DISCRETE STRUCTURES

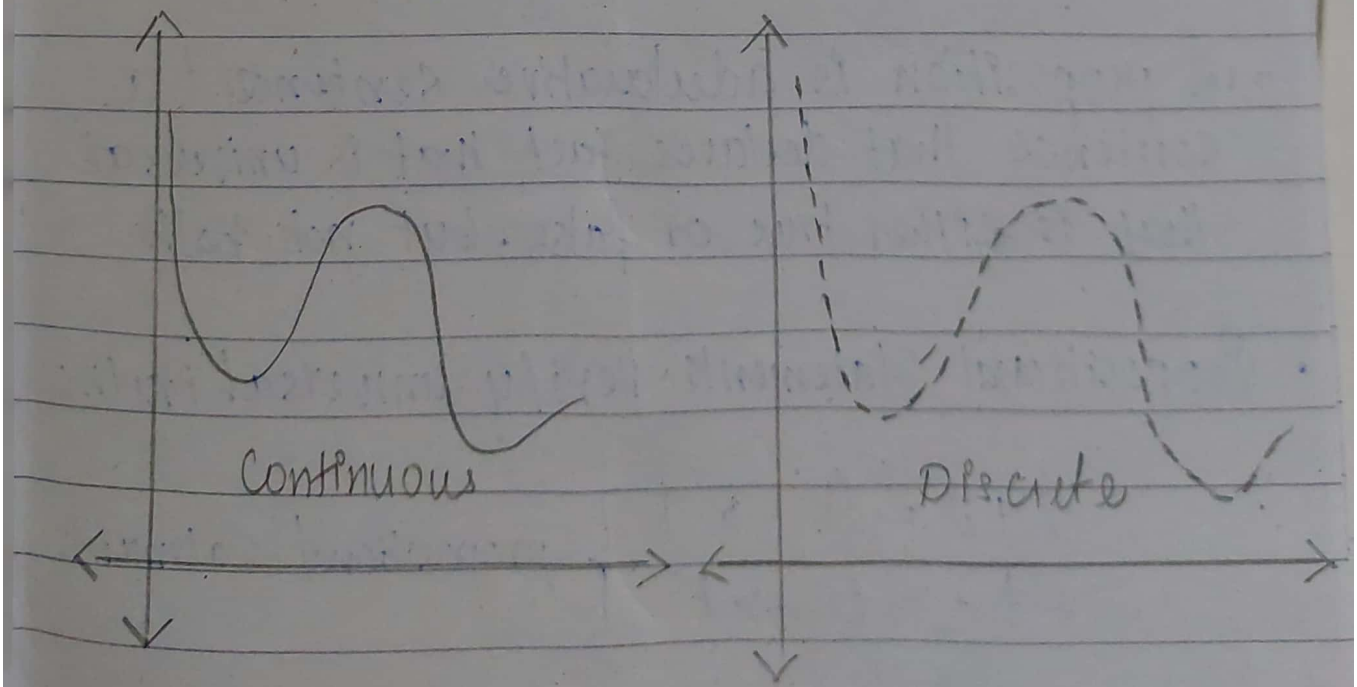
- Discrete mathematics is the mathematical study of properties, and relationships among discrete objects

* CONTINUOUS DATA :

A set of data is said to be continuous if the values belonging to the set can take on any value within a finite or infinite interval. Continuous data falls in a constant sequence or range. Continuous data is information that can be measured on a scale eg. [0, 70].

* DISCRETE DATA :

Discrete data is the type of data that has clear spaces between values. Discrete values are countable and are distinct and separate. eg. {1, 2, 3, 4, 5, 6}.



* EXAMPLES OF DISCRETE DATA:

→ Number of boys in a class
→ Number of questions answered
→ Number of candies picked at random from a jar

* EXAMPLES OF CONTINUOUS DATA:

→ Height of a person
→ BPM of a person
→ Time in a race.

* APPLICATIONS OF DISCRETE MATH:

→ Number theory
→ Public and private key cryptography
→ Graph theory

* PROPOSITIONAL LOGIC:

- A proposition is a declarative sentence (a sentence that declares fact that is universal) that is either true or false, but not both

- Propositional statements verify universal truths

$2+2=4 \rightarrow T$
$2+2=5 \rightarrow F$
} propositional statements

- We need enough information to verify the statement.

- Propositional logic ~~should~~ must follow law of the excluded middle (~~a~~ cannot be partially T/F) and law of contradiction (cannot be both T and F)

- Queries are not propositional statements. They do not hold any action.

* PROPOSITIONAL :

1) Paris is the capital of France
2) Gravitational constant is $6.67 \times 10^{-11} m^3 kg^{-1} s^{-2}$
3) The Earth revolves around the sun
4) Mount Everest is 8848 m high
5) Einstein won the Nobel Prize for his works in Photoelectric Effect.

* NON-PROPOSITIONAL :

1) Come over here
2) $x + 4 > 9$
3) I am stultified
4) Is smoking bad for your health?
5) Sit down.

~~MY WEAK~~

* FOUNDATIONS, LOGICS AND PROOFS

* Propositions: Verify universal truths
  - ↳ Paris is the capital of France
  - ↳ 1+2=3
  - ↳ Earth revolves around the Sun

* Non-Propositional:
  - ↳ Sit over there
  - ↳ 3+4 > 5
  - ↳ x = 2+y ; y >= 10

* Propositional Logic:
  1. Negation
  2. Conjunction
  3. Disjunction
  4. Exclusive OR
  5. Implications
  5.5 6a. Converse, Inverse and Contrapositive
  6. Bi-Implications

① NEGATION : $(\neg p)$

$\neg p \Rightarrow$ "It is not the case that p"

"Today is friday"
Negation ⇒ "It is not the case that today is friday"

~~¬p~~	p	¬p
	T	F
	F	T

② CONJUNCTION : $(p \wedge q)$

p: "Today is friday", q: "It is raining"

$p \wedge q \Rightarrow$ "Today is friday and it is raining"

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

③ DISJU

↳ Inclus
at lea

↳ Exclus
of the
(Stu
o
↳ bu
↳ ei
↳ n

④ Ex

p:
q:
p ⊕

③ DISJUNCTION : $(p \vee q)$

↳ Inclusive OR : The disjunction is true when at least one of the two propositions is true

↳ Exclusive OR : The disjunction is true only when one of the propositions is true.

(Students who have taken computer science OR calculus class, but not both)

↳ but not both

↳ either / or → $(\vee)$

↳ neither / nor → $(\wedge)$

} IMP

p	q	p ∨ q
T	T	T
T	F	T
F	T	T
F	F	F

④ EXCLUSIVE - OR : $(p \oplus q)$

p : Atif will pass the course CS1008

q : Atif will fail the course CS1008

$p \oplus q$ ⇒ Atif will pass or fail the course (but not both at the same time)

$p \oplus q$ ⇒ Either / OR

$$p \oplus q \Rightarrow (p \wedge \neg q) \vee (\neg p \wedge q)$$

p	q	$p \oplus q$
T	T	F
T	F	T
F	T	T
F	F	F

(5) IMPLICATIONS: $(p \rightarrow q)$

"If I am elected I then I will lower taxes"

Implication:

Elected, lower taxes	T	T	T
not elected, lower taxes	F	T	T
not elected, not lower taxes	F	F	T
elected, not lower taxes	T	F	F

p	q	$p \rightarrow q$
T	T	T
T	f	F
f	T	T
f	f	T

for an im
to be false

" If Maria
find a good

IF-THEN

$p \longrightarrow$

some

" If p then
" If p, q"
" p is suffi
" q if p"
" q when p
" q unless -

P4 : 3<
P5 : 3<

(1) P4 → P5
If 3<8
T →

For an implication to fail, only q needs to be false

"If Maria learns discrete math, then she will find a good job" $\rightarrow$ T

~~If-THEN~~

$$p \rightarrow q \Rightarrow \neg p \vee q$$

Some cases of implications

"If p then q"
"If p, q"
"p is sufficient for q"
"q if p"
"q when p"
"q unless $\neg p$"

"p implies q"
"p only if q"
"q whenever p"
"q is necessary for p"
"q follows from p"

$P_4: 3 < 8$
$P_5: 3 < 14$
$P_6: 3 < 2$
$P_7: 8 < 6$

① $P_4 \rightarrow P_5$:
If $3<8$, then $3<14$
$T \rightarrow T: T$

② $p_4 \to p_6$:
If $3<8$, then $3<2$
$T \to F : F$

③ $p_6 \to p_4$:
If $3<2$, then $3<8$
$F \to T : T$

④ $p_6 \to p_7$:
If $3<2$, then $8<6$
$F \to F : T$

5.5 CONVERSE, INVERSE & CONTRAPOSITIVE:

- Converse : $p \to q$ | $q \to p$
- Contrapositive : $p \to q$ | $\neg q \to \neg p$
- Inverse : $p \to q$ | $\neg p \to \neg q$

p	q	¬p	¬q	p→q	¬q→¬p	q→p	¬p→¬q
T	T	F	F	T	T	T	T
T	F	F	T	F	F	T	T
F	T	T	F	T	T	F	F
F	F	T	T	T	T	T	T

$p \to \neg q$ $p \to \neg q$

$\neg q \to p$

p Raining tmrw

q → ~~Not~~ going to Town

"If you get 100% in this course, you will get an A+"

$\neg q \to \neg p$

Contrapositive: "If you donot get 100% in this course, you do not get an A+"

"If you donot get an A+ in this course, you do not get 100%"

$q \to p$

Converse: "If you get an A+ in this course, you will get 100%"

Note: $p \to q \neq q \to p$

$\neg p \to \neg q$

Inverse: "If you donot get 100% in this course, you will not get an A+"

$$p \to q \neq \neg p \to \neg q$$

$$p \to q = q \to p$$

* Important points to consider.

(1) Contrapositive : $p \to q \Rightarrow = \neg q \to \neg p$

$p \to q$ and $\neg q \to \neg p$ are logically equivalent

(2) Converse : $p \to q = q \to p$

However, both are not logically equivalent

(3) Inverse: $p \to q = \neg p \to \neg q$

Both are not logically equivalent

Q) Find the converse, contrapositive and inverse of the following statement:

R: "Raining ~~down~~ tomorrow is a sufficient condition for my not going to town"

p ⇒ It will rain tomorrow
q ⇒ I will not go to town

$\therefore R : p \rightarrow q$

Converse : $q \rightarrow p$

I will not go to town if its raining tomorrow

↓

X bcz q is conclusion therefore q cannot come first

* Correct :

"If I dont go to down then it will rain tomorrow" → NON-SENSE

* Correct (2):

"My not going to down is a sufficient condition for it raining tomorrow"

* Correct (3):

"Raining tomorrow is a necessary condition for my not going to town"

sufficient $\leftarrow p \rightarrow q \rightarrow$ necessary

* Contrapositive:

$$p \to q = \neg q \to \neg p$$

'If it's I don't go to town, then it won't rain'

sufficient

"My going to town is necessary for not raining tomorrow"

* Inverse:

$$p \to q = \neg p \to \neg q$$

"My going to town is necessary for not raining tomorrow"

(b) BI-IMPLICATIONS: $p \leftrightarrow q$

$$p \leftrightarrow q$$

$$p \leftrightarrow q = (p \to q) \wedge (q \to p)$$ Imp

p	q	p → q	q → p	p ↔ q
T	T	T	T	T
T	F	F	T	F
F	T	T	F	F
F	F	T	T	T

* Basically whole

* It is nece be true

(1) "p is for

(2) "if p th

(3) "p if

"For a n necessary not be

"If a it

* Basically, if you get 1 F, then whole statement will be false

* It is necessary for a bi-implications to be true if both statement p and q are true.

(1) "p is necessary and sufficient for q"

(2) "if p then q, and conversely"

(3) "p iff q"

"For a matrix to be invertible, it is necessary and sufficient that its determinant not be zero".

OR

"A matrix is invertible if and only if its determinant is not zero"

Q $xy = 0$ if and only if $x = 0$ or $y = 0$

⇓

If $x = 0$ then $y = 0$, and conversely

* COMPOUND PROPOSITIONS:

$$(p \vee \neg q) \rightarrow (p \wedge q)$$

* Construct Truth table:

p	q	$\neg q$	$p \vee \neg q$	$p \wedge q$	$(p \vee \neg q) \rightarrow (p \wedge q)$
T	T	F	T	T	T
T	F	T	T	F	F
F	T	F	F	F	T
F	F	T	T	F	F

Q) are $(p \rightarrow r) \wedge (q \rightarrow s)$ and $(p \vee q \rightarrow r)$ equivalent? Prove by drawing a truth table.

T	F	T	T	T	F	T
T	F	F	F	T	F	F
F	T	T	T	T	F	T
F	T	F	T	F	F	F
F	F	T	T	T	F	T
F	F	F	T	T	F	T

p	q	r	p→r	q→r	p∨q	(p→r)∧(q→r)	(p∨q)→r
T	T	T	T	T	T	T	T
T	T	F	F	F	T	F	F
T	F	T	T	T	T	T	T
T	F	F	F	T	T	F	F
F	T	T	T	T	T	T	T
F	T	F	T	F	T	F	F
F	F	T	T	T	F	T	T
F	F	F	T	T	F	T	T

Equivalent

Q "If its sunny tomorrow, then I'll go for a walk in the woods"

Contrapositive: Inverse of converse
Inverse: Inverse of Inverse
Converse: Inverse of contrapositive

p ⇒ It's sunny tomorrow
q ⇒ I'll go for a walk in the woods! $\neg q \Rightarrow \neg p$

Contrapositive: ~~I will not go fo~~ (a is conclusion)
If I donot go for a walk in the woods, then it will not be sunny tomorrow. (p is conclusion)

Converse
In contrapositive, p is conclusion

Inverse: If its not sunny tomorrow, then I will not go for a walk in the woods

Converse: If I go for a walk in the woods then it will be sunny tomorrow.

$\neg p$

* Inverse of

If I do
it will

* Inverse of

If its
walk in

* Inverse

If its s

If I q
sunny

a) Ton
on

b) If yo
fail
a pe
Inclusi
pen

* Inverse of converse:

If I don't go for a walk in the wood it will not be sunny tomorrow

* Inverse of Inverse:

If its sunny tomorrow, then I will go for a walk in the woods.

* Inverse of contrapositive:

If its ~~sunny tomorrow, then~~ I will go for a walk

If I go for a walk in the woods, then it will be sunny tomorrow.

a) Tonight I will stay home or go out on a date.

Exclusive bcz not mutually connected

b) If you fail to make a payment on time or fail to pay the amount due, you will incur a penalty

Inclusive bcz you would be incurred a penalty if either of the conditions is not met

$$\begin{bmatrix} 0 & 0 & 1 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1/3 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Reduced Echelon Form

~~X~~ ——— ~~X~~

DISCRETE STRUCTURES

Compound Propositions:

Two or more propositions attached together via logical connectives (eg: implications, bi-implications)

$(p \to q) \wedge (q \to p) \to$ Bicomplications

p	q	$p \leftrightarrow q$
T	T	T
T	F	F
F	T	F
F	F	T

CONVERSELY → If p then q
If q then p

If p denotes "I am at home"
q denotes "It is raining"

$p \leftrightarrow q$ → "I am at home if and only if it is raining"

"p if and only if q"

→ p is necessary and sufficient for q
→ if p then q, and conversely
→ p iff q

Q. Without changing their meanings, convert each of the following sentences into a sentence having the form "p iff q"

1. For a matrix to be invertible, it is necessary and sufficient that its determinant is not zero.

Ans. A matrix is invertible if and only if its determinant is not zero.

$p \vee \neg q$

Q Construct the truth table of the f compound proposition.

$$(p \vee \neg q) \rightarrow (p \wedge q)$$

$\rightarrow (p \vee \neg q)$

p	q	$\neg q$	$p \vee \neg q$	$p \wedge q$	
T	T	F	T	T	T
T	F	T	T	F	F
F	T	F	F	F	T
F	F	T	T	F	F

hypothesis → P
conclusion → Q

Class Activity

1. Mov AL, 255

NESTED QUANTIFIERS:

Nested quantifiers are often necessary to express the meaning of sentences in English.

Example: Every real number has an inverse.

$\forall x \exists y (x + y = 0)$ ⇒ This is because y is additive inverse of x

↳ P(x, y)

$\forall x \exists y P(x, y)$

↓

$Q(x)$

$\forall x\, Q(x)$

$\forall x \forall y P(x, y)$

↳ for all x all y must be executed therefore nested loop

$\forall x \exists y \{ P(x,y)$

↳ termination when x and y are false

* $\forall x \forall y P(x,y) = \forall y \forall x P(x,y)$

↳ same truth value

Example: $x+y = y+x$

* $\forall x \exists y P(x,y) \neq \exists y \forall x \{ P(x,y)$

↳ different truth value

different propositional values

* $\exists x \exists y P(x,y) = \exists y \exists x \ P(x,y)$

↳ same

Define

1) $\forall x$ fa N

2) $\forall x$ Tu x

3) $\exists$ Tu

4)

1)

1)

2

Define $P(x,y) : x \cdot y = 0$

1) $\forall x \forall y P(x,y)$
False
Never true

2) $\forall x \exists y P(x,y)$
True
$x=0, y=R$

3) $\exists x \forall y (Px, y)$
True
$x=R, y=0$

4) $\exists x \exists y P(x,y)$
True
$x=0, y=0$

Define $P(x,y) : x/y=0$

1) $\forall x \forall y P(x,y)$
True

2) $\forall x \exists y P(x,y)$
True

3) $\exists x \forall y P(x,y)$

True

4) $\exists$

8.

$\forall x (C(x) \vee \exists y (C(y) \wedge F(x,y)))$

$C(x)$ is "x has a computer"

$f(x,y)$ is "x and y are friends"

Domain for both x & y consists of all students in school

Every student in your ~~class~~ school has a computer or has a friend who has a computer.

$C(y) \wedge f(x,y)$

↳ y has a computer and a friend

$\exists y (C(y) \wedge f(x,y))$

Some students

"The sum of two positive integers is always positive" into a logical expression.

$x+y$ is >0

$(x+y>0)$

$\forall x \forall y ((x>0) \wedge (y>0) \rightarrow (x+y>0))$

"There is a woman who has taken a flight on every airline in the world"

flight on an airline

$P(w,f)$ "w has taken f"

$\exists w \exists f \forall a (P(w,f) \wedge Q(f,a))$

$B(x,y)$ → brothers
$S(x,y)$ → siblings

- Brothers are sibling.

$$\forall x \forall y \, (B(x,y) \rightarrow S(x,y))$$

- Siblinghood is symmetric
  ↓ between two
  if x is brother of y
  then y is brother of x

$$\forall x \forall y \, (S(x,y) \rightarrow S(y,x))$$

- Everybody loves somebody.

$$\forall x \exists y \, (L(x,y))$$

- There is someone who is loved by everyone.

$$\exists y \forall x \, L(x,y)$$

- There is someone who loves someone

$$\exists x \exists y \, L(x,y)$$

RULES OF INFERENCE

$\forall x\,(Man(x) \longrightarrow Mortal(x))$

Man(Socrates)

$\therefore$ Mortal(Socrates)

↓ function ↳ value / argument

Man(x)

↳ argument

↓ function

If you have a current password then you can log on to the network

"You have a current password"

↳ Premises

p

$p \rightarrow q \quad \therefore \quad \frac{p}{q}$ ↳ conclusion

you logged on successfully

- $((p \to q) \wedge p) \to q$ is tautology
  - ↳ modus ponens
  - * Conclusion is part of premises
  - If p is false,
  - ↳ If you have a password, you can log in $(p \to q)$
    Since you have password, you ~~can~~ are successfully logged in $(\wedge p \to q)$

Let p be "it is snowing"
q be "I will study DS"

$$\frac{p \to q \quad p}{\therefore q}$$

DISCRETE MATH

* Using Rules of Inference to Build Arguments:

- A valid argument is a sequence of statements. Each statement is either a premise or follows from previous called statements by rules of inference. The last statement is conclusion.

$$\begin{array}{l} S_1 \\ S_2 \\ \vdots \\ S_n \\ \therefore C \end{array}$$

* Fallacies:

$$\begin{array}{l} p \text{ is false} \\ q \text{ is true} \end{array}$$

- Arguments are based on tautologies.
- Fallacies are based on contingencies
- The proposition $((p \to q) \wedge q) \to p$ is not a tautology because it is false when p is false and q is True

* SET-BUILDER NOTATION:

$S = \{ x \mid x \text{ is a positive integer less than } 100 \}$

$O = \{ x \mid x \text{ is an odd positive integer less than } 10 \}$

$O = \{ X \in Z^+ \mid x \text{ is odd and } X < 10 \}$

A predicate may be used:

$S = \{ x \mid P(x) \}$
$S = \{ x \mid \text{Prime}(x) \}$ } Functions

$Q^+ = \{ x \in R \mid x = p/q \text{ for some positive integers } p, q \}$

$\{\} = \emptyset$

$\emptyset \neq \{\emptyset\}$

* SUBSETS:

$A \subseteq B \neq B \subseteq A$

$\forall x (x \in A \rightarrow x \in B)$

$A \subseteq B$ ↘ Subset

* EQUALITY SETS:

$A = B$ if

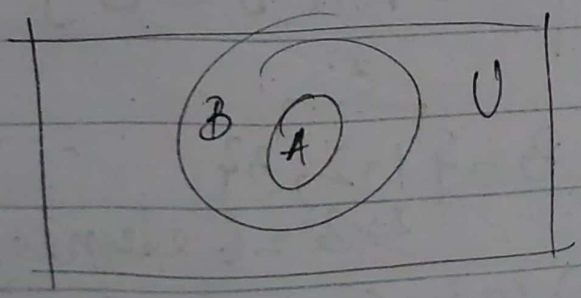
$\forall x (x \in A \leftrightarrow x \in B)$

$\forall x [(x \in A \Rightarrow x \in B) \wedge (x \in B \rightarrow x \in A)]$

PROPER SETS:

If $A \subseteq B$ but $A \neq B$, then we say A is a proper subset of B denoted by $A \subset B$

$\forall x (x \in A \rightarrow x \in B) \wedge \exists x (x \in B \wedge x \notin A)$



* POWER SETS:

If $A = \{a, b\}$ then

$$P(A) = \{\phi, \{a\}, \{b\}, \{a, b\}\}$$

If a set has n elements, then the cardinality of the power set is 2^n

* TUPLE:

Ordered collection that has a_1 as its first element and a_2 as ik second element and so on till an is last element.

2-tuples are called ordered-pairs

* CARTESIAN PRODUCT:

$$A \times B = \{(a, b) \mid a \in A \wedge b \in B\}$$

$A = \{a, b\}$ (2), $B = \{1, 2, 3\}$ (3)

$2 \times 3 = 6$ elements

$A \times B = \{(a,1), (a,2), (a,3), (b,1), (b,2), (b,3)\}$

12 elements.

$A \times B \times C$

$A = \{0,1\}$, $B\{1,2\}$, $C = \{0,1,2\}$

$A \times B \times C = \{(0,1,0),(0,1,1),(0,1,2),(0,2,0),(0,2,1)$
$(0,2,2),(1,1,0),(1,1,1),(1,1,2),(1,2,0),$
$(1,2,1),(1,2,2)\}$

* UNION:

$$\{x \mid x \in A \vee x \in B\}$$

* INTERSECTION:

$$\{x \mid x \in A \wedge x \in B\}$$

* ~~COMPLEMENT~~: DIFFERENCE:

$$A - B = \{x \mid x \in A \wedge x \notin B\} = A \cap \bar{B}$$

* COMPLEMENT:

$$\bar{A} = \{x \in U \mid x \notin A\}$$

* CARDINALITY OF THE UNION OF TWO INTEGERS:

Inclusion - Exclusion

$|A \cup B| = |A| + |B| - |A \cap B|$

(Addition or subtraction of sets is only possible when no. of elements of two sets are same)

$A = \{1, 2, 3, 4\}$
$B \{5, 6, 7, 8\}$

* SYMMETRIC DIFFERENCE:

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

$U = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$
$A = \{1, 2, 3, 4, 8\}$, $B = \{4, 5, 6, 7, 8\}$

* Solution: $\{1, 2, 3, 6, 7, 8\}$

Ans

* IDENTITY

$A \cup \phi = A$

* DOMINATION

$A \cup U = U$

* IDEMPOTE

$A \cup A =$

* COMPLEM

$A \cup \bar{A} =$

A^c or A

* IDENTITY LAWS:

$A \cup \emptyset = A$ $\quad\quad$ $A \cap U = A$

* DOMINATION LAWS:

$A \cup U = U$ $\quad\quad$ $A \cap \emptyset = \emptyset$

* IDEMPOTENT LAWS:

$A \cup A = A$ $\quad\quad$ $A \cap A = A$

* COMPLEMENT LAWS:

$A \cup \bar{A} = U$ $\quad\quad$ $A \cap \bar{A} = \emptyset$

A^c or $A = \{x \in U \mid x \notin$

DISCRETE STRUCTURES

FUNCTIONS

→ Domain → | f(x) | → Range

↓

one-value

domain

↑

$f : A \rightarrow B$ → image

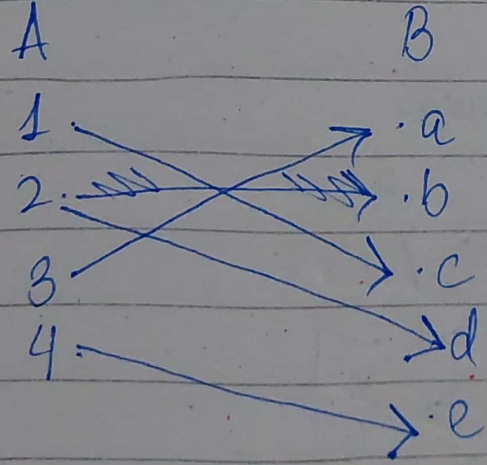
↓ ↓

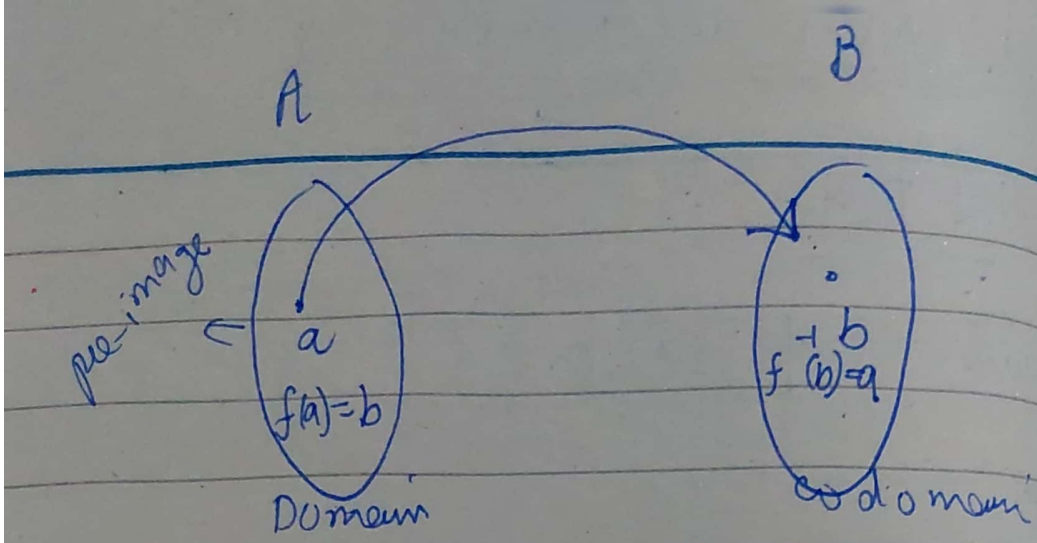
Pre-image codomain

Functions are associated with terminologies of sets in Discrete Math

$A = \{1, 2, 3, 4\}$

$B = \{a, b, c, d, e, f\}$





→ images of A are held in B.

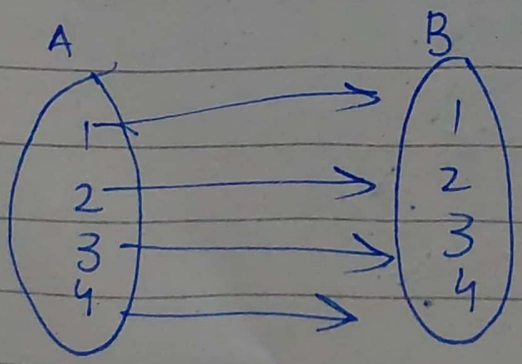
→ Domains only have 1 image

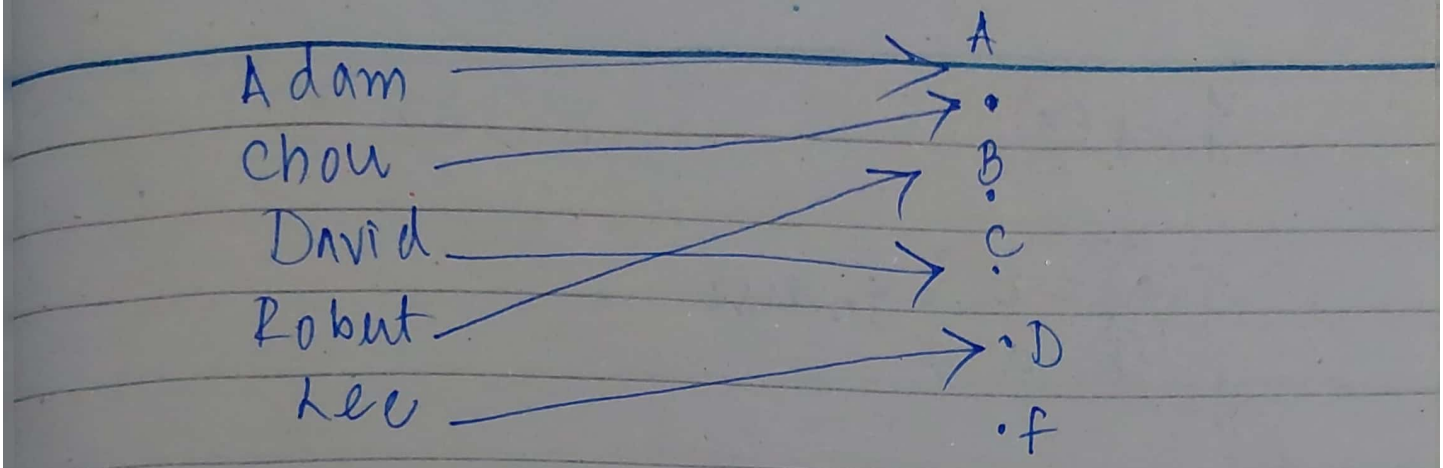
$f(a,b)$

$$\forall x [x \in A \rightarrow \exists y [y \in B \wedge (x,y) \in f]]$$

* Equal functions:

* Same domain
* have same domain





Elements = [A, B, C, D, F]

Range = [A, B, C, D] ← only mapped images

* INJECTIONS:

REAL-VALUED:

$(f_1 + f_2)(x) = f_1(x) + f_2(x)$

$f_1 f_2(x) = f_1(x) \cdot f_2(x)$

IDENTITY:

Domain & codomain are same

$y = f(x)$

$f(a) = b$ } inverse
$f^{-1}(b) = a$

↓ making image into pre-image

$f(x) = \{(x, y)\}$

If fn is not one-to-one, it does not have inverse.

$fog = f(g(x)) = 2g + 3$

$=$

5 → $A \cap C$ $\quad A \cup B = A + B - A \cap B$
4 → $A \cap B$
8 → $A \cap B \cap C$
+7

$A \Rightarrow A \cap C + A \cap B - A \cap B \cap C$
$B \Rightarrow B \cap C + A \cap B - A \cap B \cap C$

IMPLICATION:

$p \rightarrow q$

T	T	T
T	F	F
F	T	T
F	F	T

elected, lower taxes — T T T
not elected, lower taxes — F T T
not elected, not lower taxes — F F T
elected, not lower taxes — T F F

$$p \rightarrow q = \neg p \vee q$$ V.IMP

Converse $p \rightarrow q \neq q \rightarrow p$
Contra tve $p \rightarrow q = \neg q \rightarrow \neg p$
Inverse $p \rightarrow q = \neg p \rightarrow \neg q$

BIMPLICATIONS:

$p \leftrightarrow q$ → XNOR

p	q	$p \leftrightarrow q$
T	T	T
T	F	F
F	T	F
F	F	T

1. $\neg(p \wedge q) \equiv \neg p \vee \neg q$
2. $\neg(p \vee q) \equiv \neg p \wedge \neg q$
3. $p \wedge q \equiv q \wedge p$ } commutative laws
4. $p \vee q \equiv q \vee p$
5. $p \wedge (q \wedge r) \equiv (p \wedge q) \wedge r$ } Associative
6. $p \vee (q \vee r) \equiv (p \vee q) \vee r$ laws
7. $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$ } Distributive
8. $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$ } laws
9. $p \wedge t \equiv p$, $p \vee c \equiv p$ → Identity law
10. $p \vee \neg p \equiv t$; $p \wedge \neg p \equiv c$ → Negation law
11. $\neg(\neg p) \equiv p$ → Double Negation Law
12. $p \wedge p \equiv p$; $p \vee p \equiv p$ → Idempotent law
13. $p \vee t \equiv t$ } universal bound laws
14. $p \wedge c \equiv c$
15. $p \wedge (p \vee q) \equiv p$ } Absorption laws
16. $p \vee (p \wedge q) \equiv p$
17. $\neg t \equiv c$; $\neg c \equiv t$ → Negation of t and c

Q4/ $\neg(p \to q) \equiv p \wedge \neg q$

$\neg(p \to q)$

$\downarrow$

$\neg[\neg p \vee q]$

$p \wedge \neg q$

Q5/ $(p \wedge q) \to (p \vee q)$ Tautology

$\downarrow$

$\equiv \neg(p \wedge q) \vee (p \vee q)$

$\Rightarrow \neg p \vee \neg q \vee (p \vee q)$

$\Rightarrow (\neg p \vee p) \vee (\neg q \vee q)$

$(p \vee q)$ Proved!!

Q6/ $\neg(\neg p \wedge q) \wedge (p \vee q) \equiv p$

L.H.S

$\neg(\neg p \wedge q) \wedge (p \vee q)$

$(p \vee \neg q) \wedge (p \vee q)$

$\downarrow$

$p \vee p \wedge (\neg q \vee q) \Rightarrow c$

$p \vee c$

$\Rightarrow [p]$ $\Rightarrow$ Identity law

$r \to p \quad p \to q \quad \neg p \vee q$

$\neg r \vee p$

Q4/

$\neg[r \vee (q \wedge (\neg r \to \neg p))] \equiv \neg r \wedge (p \vee \neg q)$

L.H.S

$\neg[r \vee (q \wedge (\neg r \to \neg p))]$

$\neg r \wedge \neg(q \wedge (\neg r \to \neg p))$

$\neg r \wedge \neg q \vee \neg(\neg r \to \neg p)$

$\neg r \wedge \neg q \vee \neg[\neg\neg r \vee \neg p]$

$(\neg r \wedge \neg q) \vee (\neg r \vee \neg p)$

~~$\neg r \wedge \neg r \vee \neg p$~~

$\neg[r \vee (q \wedge (\neg r \to \neg p))]$

$\neg r \wedge \neg(q \wedge (r \vee \neg p))$

$\neg r \wedge (\neg q \vee \neg(r \vee \neg p))$

$\neg r \wedge (\neg q \vee (\neg r \wedge p))$

$(\neg r \wedge \neg q) \vee ((\neg r \wedge \neg r) \wedge p))$

$(\neg r \wedge \neg q) \vee (\neg r \wedge p)$

$(\neg r \wedge \neg r) \vee (\neg q \wedge p)$

$p \to q$

$\neg p \vee q$

$\neg[r \vee (q \wedge (\neg r \to \neg p))] \equiv \neg r \wedge (p \vee \neg q)$

$\neg r \wedge \neg(q \wedge (\neg s \to \neg p))$

$\neg r \wedge (\neg q \vee \neg(\neg r \to \neg p))$

$\neg r \wedge (\neg q \vee \neg(r \vee \neg p))$

$\neg r \wedge (\neg q \vee \neg r \wedge p)$

$(\neg\neg r \wedge \neg q) \vee ((\neg r \vee \neg r) \wedge p)$

$(\neg\neg r \wedge \neg q) \vee (\neg r \wedge p)$

$(\neg r \overset{\wedge}{\star} \neg r) \vee (\neg q \wedge p)$

$\neg r \vee (\neg q \wedge p)$

$\neg r \wedge (p \vee \neg q)$ Proved

$\neg(p \leftrightarrow q) \equiv p \leftrightarrow \neg q$

L.H.S

$\neg(p \leftrightarrow q)$

$\neg[(p \to q) \overset{\vee}{\star} (q \to p)]$

$\neg[(\neg p \vee q) \overset{\wedge}{\star} (\neg q \vee p)]$

$\neg(\neg p \vee q) \overset{\vee}{\star} \neg(\neg q \vee p)$

$(p \wedge \neg q) \overset{\wedge}{\star} (q \wedge \neg p)$

$(p \overset{\wedge}{\star} q) \overset{\vee}{\star} (\neg q \wedge \neg p)$

$\neg(p \leftrightarrow q) \equiv p \leftrightarrow \neg q$

$\neg(p \leftrightarrow q)$

$\neg((p \rightarrow q) \wedge (q \rightarrow p))$

$\neg((\neg p \vee q) \wedge (\neg q \vee p))$

$\neg(\neg p \vee q) \vee \neg(\neg q \vee p)$

$(p \wedge \neg q) \vee (q \wedge \neg p)$

$((p \wedge \neg q) \vee q) \vee ((p \wedge \neg q) \wedge p)$

$((p \wedge \neg q) \vee q) \wedge ((p \wedge \neg q) \vee \neg p)$

$\Rightarrow ((p \vee q) \wedge (\neg q \vee q)) \wedge ((p \wedge \neg p) \wedge (\neg q \vee \neg p))$

$\Rightarrow ((p \vee q) \wedge T) \wedge (T \wedge (\neg q \vee \neg p))$

$= (p \vee q \wedge T) \wedge T \wedge (\neg q \vee \neg p)$

$(p \vee q) \wedge (\neg q \vee \neg p)$

$= p \leftrightarrow \neg q$

$p \leftrightarrow q = (\neg p \vee q) \wedge (\neg q \vee p)$

$\hookrightarrow (p \rightarrow q) \wedge (q \rightarrow p)$

$p \leftrightarrow \neg q = (p \vee q) \wedge (\neg q \vee \neg p)$

$(p \wedge q) \vee p \Rightarrow p$

$p \vee (p \wedge q) = (p \vee p)$

$(p \wedge s) \wedge (p \to q) \wedge (q \to \neg r)$ $(p \vee q)$

$\Rightarrow (p \wedge s) \wedge (p \to q) \wedge (q \to \neg r)$

$\Rightarrow p \wedge (p \to q) \wedge (q \to \neg r)$

$\Rightarrow p \wedge (\neg p \vee q) \wedge (\neg q \vee \neg r)$

$\Rightarrow (p \wedge \neg p) \vee (p \wedge q) \wedge (\neg q \vee \neg r)$

$F \vee (p \wedge q) \wedge (\neg q \vee \neg r)$

$p \wedge (p \to q) \wedge (q \to \neg r)$

$q \wedge (q \to \neg r)$

$(p \wedge (p \to q)) \to q \Rightarrow$ Modus Ponen

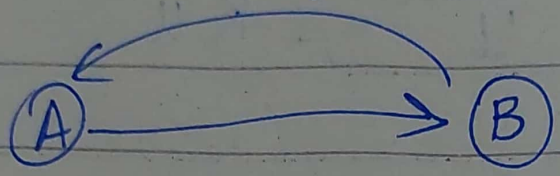
$(\neg q \wedge (p \to q)) \to p \Rightarrow$ Modus Tolen

$((p \to q) \wedge (q \to r)) \to (p \to r) \Rightarrow$ Hypothetical syllogism

$((p \vee q) \wedge \neg p) \to q \Rightarrow$ Disjunctive Syllogism

Symmetric Relations:

All links in graphs are bidirectional



Let $A = \{1, 2, 3, 4\}$

$R_2 = \{(1,1), (2,2), (3,3), (4,4)\}$
$R_3 = \{(1,1), (1,2)\}$

R_2 is symmetric and vacuously true
R_3 is symmetric but not reflexive

Irreflexive

$R_1 = \{(1,1), (2,2), (3,3)\}$

Symmetric and anti-symmetric

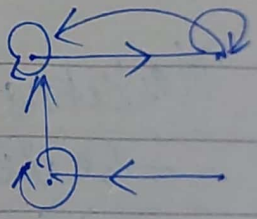
- All links should be bidirectional

Asymmetric:

→ Irreflexive and anti-symmetric

Q $R_1 = \{(1,1), (1,2), (2,1), (2,2), (3,4), (4,1), (4,4)\}$

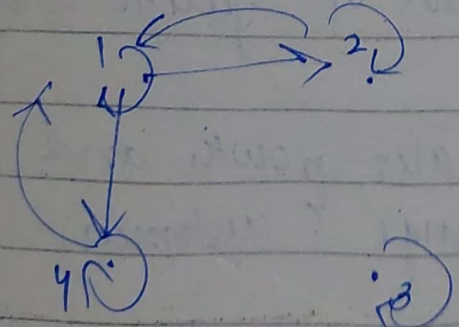
Reflexive and symmetric



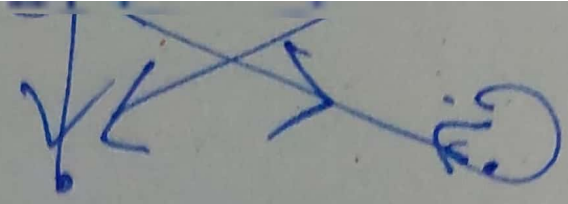
$R_2 = \{(1,1), (1,2), (2,1)\}$

Symmetric and ~~reflexive~~

$R_3 =$



Symmetric and



R_4 = Transitive

R_5 = Symmetric, reflexive

R_6 = Neither

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

MARKETING INFORMATION AND RESEARCH:

GRAPHS

* Handshaking Theorem & Edges
UNDIRECTED

Sum of degrees of all vertices
2
= No. of edges

* How many edges are there in a graph with 10 vertices of degree six?

Sum of ~~all~~ degrees of all vertices = $6 \times 10 = 60$

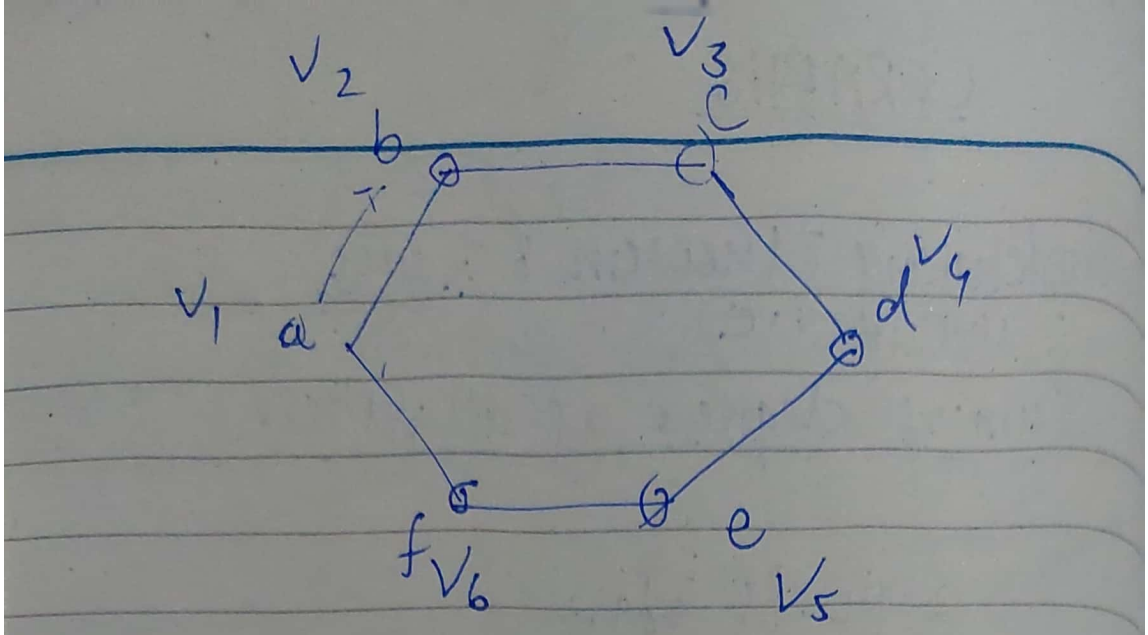
$2m = 60$
$\therefore m = 30 \longrightarrow$ even

→ Loop degree in undirected graph is 2
→ Loop degree in directed graph is 1

→ deg^+ = Outgoing
→ deg^- = Incoming

Directed graph theory:

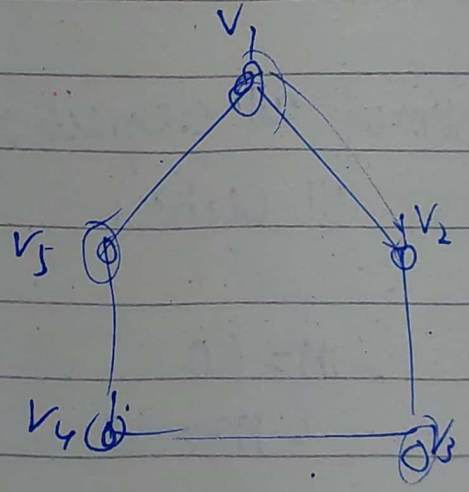
$\sum deg^+ = \sum deg^- = |E|$



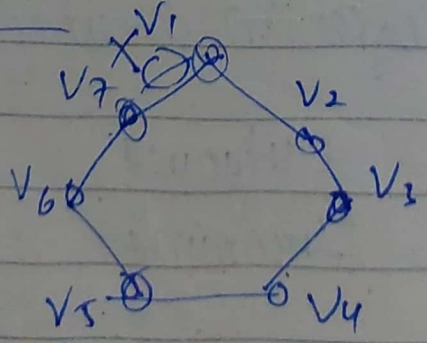
$V_1 = \{a, b, c\}$
$V_2 = \{d, e, f\}$

$V_1 = \{v_1, v_3, v_5\}$
$V_2 = \{v_2, v_4, v_6\}$

$V_1 = \{$
$V_2 =$
$V_3 =$
$V_4 =$
$V_5 =$
$V_6 =$



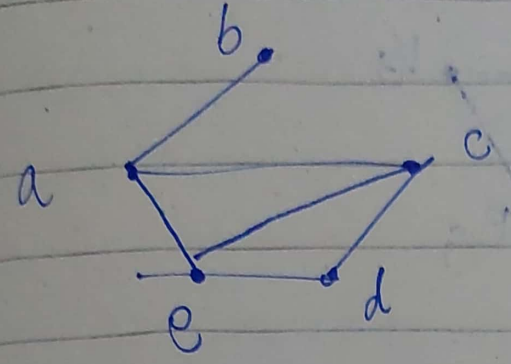
$V_1 = \{v_1, v_3, v_5\}$
$V_2 = \{v_2, v_4\}$



$V_1 = \{v_1, v_3, v_5, v_7\}$
$V_2 = \{v_2, v_4, v_6\}$

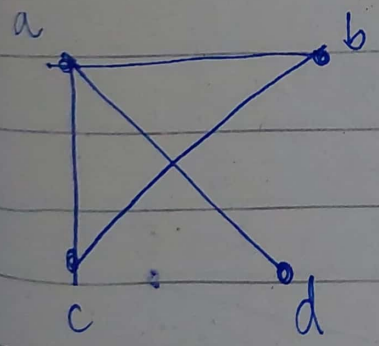
REPRESENTATION OF GRAPHS

ADJACENCY LISTS



Vertex	Adjacent vertices
a	b, c, e
b	a
c	a, d, e
d	c, e
e	a, c, d

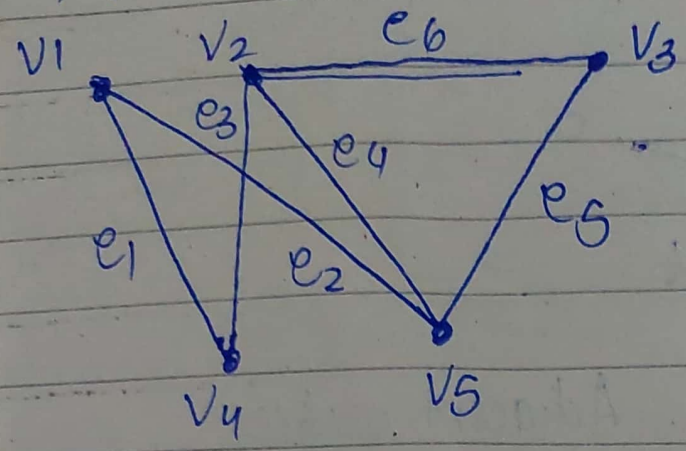
ADJACENCY MATRICES:



$$\begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}$$

edges

* INCIDENCE MATRICES:

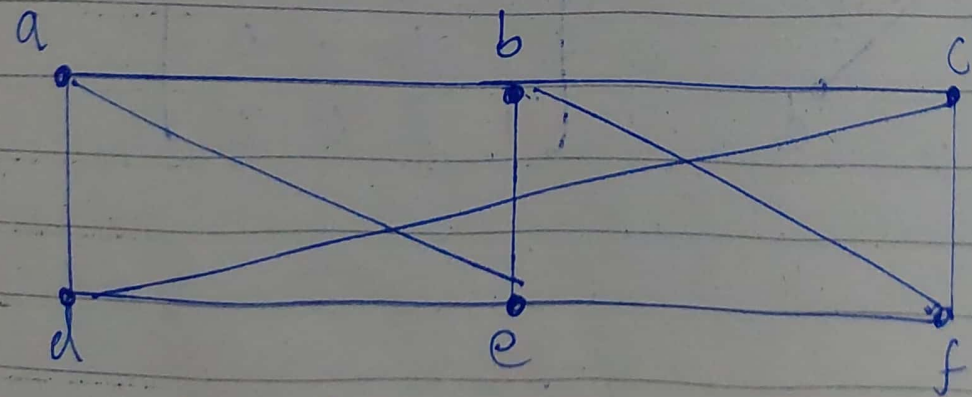


	e_1	e_2	e_3	e_4	e_5	e_6
v_1	1	0	1	0	0	0
v_2	0	0	1	1	0	1
v_3	0	0	0	0	1	1
v_4	1	0	1	0	0	0
v_5	0	1	0	1	1	0

rows : V
columns : e

CONNECTIVITY

* PATHS

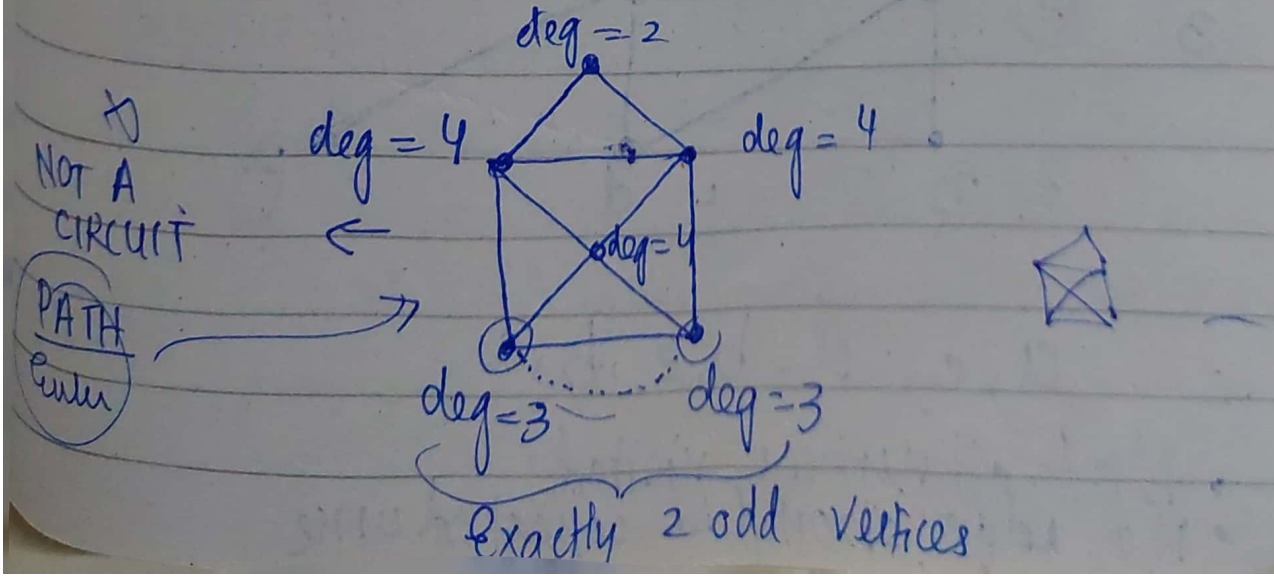


a, d, c, f, e is a path of length
d, e, c, a is not a path

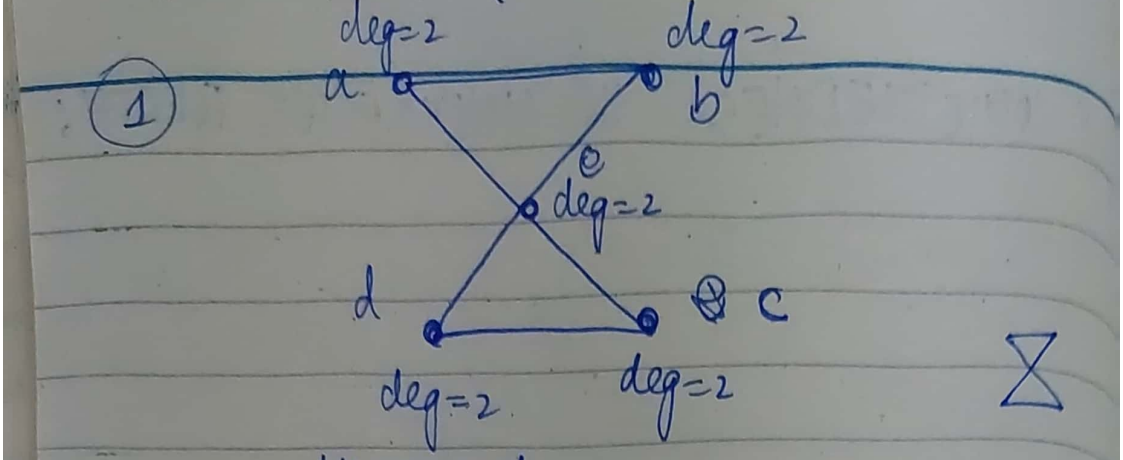
EULER AND HAMILTONIAN GRAPHS

*Euler Theorem:

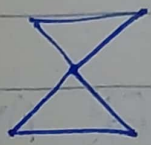
↳ don't visit the already visited graph twice
↳ visit all vertices
↳ No edge should visit more than once
↳ For Euler circuit every vertex has the ~~degree~~ even degree and the initial and final vertex have same degree
↳ for Eulers path there must be exactly two odd vertices



circuit



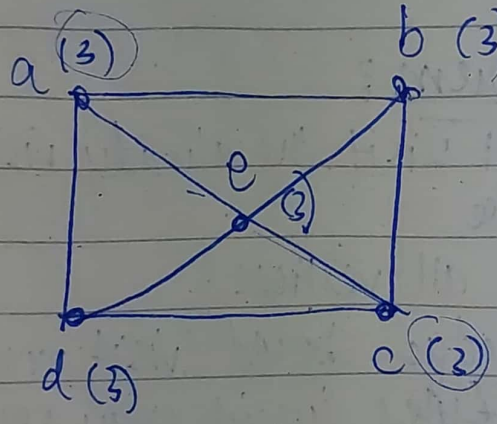
All even degrees



(1) {a, b, e, c, d, e, a}

(2) {a, b, e, d, c, a}

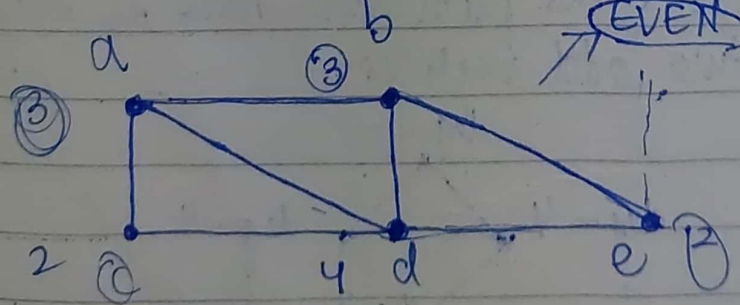
(2)



NOT A CIRCUIT

* source & destination should have same EVEN degree

(3)



a, e, d, b, e, b, a

- Not all vertices visited

HAMILTONIAN CYCLE:

* U should ~~not~~ visit all vertices
* U should not visit the same vertex more than once.

eg.

① Not a Hamiltonian cycle, but a Hamiltonian path

{ⓐ, b, e, d, c, ⓐ} → No repetition allowed

② {ⓐ, b, e, c, d, ⓐ} → repitition

Hamiltonian cycle

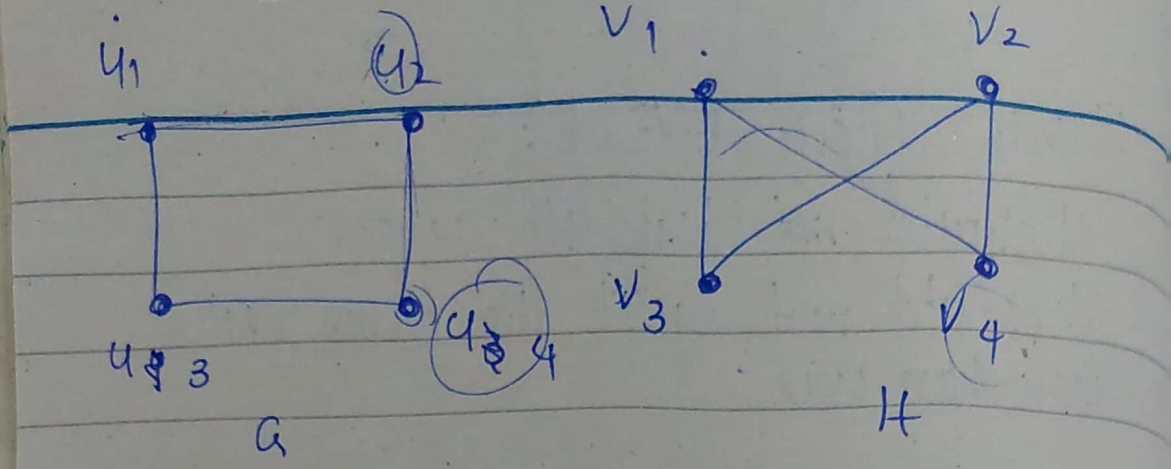
③ Hamiltonian cycle

ISOMORPHISM of GRAPHS

→ One-one & onto function exists (bijective functions)
→ All images are unique
→ Shapes can be and cannot be same, but no. of vertices and edges must be same

$u_4 \Rightarrow u_3, u_4, u_2$

$v_2 \Rightarrow v_3$ and v_2



* $f(u_1) = v_1$
* $f(u_2) = v_4$
* $f(u_3) = v_3$
* $f(u_4) = v_2$

→ This is because in G, u_2 is connected to u_1 and u_3, whereas in H, v_2 is connected to v_3 and v_4, therefore $f(u_2) \neq v_2$

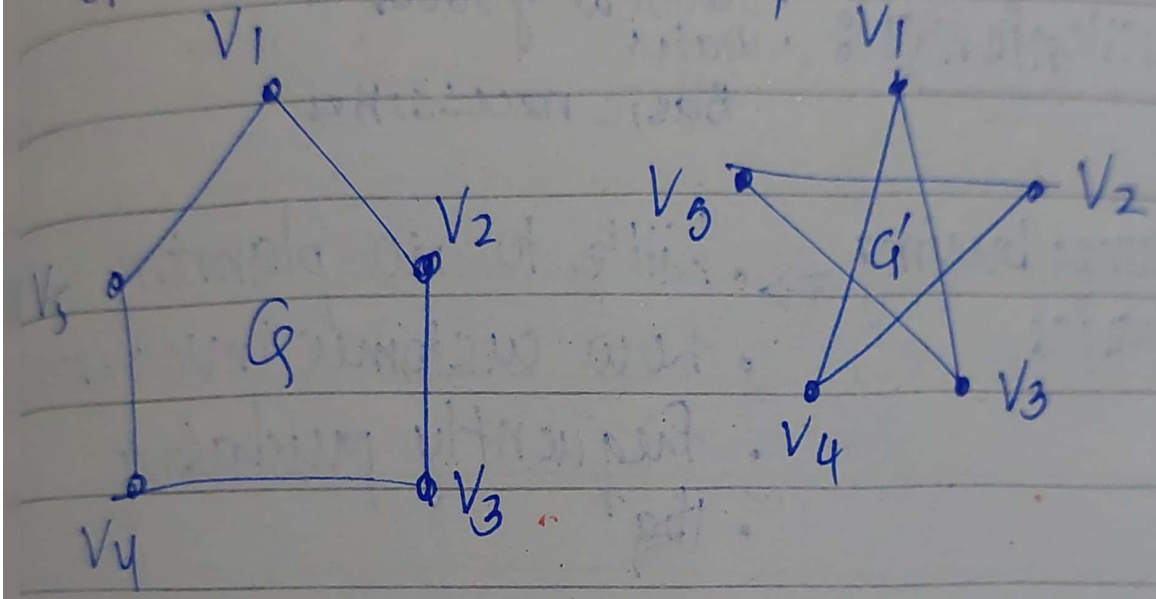
→ Always check for corresponding vertices

- u_2 is connected to u_3 and u_4
- v_4 is connected to v_1 and v_4

Similarly:

Friday : Quiz and Assignment submission

Show that graphs $G(V,E)$ and $G' = (W,f)$ are isomorphic



$f(V_1) = V_1$, $f(V_2) = V_3$, $f(V_3) = V_5$ and $f(V_4) = V_2$ is a one-one correspondence b/w V and W

DISCRETE STRUCTURES

Weighted graphs:

Graphs that have a number assigned to each edged are called weighted graphs

- Fares
- Flight time
- miles
- capacity

* DIJKSTRA's ALGORITHM:

→ Finding the shortest path

Exercise: Solve two problems

Travelling salesman:

Shortest circuit path

Hamiltonian cycle.

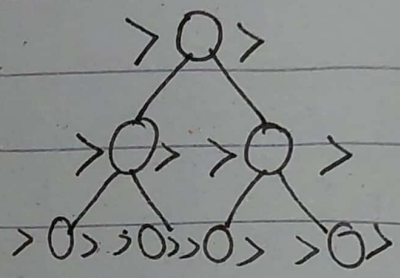
Weighted graphs

Max possible paths = $(n-1)!$

n = no. of nodes

* BINARY SEARCH TREE :

- Vertices are labeled with items so that a label of a vertex is greater than the labels of all vertices in the left subtree of this vertex and is less than the labels of all vertices in the right subtree of this vertex
- 0, 1, 2 child



- Preorder traversal :
  Root → left → right
- Inorder traversal :
  left → root → right
- Postorder traversal :
  left → right → root

* Expression Tree:

- Infix trees are made via operators (nodes) and operands (edges)

- Prefix notation: Solve from r.h.s

1st operator picked ↓ right-left

+ - * 2 3 5 / ↑ 2 3 4

2↑3 = 8

+ - * 2 3 5 / 8 4

8/4 = 2

+ - * 2 3 5 2

2*3 = 6

+ - 6 5 2

- 1 2

1 + 2 = 3 Ans

- Postfix Notation: left-left

7 2 3 * - 4 ↑ 9 3 / +

2*3

7 6 - 4 ↑ 9 3 / +

7-6

1 4 ↑ 9 3 / +

1↑4

1 9 3 / +

9/3

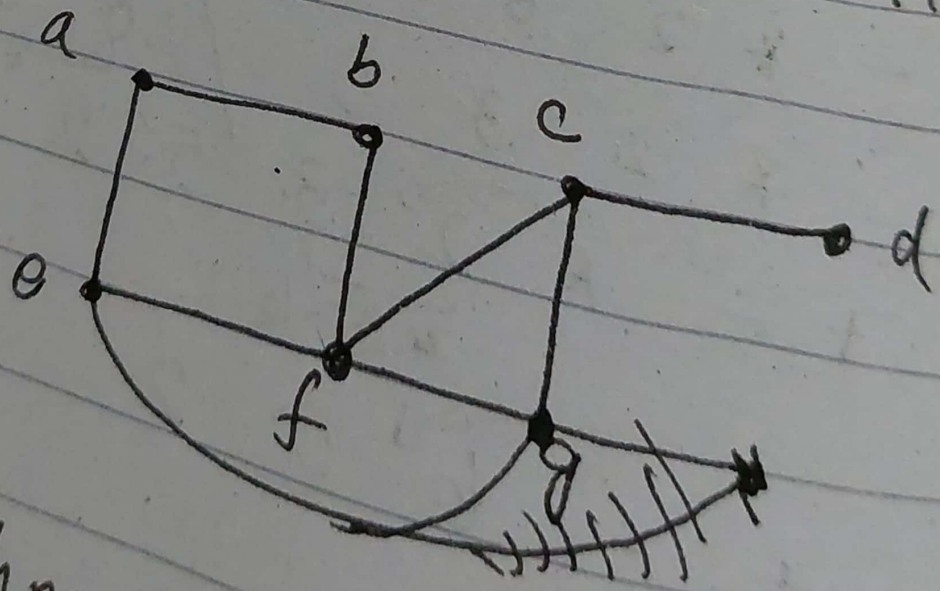
1 3 +

1 + 3 = 4 Ans

• Spanning Tree:

Let G be a simple graph. A spanning tree of G is a subgraph of G that never forms a simple circuit a tree containing every vertex of G.

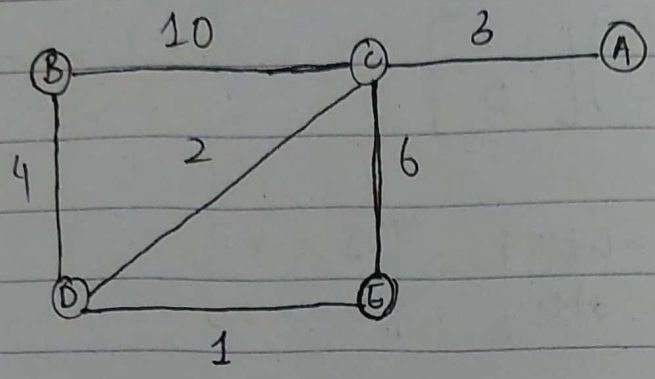
• Undirected graphs subgraph.
• Weight of spanning tree
• Neither Hamiltonian nor Eulea circuit



ns' Algorithm:

MST → minimum spanning tree
ignore edges that form cycle.

* PRIM'S ALGORITHM :



* First we have to select the minimum edge
* Then continue selecting on minimum edge but they must be connected to the edge we selected previously.
* Continue this process until MST formed with minimum weight and MST have all the vertices of the graph

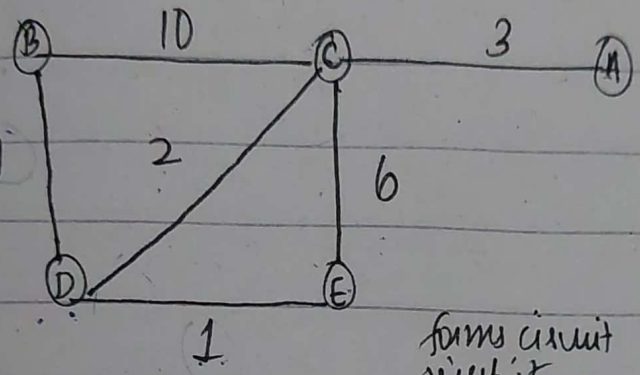
* KRUSKAL'S ALGORITHM :

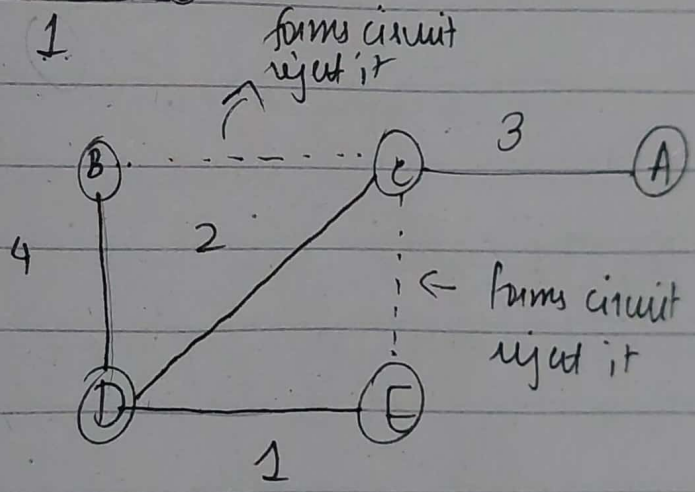
* First sort all the edges of the graph from low to high weight
* Then start the MST by selecting minimum edge from the sorted edge
* (If during selection edges are not connected to the selected edges then its not a problem according to Kruskal. But we have to reject the minimum edge that forms simple circuit)

formed

* Continue this process until MST with minimum weight and MST must have all the vertices of the graph.

① Prims Algorithm method:





② Kruskal Algorithm method:

DE = 1

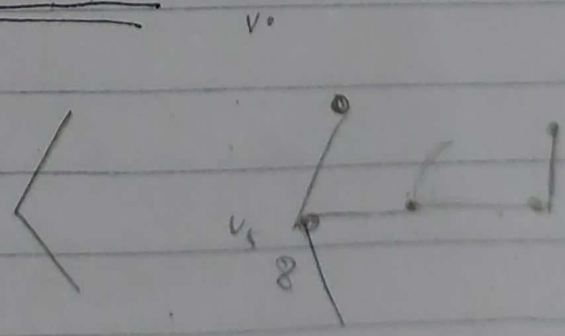
CD = 2

AC = 3

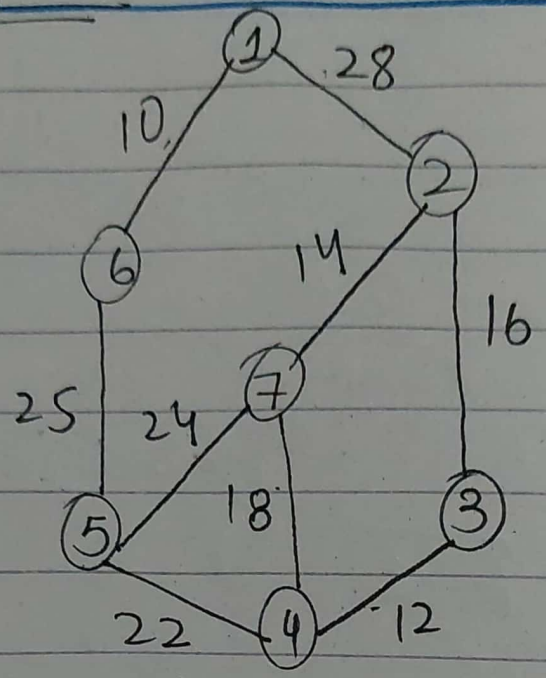
BD = 4

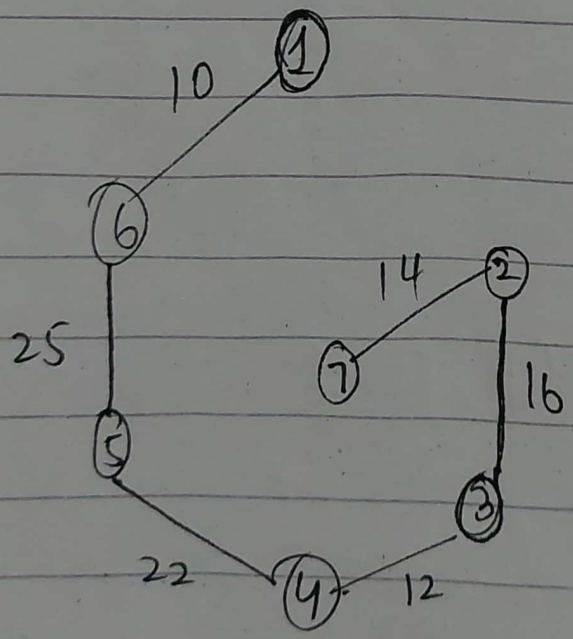
CE = 6

BC = 10



Prim's Algorithm:

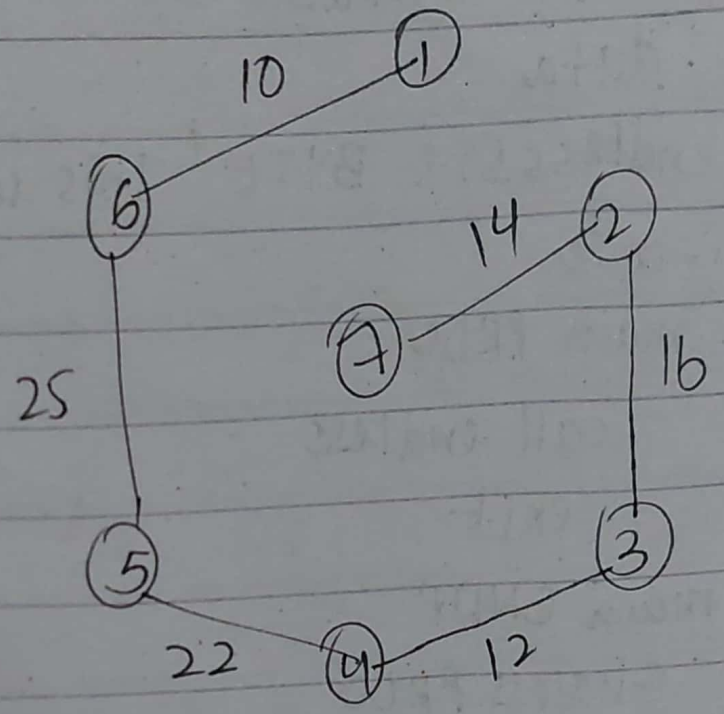




MST = 99 | Ans

* Kruskal's Algorithm *

(6,1) = 10
(4,3) = 12
(7,2) = 14
(3,2) = 16
(7,4) = 18
(4,5) = 22
~~(5,7) = 24~~
(6,5) = 25
(1,2) = 28



NUMBER THEORY AND CRYPTOGRAPHY

* Division:

$a|b \Rightarrow b/a$

↓ a divides b

↓ b is divided by a

↗ pipe

$2|8 \Rightarrow 8/2 \Rightarrow 4$

$3|7 \Rightarrow 7/3$

$3|12 \Rightarrow 12/3 \Rightarrow 4$

(c) ⇒ quotient

(a) ⇒ divisor

(b) ⇒ divident

$b = ac$

* PROPERTIES OF DIVISIBILITY:

Theorem 1: Let a, b and c are integers, where $a \neq 0$

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

ii) If $a|b$, then $a|bc$ for all integer c;

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

i) Proof of i):

* Suppose a|b and a|c, then it follows that there are integers s and t with b = as and c = at. Hence

b + c = as + at = a(s + t)

* c > a & b

Hence, a|(b+c)

c should always be greater than a & b

a = 2, b = 8, c = 4

a|(b+c)	a|b	a|c
2|12 ⇒ $\frac{12}{2}$ ⇒ 6	$\frac{8}{4} = 2$	$\frac{4}{2} = 2$

ii) Proof of ii):

iii) Proof of iii):

* Suppose a, b and c are arbitrarily chosen integers such that a|b and b|c.

a|c ⇒ c = a(some integer)

a|b ⇒ b = ar

b|c ⇒ c = bs

↳ (ar)s → a(rs) → aK

∴ c = aK

proved!

* DIVISION A

→ When an integer, the

a = d

* Where

• d is divi

• a is divi

• q is quo

• r is remo

Example:

Q) What are

101 is d

dq + r =

q = 9

r = 2

Q) What

−11

q = −

r = 1

* Remem

* DIVISION ALGORITHM:

→ When an integer is divided by a positive integer, there is a quotient and a remainder.

$$a = dq + r$$

* Where
  - d is divisor
  - a is dividend
  - q is quotient
  - r is remainder (remainder is always >= 0)

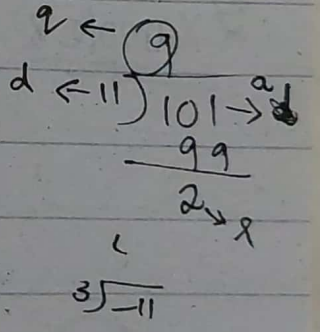
Example:

Q what are quotient and remainder when 101 is divided by 11?

$dq + r = a$

$q = 9$ 101 div 11

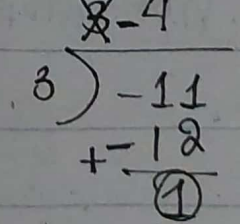
$r = 2$ 101 mod 11



Q) What are quotient and remainder when -11 is divided by 3?

$q = -4$

$r = 1$



* Remainder should always be positive or 0.

* CONGRUENCE RELATIONS :

If a and b are integers and m is a positive integer, then a is congruent to b modulo m if m divides a - b.

- $a \equiv b \pmod{m} \Rightarrow$ a is congruent to b modulo m
- $a \equiv b \pmod{m}$ is a congruence and m is its modulus
- If a is not congruent to b modulo m, we write
  $a \not\equiv b \pmod{m}$

Example : Determine where 17 is congruent to 5 modulo 6 and whether 24 and 14 are congruent modulo 6.

- $17 \equiv 5 \pmod{6}$ because $17 - 5 = 12$
- $24 \not\equiv 14 \pmod{6}$ since 6 divides $24 - 14 = 10$ is not divisible by 6

k is the factor m is using to divide a-b

Theorem 4:

* Let m be a positive integer. The integers a and b are congruent modulo m iff there is an integer such that $a = b + km$

Proof:

If $a \equiv b \pmod m$, then $m | a-b$.
Hence there is an integer k such that $a - b = km$ and equivalently $a = b + km$

Conversely, if there is an integer k such that $a = b + km$ then $km = a - b$.
Hence $m | a-b$ and $a \equiv b \pmod m$

* EXAMPLE: $17 \equiv 5 \pmod 6$

$17 = 5 + 6K$

$\frac{12}{6} = K$

$\boxed{K = 2}$

Theorem 3:

- The use of "mod" in $a \equiv b \pmod m$ and $a \bmod m = b$ are different

$a \equiv b \pmod m$ ↓ applied on a & b

$a \bmod m = b$ ↓ applied on a

- If $a \equiv b \pmod m$ is a relation on the set of integers ($\equiv$ is a relation)
- In $a \bmod m = b$, the notation "mod" denotes a function.

* CONGRUENCIES OF SUMS AND PRODUCTS:

Let m be a positive integer. If $a \equiv b \pmod m$ and $c \equiv d \pmod m$, then $\Rightarrow$ same (mod m)

* $a + c \equiv b + d \pmod m$
* $ac \equiv bd \pmod m$

same mod m

EXAMPLE:

$a \leftarrow 7 \equiv 2 \pmod 5$ (b)

$7 - 2 = 5K$

$\frac{5}{5} = K$

$\boxed{K = 1}$

$c \leftarrow 11 \equiv 1 \pmod 5$ (d)

$\boxed{K = 2}$

* $7 + 11 = 2 + 1 \pmod 5$

$18 = 3 \pmod 5$

$3 = 3$

$7 \cdot 11 = 2 \pmod 5$

$77 - 2 = \text{mod } 5K$

$\frac{75}{5} = K \quad K = 15$

* ALGEBRAIC MANIPULATION OF CONGRUENCIES:

(1) Multiplying both sides of a valid congruence by an integer preserves validity

If $a \equiv b \pmod{m}$ holds then

$c \cdot a = c \cdot b \pmod{m}$, where c is any integer, holds Theorem 5 with $d = c$

(2) Adding an integer to both sides of a valid congruence preserves validity

If $a \equiv b \pmod{m}$ holds then

$c + a \equiv c + b \pmod{m}$, where c is any integer.

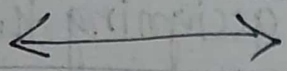
(3) Dividing a congruence by an integer does not always produce a valid congruence.

EXAMPLE:

$14 \equiv 8 \pmod{6} \not\equiv 7 \equiv 4 \pmod{6}$

* ADDITION FACTOR IS PRESERVED
* MULTIPLICATION FACTOR IS PRESERVED
* DIVISION FACTOR IS NOT PRESERVED

↳ platforms like this are available for software practitioners to solicit help and solutions to their problems.



* APPLICATIONS OF CONGRUENCES:

1) Hashing functions
2) Pseudorandom Numbers
3) Check digits

1) Hashing functions:

Converts a given numeric or alphanumeric key to a practical integer value.

A hashing function h assigns memory location h(k) to the record that has k as its key.

- A common hashing function is $h(k) = k \bmod m$ where m is no. of memory locations.
- Because this hashing function is onto, all memory locations are possible.

Example: $h(k) = k \bmod 111$

This hashing function assigns the records of customers with social security numbers as keys to memory locations in the following manner: (memory address)

$h(064212848) = 064212848 \bmod 111 = 14$

$h(037149212) = 037149212 \bmod 111 = 65$

$h(107405273) \Rightarrow 14$; however occupied hence 15

- hashing function is one-to-one as there are many more possible keys than memory locations. When more than one record is assigned to the same location, we say a collision occurs.
- A collision is resolved by assigning the record to first free location.

* Use linear-probing function:

$$h(k, i) = (h'(k) + i) \bmod m,$$

where i runs from 0 to $m-1$

- hash functions are not reversible
- It is more suited that m is a prime number as that can make sure the keys are more uniformly distributed.

2) Pseudorandom Numbers:

→ Randomly chosen numbers are needed for many purposes including computer simulations

→ These numbers are not truly random since they are generated by systematic methods.

→ Linear congruential method is one commonly used procedure for generating pseudorandom numbers

→ 4 integers are needed: modulus m, multiplier a, increment c, and seed x_0 with $2 \le a < m$, $0 \le c < m$, $0 \le x_0 < m$

→ Recursive funct

$x_{n+1} =$

Example: Fir

numbers generat

with modulus m

and seed $x_0 = 3$

$x_1 = 7x_0 + 4 \bmod$

$x_2 = 7x_1 + 4 \bmod$

$x_3 = 7x_2 + 4 \bmod$

$x_4 = 7x_3 + 4 \bmod$

$x_5 = 7x_4 + 4 \bmod$

$x_6 = 7x_5 + 4 \bmod$

$x_7 = 7x_6 + 4 \bmod$

$x_8 = 7x_7 + 4 \bmod$

$x_9 = 7x_8 + 4 \bmod$

3, 7, 8, 6, 1,

9 terms

3) Check Digits

* UPCs: Un

→ A common m

digits is to a

evaluated usin

correct, then th

→ Recursive function

$$x_{n+1} = (ax_n + c) \bmod m$$

Example: Find the sequence of pseudorandom numbers generated by the Linear Congruential method with modulus $m=9$, multiplier $a=7$, increment $c=4$ and seed $x_0 = 3$

$x_1 = 7x_0 + 4 \bmod 9 = 21 + 4 \bmod 9 = 25 \bmod 9 = 7$

$x_2 = 7x_1 + 4 \bmod 9 = 53 \bmod 9 = 8$

$x_3 = 7x_2 + 4 \bmod 9 = 60 \bmod 9 = 6$

$x_4 = 7x_3 + 4 \bmod 9 = 46 \bmod 9 = 1$.

$x_5 = 7x_4 + 4 \bmod 9 = 11 \bmod 9 = 2$

$x_6 = 7x_5 + 4 \bmod 9 = 18 \bmod 9 = 0$

$x_7 = 7x_6 + 4 \bmod 9 = 4 \bmod 9 = 4$

$x_8 = 7x_7 + 4 \bmod 9 = 32 \bmod 9 = 5$

$x_9 = 7x_8 + 4 \bmod 9 = 39 \bmod 9 = 3$

3, 7, 8, 6, 1, 2, 0, 4, 5, 3..... repeated after 9 terms

3) Check Digits:

* UPCs: Universal Product Codes

→ A common method of detecting errors in strings of digits is to add an extra digit at the end, which is evaluated using a function. If the final digit is not correct, then the string is assumed not to be correct.

$9 \overline{)20}$ r 2 ; $10 \overline{)00000}$; $10 \overline{)100}$ r 0 ; $10 \overline{)98}$ r 8 ; $10 \overline{)98}$ r 8 ; $98 + x_{12} = 2$ (mod 10)

Example:

Retail producers are identified by their Universal Product Codes (UPCs). Usually these have 12 decimal digits, the last one being the check digit. The check digit is determined by the congru

$$3x_1 + x_2 + 3x_3 + x_4 + 3x_5 + x_6 + 3x_7 + x_8 + 3x_9 + x_{10} + 3x_{11} + x_{12} \equiv 0 \pmod{10}$$

a. Suppose that the first 11 digits of the UPC are 79357343104. What is the check digit?

$3 \cdot 7 + 9 + 3 \cdot 3 + 5 + 3 \cdot 7 + 3 + 3 \cdot 4 + 3 + 3 \cdot 1 + 0 + 3 \cdot 9 + x_{12} \equiv 0 \pmod{10}$

$21 + 9 + 9 + 5 + 21 + 3 + 12 + 3 + 3 + 0 + 12 + x_{12} \equiv 0 \pmod{10}$

$98 + x_{12} \equiv 0 \pmod{10}$

~~$x_{12} \equiv 0 \pmod{10}$~~

$98 + x_{12} = 0 + 10k$

$98 + x_{12} = 10k$

$\frac{98 + x_{12}}{10} = k$

$10 \overline{)100}$ r 0 ; $98 + 2 = 100$

$\frac{98 + 2}{10} = k \therefore$ ~~k~~ = ~~m~~ $\boxed{x_{12} = 2}$

$a = dq + r$

$-98 = (10)(-10) + r$

$\boxed{r = 2}$

$x_{12} = -98 \bmod 10$

$10 \overline{)-98}$; $-98 + 100 = 2$

$10 \overline{)-98}$; $-98 + 90 = -8$

$-8 + 10 \rightarrow 21$

* ISBN:

$x_{10} =$

a) Suppose that 0072 88008

$x_{10} = 1 \cdot 0 + 2 \cdot 0 + 3 \cdot 7$

$x_{10} = 21 + 8 + 40$

$x_{10} = 197 \pmod{}$

$x_{10} = 117 + 7$

$x_{10} = 189$ (mo

$\boxed{x_{10} = 2}$

SCASB, SC

→ These instr to a byte

* ISBN:

$$x_{10} = \sum_{i=1}^{9} i x_i \pmod{11}$$

a) Suppose that the first 9 digits of ISBN-10 are 007288008. What is check digit?

$x_{10} = 1\cdot0 + 2\cdot0 + 3\cdot7 + 4\cdot2 + 5\cdot8 + 6\cdot8 + 7\cdot0 + 8\cdot0 + 9\cdot8 \pmod{11}$

$x_{10} = 21 + 8 + 40 + 48 + 72 \pmod{11}$

~~$x_{10} = 197 \pmod{11}$~~

$x_{10} = 117 + 72 \pmod{11}$

$x_{10} = 189 \pmod{11}$

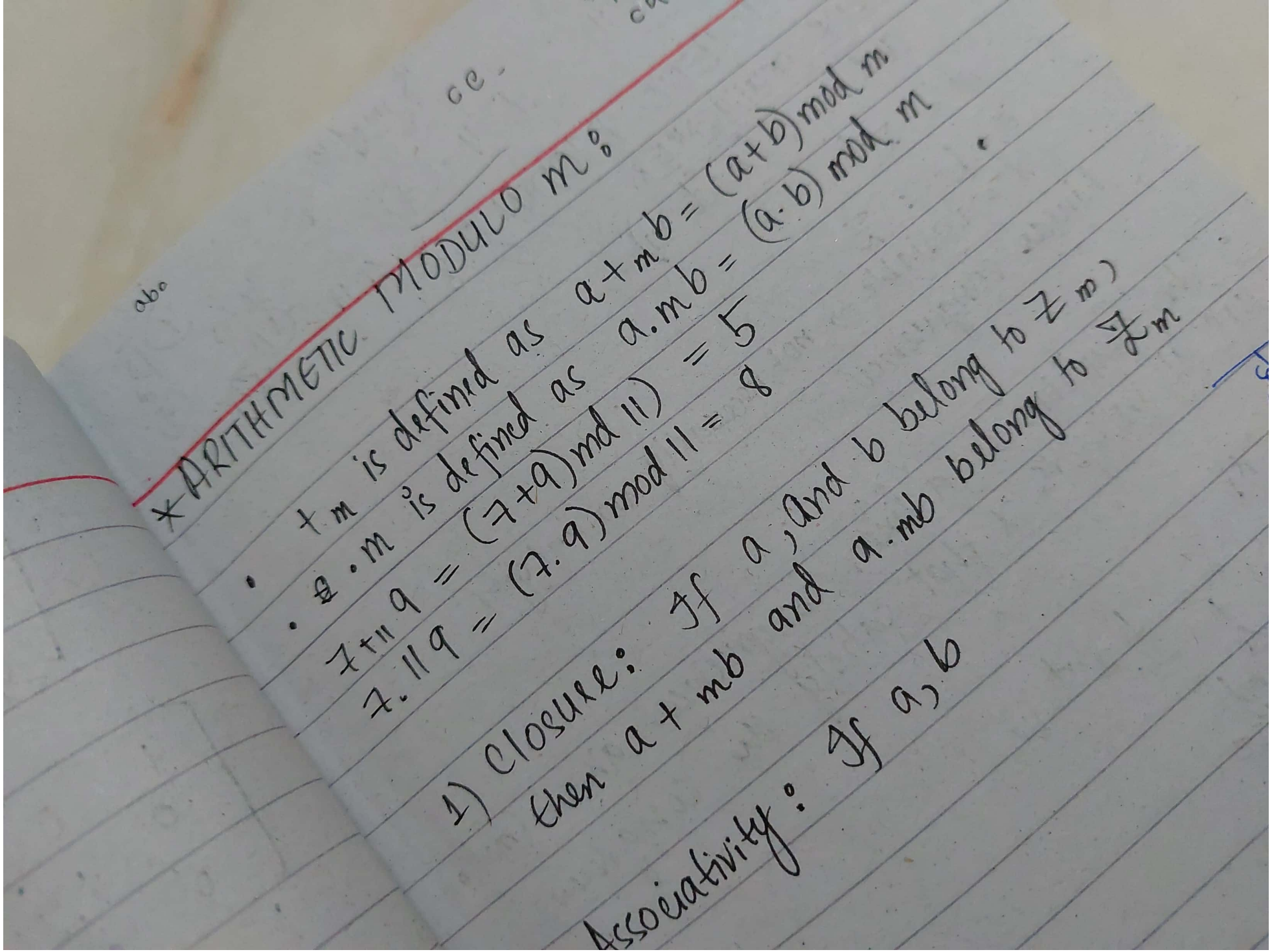
$\boxed{x_{10} = 2}$

$$\begin{array}{r} 17 \\ 11\overline{)189} \\ \underline{11} \\ 79 \\ \underline{77} \\ 2 \end{array}$$

$189 + 11k$

SCASB, SCASW, & SCASD:

→ These instructions compare a value in AL/AX/EAX to a byte, word or double word respectively.


* ARITHMETIC MODULO m :
• $+_m$ is defined as $a +_m b = (a+b) \bmod m$
• $\cdot_m$ is defined as $a \cdot_m b = (a \cdot b) \bmod m$
$7 +_{11} 9 = (7+9) \bmod 11 = 5$
$7 \cdot_{11} 9 = (7 \cdot 9) \bmod 11 = 8$
1) closure: If a, and b belong to $\mathbb{Z}_m$
then $a + mb$ and $a \cdot mb$ belong to $\mathbb{Z}_m$
Associativity: If a, b

3 mod 7

3 - 7 = -4

15 mod 4

15 - 4

7 - 4 = 3

4 - 11

*ARITHMETIC MODULO :

* LINEAR CONGRUENCE :

$$ax \equiv b \pmod{m}$$

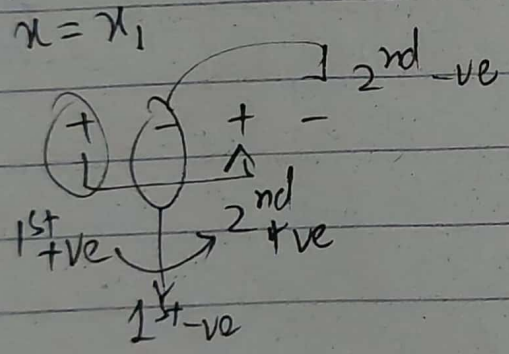
$m = z^+$

$a, b : z$

x = variable → not necessarily an integer

linear congruence

- The solutions to a linear congruence $ax \equiv b \pmod{m}$ are all integers x that satisfy the congruence



- One method of solving linear congruences makes use of an inverse $\bar{a}$, if it exists. Although we cannot divide both sides of the congruence by a, we can multiply by $\bar{a}$ to solve for x.

- An integer $\bar{a}$ such that $a\bar{a} \equiv 1 \pmod{m}$ is said to be inverse of modulo m.

4 mod 9
4 - 9 = -5 9 - 5 = 4

gcd(a, m)

modulo

7)3 -2 3 (mod 7)

* INVERSE of A MODULO m :

$a\bar{a} = 1$ → Base condition

- Inverse of a modulo m exists whenever a and m are relatively prime. Two integers a and b are relatively prime when $\gcd(a,b) = 1$

* a & m should be relatively prime ($m > 1$)

* $\bar{a}$ can be +ve or -ve depending on the given congruency

* always pick +ve modulo for making series

hello world

Direct proof: Implication

{ begins with premises, continues with a sequence of deductions, and ends with conclusion }

* IMPLICATION: $p \rightarrow q$

Indirect proof:

Does not start with premises / hypothesis ends with conclusion

* CONTRAPOSITIVE:

$\neg q \rightarrow \neg p$

Prove that if n is an integer and $3n+2$ is odd, then n is odd

→ Change it to ~~contradict~~ contrapositive for indirect proof.

"If n is even then $3n+2$ is even

n is even then

$n = 2k$

$$3n+2 = 3(2k)+2$$
$$= 2(3k+1)$$
$$= 2l \qquad l = (3k+1)$$

* MATHEMATICAL INDUCTION :

Conjecture:

The sum of first n odd natural numbers equals n^2.

		n^2
1	$1 =$	1^2 1
2	$1+3 =$	4
3	$1+3+5 =$	9
4	$1+3+5+7 =$	16
5	$1+3+5+7+9 =$	25
⋮	⋮	⋮
n	$1+3+5+7+9+11+\cdots(2n-1) =$	n^2 $\forall n \geq 1$

→ Mathematical statements asserts that a property is "true" for all positive integers.

① First, they show that the statement holds for positive integer 1 (base case)

② Second, they show that if statement ho for a positive integer then it must also h for the next large integer (inductive case) {if true for k then also true for k+1}

↳ for k+1 to be true, k must be true

IC : $n = k+1$ where k is any $\mathbb{Z}^+$

* Sequence & series is value of the term

* Mathematical induct upcoming values hold

. The method can be ex about more general we as trees. This gener Structural Induction and mathematical log

→ EXAMPLE : The (If 1st value values are also

→ k^{th} statement to fall, hence

. PRINCIPLE of M

1. Basis Step: The Propos

2. Inductive S If P(k) all intege

* Sequence & series is used to solve cumulative value of the term
* Mathematical Induction is used to check if upcoming values hold truth property.

→ The method can be extended to prove statements about more general well-founded structures such as trees. This generalization is known as Structual Induction. It is used in Computer science and mathematical logic.

→ EXAMPLE : The Domino Effect
(If 1st value is true, other upcoming values are also determined to be true)
→ K^{th} statement causes $(K+1)^{th}$ statement to fall, hence upcoming values hold truth value

. PRINCIPLE of MATHEMATICAL INDUCTION:

1. Basis Step:
The Proposition P(1) is true

2. Inductive Step:
If P(K) is true then P(K+1) is true for all integers $K \geq 1$ i.e. $\forall k\ p(k) \rightarrow p(k+1)$

Q) Use mathematical induction to prove that

$1+2+3+\cdots+n = \frac{n(n+1)}{2}$ for all integers

Sol:

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

1. Basis step: $P(1)$ is true

For $n=1$

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

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

2. Inductive Step:

Suppose $P(k)$ is true

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

Proving $P(k+1)$ is true

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

L.H.S

$\Rightarrow 1+2+3+\cdots+(k+1)$

$\Rightarrow \underline{1+2+3+\cdots+k}+(k+1)$

Substitute ~~in~~ ① in ②

$$\Rightarrow \frac{K(K+1)}{2} + (K+1)$$

$$\Rightarrow (K+1)\left[\frac{K}{2}+1\right]$$

$$\Rightarrow n = K+1$$

$$\therefore \frac{(K+1)(K+2)}{2} = R.H.S \text{ of } ②$$

Q) $1+3+5+\cdots+(2n-1) = n^2$

① Basis Step:
P(1) is true

P(1) $\therefore 2(1)-1 = 2-1 = 1$

$n^2 = 1^2 = 1$

L.H.S = R.H.S

② Inductive Step:
P(K) is true

P(K)

$1+3+5+\cdots+(2K-1) = K^2 \rightarrow (1)$

Proving P(K+1) is true

$1+3+5+\cdots+[2(K+1)-1] = (K+1)^2 \rightarrow (2)$

$1+3+5+\cdots+[2k+2-1] = (k+1)^2$.

$1+3+5+\cdots+(2k+1) = (k+1)^2$

$P(k) \leftarrow P(k+1)$

Substitute ① in ②

$\underbrace{1+3+5+\cdots+(2k-1)}_{k^2}+(2k+1)$

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

$= (k+1)^2$

$= R.H.S$

∴ $P(n): 2^0+2^1+2^2+\cdots+2^n = 2^{n+1}-1$

① Basis step: $P(0): 2^0 = 1,\ 2^{0+1}-1 = 1$

$1 = 1$

② Inductive step

P(k) is true:

$P(k): 2^0+2^1+2^2+\cdots+2^k = 2^{k+1}-1$

P(k+1) is true:

$P(k+1): 2^0+2^1+2^2+\cdots+2^{k+1} = 2^{k+2}-1$

$2^0+2^1+2^2+\cdots+2^k+2^{k+1} = 2^{k+2}-1$

$(k+1)+1$

$\therefore 2^0+2^1+2^2+\cdots+2^k+2^{k+1} = 2^{k+1}-1+2^{k+1}$

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

$= 2(2k+1)$

$P(k) = 2^0+2$

$P(k+1) = 2^0+2^1+$

$= 2^0+2^1+$

$\therefore 2^0+2^1+2^2+$

Consider L.H.S

(8) 2^0+2^1

① Basis s

$P(0) = 2$

2

② Inductive

$P(k): 2^0$

$P(k+1): 2^0+$

Consider L.H.S

$\Rightarrow (2^0+2^1+2^$

$\rightarrow (2^{k+1}-1$

$\rightarrow 2^{k+1}+2^{k+1}$

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

$= 2^{k+2}$

$P(k) = 2^0 + 2^1 + 2^2 + \cdots + 2^k = 2^{k+1} - 1 \rightarrow (A)$

$P(k+1) = 2^0 + 2^1 + 2^2 + \cdots + 2^{k+1} = 2^{(k+1)+1} - 1$

$= 2^0 + 2^1 + 2^2 + \cdots + 2^{k+1} = 2^{(k+2)} - 1 \rightarrow (B)$

$\therefore 2^0 + 2^1 + 2^2 + \cdots + 2^k + 2^{k+1} = 2^{k+1} - 1 + 2^{(k+2)} - 1$

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

$= 2($

Consider L.H.S of

(8) $2^0 + 2^1 + 2^2 + \cdots + 2^n = 2^{n+1} - 1$

① Basis step:

$P(0) = 2^0 = 1$

$2^1 - 1 = 1$

② Inductive step:

$P(k): 2^0 + 2^1 + 2^2 + \cdots + 2^k = 2^{k+1} - 1 \rightarrow (i)$

$P(k+1): 2^0 + 2^1 + 2^2 + \cdots + 2^{k+1} = 2^{k+1+1} - 1 \rightarrow (ii)$

Consider L.H.S of (ii)

(ii) $\rightarrow (2^0 + 2^1 + 2^2 + \cdots + 2^k) + 2^{k+1}$

$\rightarrow (2^{k+1} - 1) + 2^{k+1}$ // Substitute (i) in L.H.S of (ii)

$\rightarrow 2^{k+1} + 2^{k+1} - 1$

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

$= \boxed{2^{k+2} - 1}$: R.H.S

2^{k+1}

$2^k \cdot 2$

Q) $1^3+2^3+3^3+\cdots+n^3=\frac{1}{4}n^2(n+1)^2$

(1) Basis step:

$1^3=\frac{1}{4}\times 1^2\times(1+1)^2=1$

$2^3=\frac{1}{4}+2^2+(3)^2\Rightarrow 8$

True

(2) Inductive step:

$P(K):\ 1^3+2^3+3^3+\cdots+K^3=\frac{1}{4}K^3(K+1)^2\rightarrow(A$

$P(K+1):1^3+2^3+3^3+\cdots+(K+1)^3=\frac{1}{4}(K+1)^3(K+1+1$

Consider L.H.S of (B)

(B) $\Rightarrow$ (A)

$\Rightarrow 1^3+2^3+3^3+\cdots+K^3+(K+1)^3$

$\Rightarrow \frac{1}{4}K^3(K+1)^2+(K+1)^3$

$\rightarrow (K+1)^2\left(\frac{1}{4}K^3(K+1)^2\right)$

$\rightarrow (K+1)^2\left[\frac{1}{4}K^3(\quad)+K+1\right]$

$\rightarrow (K+1)^2\left[\frac{1}{4}K^3+K+1\right]$

(A

$1^3+2^3+3^3+$

$\Rightarrow$

$\frac{1}{4}K^2(K$

$K^2(K+1$

(K^2+1)

K^2+4

K^2+4

L.H

* COMBI

→ Combin
and a
Counti
is req
of P

→ applica
codes,

(A)

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

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

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

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

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

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

L.H.S = R.H.S Proved

COUNTING

* COMBINATRONICS:

→ Combinatronics is the mathematics of counting and arranging objects.
Counting with certain properties (enumeration) is required to solve many different types of problems.

→ applications include topics as diverse as codes, circuit design and algorithm complexity.

* COUNTING :

→ Enumeration is the counting of objects wi certain properties

<> Counting is used to :

1. Determine number of ordered or unorde arrangement of objects
2. Generate all the arrangements of a specified kind which is important in computer simulations
3. Compute probabilities of events
4. Analyze the chance of winning games, lotteries etc.
5. Determine complexity of algorithms

* BASIC COUNTING PRINCIPLES :

(1) The Sum Rule
(2) The Product Rule
(3) The Subtraction Rule
(4) The Division Rule
(5) Examples, Examples & Examples
(6) Tree Diagrams

(1) THE SU

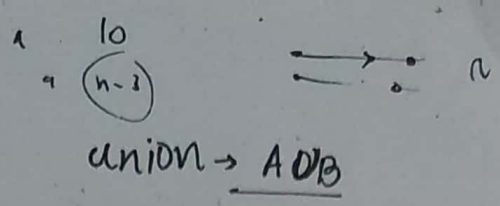
→ If a tas the n_1 ways t are n_2 n_1 set

⇒ $|A \cup B$

→ $|A_1 \cup A_2$ wh

(2) Suppo cours diff How the

$|A \cup$



union → A ∪ B

(1) THE SUM RULE :

→ If a task can be done either in one of the n_1 ways or in one of the n_2 ways to do the second task, then there are $n_1 + n_2$ ways to do a task where n_1 set is not same as n_2 set.

$$\Rightarrow |A \cup B| = |A| + |B|$$

$$\rightarrow |A_1 \cup A_2 \cup \dots \cup A_m| = |A_1| + |A_2| + \dots + |A_m|$$

when $A_i \cap A_j = \emptyset$

(Q) Suppose there are 7 different optional courses in Computer Science and 3 different optional courses in Mathematics. How many ways student can choose the course?

$$|A \cup B| = |A| + |B|$$
$$= 7 + 3$$
$$= 10 \text{ options to take one optional course}$$

Q A student can choose a computer project from one of the three lists. The lists contain 23, 15 and 19 possible projects respectively. How many possible projects are there to choose from?

- 23 + 15 + 19 = 57 projects to choose from.

* PIGEONHOLE PRINCIPLE:

If k is a positive integer and k+1 objects are placed into k boxes, then atleast one box contains two or more objects

- If a flock of 20 pigeons in a set of 19 pigeonholes, one of the pigeonholes must have more than 1 pigeon.

PERMUTATIONS

* A permutation of a set of distinct objects is an ordered arrangement of these objects.

* Ordered arrangement of a set of distinct objects

* Ordered arrangement of r elements of a set is called r-permutation.

Example:

Let $S = \{1, 2, 3\}$

ordered arrangement 3, 1, 2 is a permutation of S

ordered arrangement 3, 2 is a 2-permutation of S

2-permutations are 1, 2 ; 1, 3 ; 2, 1 ; 2, 3 ; 3, 1 and 3, 2

$\therefore P(3, 2) = 6$

Theorem:

$$P(n, r) = n(n-1)(n-2)\cdots(n-r+1)$$

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

Q) How many ways are there to select a first-prize winner, a second-prize winner, and a third-prize winner from 100 different people who have entered a contest?

$P(100, 3) = 100 \cdot 99 \cdot 98 = 970,200$

Ans

* For permutations ⇒ order matters, no repetition, distinct elements

* for combinations ⇒ order doesn't matter, repitition can occur distinct elements not necessary.

$\frac{52 \times 51 \times 50 \times 49 \times 48 \times 47 \times 46 \times \cdots \times 5 \times 4 \times 3 \times 2 \times 1}{(15,21)!}$

11	11, 15
3	11, 15
	11,

gcd (11, 15)

3	15, 21
	14, 21

NOTE: gcd is the largest factor that can divide its multiples

eg. gcd (15, 21) = 3 since 3 is largest value that can divide both 15 and 21

gcd i) (11, 15, 19) check whether integers in each of these sets are relatively prime

gcd (11, 15) → 1
gcd (15, 19) → 1
gcd (11, 19) → 1
pairwise prime

Find prime factorization of 126 and 729
LCM

2	126
3	63
3	21
7	7

$2 \times 3 \times 3 \times 7$
$\rightarrow 2 \times 3^2 \times 7$

4) Use extended Euclidean algorithm to express gcd (144, 89) and gcd (1001, 4) as a linear combination.

gcd (144, 89)

144 → (1)(89) + 55

89 = (1)(55) + 34

55 = (1)(34) + 21

34 = 1(21) + 13

21 = 1(13) + 8

13 = 1(8) + 5

8 = 1(5) + 3

5 = 1(3) + 2

3 = 1(2) + 1

* Backward substitution:

3 = 1(2) + 1

1·3 − 1·(2) = 1 → (i)

∴ (2) = 1·5 − 1·3

Put in (i)

1·3 − 1(1·5 − 1·3)

1·3 − 1·5 + 1·3

1 = 2·3 − 1·5 → (ii)

$3 = 1 \cdot 8 - 1 \cdot 5$

Put in (ii)

$1 = 2(1 \cdot 8 - 1 \cdot 5) + 1 \cdot 3$

$1 = 2 \cdot 8 - 2 \cdot 5 + 1 \cdot 3$

Backward substitution:

$3 = 1(2) + 1$

$1 = 1 \cdot 3 - 1 \cdot 2 \longrightarrow (i)$

$2 = 1 \cdot 5 - 1 \cdot 3$

Put in (i)

$1 = 1 \cdot 3 - 1(1 \cdot 5 - 1 \cdot 3)$

$1 = 1 \cdot 3 - 1 \cdot 5 + 1 \cdot 3$

$1 = 2 \cdot 3 - 1 \cdot 5 \rightarrow (ii)$

$3 = 1 \cdot 8 - 1 \cdot 5$

Put in (ii)

$1 = 2(1 \cdot 8 - 1 \cdot 5) - 1 \cdot 5$

$1 = 2 \cdot 8 - 2 \cdot 5 - 1 \cdot 5$

$1 = 2 \cdot 8 - 3 \cdot 5 \longrightarrow (iii)$

$5 = 1 \cdot 13 - 1 \cdot 8$

Put in (iii)

$1 = 2 \cdot 8 - 3(1 \cdot 13 - 1 \cdot 8)$

$1 = 2 \cdot 8 - 3 \cdot 13 + 3 \cdot 8$

$1 = 5 \cdot 8 - 3 \cdot 13 \longrightarrow (iv)$

$8 = 1 \cdot 21 - 1 \cdot 13$

Put in (iv)

$1 = 5(1 \cdot 21 - 1 \cdot 13) - 3 \cdot 13$

$1 = 5 \cdot 21 - 5 \cdot 13 - 3 \cdot 13$

$1 = 5 \cdot 21 - 8 \cdot 13 \rightarrow (v)$

$13 = 1 \cdot 34 - 1 \cdot 21$

Put in (v)

$1 = 5 \cdot 21 - 8(1 \cdot 34 - 1 \cdot 21)$

$1 = 5 \cdot 21 - 8 \cdot 34 + 8 \cdot 21$

$1 = 13 \cdot 21 - 8 \cdot 34 \rightarrow (vi)$

$21 = 1 \cdot 55 - 1 \cdot 34$

Put in (vi)

$1 = 13(1 \cdot 55 - 1 \cdot 34) - 8 \cdot 34$

$1 = 13 \cdot 55 - 13 \cdot 34 - 8 \cdot 34$

$1 = 13 \cdot 55 - 21 \cdot 34 \rightarrow (vii)$

$34 = 1 \cdot 89 - 1 \cdot 55$

Put in (vii)

$1 = 13 \cdot 55 - 21(1 \cdot 89 - 1 \cdot 55)$

$1 = 13 \cdot 55 - 21 \cdot 89 + 21 \cdot 55$

$1 = 1 \quad 34 \cdot 55 - 21 \cdot 89 \rightarrow (viii)$

$55 = 1 \cdot 144 - 1 \cdot 89$

Put in (viii)

$1 = 34(1 \cdot 144 - 1 \cdot 89) - 21 \cdot 89$

$1 = 34 \cdot 144 - 34 \cdot 89 - 21 \cdot 89$

$1 = 34 \cdot 144 - 55 \cdot 89$

$1 = (34)(144) + (-55)(89)$

Linear combination

gcd (1001, 100001) → always take left val.

$1001 = (0)(100001) + 1001$

$100001 = (99)(1001) + 902$

$1001 = (1)902 + 99$

$902 = (9)99 + 11$

$99 = 9(11) + 0$

Backward substitution

$11 = 1 \cdot 902 - 9 \cdot 99 \rightarrow (i)$

$99 = 1 \cdot 1001 - 1 \cdot 902$

Put in (i)

$11 = 1 \cdot 902 - 9(1 \cdot 1001 - 1 \cdot 902)$

$11 = 1 \cdot 902 - 9 \cdot 1001 + 9 \cdot 902$

$11 = 10 \cdot 902 - 9 \cdot 1001 \longrightarrow (ii)$

$902 = 1 \cdot 100001 - 99 \cdot 1001$

Put in (ii)

$11 = 10(1 \cdot 100001 - 99 \cdot 1001) - 9 \cdot 1001$

$11 = 10 \cdot 100001 - 108 \cdot 1001$

$999 \cdot 1001 - 9 \cdot 1001$

Solve each of these congruences by using modular inverses:

a) $55x \equiv 34 \pmod{89}$

$55x \equiv 34 \pmod{89}$

$55 = 0(89) + 55$

$89 = 1(55) + 34$

$55 = 1(34) + 21$

$34 = 1(21) + 13$

$21 = 1(13) + 8$

$13 = 1(8) + 5$

$8 = 1(5) + 3$

$5 = 1(3) + 2$

$3 = 1(2) + 1$

Backward sub:

$3 = 1 \cdot 2 + 1 \rightarrow (i)$

$2 = 1 \cdot 5 - 1 \cdot 3$

Put in (i)

$3 = 1(1 \cdot 5 - 1 \cdot 3) + 1$

$3 = 1 \cdot 5 - 1 \cdot 3 + 1$

$1 = 1 \cdot 3 - 1 \cdot 2 \rightarrow (i)$

$2 = 1 \cdot 5 - 1 \cdot 3$

$1 = 1 \cdot 3 - 1(1 \cdot 5 - 1 \cdot 3)$

$1 = 1 \cdot 3 - 1 \cdot 5 + 1 \cdot 3$

$1 = 2 \cdot 3 - 1 \cdot 5 \rightarrow (ii)$

$3 = 1 \cdot 8 - 1 \cdot 5$

Put in (ii)

$1 = 2(1 \cdot 8 - 1 \cdot 5) - 1 \cdot 5$

$1 = 2 \cdot 8 - 2 \cdot 5 - 1 \cdot 5$

$1 = 2 \cdot 8 - 3 \cdot 5 \rightarrow (iii)$

$5 = 1 \cdot 13 - 1 \cdot 8 \rightarrow$

Put in (iii)

$1 = 2 \cdot 8 - 3(1 \cdot 13 - 1 \cdot 8)$

$1 = 2 \cdot 8 - 3 \cdot 13 + 3 \cdot 8$

$1 = 5 \cdot 8 - 3 \cdot 13 \rightarrow (iv)$

$8 = 1 \cdot 21 - 1 \cdot 13$

Put in (iv)

$1 = 5(1 \cdot 21 - 1 \cdot 13) - 3 \cdot 13$

$1 = 5 \cdot 21 - 5 \cdot 13 - 3 \cdot 13$

$1 = 5 \cdot 21 - 8 \cdot 13 \rightarrow (v)$

$13 = 1 \cdot 34 - 1 \cdot 21$

Put in (v)

$1 = 5 \cdot 21 - 8(1 \cdot 34 - 1 \cdot 21)$

$1 = 5 \cdot 21 - 8 \cdot 34 + 8 \cdot 21$

$1 = 13 \cdot 21 - 8 \cdot 34 \rightarrow (vi)$

$21 = 1 \cdot 55 - 1 \cdot 34$

Put in (vi)

$1 = 13(1 \cdot 55 - 1 \cdot 34) - 8 \cdot 34$

$1 = 13 \cdot 55 - 13 \cdot 34 - 8 \cdot 34$

$1 = 13 \cdot 55 - 21 \cdot 34 \rightarrow (vii)$

$34 = 1 \cdot 89 - 1 \cdot 55$

Put in (vii)

$1 = 13 \cdot 55 - 21(1 \cdot 89 - 1 \cdot 55)$

$1 = 13 \cdot 55 - 21 \cdot 89 + 21 \cdot 55$

$1 = 34 \cdot 55 - 21 \cdot 89 \rightarrow (viii)$

Use the construction in the proof of Chinese remainder theorem to find all solutions of the system of congruencies.

i) $x \equiv 1 \pmod 5$, $x \equiv 2 \pmod 6$, $x \equiv 3$(

① Finding gcds of mods:

$\gcd(5,6)=1$, $\gcd(5,7)=1$, $\gcd(6,7)=1$

They are pairwise prime

② Finding cumulative mod:

$$m = m_1 * m_2 * m_3$$
$$= 5 * 6 * 7$$
$$= 210$$

③ $M_k = \frac{m}{m_k}$

$$\therefore M_1 = \frac{m_1}{m_1} = \frac{210}{5} = 42$$

$$M_2 = \frac{m}{m_2} = \frac{210}{6} = 35$$

$$M_3 = \frac{m}{m_3} = \frac{210}{7} = 30$$

④

$x = (a_1 y_1$

$y_k = \cancel{m_k}$ M_k

$y_1 = M_1 \_ m$

$y_1 = 42$ m

$42 = (8)$

$5 = 1($

Backwa

$1 = 1 \cdot 5$

$2 = 1 \cdot 4$

Put in (

$1 = 1 \cdot$

$1 = 1$

④

$$x = (a_1 y_1 M_1 + a_2 y_2 M_2 + a_3 y_3 M_3) \bmod m \longrightarrow (A)$$

$y_k = \overline{M_k} \bmod m_k$

$y_1 = \overline{M_1}^{-1} \bmod m_1$

$y_1 = 42 \bmod 5 \longrightarrow$

$42 = (8)(5) + 2$

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

$42 =$

$42 = (8)(5) + 2$

$5 = (2)(2) + 1$

Backward substitution:

$1 = 1 \cdot 5 - 2 \cdot 2 \rightarrow (i)$

$2 = 1 \cdot 42 - 5 \cdot 8 \rightarrow (ii)$

Put in (i)

$1 = 1 \cdot 5 - 2(1 \cdot 42 - 8 \cdot 5)$

$1 = 1 \cdot 5 - 2 \cdot 42 + 16 \cdot$

ii) $x \equiv 1 \pmod 2$, $x \equiv 2 \pmod 3$, $x \equiv (3 \bmod 5)$,
$x \equiv 4 \pmod{11}$

① Check if gcds are pairwise prime

gcd(1, 2)

② finding cumulative mod m:

$m_1 = 2, m_2 = 3, m_3 = 5, m_4 = 11$

$m = m_1 m_2 m_3 m_4 = 330$

$M_1 = \frac{m}{m_1} = \frac{330}{2} = 165$

$M_2 = \frac{m}{m_2} = \frac{330}{3} = 110$

$M_3 = \frac{m}{m_3} = \frac{330}{5} = 66$

$M_4 = \frac{m}{m_4} = \frac{330}{11} = 30$

$x = (a_1 y_1 M_1 + a_2 y_2 M_2 + a_3 y_3 M_3 + a_4 y_4 M_4) \bmod m$

$y_k = \overline{M_k} \bmod m_k$

$y_1 = \overline{M_1} \bmod m_1$

$y_1 = 165^{-1} \bmod 2$

3 mod 5

$165 = (82)(2) + 1$

Substitution:

$1 = 1 \cdot 165 - 82 \cdot 2$

$1 = 1(165) + (-82)(2)$

$\boxed{y_1 = 1}$

$y_2 = M_2 \bmod m_2$

$y_2 = 110^{-1} \bmod 3$

$110 = 36(3) + 2$

$2 = 1 \cdot 110 - 36 \cdot 3$

$2 =$

$3 = 1(2) + 1$

$1 = 1 \cdot 3 - 1 \cdot 2 \rightarrow (i)$

$2 = 1 \cdot 110 - 36 \cdot 3$

Put in (i)

$1 = 1 \cdot 3 - 1(1 \cdot 110 - 36 \cdot 3)$

$1 = 1 \cdot 3 - 1 \cdot 110 + 36 \cdot 3$

$1 = 37 \cdot 3 - 1 \cdot 110$

$1 = 37(3) + (-1)(110)$

$y_2 = 3 - 1 = 2$

BINOMIAL THEOREM

$$(x+y)^n = {}^nC_0 x^n y^0 + {}^nC_1 x^{n-1} y^1 + \cdots + {}^nC_n x^0 y^n$$

Q) what is the coefficient of $x^{12}y^{13}$ in the expansion of $(2x-3y)^{25}$?

$$(2x+(-3y))^{25} = \sum_{j=0}^{25} \binom{25}{j} (2x)^{25-j} (-3y)^j$$

$j = 13$

$$\therefore \binom{25}{13} 2^{12} (-3) \Rightarrow -\frac{25!}{13!\,12!} 2^{12} 3^{13} \quad \text{Ans}$$

$x^{10}y^{11}$, $n = 21$

$$\binom{21}{11} 2^{10} (-3)^{11} \Rightarrow -\frac{21!}{11!\,10!} 2^{10} 3^{11} \quad \text{Ans}$$

* PASCAL'S IDENTITY:

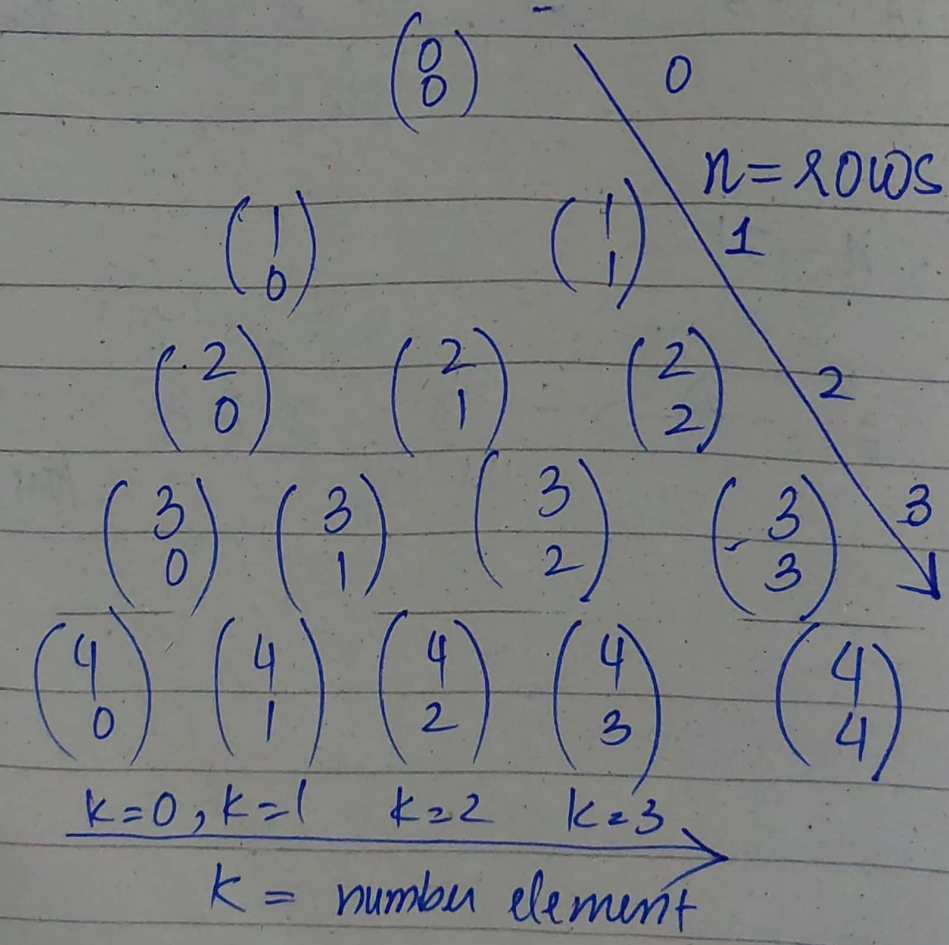
$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$$

$n = 10, k = 5$

$$\binom{10}{5} = \binom{9}{4} + \binom{9}{5}$$

$$252 = 126 + 126$$

$$252 = 252$$



$(x+y)^n \Rightarrow n=3$

find coefficient at $n=3$

$(x+y)^3 = a_0 / {}^nC_0$

$= {}^3C_0 (x)^3 (y)^0 + {}^3C_1 (x)^2 (y)^1 + {}^3C_2 (x)^1 (y)^2 + {}^3C_3 (x)^0 (y)^3$

$= 1y^3\ 1x^3 + 3x^2y + 3xy^2 + 1y^3$

$= 1, 3, 3, 1$

find coefficient at $n=9$

$= {}^9C_0 (x)^9 (y)^0 + {}^9C_1 (x)^8 (y)^1 + {}^9C_2 (x)^7 (y)^2 + {}^9C_3 (x)^6 (y)^3$
$+ {}^9C_4 (x)^5 (y)^4 + {}^9C_5 (x)^4 (y)^5 + {}^9C_6 (x)^3 (y)^6$
$+ {}^9C_7 (x)^2 (y)^7 + {}^9C_8 (x)^1 (y)^8 + {}^9C_9 (x)^0 (y)^9$

$= x^9 + 9x^8y + 36x^7y^2 + 84x^6y^3 + 126x^5y^4$
$+ 126x^4y^5 + 84x^3y^6 + 36x^2y^7$
$+ 9xy^8 + x^9$

1, 9, 36, 84, 126, 126, 84, 36, 9, 1

at $n=9$

Ans

• Inner Triangle / Pascals' formula:

$$\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}$$

↓ position at Pascal's Triangle

members through which position is derived

What is the value where $n=7$ and $k=5$ at Pascals' Triangle?

$$\binom{8}{5} = \binom{7}{4} + \binom{7}{5}$$

$$56 = 34 + 22 \quad 35+21$$

$$56 = 56$$

Find the 3rd element in the 4th row of Pascal Triangle.

$k=3$, $n=3$

$$\binom{5}{2} = \binom{4}{2}$$

$$\binom{4}{3} = \binom{3}{2} + \binom{3}{3}$$

$$4 = 3+1$$

RSA:

p & q both be prime numbers.

① $n = p \cdot q$

② $k = (p-1)(q-1)$

③ $e > 1$ & $e < k$, $\gcd(e, k) = 1$

④ d = inv of $e \bmod k$

$c = m^e \bmod n$

$m = c^e \bmod n$

$m = 19$

$p = 7, q = 17$

① ~~$n = 7 \cdot 17$~~ $= p = 11, q = 13$

$n = 11 \times 13 = 143$

② $k = (10)(12) = 120$

③ $e > 1$ & $e < k$

$e = 17$

$\gcd(17, 120) = 1$

$d = e \bmod k$

$d = 17 \bmod 120$

$120 = 17.7 + 1$

$1 = 120 \quad 17$

+120

-7

113

$c = m^e$

$c = 19^$

3.832

{

a = 34,

↓

34 = (0)(

89 = (2)

34 = (1)(

21 = (1)(

13 = (1)(

8 = (1)(

5 = (1)

3 = (1)

1 = 1.

2 = 1.

Put (ii)

1 = 1.

1 = 1.

$+120 \quad -120$

$-7 \quad -7$

$\boxed{113} \quad -127$

$5 \bmod 3$

$2 \quad 3x$

$5-3=2 \quad 3x1=3$

19^{17}

mod 143.

$C = m^e \bmod n$

$C = 19^{17} \bmod 143$

$3.832438362 \times 10^{19}$

$\{872700000\}$

$a = 34, \; m = 89$

↓

$34 = (0)(34) + 89$

$89 = (2)(34) + 21$

$34 = (1)(21) + 13$

$21 = (1)(13) + 8$

$13 = (1)(8) + 5$

$8 = (1)(5) + 3 \rightarrow 3 = 1.8 - 1.5$

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

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

$1 = 1.3 - 1.2 \rightarrow (i)$

$2 = 1.5 - 1.3 \rightarrow (ii)$

Put (ii) in (i)

$1 = 1.3 - 1(1.5 - 1.3)$

$1 = 1.3 - 1.5 + 1.3$

$1 = 2.3 - 1.5 \rightarrow (iii)$

* INDIRECT PROOFS

- $p \rightarrow q$

$\neg q \rightarrow \neg p$

If n is integer and $3n+2$ is odd then n is odd

- If n is integer and $3n+2$ is even then n is even

$n = 2K$

$3n+2$

$\Rightarrow 3(2K)+2$

$\Rightarrow 2(3K+1)$

$\rightarrow 2e$

odd

* CONTRADICTION:

If n^2 is even and n is even

at n is odd

$n = 2k+1$

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

- Proof by contradiction that set of prime numbers is ~~even~~ infinite.

Let q is prime

$q = \infty$

$q \neq \infty$

$n = r \cdot s$

$\Rightarrow r = 1$ or $s = 1$

$7 = 1.$

$n = r \qquad r \geq 1$

Infinitely

$x = p_1 * p_2 * \dots + p_n$

add 1 to x.

$x = x + 1$

Now, if this number x is divided by any of the primes in the list the remainder is 1