Bharathidasan University
Tiruchirappalli - 620 024
Tamil Nadu, India

Programme: M.Sc., Mathematics

Course Title :Theory of Numbers
COurse Code : 21M04CC

Preliminaries

Dr. V. Piramanantham
Professor
Department of Mathematics

Divisibility: Let a, b be integers with $a \neq 0$. Then if there exists $m \in \mathbb{Z}$ such that $b = ma$, then we say that b is divisible by a.

Does the equation $ax = b$, $a \neq 0$, $a, b \in \mathbb{Z}$. have solution (in integers)

If yes, a divides b,

Comparison: $a - b \in \mathbb{Z} \Rightarrow c = a - b$

$a, b \in \mathbb{Z}$

$$\Rightarrow c + b = (a - b) + b = a + (-b + b) = a + 0 = a$$

Principles :

① The well-ordering principle :

Every nonempty subset of the set of all positive integers has a smallest element.

(or)

A least element exists in any non-empty set of +ve integers.

The Pigeonhole Principle:

If s objects are placed in k boxes for $s > k$, then atleast one box contains more than one object.

(or)

If n elements are contained in m sets where $n > m$, then atleast one set contains more than one element.

③ The Principle of Mathematical induction:

first

If $S \subseteq \mathbb{N}$ with property that

S is set of +ve integers

Math

(i) $1 \in S$

(ii) If $k \in S$, $k+1 \in S$

then $S = \mathbb{N}$ //

The first principle of mathematical induction:

If a property concerning the +ve integers is true for $n=1$ and is true for the integer $n+1$ whenever it is true for the integer n, then the property must be true for all +ve integers.

... ple of induction

for all +ve integers.

Remark : weak form of principle of induction.

Remark

$P(n)$ is a property on n.

Ex: The sum of the first n +ve integers is equal to $\frac{n(n+1)}{2}$

$$S = \{ n \in \mathbb{N} / P \text{ is true for } n \}$$

$S \subseteq \mathbb{N}$.

(i) $1 \in S$

(ii) $n+1 \in S$ whenever $n \in S$

Then $S = \mathbb{N}$

Prove that the sum of first n +ve integers is equal to $\dfrac{n(n+1)}{2}$

(or)

prove that $\displaystyle\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$

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

P : The sum of first n integers is equal to $\dfrac{n(n+1)}{2}$

$n=1$, $\displaystyle\sum_{i=1}^{1} i = 1$

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

$\displaystyle\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$ is true for $n=1$

(1) The property is true for $n=1$.

Assume that the property is true for n

(ie)
$$\sum_{j=1}^{n} j = \frac{n(n+1)}{2}$$

we prove that
$$\sum_{j=1}^{n+1} j = \frac{(n+1)((n+1)+1)}{2}$$

$$\sum_{j=1}^{n+1} j = \sum_{j=1}^{n} j + n+1$$

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

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

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

The property is true for $n+1$

By the first principle of math. induction
The property P is true for all +ve int. n

$$\boxed{\therefore \quad \sum_{i=1}^{n} i = \frac{n(n+1)}{2} \quad \forall\, n}$$

Ex Prove that $n! \leq n^n$ for any +ve int.

induction on n :

$n! = n(n-1)(n-2) \cdots 2 \cdot 1$

$n^n = n \cdot n \cdot n \cdots$ (n factors)

$P: \; n! \leq n^n$ for all +ve integer

$$S = \{ n \in \mathbb{N} \,/\, n! \le n^n \}$$

$1 \in S \qquad 1! = 1^1$

$1 < 2$

$1 \le 2$

Assume $n \in S$, $\quad n! \le n^n$

$(n+1) \in S$ (prove)

$$(n+1)! = n!\,(n+1) = n^n (n+1) \le (n+1)^n (n+1) = (n+1)^{n+1}$$

1st principle math induction, $\quad S = \mathbb{N}$

$n! \le n^n \quad \forall\, n \in \mathbb{N}$

The second principle of mathematical induction

A property concerning the set of all +ve integers that is true for $n=1$ and that is true for +ve integers upto $n+1$ whenever it is true for +ve integers upto n is true for all +ve integers.

Mathematically: If a set S of +ve integers satisfies: (i) $1 \in S$

(ii) $n+1 \in S$ whenever $1, 2, \cdots n \in S$

then $S = \mathbb{N}$.

Remark It is also known as strong form of mathematical induction.

we can prove induction principle using well-ordering principle

Theorem: (Fundamental Theorem of Algebra)

" FTA " –

Linear algebra, complex Analysis, Topology

<u>Statement</u>: Every non zero polynomial of degree n has <u>atmost</u> n real roots.

<u>Proof</u>: We use the second principle of induction

$$p(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$$

$a_n \neq 0$, $\deg p = n$. $\boxed{\text{no. of roots} \leq n}$

$m = n+1$

Use induction on m

$m = 1 \Rightarrow n = 0 \Rightarrow p(x) = a_0$ $\quad a_0 \neq 0$

(i) There is no x s.t. $p(x) = 0$

The no of roots is zero

$p(x)$ has atmost zero root

The result is true for $n = 1$

suppose that the result is true for the integers upto n. $0, 1, 2, \ldots n$.

Take polynomial p of degree $\leq n+1$

If $\deg p \leq n$, the induction assumption implies that no of roots is atmost $\deg p$.

$\deg p = n+1$

we have to prove that $p(x)$ has atmost $(n+1)$ roots.

Suppose not, the no. of roots of $p(x)$ is more than $n+1$

$K \leq n+1$

$\boxed{K > n+1}$

$k \geq n+1$

$n \geq 0$

Let $b_0, b_1, b_2, \ldots, b_n$ be $(n+1)$ roots of $p(x)$ (ie)

$$p(b_0) = p(b_1) = \cdots = p(b_n) = 0$$

consider the polynomial

$$q(x) = p(x) - a_{n+1}(x-b_0)(x-b_1)\cdots(x-b_n)$$

where a_{n+1} is the leading coefficient

$q(x)$ has roots, namely, $b_0, b_1, \ldots, b_n$

$q(x)$ has more than n roots — (1)

$\cancel{a_{n+1}}\ {}^{n+1}$? $a_n x^n$ $\neq 0$

$q(x)$ has $\deg \leq n$

By induction (second) principle assumption

$q(x)$ has atmost n roots — (2)

$\rightarrow \Leftarrow$ to (1)

Pigeon hole - principle :

If n objects are placed m boxes, $n > m$
then atleast one box contains
two or more objects

Pigeon-hole principle can be proved
using induction method

weak form

If $S \subseteq \mathbb{N}$ with (i) $1 \in S$ (ii) $n+1 \in S$ whenever $n \in S$
then $S = \mathbb{N}$

strong form

If $S \subseteq \mathbb{N}$ with (i) $1 \in S$ (ii) $n+1 \in S$ whenever $1, 2, \dots, n \in S$
then $S = \mathbb{N}$