Date

Page

(iv) $d_n = 4d_{n-1} - 4d_{n-2}$, $d_1 = 1$, $d_2 = 7$

This is linear homogeneous recurrence relation of degree 2. It's characteristics equ^n. So

So,

$x^2 = 4x - 4$

or, $x^2 - 4x + 4 = 0$

or, $x^2 - 2x - 2x + 4 = 0$

or, $x(x-2) - 2(x-2) = 0$

or, $(x-2)(x-2) = 0$

$x = 2$, $x = 2$

It's roots are,

$s_1 = 2$, $s_2 = 2$

and it's explicit formula is,

$d_n = u \cdot s_1^n + v s_2^n$ $\qquad$ $d_n = u \cdot s_1^n + v \cdot s_2^n$

or, $d_n = u \cdot 2^n + vn2^n$ $\qquad$ $d_n = u \cdot s_1^n + v \cdot n s_1^n$

Applying initial Conditions, we get

$d_1 = u \cdot 2^1 + vn2^1 \Rightarrow 2u + 2v = 1$ — (1)

$d_2 = u \cdot 2^2 + vn2^2 \Rightarrow 4u + 8v = 7$ — (2)

Now,

~~or, $4u = 7 - 4v$~~

~~from (1) and (2)~~

~~$4u + 8v = 4$~~ $\} \times 2$

~~$4u + 8v = 7$~~

~~(-) (-) (-)~~

Date
Page

Now, $\cancel{4u} + 4v = 2 \quad \} \times 2 \qquad -(1)$

$\cancel{4u} + 8v = 7 \qquad -(2)$

$(-) \quad (-) \qquad (-)$

$-4v = -5$

or, $v = +5/4$

Now, from (2)

$4u + 8\left(+\frac{5}{4}\right) = 7$

or, $4u + 10 = 7$

or, $4u = -3$ or, $u = \cancel{17/4} \; -3/4$

Now,

$d_n = u s_1^n + v . n s_1^n$

$= \left(-\frac{3}{4}\right) 2^n + \left(\frac{5}{4}\right) n . 2^n$

(9) Since by def^n

$A \triangle B = (A - B) \cup (B - A)$

So,

$A \triangle B = \{x : x \in A \triangle B\}$

$= \{x : x \in (A - B) \cup (B - A)\}$

$= \{x : x \in (A - B)$ or $x \in (B - A)\}$

$= \{x : (x \in A$ but $x \notin B)$ or $(x \in B$ but $x \notin A)\}$

What do you mean by set? (Interpretation)

→ The status of the element is defined by the status of set.

Set : A collection of well defined objects.

[relation types]

Operations on sets :

Total operations : 5

Independent ⇒ 2 = Union, Intersection

Dependent ⇒ 3 = Compliment, Difference, Symmetric Difference

- Union :

Defⁿ : Consider union of two sets A and B, denoted by $A \cup B$, is a set that includes the elements either from A or from B or both.

Symbolically $A \cup B = \{x : x \in A \text{ or } x \in B\}$

Interpretation : Union is weak.

Application : OR gate

Output : Bigger ~~gate~~ set / superset

Eg: $A=\{1,2,3\}$, $B=\{2,3,4\}$
$A\cup B=\{1,2,3,4\}$

Weak because it has many alternatives.

- Intersection:
  Def^n: The intersection of two sets A and B is denoted by $A\cap B$, is a set that includes the elements from A and B.

Symbolically: $A\cap B=\{x : x\in A \text{ and } x\in B\}$

Interpretation: strong

Application: AND gate

Output: subset

Theorem 1:
(Properties on sets: Algebra)

- Commutativity : $A\cup B=B\cup A$ $A\cap B=B\cap A$
- Associativity : $A\cup(B\cup C)=(A\cup B)\cup C$, $A\cap(B\cap C)=(A\cap B)\cap C$
- Distributive : $A\cap(B\cup C)=(A\cap B)\cup(A\cap C)$
- Indempotent
- Complement : $\overline{A\cup B}=\bar{A}\cap\bar{B}$. De Morgans law

- Universal set
- Empty set

* Applications of sets:

a) • Probability Theory

b) • Digital system : $\cup\rightarrow$ OR gate, $\cap\rightarrow$ AND gate
$A^c\rightarrow\sim$

c) • In computer

(a) Cardinality of set:
Number of elements of a set is called its cardinality. It is denoted by $n(A)$ or $|A|$ or $\#(A)$.
It is finite or infinite; countable or uncountable.
So, the probability theory is application of sets relative to its cardinality.

$$\frac{n(E)}{n(U)} \in Q \rightarrow [0,1]$$

But higher level statistics is again a part of mathematics.

# Theorem 2: (Addition principle)
If A and B are finite sets then
$|A \cup B| = |A| + |B| - |A \cap B|$

Theorem 3:
If A and B and C are finite sets. Then,
$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |B \cap C| - |C \cap A| + |A \cap B \cap C|$
A sequence is an ordered set of numbers.

* Characteristic function:
Def^n: If A is a subset of universal set U, then the characteristic function f_A of A is defined as:

$$f_A(x) = \begin{cases} 1 & \text{if } x \in A \\ 0 & \text{if } x \notin A \end{cases}$$

so that,
$D_f : U$
$R_f : \{0, 1\}$

Theorem:
Characteristic functions of subset satisfies the following properties:
i) $f_{A \cap B} = f_A \cdot f_B$

ii) $f_{A \cup B} = f_A + f_B - f_A \cdot f_B$

iii) $f_{A \oplus B} = f_A + f_B - 2 f_A \cdot f_B$

i) Proof:
To prove: $f_{A \cap B}(x) = f_A \cdot f_B$

Case I: If $x \in A$ and $x \in B$ then $x \in A \cap B$.
By def^n of characteristic function,
$f_A(x) = 1$, $f_B(x) = 1$, $f_{A \cap B}(x) = 1$

$\Rightarrow f_{A \cap B}(x) = 1 = 1 \cdot 1 = f_A(x) \cdot f_B(x)$

Case II: If $x \in A$ & $x \notin B$
Case III: If $x \notin A$ & $x \in B$
Case IV: $x \notin A, x \notin B$ [Proved]

* Computer representation of sets and subsets:

Consider a finite universal set $U = \{x_1, x_2, \ldots x_n\}$ and A, subset of U. Then f_A can be represented by a sequence of 0's and 1's of length n. (bytes!!)

Eg: If $U = \{1, 2, 3, \ldots, 10\}$ and $A = \{2, 4, 6, 8\}$
Then, f_A corresponds to the sequence.
0, 1, 0, 1, 0, 1, 0, 1, 0, 0

Prove the following:

i) $A\cup(B\cap C) = (A\cup B)\cap(A\cup C)$

ii) $A-(B\cup C) = (A-B)\cap(A-C)$

iii) $\overline{A\cup B} = \bar{A}\cap\bar{B}$

iv) $f_{A\cup B} = f_A + f_B - f_A f_B$, f_A being characteristics function

i) $A\cup(B\cap C) = (A\cup B)\cap(A\cup C)$ $= \{x : x \in A\cup(B\cap C)\}$ $= \{x : x\in A \text{ or } x\in(B\cap C)\}$

L.H.S, $A\cup(B\cap C) = \{x : x\in A \text{ or } (x\in B \text{ and } x\in C)\}$

$= \{x : (x\in A \text{ or } x\in B) \text{ and } (x\in A \text{ or } x\in C)\}$

$= \{x : (x\in A\cup B) \text{ and } (x\in A\cup C)\}$

$= \{x : x\in(A\cup B) \cap (A\cup C)\}$

$= (A\cup B)\cap(A\cup C)$ // [proved]

ii) $A-(B\cup C) = (A-B)\cap(A-C)$ $= \{x : x\in A-(B\cup C)\}$

L.H.S, $A-(B\cup C) = \{x : x\in A \text{ and } x\notin(B\cup C)\}$

$= \{x : x\in A \text{ and } (x\notin B \text{ and } x\notin C)\}$

$= \{x : (x\in A \text{ and } x\notin B) \text{ and } (x\in A \text{ and } x\notin C)\}$

$= \{x : x\in(A-B) \text{ and } x\in(A-C)\}$

$= \{x : x\in(A-B)\cap(A-C)\}$

$= (A-B)\cap(A-C)$ //

iii) $\overline{A\cup B} = \bar{A}\cap\bar{B}$

L.H.S, $\overline{A\cup B} = \{x : x\in U \text{ and } x\notin(A\cup B)\}$

$= \{x : x\in U \text{ and } x\in A$

iii) $\overline{A\cup B} = \bar{A}\cap\bar{B}$ $= \{x : x\in\overline{A\cup B}\}$ $\{x : x\notin(A\cup B)\}$

$= \{x : x\notin A \text{ and } x\notin B\}$

$= \{x : x\in\bar{A} \text{ and } x\in\bar{B}\}$

L.H.S, $\overline{A\cup B} = \{x : x\notin(A\cup B)\}$

$= \cancel{\{x : x\notin A \text{ and } x\notin B\}}$

$= \bar{A}\cap\bar{B}$,

$= \{x : (x\notin A) \text{ and } (x\notin B)\}$

$= \{x : x\in\bar{A} \text{ and } x\in\bar{B}\}$

$= \{x : x\in(\bar{A}\cap\bar{B})\}$

$= \bar{A}\cap\bar{B}$ // proved

iv) $f_{A\cup B} = f_A + f_B - f_A f_B$

Sol^n: If $x\in A$ or $x\in B$ then $x\in A\cup B$.

By def^n of characteristic function.

$f_A(x) = 1$, $f_B(x) = 1$; $f_{A\cup B}(x) = 1$

$\Rightarrow f_{A\cup B} = 1+1-1.1 = f_A(x) + f_B(x) - f_A(x).f_B(x)$

$f_{A\cup B}(x) = f_A(x) + f_B(x) - f_A(x).f_B(x)$. // proved

Case II :

If $x\in A$ and $x\notin B$ then $x\in(A\cup B)$

By def^n of characteristic function

$f_A(x)=1$, $f_B(x)=0$, $f_{A\cup B}(x)=1$

$\Rightarrow f_{A\cup B} = 1+0-1.0$

$= f_A(x) + f_B(x) - f_A(x).f_B(x)$ proved.

Case III:

If $x \notin A$ and $x \in B$ then $x \in (A \cup B)$

By defn of characteristic function.

$f_A(x) = 0$; $f_B(x) = 1$, $f_{A\cup B}(x) = 1$

$\Rightarrow f_{A\cup B}(x) = 0 + 1 - 0 \cdot 1$

$= f_A(x) + f_B(x) - f_A(x) \cdot f_B(x)$ proved

Standard sets of integers

Natural, $\mathbb{N} = \{1, 2, 3, \ldots\}$

Whole, $J = \{0, 1, 2, 3, \ldots\}$

Integer, $\mathbb{Z} = \mathbb{Z}^- \cup \{0\} \cup \mathbb{Z}^+$, $-\mathbb{Z}^+ = \mathbb{Z}^-$

Rational, $\mathbb{Q}$ = Used in cryptography

Real, $\mathbb{R}$ = MATH 101 + MATH 104

Complex, $\mathbb{C}$ = MATH 207

$\mathbb{N} \subset J \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$

Division in integers : ($m \div n$, $m, n \in \mathbb{Z}$)

Objective to discuss properties of number set.

Number set is never easy.

Eg: Now, we have MS 2000. (Problem = Y2K)

1999+1 = 2000 (adding 1 was very difficult)

Domain of MCSC 201 = set of positive integers.

Division in integers:

Consider two numbers $m = 7$ and $n = 2$ with division operation ($\div$):

Two possibilities : $7 \div 2$ and $2 \div 7$

decimal decimal

$7 \div 2 = 3.2 + 1 \Rightarrow \boxed{m = q.n + r}$

Theorem:

A.] Division Algorithm Theorem:

If m and n are integers, $n > 0$ then ~~can~~ we can write $m = q.n + r$, for integers q, r with $0 \le r < n$

Note: If $r = 0$ then $m = q.n$ so m is a multiple of n and we write ~~then~~ $n | m$.

: If $n | m$ then $m = qn$ and $n \le |m|$

: If m is not a multiple of n then $n \nmid m$.

Properties : factor/multiple, even/odd, prime/composite, GCD/LCM etc.

prime$^{\text{power}}$ → bites

B.] Let a, b and c be integers.

i) If $a|b$ and $a|c$, then $a|(b+c)$.

ii) If $a|b$ and $a|c$ when $b>c$ then $a|(b-c)$.

iii) If $a|b$ or $a|c$ then $a|bc$.

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

In general, $a|b$ and $a|c$ then ~~$a|(b+c)$~~ $a|(mb+nc)$, for any integer m and n.

A number $p>1$ in $\mathbb{Z}^+$ is called prime if the only positive integers that divide p are p and 1. Otherwise, it is composite.

i) Algorithm to check a prime number $N>1$:

Step 1: Check whether $N=2$. If so, N is prime. If not so proceed to

Step 2: Check whether $2|N$. If so, N is not prime. If not so proceed to

Step 3: Compute the largest integer $K \le \sqrt{N}$. Then

Step 4: Check whether $D|N$, where D is any odd number such that $1<D\le K$. If $D|N$, then N is not prime. Otherwise, N is prime.

Proof:

a) To prove: $a|b$ and $a|c \Rightarrow a|(b+c)$.

If $a|b$ then by def^n $b = n_1 a$ for some integer n_1.

If $a|c$ then by def^n $c = n_2 a$ for some integer n_2.

So that,

$$b+c = n_1 a + n_2 a$$
$$= (n_1+n_2)\,a$$
$$= n.a \quad \text{for some integer, } n = n_1+n_2$$

This implies $a|(b+c)$

C.] Every positive integer $n>1$ can be written uniquely as, $p_1^{k_1} p_2^{k_2} p_3^{k_3} \cdots p_s^{k_s}$

where, $p_1<p_2<p_3<\cdots<p_s$ are distinct primes that divides n and the k's are positive integers giving the number of times each prime occurs as a factor of n.

Eg: $24 = 2^3 \cdot 3$ / ~~$3 \cdot 2^3$~~

$108 = 2^2 \cdot 3^3$

D. GCD: If a, b and k are in $\mathbb{Z}^+$ and $k|a$, $k|b$ then k is common divisor of a and b. The largest of such k, denoted by d is called the greatest common divisor or GCD of a and b. We write: $d = GCD(a,b)$.

D.] If $d = GCD(a,b)$. Then:

a) $d = sa+tb$ for some integers s and t. (not necessarily positive)

b) If c is any other common divisor of a & b, then $c|d$.

$d = sa + tb \Rightarrow$ linear combination

Proof:

Let x be the smallest positive integer than can be written as $sa+tb$ for some integers s and t, and let c be the common divisor of a and b. Then, since $c|a$ and $c|b$. So $c|x$ and $c \le x$. We claim x is a common divisor of a and b.

Using division Algorithm theorem,

$a = qx + r$ for $0 \le r < x$

Then,

$r = a - qx$

$= a - q(sa+tb)$

$= a - qsa - qtb$

$= (1-qs)a + (-qt)b$

If $r \neq 0$ then since $r < x$ and r is the sum of multiple of 'a' and a multiple of 'b'. This is a contradiction to the assumption of x. Hence $r = 0$ and $a = qx$. This implies $x|a$. Similarly, $x|b$.

Hence, $x = GCD(a,b)$. [Proved]

Prove:

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

ii) Verify the prime nature of

ii) $N = 137$

iii) $N = 3747$

iv) $N = 74372$

Soln:

i) ~~Let a, b be the integers.~~

~~If a|b and b|c~~

i) If $a|b$ then by definition $b = q_1 a$ for some integer q_1

If $b|c$ then by definition $c = q_2 b$ for some integer q_2

So that,

$\cancel{c = n_2 b}$ $\quad c = q_2 b$

or, $\cancel{c = n_2 \cdot n_1 a}$ $\quad$ or, $c = q_2(q_1 a) = (q_2 q_1)a$ for some integers

or, $\quad$ or, $c = qa$ $\quad [q = q_1 q_2]$

This implies, $a|c$. [Proved]

ii) $N = 137$

Step 1: Here, $N \neq 2$.

Step 2: $2 \nmid N$

Step 3: There exists $k = 11 < \sqrt{N}$

~~Step 3: $\sqrt{137}$ $k < \sqrt{137}$, $k = 11$~~

Step 4: We get odd numbers $D = 3, 5, 7, 9, 11$ such than $D \nmid N$.

Step 4: ~~$1 < D \le k$~~. So N is a prime.

~~$D = 3, 5, 7, 9, N$~~

~~$3 \nmid 137$, $5 \nmid 137$, $7 \nmid 137$, $9 \nmid 137$, $11 \nmid 137$ are not divisible~~

iii) $N = 3747$

Step 1: $N \neq 2$.

Step 2: $2 \nmid N$

Step 3: There exists $k = 61 < \sqrt{N}$

Step 4: We get odd numbers, $D = 3, 5, 7, 9, 11, 13, 15, 17, 19,$

21, 23, 25, 27, 29, 31, 33, 35, 37, 39, 41, 43, 45, 47, 49, 51, 53, 55, 57, 59, 61 such that $3|N$
so, N is not prime

Division algorithm to find $GCD(a,b)$ + to get $s,t \in \mathbb{Z}^+$;
Suppose $a,b \in \mathbb{Z}^+$, $a>b>0$. Then using division algorithm theorem, we have

$a = kb + r_1$ where $0 \le r_1 < b$.

Since $GCD(a,b) = GCD(b, r_1)$ so,

Dividing b by r_1, $b = k_1 r_1 + r_2$ $0 \le r_2 < r_1$

Dividing r_1 by r_2, $r_1 = k_2 r_2 + r_3$ $0 \le r_3 < r_2$

Dividing r_2 by r_3, $r_2 = k_3 r_3 + r_4$ $0 \le r_4 < r_3$

Continuing the process we get

Dividing r_{n-2} by r_{n-1} : $r_{n-2} = k_n r_{n-1} + r_n$ $0 \le r_n < r_{n-1}$

Dividing r_{n-1} by r_n : $r_{n-1} = k_{n+1} r_n + r_{n+1}$ $0 \le r_{n+1} < r_n$

Since $a > b > r_1 > r_2 > \ldots$, so at some point $r_{n+1} = 0$

Hence, $r_n = GCD(a,b)$

Find GCD (98, 273) and express it as $sa+tb$.

Soln:

The given numbers are:

$a = 273$, $b = 98$

Using Euclidean Algorithm Theorem, we get

Dividing 273 by 98 : $273 = 2 \cdot 98 + 77$

Dividing 98 by 77 : $98 = 1 \cdot 77 + 21$

Dividing 77 by 21 : $77 = 3 \cdot 21 + 14$

Dividing 21 by 14 : $21 = 1 \cdot 14 + 7$

Dividing 14 by 7 : $14 = 2 \cdot 7 + 0$

$\therefore GCD(98, 273) = 7$

Also, $d = GCD(a,b) = sa + tb$

Now,

$$
\begin{aligned}
7 &= 21 - 1 \cdot 14 \\
&= 21 - 1[77 - 3 \cdot 21] \\
&= 4 \cdot 21 - 1 \cdot 77 \\
&= 4[98 - 1 \cdot 77] - 1 \cdot 77 \\
&= 4 \cdot 98 - 5 \cdot 77 \\
&= 4 \cdot 98 - 5[273 - 2 \cdot 98] \\
&= 14 \cdot 98 - 5 \cdot 273 \text{ (unique representation)}
\end{aligned}
$$

which takes the form $sa+tb$ where ~~s=14, t=-5~~

$s = -5$, $t = 14$.

- Theorem:
  If a and b are in Z^+, $b > a$. Then $GCD(a,b) = GCD(b, b-a)$

Def^n: (least common multiple of a and b).
If a, b and k are in Z^+, and $a|k$, $b|k$ then k is said to be a common multiple of a and b. The least of such k, denoted by c if it exists is called the least common multiple of a and b. It is denoted by
$LCM(a,b) = c$

- Theorem:
  If a and b are positive integers then $\boxed{GCD(a,b) \cdot LCM(a,b) = a \cdot b}$

Proof:
Suppose $p_1, p_2, \ldots, p_k$ be prime factors of either a or b. Then, we have, $a = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$
and $b = p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}$, where some of a_i or b_i may be zero.
Then,

$$GCD(a,b) = p_1^{\min(a_1,b_1)} \cdot p_2^{\min(a_2,b_2)} \cdots p_k^{\min(a_k,b_k)}$$

$$LCM(a,b) = p_1^{\max(a_1,b_1)} \cdot p_2^{\max(a_2,b_2)} \cdots p_k^{\max(a_k,b_k)}$$

So that,

$$GCD(a,b) \cdot LCM(a,b) = p_1^{a_1+b_1} \cdot p_2^{a_2+b_2} \cdots p_k^{a_k+b_k}$$

$$= a \cdot b \quad \text{(Proved)}$$

GCD more imp than LCM.

$GCD(a,b) = d$, $LCM(a,b) = c$ } important

If $a, b \in Z^+$
$GCD(a,b) = d = sa + tb$
$GCD(a,b) \cdot LCM(a,b) = a \cdot b$

MATRIX: (Def^n, types, properties, operations)

Boolean Matrix:

A Boolean matrix (also called a bit matrix) is an $m \times n$ matrix whose entries are either zero or one. Eg: an identity matrix I_3 is a Boolean matrix.

Operations: join ($\vee$), meet ($\wedge$), product ($\odot$)

Consider two Boolean matrices, $A = [a_{ij}]$ and $B = [b_{ij}]$ of order $m \times n$. Then, the join of A and B is $C = [c_{ij}]$ defined by
$$c_{ij} = \begin{cases} 1 & \text{if } a_{ij} = 1 \text{ or } b_{ij} = 1 \\ 0 & \text{if } a_{ij} = 0 \text{ and } b_{ij} = 0 \end{cases}$$

The meet of A and B denoted by $A \wedge B$ is a Boolean matrix $D = [d_{ij}]$ where d_{ij} is defined as
$$d_{ij} = \begin{cases} 1 & \text{if } a_{ij} = 1 \text{ and } b_{ij} = 1 \\ 0 & \text{if } a_{ij} = 0 \text{ or } b_{ij} = 0 \end{cases}$$

If $A = [a_{ij}]$ is a Boolean matrix of order $m \times p$ and $B = [b_{ij}]$ is a Boolean matrix of order $p \times n$ then the product AB is conformable with order $m \times p$ and it is $AB = F = [f_{ij}]$, where

$$f_{ij} = \begin{cases} 1 & \text{if } a_{ik} = 1 \text{ and } b_{kj} = 1 \quad \text{for some } k,\ 1 \le k \le p \\ 0 & \text{otherwise} \end{cases}$$

Example:

Consider two matrices:

$A = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ and $B = \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}$

Then $A \vee B = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ $\quad A \odot B = \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}$

$A \wedge B = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$

Mathematical structure or system : Applications?

↳ (Set, operation, properties) form a system

independent

- → commutative
- → associative
- → existence of identity (e)
- → existence of inverse (i)
- → distribution

Assignment I (6th edition Text Book) (3 weeks)

Numbers	Pages
Algebraic properties	8-9
30 :	1-34
40 :	1-45
44 :	1-29

(only copy not sheets)

- Find GCD of given numbers and express it as $sa + tb$.

1.) 540, 504

2.) 14268, 16234

3.) 1242, 3246

- find $A \vee B$, $A \wedge B$ & $A \odot B$ where

$A = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix}$ and $B = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 0 & 1 \end{bmatrix}$

Sol^n:

1.) 540, 504

- $A \vee B = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}$

$A \wedge B = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix}$

$A \odot B = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix}$

$d_{12} = a_{1p}\ b_{p2} = a_{11}\ b_{12} \cdot a_{12}\ b_{22} \cdot a_{13}\ b_{32}$

$a_{1p}\ b_{p1}$, $a_{11}\ b_{11}$, $a_{12}\ b_{21}$, $a_{13}\ b_{31}$

$a_{2p}\ b_{p2}$, $a_{21}\ b_{12}$, $a_{22}\ b_{22}$, $a_{23}\ b_{32}$

$a_{3p}\ b_{p3}$, $a_{31}\ b_{13}$, $a_{32}\ b_{23}$, $a_{33}\ b_{33}$

a) 540, 504

The given numbers are:

$a = 540,\ b = 504$

Using Euclidean Algorithm Theorem

Dividing 540 by 504: $540 = 1 \cdot 504 + 36$

Dividing 504 by 36: $504 = 14 \cdot 36 + 0$

$\therefore GCD(540, 504) = 36$

Also, $d = GCD(a, b) = sa + tb$

Now,

$36 = 540 - 1 \cdot 504$

which takes the form $sa + tb$ where, $s = 1,\ t = -1$.

b) 14268, 16234

The given numbers are:

$a = 16234,\ b = 14268$

Using Euclidean Algorithm Theorem.

Dividing 16234 by 14268: $16234 = 1 \cdot 14268 + 1966$

Dividing 14268 by 1966: $14268 = 7 \cdot 1966 + 506$

Dividing 1966 by 506: $1966 = 3 \cdot 506 + 448$

Dividing 506 by 448: $506 = 1 \cdot 448 + 58$

Dividing 448 by 58: $448 = 7 \cdot 58 + 42$

Dividing 58 by 42: $58 = 1 \cdot 42 + 16$

Dividing 42 by 16: $42 = 2 \cdot 16 + 10$

Dividing 16 by 10: $16 = 1 \cdot 10 + 6$

Dividing 10 by 6: $10 = 1 \cdot 6 + 4$

Dividing 6 by 4: $6 = 1 \cdot 4 + 2$

Dividing 4 by 2: $4 = 2 \cdot 2 + 0$

$\therefore GCD(14268, 16234) = 2$.

Now,

$2 = 6 - 1 \cdot 4$

$= 6 - 1 \cdot [10 - 1 \cdot 6]$

$= 2 \cdot 6 - 1 \cdot 10$

$=$

Chapter - 2

LOGIC WITH APPLICATION(S)

Logic
Statement
Operations
Types
Quantifiers
Algebra
Methods of proof

- Logic : (Imp for objective)
  - deals with the method of reasoning.
  - provides rule & technique for determining whether a given arguement is valid.
  - logical reasoning is used in maths to prove theorems in computer science to verify the corrections of program
  - contributions from De Morgan (1806 - 1871) and George Boole (1815 - 1864)

- Statement :
  - A statement or proposition is a declaration sentence i.e either true or false.
  Eg : $2+3=6$ (F), AOB = BOA (T)

- Operations : (logical connectives with truth table)
  negation ($\sim$), disjunction ($\vee$), conjuction ($\wedge$)
  If p is a statement then the negation of p is the statement "not p" denoted by $\sim p$. It's truth table is

p	$\sim p$
T	F
F	T

Eg : p : Ram is present in class.
$\sim p$: Ram is not present in class.

If p and q are statements, the conjuction of p and q is the compound statement i.e "p and q" denoted by $p \wedge q$. It's truth table is :

p	q	$p \wedge q$
T	T	T
T	F	F
F	T	F
F	F	F

Similarly,
If p and q are statements, the disjunction of p and q is the compound statement i.e "p or q" denoted by $p \vee q$.

p	q	$p \vee q$
T	T	T
T	F	T
F	T	T
F	F	F

- Types of statements :
  Compound : Conjuction ($\wedge$), disjunction ($\vee$)
  Conditional : Implication ($\Rightarrow$), Converse, Contrapositive, biconditional (equivalence), tautology.

classmate
Date
Page

contradiction or absurdity, contingency.

- Quantifiers :

  predicate (propositional function : $P(x)$), universal ($\forall$ for all), existential ($\exists$ → there exists).

An element of $\{x | P(x)\}$ is an object t for which the statement $P(t)$ is ~~the~~ true, such ~~that~~ a sentence $P(t)$ is called a predicate.

Example: Consider a set $A = \{x | x$ is an integer less than $8\}$. Then, $P(x)$ is the sentence "x is an integer less than 8" is a predicate since $P(1)$ is true, $1 \in A$.

The universal quantification of a predicate $P(x)$ is the statement "For all values of x, $P(x)$ is true". It is denoted by $\forall x\ P(x)$ is true.

Example: The sentence $P(x): -(-x) = x$ is the predicate that is ~~the~~ true for all real numbers.

But the sentence $Q(x): x+1 < 4$ is not universal as $\exists 5$ such that $P(5)$ is false.

Consider $P(x)$: x is a root of $x^2 + 5x + 6 = 0$.

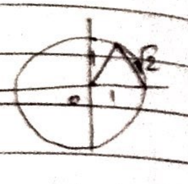
Is it universal or existential? ⇒ existential.

Truth table for implication ($\Rightarrow$):

If p and q are statements then the compound statement "if p then q", denoted by $p \Rightarrow q$ or $p \to q$ is called a conditional statement or implication.

- Methods of proof :
  - ↳ Direct $(p \Rightarrow q)$
  - ↳ Indirect $(\sim p\ (\sim q \Rightarrow \sim p)$ Contrapositive.

i.) $\sqrt{2}$ is irrational



Soln:

Given number is $N = \sqrt{2}$

Using direct method : $N = \sqrt{2} = 1.1416\ldots$

Using indirect method :

Suppose N is not irrational. Then N is rational so that $\sqrt{2} = p/q$, $p, q \in \mathbb{Z}$, $q \neq 0$.

$\Rightarrow p = q\sqrt{2}$

Squaring both sides,

$p^2 = q^2 \cdot 2$.

p^2 is even integer so p is even. Thus, $p = 2m$, $m \in \mathbb{Z}$

Therefore,

$2 \cdot m^2 = q^2$, so q^2 is even and q is even. Let,

$q = 2n$, $n \in \mathbb{Z}$.

This implies $\sqrt{2} = m/n$, which is a contradiction.

I.] Use truth table to prove :

i.) $\sim(p \vee q) \equiv (\sim p) \wedge (\sim q)$

ii.) $\sim(p \Leftrightarrow q) \equiv ((p \wedge \sim q) \vee (q \wedge \sim p))$.

II.] i.) Show that : if x^2 is an even integer, x is an an even

ii.) $2 + 3 = 5$.

I.] ~~i.) p q p∨q ~(p∨q) (~p) (~q) ~p~~

ii.)

p	q	$p \Leftrightarrow q$	$\sim(p \Leftrightarrow q)$	$\sim p$	$\sim q$	$p \wedge \sim q$	$q \wedge \sim p$	$(p \wedge \sim q) \vee (q \wedge \sim p)$
T	T	T	F	F	F	F	F	F
T	F	F	T	F	T	T	F	T
F	T	F	T	T	F	F	T	T
F	F	T	F	T	T	F	F	F

$\sim(p \Leftrightarrow q) \equiv ((p \wedge \sim q) \vee (q \wedge \sim p))$

T

T

T

T

which is a tautology

Hence, $\sim(p \Leftrightarrow q) \equiv ((p \wedge \sim q) \vee (q \wedge \sim p))$.

(Indirect method)

II.] To prove : if x^2 is even integer then x is even integer.

Proof : Suppose x is not even. Then, x is odd. So, $x = 2m+1$, for some integer m.

Now, $x^2 = (2m+1)^2 = 4m^2 + 4m + 1 = 2(2m^2 + 2m) + 1$, ~~when~~ $= 2 \cdot n + 1$

which is of an odd form.

So, x^2 is even. [Proved]

Prove : If x is even integer, then x^2 is even. (Direct metho

Mathematical Induction Theorem
(Application of logic to non-negative integer)

Statement (first form): To prove that the statement $p(n)$ is true for all integer $n \geq x$, where n is some fixed integer (position zero or non-negative)
we have the following steps:

i) Basic step $p(n)$ is true
ii) Induction step $p(n)$ is true for some $k \geq n$, then $p(k+1)$ must be true. Then, $p(n)$ is true for $n \geq n_0$. The result is called principle of induction.

Stronger form or strong Induction:

$P(n_0) \wedge P(n_0+1) \wedge P(n_0+2) \wedge \dots \wedge P(1) = P(k+1)$ is a tautology.

Chapter-3

COUNTING WITH APPLICATION

i) Basic principles of counting
- Multiplication principle of counting
- Permutation $P(n,r)$ (order)
- Combination $C(n,r)$ (not order)

Relation betn $P(n,r)$ and $C(n,r)$
- Application: Element of probability (MATH 208)

The pigeonhole principle + its extension

$P(n,r) = \frac{n!}{(n-r)!}$, $C(n,r) = \frac{P(n,r)}{r!}$

$\therefore P(n,r) = r! \cdot C(n,r)$

$\therefore P(n,r) > C(n,r)$

- Theorem (Pigeonhole Theorem)
If n pigeons are assigned to ~~the~~ m pigeonholes and $m < n$, then at least one pigeonhole contains two or more pigeons.

- Theorem (Extended pigeon theorem)
If n pigeons are assigned to m pigeonholes, then one of the pigeonhole must contain $\left[(n-1)/m\right] + 1$ pigeons.
eg: If $n = 13$ & $m = 9$, then one of the pigeon hole contain atleast

$[(13-1)/9]+1 = 2$ pigeons.

* **Recurrence Relation:**

To find explicit ~~form~~ formula for a recurring defined sequence.

Consider ~~$a_n = a_{n-1} + $~~ $\boxed{a_n = a_{n-1} + 3}$ then,

$a_{100} = ?$

Methods for finding explicit formula for a recursively defined sequence:

i) Backtracking (Basic Method) -

Consider the recurrence relation a_n defined by $a_n = a_{n-1} + 3$ with $a_1 = 2$.

Then, its explicit formula,

Using backtracking, we get

$a_n = a_{n-1} + 3$

$= (a_{n-2} + 3) + 3 = a_{n-2} + 2\cdot 3$

$= (a_{n-3} + 3) + 2\cdot 3 = a_{n-3} + 3\cdot 3$

$= (a_{n-4} + 3) + 3\cdot 3 = a_{n-4} + 4\cdot 3$

In general,

$a_n = a_{n-(n-1)} + (n-1)3$

$= a_1 + (n-1)3$

$= 2 + 3(n-1)$, which is the required formula.

Now, $a_{1000} = 2 + 3\cdot 999 =$

ii) General (Algebraic) Method:

Only upto linear homogenous relations

For a linear homogeneous recurrence relation of degree k defined by $a_n = r_1 a_{n-1} + r_2 a_{n-2} + \dots + r_k a_{n-k}$, the associated polynomial of degree k is, $x^k = r_1 x^{k-1} + r_2 x^{k-2} + \dots + r_k$, which is called the characteristic equation

a) If the characteristic equation $x^2 - r_1 x + r_2 = 0$ for the recurrence relation $a_n = r_1 a_{n-1} + r_2 a_{n-2}$ has the distinct roots say s_1 and s_2, then $\boxed{a_n = u s_1^n + v s_2^n}$, when u and v depend ~~defined~~ on the intial conditions is the explicit formula for the sequence.

In case of equal roots $s_1 = s_2 = s$, the explicit formula is ~~$a_n = us^n + vs^n$~~ $\boxed{a_n = us^n + vns^n}$ where u and v depend on initial conditions.

We exclude the case for,

$s_1 = \alpha + i\beta$, $s_2 = \alpha - i\beta$ where $\alpha, \beta \in \mathbb{R}$.

Example:

Find the explicit formula for the sequence defined by $C_n = 3C_{n-1} - 2C_{n-2}$ with initial conditions $C_1 = 5$ & $C_2 = 3$.

Sol^n:

The given recurrence ~~recursive~~ relation is.

$C_n = 3C_{n-1} - 2C_{n-2}$

with initial condition $C_1 = 5$ and $C_2 = 3$.

This is linear homogenous recurrence relation of degree 2.

Its characteristic eqⁿ is, $x^2 = 3x - 2 \Rightarrow x^2 - 3x + 2 = 0$

The roots are $s_1 = 1$, $s_2 = 2$, which are distinct.

So that, the explicit formula is,

$C_n = us_1^n + vs_2^n$

$\Rightarrow C_n = u \cdot 1^n + v \cdot 2^n$

$\Rightarrow C_n = u + v \cdot 2^n$.

Applying initial conditions, we get

$C_1 = u + 2v \Rightarrow u + 2v = 5$,

$C_2 = u + v \cdot 2^2 \Rightarrow u + 4v = 3$,

Solving these for u and v, we get.

Therefore, the required explicit function is,

Solving the equations,

$-2v = 2$

$\therefore v = -1$,

$\therefore u = 5 - 2v = 5 + 2 = 7$

$\therefore u = 7, v = -1$,

* Recurrence relation to find explicit :

Use math induction to prove

i) $1 + 2 + 3 + \dots + n = \frac{n(n+1)}{2}$, $n \geq 1$

ii) $\overline{(A_1 \cap A_2 \cap \dots A_n)} = \bar{A}_1 \cup \bar{A}_2 \cup \dots \cup \bar{A}_n$, $n \geq 2$.

\# Find explicit formula for

iii) $a_n = 4a_{n-1} + 5a_{n-2}$, $a_1 = 1$, $a_2 = 4$ & then find the five consecutive terms.

iv) $f_n = f_{n-1} + f_{n-2}$ with $f_1 = f_2 = 1$.

Solⁿ:

iii) $a_n = 4a_{n-1} + 5a_{n-2}$, $a_1 = 1$, $a_2 = 4$

The given recurrence relation is,

$a_n = 4a_{n-1} + 5a_{n-2}$ with initial conditions $a_1 = 1$ & $a_2 = 4$

This is linear homogeneous recurrence relation of degree 2.

Its characteristic eqⁿ is, $x^2 = 4x + 5 \Rightarrow x^2 - 4x - 5 = 0$.

The roots are $s_1 = 5$ and $s_2 = -1$ which are distinct.

So that, the explicit formula is,

$a_n = us_1^n + vs_2^n$

$\Rightarrow a_n = u \cdot 5^n + v(-1)^n$

~~$\Rightarrow a_n = u + v \cdot 2^n$~~ $\Rightarrow a_n = u\,5^n + v \cdot (-1)^n$

Applying initial conditions, we get

$a_1 = 5u - v \Rightarrow \cancel{u + 2v = 1} \Rightarrow 5u - v = 1$

$a_2 = 25u + v \Rightarrow 25u + v = 4$

Solving these for u and v, we get

$\therefore$ The required explicit function is,

Solving the eqⁿs,

~~$-2v = -3$~~ $\quad 30u = 5 \Rightarrow u = 1/6$, $\therefore v = 5 \times 1/6 - 1$

~~$\therefore v = 3/2$,~~ $\quad$ ~~$\therefore u = 1 - 2 \cdot 3/2 = -2$~~ $\quad = -1/6$

~~$\therefore u = -2, v = 3/2$~~

iv.) $f_n = f_{n-1} + f_{n-2}$ with $f_1 = f_2 = 1$

The given recurrence relation is
$f_n = f_{n-1} + f_{n-2}$ with initial conditions $f_1 = f_2 = 1$.

This is linear homogeneous recurrence relation of degree 2.
Its characteristic eqn is $x^2 = x + 1 \Rightarrow x^2 - x - 1 = 0$
The roots are $s_1 = 1.6$ and $s_2 = -0.6$
So that, the explicit formula is
$\cancel{f_n = us_1^n + vs_2^n}$ $f_n = us_1^n + vs_2^n$
$= u(1.6)^n + v(-0.6)^n \Rightarrow f_n = u(1.6)^n + v(-0.6)^n$

Applying initial condition, we get
$f_1 = 1.6u - 0.6v \Rightarrow 1.6u - 0.6v = 1$
$f_2 = 2.56u + 0.36v \Rightarrow 2.56u + 0.36v = 1$
Then, solving these for u and v, we get
$0.96u - 0.36v = 0.6$
$+\ 2.56u + 0.36v = 1$
$3.52u = 1.6$
$\therefore u = 0.45$
$\therefore v = \frac{1.6u - 1}{0.6} = -0.45$

i.) $1 + 2 + 3 + \dots + n = \frac{n(n+1)}{2}, n \geq 1$

Soln:
~~for basis term $n_0 = 1$~~
Consider the statement.
$P(n): 1 + 2 + \dots n = \frac{n(n+1)}{2}$ with $n_0 = 1$.

Basis step: $P(1): 1 = \frac{1(1+1)}{2}$, which is true.
Induction step:
Suppose $P(t)$ is true, then we claim $P(k+1)$ is true.
Since, $P(k)$ is true, we have
$1 + 2 + 3 + \dots + k = \frac{k(k+1)}{2}$
Now,
$P(k+1): 1 + 2 + 3 + \dots + k + (k+1)$
$= \frac{k(k+1)}{2} + (k+1)$ $\because P(k)$ is true.
$= \frac{(k+2)(k+1)}{2}$
$= \frac{[(k+1)+1](k+1)}{2}$ which is true, hence $P(k+1)$ is true.

Since, $P(1)$ is true, $P(2)$ is true, $P(3)$ is true and so by the principle of mathematical induction, $P(n)$ is true for all $n \geq 1$.