2. Divisibility theory in integers,

Well ordering principle.

Every non-empty set S of non-negative integers contain atleast one element i.e. their is some integer $a \in S$ such that $a \leq b \ \forall \ b \in S$

1^{st} principle of induction :-

For each $n \in N$, a statement $P(n)$ is given if a) $P(1)$ is true
b) For $k \geq 1$, $P(k)$ is true then implies $P(k+1)$ is also true.

Then $P(n)$ is a true for each positive integer n.

Q1) For any natural number n, show that $1+2+3+\ldots+n = \frac{n(n+1)}{2}$

→ For $n \in \mathbb{N}$

$P(n) = 1+2+3+\ldots+n = \frac{n(n+1)}{2}$

We have to show that for each $n \in \mathbb{N}$, $P(n)$ is true.

i) For $n=1$

~~$P(1) = 1+2+3$~~ ....

$P(1) = 1 = \frac{1(1+1)}{2} = \frac{1(2)}{2} = \frac{2}{2} = 1$

$\therefore P(1)$ is true,

ii) For $k \geq 1$, assume that $P(k)$ is true then we have to prove that $P(k+1)$ is true.

i.e $n = k$

$$P(k) = 1 + 2 + 3 + \dots k = \frac{k(k+1)}{2}$$

Now

$$P(k+1) = 1 + 2 + 3 + \dots k + (k+1) =$$

$$P(k+1) = \frac{k(k+1)}{2} + (k+1)$$

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

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

Thus $P(k+1)$ is true.

Thus $P(k)$ is true $\Rightarrow P(k+1)$ is also true.

$\therefore$ 1st principle of induction $P(n)$ is true, $\forall n \in N$.

Q.2. For any natural number n show that

$$1^2 + 2^2 + 3^2 \dots + n^2 = \frac{n(n+1)(2n+1)}{6}.$$

$\longrightarrow$ For $n \in \mathbb{N}$

$$P(n) = 1^2 + 2^2 + 3^2 + \dots + n^2 = \frac{n(n+1)(2n+1)}{6}$$

We have to show that for each $n \in \mathbb{N}$ $P(n)$ is true.

i) for $n = 1$

$$P(1) = 1^2 = 1 = \frac{1(n+1)(2n+1)}{6} = \frac{1(1+1)(2\times1+1)}{6}$$

$$= \frac{2\times3}{6} = \frac{6}{6} = 1$$

$\therefore P(1)$ is true.

DATE / /

ii) for $k \geq 1$ assume $P(k)$ is true.

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

Now

$$P(k+1) = 1^2 + 2^2 + 3^2 + \dots k^2 + (k+1)^2 = \cancel{(k+1)(k+1}$$

$$p(k+1) = \frac{k(k+1)(2k+1)}{6} + (k+1)^2$$

$$= \frac{k(k+1)(2k+1) + \cancel{(6k+6)}}{6} + \cancel{k^2 + 2k + 1)}$$

$$= (k^2+1)(2k+1) + 6k^2 + 12k + 6$$

Now,

$$P(k+1) = 1^2 + 2^2 + 3^2 + \dots + k^2 + (k+1)^2 = \frac{(k+1)(k+1+1)(2(k+1)+1)}{6}$$

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

$$L.H.S = 1^2 + 2^2 + 3^2 + \dots k^2 + (k+1)^2$$

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

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

$$= \frac{k(k+1)(2k+1) + 6[(k+1)(k+1)]}{6}$$

$$= \cancel{k(k+1)(2k+1) +}$$

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

$$= \frac{(k+1)[2k^2 + k + 6k + 6]}{6}$$

$$= (k+1)(2k^2 + 7k + 6]/6$$

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

L.H.S = R.H.S $\therefore$ Pk is true.

$\therefore$ 1st principle of induction

Teacher's Signature.........................

PAGE No.
DATE / /

Q. For $n \geq 1$

$P(n) = 1 + 2^1 + 2^2 + 3^3 \cdots 2n^{-1} = 2^n - 1$

i) $P(1) = 2^{1-1} = 2^0 = 1 \quad = 2^1 - 1 = 2 - 1 = 1$

ii) $P(k) = 1 + 2^1 + 2^2 + \cdots + 2k^{-1} = \cancel{2k^{-1}}\ 2^{k} - 1$

iii) $P(k+1) = 1 + 2^1 + 2^2 + 2^3 + \cdots + 2^k = \cancel{2k}\ 2^{k+1} - 1$

Let L.H.S $= P(k+1)$

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

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

$= 2^k + 2^k - 1$

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

$= 2^k(2) - 1$

$= 2 \cdot 2^k - 1$

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

$= R.H.S$

$P(k+1)$ is true.

Divisibility

An integer b is said to be divisible by an integer $a \neq 0$, if their exist same integer c such that $b = ac$

Notation $= a|b$

e.g.

$3|12 \Rightarrow 12 = 3 \cdot 4$

IMP.

Properties of divisibility

1) Let ~~A, B, C, D~~, a, b, c, d, m, x, y be an integer.

i) If $A|B$ then $a|bc$, for any integer c.

Teacher's Signature: ....

Let, $a|b$

$b = aq \quad , q \in \mathbb{Z}$

multiply both side by c,

$bc = aqc \quad , c \in \mathbb{Z}$

$a | bc$

ii) If $a|b$ & $b|c$ then $a|c$

Let

$a|b$

$\Rightarrow b = am \quad , \text{—} ① \quad m \in \mathbb{Z}$

& $b|c$

$\Rightarrow c = bn \quad , n \in \mathbb{Z} \text{ —} ②$

put eqⁿ 1 in 2,

we get

$c = (am)n$

i.e. $c = amn$

as $m \in \mathbb{Z}, n \in \mathbb{Z} \Longrightarrow mn \in \mathbb{Z}$

$a|c \quad , mn \in \mathbb{Z}$

iii) If $a|b$ & $a|c$ then $a | bx+cy$, for x, y be an integers.

→ Let,

$a|b$

$\Longrightarrow b = a\cancel{x}q_1 , q_1 \in \mathbb{Z} \text{ —} ①$

& $a | c$

$c = aq_2 \quad , q_2 \in \mathbb{Z} \text{ —} ②$

multiply eqⁿ ① by x & ② by y

$bx = aq_1x \text{ —} ③$

$cy = aq_2y \text{ —} ④$

Teacher's Signature:..........

add eq^n 3 & 4

$bx + cy = aq_1x + aq_2y$

$bx + cy = a(q_1x + q_2y)$

$\Rightarrow a \mid bx + cy \quad \cdots \quad q_1x + q_2y \in \mathbb{Z}$

iv) If $a \mid b$ & $b \neq 0$ then $|a| \leq |b|$.

Let

$a \mid b$

$b = aq, \quad q \in \mathbb{Z}$ — ①

here $q \neq 0 \because b \neq 0$

$\therefore$ we have $|q| \geq 1$

Hence Taking mod on both side

$|b| = |aq|$

$|b| = |a| \cdot |q|$

$|a| \leq |b|$

v) If $a \mid b$ & $b \mid a$ then $a = \pm b$

let

$a \mid b$

$\Rightarrow |a| \leq |b|$ — ① From If $a \mid b$, $b \neq 0$. then $|a| \leq |b|$

also,

$b \mid a$

$\Rightarrow |b| \leq |a|$ — ② — " —

$\Rightarrow |a| = |b|$ — From 1 & 2

$\Rightarrow a = \pm b$

DATE / /

e.g. $n(n+1)$ is divisible by 2, for any integer n

→ By division al

we have any integer n is of the formed $2k$ or $2k+1$

case i)

If n is even

$\therefore n = 2k,\ k \in \mathbb{Z}$

$n(n+1) = 2k(2k+1) = 2[k(2k+1)]$

$\therefore 2 / n(n+1) \qquad k(2k+1) \in \mathbb{Z}$

case 2

If n is odd

$n = 2k+1$

$\therefore n(n+1) = (2k+1)(2k+1+1)$

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

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

$2 / n(n+1) \qquad (2k+1)(k+1) \in \mathbb{Z}$

In both cases $2 / n(n+1)$

$\therefore n(n+1)$ is divisible by 2.

IMP 2022

e.g. If n is odd integer, then n^2-1 is divisible by 8.

→ By division algorithm

if n is an odd interger $\quad n = 2k+1$

$n = 2k+1$

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

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

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

$= 4k^2 + 4k$

$= \cancel{4(k^2+k)}\ 4k(k+1) \quad \because k(k+1)$ is divisible by 2

$= 4(2m) \qquad m \in \mathbb{Z}$

$= 8m \qquad m \in \mathbb{Z}$

$\therefore 8 / n^2-1$

Teacher's Signature:..........................

PAGE No.
DATE / /

e.g. If $m \neq 0$ then show that a/b iff ma/mb.

→ If a/b then w.h.t.s.t ma/mb

Let

a/b

$\Rightarrow b = ac \qquad c \in \mathbb{Z}$

multiply m on both side.

$mb = mac \quad , \quad m \in \mathbb{Z}$

$\Rightarrow ma/mb$.

If ma/mb then we have to show that a/b

Let

ma/mb

$\Rightarrow mb = mad \; , \; d \in \mathbb{Z}$

divide m on both side

$$\frac{mb}{m} = \frac{mad}{m} \quad , m \in \mathbb{Z}$$

$b = ad$

$\therefore a/b$.

~~Even~~ Given integer a and b, $a>0$ we make a repeated application of division algorithm to obtain a series of equation.

$$b = aq + r_1 \qquad 0 < r_1 < a$$
$$a = r_1 q_1 + r_2 \qquad 0 < r_2 < r_1$$
$$r_1 = r_2 q_2 + r_3 \qquad 0 < r_3 < r_2$$
$$\vdots$$
$$r_{j-3} = r_{j-2} q_{j-2} + r_{j-1} \qquad 0 < r_j < r_{j-1}$$
$$r_{j-2} = r_{j-1} q_{j-1} + r_j \qquad 0 < r_j < r_j'$$
$$r_{j-1} = r_j q_j$$

ex. Find $(12378, 3054)$ and express in the form of $12378x + 3054y$ for same integer x & y.

By euclidean algorithm we have

$$12378 = 3054(4) + 162$$
$$3054 = 162(18) + 138$$
$$162 = 138(1) + 24$$
$$138 = 24(5) + 18$$
$$24 = 18(1) + \boxed{6} \leftarrow \text{gcd}$$
$$18 = 6(3) + 0$$

Now

$$6 = 24 - 18(1)$$
$$= 24 - [138 - 24(5)](1)$$
$$= (1)24 - 138(1) + 24(5)$$
$$= (6)24 - 138(1)$$
$$= (6)[162 - 138(1)] - 138(1)$$
$$= (6)162 - (6)138 - 138(1)$$
$$= (6)162 - (7)(138)$$
$$= (6)162 - (7)[3054 - 162(18)]$$

Teacher's Signature: ....

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

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

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

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

$= (132)(12378) - \cancel{528}\ 535(3054$

Thus

$x = 132 \quad y = -535$

ii) (119, 272) also find x & y such that $272x + 119y$.

$272 = 119(2) \cancel{23} + 34$

$119 = 34(3) + \boxed{17}$ gcd

$34 = 17(2) + 0$

Now

$17 = 119 - 34(3)$

$= 119 - [272 - 119(2)](3)$

$= 119 - (3)272 + (6)119$

$= 7(119) - (3)272$

Thus $= -272x + 119y$

$x = -3 \quad y = 7$

iii) (1819, 3587) also find x & y such that $1819x + 3587y$.

$3587 = 1819(1) + 1768$

$1819 = 1768(1) + 51$

$1768 = 51(34) + 34$

$51 = 34(1) + \boxed{17} \longrightarrow$ gcd

$34 = 17(2) + 0$

Now.

$17 = 51 - 34(1)$

$17 = 51 - [1768 - 51(34)](1)$

$= 51 - 1768 + 51(34)$

Teacher's Signature:..............................

$$17 = 35(51) - (1)1768$$

$$17 = 35\,[1819 - (1)1768] - (1)\,1768$$

$$= 35\,(1819) - 35\,(1768) - (1)\,1768$$

$$= 35\,(1819 - 36\,(1768)$$

$$= 35\,(1819) - 36\,[3587 - (1)\,1819]$$

$$= 35\,(1819) - 36\,(3587) + 36\,(1819)$$

$$= 71\,(1819) - 36\,(3587)$$

$$= y\,(1819) - x\,(3587)$$

$$= -\cancel{x}\,3587x + 1819\,(y)$$

$\boxed{x = -36}$ $\boxed{y = 71}$

* ## GCD Theorem :-

If a, b are integers not both zero, then their exist a unique positive integer (a, b) which can be expressed in the form of

$$\gcd(a.b) = ax_0 + by_0$$

Proof :-

Consider the set

$$S = \{ax + by,\ x, y \in \mathbb{Z},\ ax + by > 0\}$$

$\because$ a and b not both zero, we have

$$a^2 + b^2 > 0$$

$\therefore$ $a.a + b.b > 0$

Here

$x = a$ & $y = b$

$\therefore$ $a^2 + b^2$ is of the form $ax + by$

Hence $a^2 + b^2 \in S$

$\therefore$ S is non empty

$\therefore$ By well-ordering principle

S has smallest element say d

$d \in S$

$d = ax_0 + by_0$ —— ①

Claim 1] d is gcd of a & b.

i) we 1st ly show that, d/a & d/b.

suppose $d \nmid a$ (d does not divide) a

$\Rightarrow a = dq + r, \quad 0 < r < d$

$a - dq = r$

$a - (ax_0 + by_0)q = r$ —— From eqn 1.

$a - ax_0q + by_0q = r$

$a(1 - x_0q) - b(y_0q) = r$

If we take $x = 1 - x_0q$

$y = y_0q$

then ~~a~~ r is the form of $ax + by$

also

$r > 0$

$\therefore r \in S$ & $r < d$

but that is the contradiction

$\because$ d is smallest element of S.

$\therefore d/a$.

lly we prove d/b.

2] Now, suppose c/a & c/b

$\Rightarrow c/ax_0 + by_0$

$\Rightarrow c/d$

$\therefore$ By definition of g.c.d

d is gcd of a & b.

claim 2) d is unique

suppose d_1 is another gcd of a, b i.e. d_1 is common divisor of a, b and d is gcd of $a \& b$.

$\therefore \ d_1 / d$

again,

d is common divisor of a, b and d_1 is gcd of a, b

$\therefore \ d / d$

As

d / d_1 & d_1 / d

$\Longrightarrow d = d_1$

very Imp for 5 marks

Division algorithm.

Given integer a and b with $b \neq 0$ exist unique integers q and r satisfying

$a = qb + r$ where $0 \leq r \leq |b|$

The integers q & r are called respectively the quotient and reminder in the division of $a \& b$.

consider,

$a = bq + r$ ——— ①.

consider set of multiple of b are

$0, \pm b, \pm 2b, \pm 3b, \ldots\ldots$

case (i)

a i multiple of b

$\therefore \ a = bq \quad , q \in \mathbb{Z}$

campare with eqn 1.

$\Longrightarrow \boxed{r = 0}$

case ii) a is not multiple of b.

Let a is lies between two consecutive multiple of b

$\therefore bq < a < b(q+1)$

$\therefore bq < a < bq + b$

substract bq on both side.

$bq - bq < a - bq < bq + b - bq$

$0 < a - bq < b$

If eq^n 1

$a = bq + r$

$\Rightarrow r = a - bq$

$\therefore 0 < r < b$

$\therefore a = bq + r, \quad 0 < r < b$

Uniqueness

suppose their exist another two integer q_1 and r_1 such that

$a = bq_1 + r_1, \ 0 \le r < b.$ — ②.

From eq^n 1 & 2

$\Rightarrow bq + r = bq_1 + r_1$

$\Rightarrow bq - bq_1 = r_1 - r$

$\Rightarrow b(q - q_1) = r_1 - r$ — by def^n of divisibility)

$\Rightarrow b / r_1 - r$ — ③

but

$r < b$ & $r_1 < b$

$\Rightarrow r_1 - r < b$

so, eq^n 3 is possible iff $r_1 - r = 0$

$\therefore r_1 = r$

||ly we prove that

$q = q_1$

Hence proved.

Teacher's Signature:..................

Find G.C.D of (2210, 357)

$2210 = 357(6) + 68$
$357 = 68(5) + \boxed{17} \leftarrow$ g.c.d.
$68 = 17(4) + 0$

$17 = 357 - 68(5)$
$17 = 357 - [2210 - 357(6)]5$
$17 = 357 - (5)2210 + (30)357$
$17 = (31)357 - (5)2210$.

compare with with

$d = 2210x + 357y$

we get

$d = 17,\ x = -5,\ y = 31$