 P_3 \cdots P_n$ are the only primes.

Consider,

$$P = (P_1 P_2 P_3 \cdots P_n) + 1 \quad \text{---} (*)$$

Clearly $P > 1$.

∴ By fundamental theorem of arithmetic, 'P' has a prime factorisation.

Let 'p' be the prime factor of 'P' then this 'p' must be one $(P_1 P_2 P_3 \cdots P_n)$

∴ We have,

$$p | P_1 P_2 P_3 \cdots P_n$$

Further $p|P$.

$\therefore p | P - P_1 P_2 P_3 \cdots P_n$.

∴ From eqⁿ (*) we have,

$p \mid 1$.

Which is contradiction.

Hence our assumption is wrong

∴ There are infinitely many primes.

Hence the proof.

* Goldbach Conjecture -:

Every even integer greater than 4 can be written as sum of two odd primes. It has been verified by computations for all even integers less than $4 \cdot 10^{11}$

G.H. Hardy in his address to the mathematical society of openhagen in 1921 stated that the goldbach conjecture appeared "probably as difficult as any of the unsolved problems in mathematics it is currently known that every even integer is the sum of 6 or fewer primes."

* Lemma -:

The product of two or more integers is of the form $4n+1$ is of the same form.

Proof:

Let $4m+1$ and $4n+1$ be two integers then,

$$(4m+1)(4n+1) = 16mn + 4(m+n) + 1$$
$$= 4(4mn + m + n) + 1$$
$$= 4t + 1 \quad ; t = 4mn + m + n$$

Which is required form.

Hence the proof.

* Theorem -:

There is an infinite number of primes of the form $4n+3$.

Proof:

Suppose that there are only finite number of primes of the form $4n+3$ namely $p_1, p_2, p_3, \ldots, p_r$.

consider,

$$N = 4p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_r - 1$$
$$= 4(p_1 \cdot p_2 \cdot p_3 \ldots p_r - 1) + 3$$

clearly, $N > 1$ and is of the form $4n+3$.

since $N > 1$, it has prime factorisation

$$N = q_1 q_2 q_3 \ldots q_s.$$

Further N being odd number $q_k \neq 2$ $(1 \leq k \leq s)$

If some q_k divides $p_1 \cdot p_2 \cdot p_3 \ldots p_r$ then as

$q_k \mid N$, $q_k \mid 4 \cdot p_1 \cdot p_2 \cdot p_3 \ldots p_r - N = 1$

$\Rightarrow q_k \mid 1$

$\Rightarrow q_k = 1$

which is absurd.

Further, each q_k $(1 \leq k \leq s)$ being odd it is of the form $4n+3$, all q_k's can not be of the form $4n+1$ because product of finite number of integers of the form $4n+1$ is of the same form. Therefore there is atleast one 'q_k' of the form $4n+3$. Thus 'q_k' is a prime of the form $4n+3$ other than $p_1, p_2, p_3, \ldots, p_r$.

Thus, we arrive at contradiction.

Therefore, there are infinitely many primes of the form $4n+3$.

Hence the proof.

* Theorem [Dirichlet's Theorem] -:

* Statement:

If 'a' and 'b' are relatively prime positive integers, then the arithmetic progression a, a+b, a+2b, --- contains infinitely many primes.

* Theorem -:

If all $n > 2$ terms of the arithmetic progression $P, P+d, P+2d, \cdots, P+(n-1)d$ are prime numbers then the common difference d is divisible by every prime $q < n$.

Proof:

Let q be a prime less than n and if possible $q \nmid d$.

Claim: The first 'q' terms of the progression namely $P, P+d, \cdots, P+(q-1)d$ will leave different remainders upon division by 'q'

On contrary that $P+rd$ and $P+sd$ $(0 \le r < s < q)$ leave the same remainders, upon division by 'q'.

Then $P+rd = q_1 \cdot q + r$ and $P+sd = q_2 \cdot q + r$.

Where 'q_1' and 'q_2' are quotients.

Thus, $q \mid (s-r)d$

since 'q' is prime and $q \nmid d$, $\gcd(q, d) = 1$

Hence by Euclid's lemma,

$$q \mid (r-s)$$

which is absurd as $0 \le r < s < q$.

Hence the claim.

since the 'q' is integer.

$P, P+d, P+2d, \cdots, P+(q-1)d$ leave different

remainders upon division by q, there is atleast one integer amongst $P, P+d, \cdots, P+(q-1)d$ that leaves remainder zero.

Note that the 'q' remainders division upon by 'q' are $0, 1, 2, \cdots, q-1$.

Let $0 \leq t < q$ be such that $q \mid P+rd$.

Note that if $P<n$, then one of the members of the progression $P, P+d, \cdots, P+(n-1)d$ is of the form $P+Pd = P(1+d)$.

Contradicting the fact that all members of the progression are primes.

$\therefore$ We have $q < n \leq P \leq P+td$.

Thus we arrive at the contradiction that $P+td$ is prime.

Which is absurd.

$\therefore$ $q \mid d$.

Hence the proof.