NCER

Unit I (BTCO302) D.M.

1) Fundamental Structures & Basic Logic
Sets, Venn diagram, Cartesian product, Power sets, Cardinality & Countability, Propositional logic, Logical Connectives, Truth Tables, Normal forms, validity, Predicate logic, Limitation of Predicate logic, Universal & existential quantification First Order Logic.

2) Principles of Mathematical Induction
The well ordering principle, Recursive def^n, the division Algorithm, Prime no.s the greatest common divisor, Euclidean algorithm, the fundamental thm. of Arithmetic.

Unit I.

Chapter 2 Principles of Mathematical Induction

Basic properties of Integers.

We denote the set of natural nos (called as positive integers) by N.

$\therefore N = \{1, 2, 3, \cdots\}$

and the set of integers as I,

$I = \{\cdots -3, -2, -1, 0, 1, 2, 3, \cdots\}$

* The following are simple rules concerning the addition & Multiplication of integers.

a) Associative law for Multiplication & Addition

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

$\forall\ a, b, c \in I$.

b) Commutative law for Multiplication & Addition

$a+b = b+a$ & $ab = ba$, $\forall\ a, b \in I$.

c) Distributive Law

$a(b+c) = ab + ac$, $\forall\ a, b, c \in I$

d) Additive Identity 0 & Multiplicative identity 1

$a+0 = 0+a = a$, $a \cdot 1 = 1 \cdot a = a$.

e) Additive Inverse $-a$ for any integer a

$a + (-a) = (-a) + a = 0$

The well ordering Principle :-

A least element exist in any non empty set of positive integers.

OR

Let S be a non empty set of positive integers. Then S contains a least element that is S contains an element a such that $a \leq s$ for every element s in S

Divisibility And The Division Algorithm.

Divisibility

Def^n An integer b is divisible by an integer a, not zero if there is an integer x such that $b = ax$ & we write $a|b$.

In case b is not divisible by a, we write $a \nmid b$.

OR A non zero integer a is said to be divisor or factor of an integer b if there exist an integer q such that $b = aq$.

If a is divisor of b then we write $a|b$ (read as a divides b or a is a divisor of b)

If a is a divisor of b then we can also say that b is divisible by a or a is factor b or b is multiple of a.

For Ex.

1) $6 \mid 12$ but $6 \nmid 15$

since $12 = 6 \times 2$.

2) $-4 \mid 16$ as $16 = -4 \times -4$.

3) $a \mid 0 \quad \forall\ a \in I$ & $a \neq 0$ because $0 = a \times 0$.

Jump

Note 1) In the notation $b \mid a$, b is always assumed to be non zero.

2) If a divides b then $-a$ also divides b.

because $b = aq$ then this implies $b = (-a)(-q)$

Hence it is enough to consider only positive divisors of an integers.

Proper & Improper Divisors.

For every integer a, ± 1 & $\pm a$ are divisors of a since $a \times 1 = (-a) \times (-1) = a$ $\forall\ a \in I$. These are called 'Improper divisors of a'.

If a has any divisor other than these then these are called 'proper divisors of a'

eg proper divisors of 12 are $\pm 2, \pm 3, \pm 4, \pm 6$.

Prime Number

A non zero integer p is called prime provided it is neither 1 nor -1 & its only divisors are ± 1 & $\pm p$.

OR

An integer $p > 1$ is called a prime number (or just a prime) if it has no positive proper divisor ie if p has no divisor d such that $1 < d < p$.

For ex. First few primes are 2, 3, 5, 7, 11, 13, ...

Composite Integer.

An integer $a > 1$ is called composite (number) integer if a is not prime.

OR

If an integer a can be written as $a = bq$ where b & q are integers such that $|b| > 1$ & $|q| > 1$ then a is called composite integers.

For ex.

$6 = 2 \cdot 3$ & $15 = 3 \cdot 5$ are composite.

Note ① For every integer $a \neq 0, \pm 1$ is either prime or composite.

② If a is positive integer, & a is not prime then a is composite integer iff there exist positive integers a_1 & a_2 such that $a = a_1 \cdot a_2$ where $1 < a_1 < a$ & $1 < a_2 < a$.

Properties of Divisibility

Thm Let a, b, c be any integers.

a) $a|b \Rightarrow a|bc$ for any integer c.

b) $a|b$ & $b|c \Rightarrow a|c$

c) $a|b$ & $a|c \Rightarrow a|bx+cy$ for any integer x & y

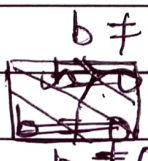
d) If $a|b$ & $b|a \Rightarrow a = \pm b$

e) $a|b$, $a>0$, $b>0 \Rightarrow a \leq b$

f) if $m \neq 0$, $a|b$ implies & implied by $ma|mb$

Division Algorithm

Thm:- Given integers a, b where $b \neq 0$, there exist unique integers q and r such that $a = bq + r$ where $0 \leq r < |b|$.



Proof:- Case (1) Let $b > 0$

Consider the set,

$S = \{a - bx \mid x \in I \text{ & } a - bx \geq 0\}$

To show that S is non empty

Note that $b \geq 1$

So that $|a|\, b \geq |a|$

By taking $x = -|a|$.

Hence $a - bx = a - b(-|a|)$

$= a + |a|\, b \geq a + |a| \geq 0$

Hence $a + |a|\, b \in S$

$\Rightarrow S$ is non empty.

$\therefore$ S is a non empty set of non negative integers and so by the well ordering principle S has least element say r.

Then $r \geq 0$ & $r = a - bq$ for some $q \in I$ since $r \in S$.

Now to prove $r < b$.

if $r \geq b$ (assume)

then $r - b \geq 0$

$\Rightarrow$ { $a - bq - b \geq 0$

~~$a - b(q+1) \geq 0$~~

$\Rightarrow r - b \geq 0$ }.

$\Rightarrow r - b \in S$ But $r - b < r$ since $b > 0$

This contradicts to the fact that r is the least element of S

Hence $r < b$.

Thus there exist $q, r \in I$ s.t.

$$a = bq + r \quad \text{---(1)}$$

& $0 \leq r < b$ ---(2)

To prove uniqueness.

Suppose we also have,

$a = bq_1 + r_1$ & $0 \leq r_1 < b$

---(3) ---(4)

For some $q_1, r_1 \in Z$ then from (2) & (4)

$$0 \leq |r - r_1| < b \quad -(5)$$

Also by (1) & (3)

$$bq + r = bq_1 + r_1 \text{ & so,}$$

$$b|q - q_1| = |r - r_1| \quad -(6)$$

Let if possible $q \neq q_1$

then,

$$|q - q_1| \geq 1 \quad \text{& so } b > 0$$

$$|r - r_1| = b|q - q_1| \geq b$$

But this contradicts (5)

Hence $q = q_1$ then $r = r_1$ by (6)

Hence the integers q & r satisfying (1) & (2) are unique.

Case (2) Let $b < 0$ then $|b| = -b > 0$

and so by case (1)

$$a = |b|q' + r, \quad 0 \leq r < |b|.$$

For unique integers q' & r.

Hence taking $q = -q'$ we get

$$a = -bq' + r = bq + r \text{ & } 0 \leq r < |b|$$

(Hence proved)

Remark

The nos q & r in the division thm. are called quotient & remainder resp.

corollary of Division Algorithm Thm.

If $a, b \in I$ & $b \neq 0$ then $b|a$ iff remainder on dividing a by b is zero.

Examples $a = bq + r$

1) If $a = 16$, $b = 5$ $0 \leq r < |b|$

then

$16 = 3 \times 5 + 1$, $0 \leq 1 < |5|$.

$a = q \times b + r$

$r = 1$, $q = 3$

2) If $a = 17$, $b = -3$

then

$17 = -3 \times -5 + 2$, $0 \leq 2 < |-3|$.

$a = b \times q + r$

$q = -5$, $r = 2$

3) If $a = -24$, $b = 7$

then

$-24 = 7 \times -4 + 4$, $0 \leq 4 < |7|$.

$a = b \times q + r$

$b = 7$, $q = -4$, $r = 4$

4) Let $a, b \in I$

i) If $a = bq$ for $q \in I$,

then $-a = (-q)b$.

Thus when $-a\ (< 0)$ is divided by $b\ (> 0)$, the quotient is $-q < 0$ & remainder is 0.

ii) If $a = bq + r$, for $q \in I$ & $0 < r < b$

then,

$$\begin{aligned} -a &= (-q)b - r \\ &= (-q)b - b + b - r \\ &= (-q-1)b + (b-r) \end{aligned}$$

Thus when $-a\ (<0)$ is divided by $b\ (>0)$ the quotient is $-q-1 < 0$ & remainder is $b-r$ where $0 < b-r < b$.

Exs based on division Algorithm.

For each pair of integers a & b find integers q & r such that $a = bq + r$ & $0 \leq r < |b|$.

1) $a = 258$, $b = 12$

2) $a = 573$, $b = -16$

3) $a = -381$, $b = 14$

4) $a = -433$, $b = -17$

5) $a = 4461$, $b = 16$.

6) $a = -262$, $b = 3$.