1. SET THEORY

SET: A set is an unordered collection of objects, called elements or members of the set.

SET REPRESENTATION: There are several ways to describe a set.

- One way is to list all the members of a set, when this is possible. We use a notation where all members of the set are listed between braces.

Example:

The set V of all vowels in the English alphabet can be written as V = {a, e, i, o, u}.

The set O of odd positive integers less than 8 can be expressed by O = {1, 3, 5, 7}.

- Sometimes the **roster method** is used to describe a set without listing all its members. Some members of the set are listed, and then ellipses (...) are used when the general pattern of the elements is obvious.

Example:

The set of positive integers less than 100 can be denoted by {1, 2, 3,..., 99}.

- Another way to describe a set is to use set **builder notation.** We characterize all those elements in the set by stating the property or properties they must have to be members.

Example:

(a) The set O of all odd positive integers less than 10 can be written as

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

OR

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

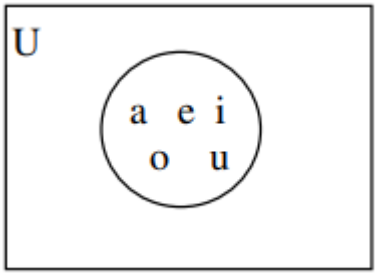
(b) The set Q^+ of all positive rational numbers can be written as

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

1.1 SOME DEFINITIONS

1. VENN DIAGRAM: A Venn diagram is a graphical representation of sets. In Venn diagrams the universal set U, which contains all the objects under consideration, is represented by a rectangle. Inside this rectangle, circles or other geometrical figures are used to represent sets.

For e.g. set of vowel as given above can be represented as:



2. SUBSET: A subset is a set whose elements are members of another set. Subsets are classified as:

(a) Proper Subset: Set A is considered to be a proper subset of Set B if Set B contains at least one element that is not present in Set A. It is denoted by $\subset$ **($A \subset B$)**

Example: If set A has elements as {12, 24} and set B has elements as {12, 24, 36}, then set A is the proper subset of B because 36 is not present in the set A.

(b) Improper Subset*:* Set A is considered to be improper subset of Set B if and only if both set are equal. It is denoted by $\subseteq$ (**$A \subseteq B$**). Symbolically: **$\forall x(x \in A \rightarrow x \in B)$**

Example: If set A has elements as {12, 24, 36} and set B has elements as {12, 24, 36}, then set A is the improper subset of B because both set are equal.

If a set has "n" elements, then the number of subset of the given set is 2^n and the number of proper subsets of the given subset is given by 2^n-1.

Example: Set P = {2, 4, 6} Then, the subsets of P are;

{}, {2}, {4}, {6}, {2,4}, {4,6}, {2,6} and {2,4,6}.

Where, {}, {2}, {4}, {6}, {2, 4}, {4, 6}, {2, 6} are the proper subsets and {2, 4, 6} is the improper subsets.

3. EMPTY SET: The set that contains no element is called empty set and denoted by $\emptyset$. It is also called null set. We have $\emptyset = \{\}$ but $\emptyset \neq \{\emptyset\}$

4. EQUAL SETS: Two sets A and B are equal if and only if they contain exactly same elements. In other words if $A \subseteq B$ and $B \subseteq A$ then $A = B$.

For e.g. $A = \{1, 2, 3, 4, 5\}$ and $B = \{2, 5, 4, 1, 3\}$ are equal sets.

5. CARDINALITY: For the set S, if there are exactly n distinct elements in S where n is a number then we say that cardinality of the set S is n denoted by |S|.

For e.g. $|\emptyset| = 0$; $|\{a, b, b, c, a\}| = 3$

If $n \in N$ then the set is finite otherwise, it is infinite.

6. POWER SET: Given a set S, power set denoted by P(S) is the set that contains all the subsets of the set S. Symbolically we can write $P(S) = \{x \mid x \subseteq S\}$. The number of elements in the power set of set having n elements is 2^n

For e.g. power set for the set {2, 3} is {∅, {2}, {3}, {2, 3}}.

Q. What is the power set of the empty set? What is the power set of the set {∅}?

Solution:

The empty set has exactly one subset ($2^0=1$), namely, itself. Consequently,

$P(\emptyset) = \{\emptyset\}$.

The set {∅} has exactly two subsets ($2^1=2$), namely, ∅ and the set {∅} itself. Therefore,

$P(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}$

1.2 SET OPERATIONS

1. UNION OPERATOR: Given two sets A and B, the union of set A and set B is the set that contains those elements that are either in A or in B, or in both, denoted by A ∪ B.

Symbolically, we write union of A and B as: $A \cup B = \{x \mid x \in A \vee x \in B\}$.

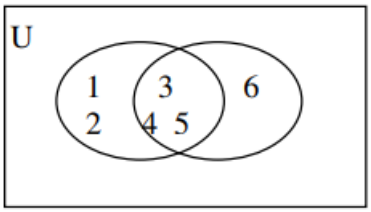
Example:

i. A= {2, 3} B= {a, b, c}

A ∪ B = {2, 3, a, b, c}.

ii. A= {1, 2, 3, 4, 5} B= {3, 4, 5, 6, 7}

A ∪ B= {1, 2, 3, 4, 5, 6, 7}. This can be shown in Venn diagram as:



2. INTERSECTION OPERATOR: Given two sets A and B, the intersection of set A and set B is the set that contains those elements that are in both A and B, denoted by A ∩ B. If the intersection of two set is null set then it is called **Disjoint Sets.**

Symbolically, we write intersection of A and B as: $A \cap B = \{x \mid x \in A \wedge x \in B\}$.

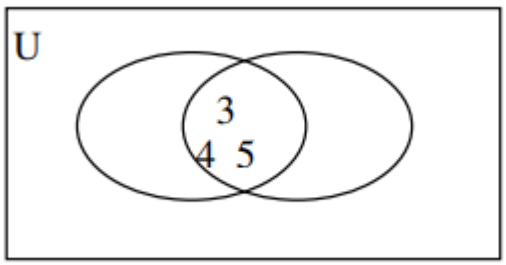
Example:

i. A= {2, 3} B= {a, b, c}

A∩B= { }

ii. A= {1, 2, 3, 4, 5} B= {3, 4, 5, 6, 7}

A∩B= {3, 4, 5}. This can be shown in Venn diagram as:

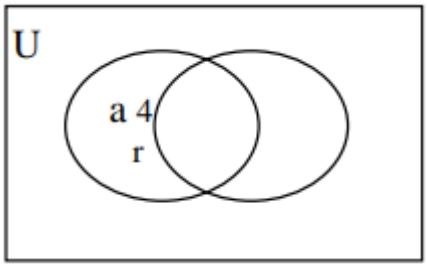


3. SET DIFFERENCE: Given two sets A and B, the difference of A and B is the set that contains all the elements that are in A but not in B, denoted by A –B.

Symbolically we write difference of A and B as $A - B = \{x \mid x \in A \wedge x \notin B\}$.

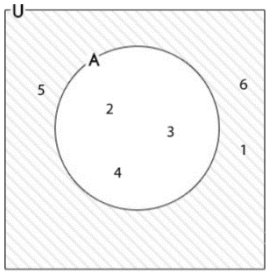
Example:

A = {2, 4, a, r} and B = {1, 2, a, s, t} then A – B = {4, r}. Venn diagram is given below:



4. COMPLEMENT: Complement of set S is denoted by U – S or $\overline{S}$, where U is the universal set, is the difference of universal set U and set S.

Symbolically complement is written as $S' = \{x \in U \mid x \notin A\}$.



Example:

If U = {1, 2, 3, 4, 5, 6} and A = {2, 3, 4}, then $\overline{A}$= {1, 5, 6}

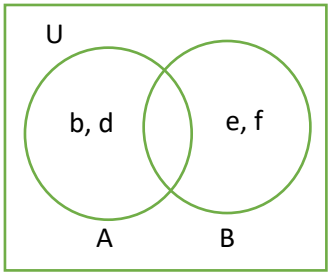
5. SYMMETRIC DIFFERENCE: Given two sets A and B, The symmetric difference of A and B is the set that belongs to A or to B but not to both A and B, denoted by A⊕ B.

Symbolically we write $A \oplus B = \{x \mid (x \in A \wedge x \notin B) \text{ or } (x \in B \wedge x \notin A)\}$.

$$\mathbf{A \oplus B = (A - B) \cup (B - A)}$$

Example:

A= {a, b, c, d} B= {a, c, e, f, g} then A ⊕ B = {b, d, e, f, g}



1.3 SET IDENTITES

$A \cap U = A$	Identity law
$A \cup \varnothing = A$	Identity law
$A \cap \varnothing = \varnothing$	Domination law
$A \cup U = U$	Domination law
$A \cap A = A$	Idempotent law
$A \cup A = A$	Idempotent law
$(A')' = A$	Complementation law
$A \cap B = B \cap A$	Commutative law
$A \cup B = B \cup A$	Commutative law
$(A \cap B) \cap C = A \cap (B \cap C)$	Associative law
$(A \cup B) \cup C = A \cup (B \cup C)$	Associative law
$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$	Distributive law
$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	Distributive law
$(A \cap B)' = A' \cup B'$	De Morgan's law
$(A \cup B)' = A' \cap B'$	De Morgan's law

1.4 PROVING SET IDENTITES

Different ways to prove set identities:

a. Prove that each set (i.e. each side of the identity) is a subset of the other (Double Inclusion).

b. Use set builder notation and propositional logic.

c. Membership Tables

A. DOUBLE INCLUSION METHOD:

It is based on the set equality definition: Two sets **A** and **B** are said to be equal if **A ⊆ B** and **B⊆ A**. In this method, we need to prove that the left-hand side (L.H.S.) of a set identity is a subset of the right-hand side (R.H.S.) and vice versa.

Q. Prove that $\overline{A \cup B} = \overline{A} \cap \overline{B}$

Solution:

Let P = $\overline{A \cup B}$ and Q = $\overline{A} \cap \overline{B}$

Let x be an arbitrary element of P then x ∈ P ⇒ x ∈ = $\overline{A \cup B}$

⇒ x ∉ (A U B)

⇒ x ∉ A and x ∉ B

⇒ x ∈ $\overline{A}$ and x ∈ $\overline{B}$

⇒ x ∈ $\overline{A} \cap \overline{B}$

⇒ x ∈ Q

Therefore, P ⊆ Q …….. (i)

Again, let y be an arbitrary element of Q then y ∈ Q ⇒ y ∈ $\overline{A} \cap \overline{B}$

⇒ y ∈ $\overline{A}$ and y ∈ $\overline{B}$

⇒ y ∉ A and y ∉ B

⇒ y ∉ (A U B)

⇒ y ∈ $\overline{A \cup B}$

⇒ y ∈ P

Therefore, Q ⊆ P …….. (ii)

Now by combining (i) and (ii) we get, P = Q i.e. $\overline{A \cup B} = \overline{A} \cap \overline{B}$

B. SET BUILDER NOTAION:

Q. Prove that $\overline{A \cap B} = \overline{A} \cup \overline{B}$

Solution:

Let x be an arbitrary element of $\overline{A \cup B}$ **.** Then by definition of complement we can write,

$\overline{A \cap B}$ = {x | x∉$\overline{A \cap B}$ } by definition of complement

= {x | ¬(x ∈ (A ∩ B))} by definition of does not belong symbol

= {x | ¬(x ∈ A ∧ x ∈ B)} by definition of intersection

= {x | ¬(x ∈ A) ∨ ¬(x ∈ B)} by the first De Morgan law for logical equivalences

= {x | x ∉ A ∨ x ∉ B} by definition of does not belong symbol

= {x | x ∈ $\overline{A}$ ∨ x ∈ $\overline{B}$ } by definition of complement

= {x | x ∈ $\overline{A}$ ∪ $\overline{B}$ } by definition of union

= $\overline{A}$ ∪ $\overline{B}$ by meaning of set builder notation

C. MEMBERSHIP TABLE:

Q. Use a membership table to show that A ∩ (B ∪ C) = (A ∩ B) ∪ (A ∩ C).

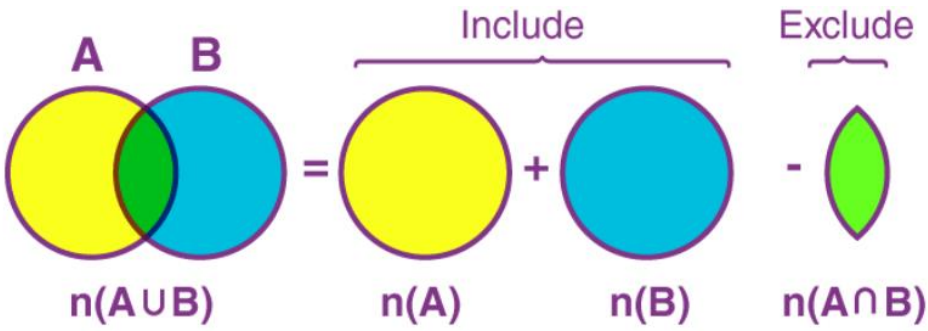
A	B	C	$B \cup C$	$A \cap (B \cup C)$	$A \cap B$	$A \cap C$	$(A \cap B) \cup (A \cap C)$
1	1	1	1	1	1	1	1
1	1	0	1	1	1	0	1
1	0	1	1	1	0	1	1
1	0	0	0	0	0	0	0
0	1	1	1	0	0	0	0
0	1	0	1	0	0	0	0
0	0	1	1	0	0	0	0
0	0	0	0	0	0	0	0

1.5 INCLUSION EXCLUSION PRINCIPLE/ ADDITION PRINCIPLE

Principle of Inclusion and Exclusion is an approach which derives the method of finding the number of elements in the union of two finite sets.

Consider two finite sets A and B. We can denote the Principle of Inclusion and Exclusion formula as follows.

n(A∪B) = n(A) + n(B) – n(A∩B)



Here n(A) denotes the cardinality of set A, n(B) denotes the cardinality of set B and n(A∩B) denotes the cardinality of (A∩B). We have included A and B and excluded their common elements.

If we have 3 sets A, B, and C, then according to the Principle of Inclusion and Exclusion,

n (A∪B∪C) = n(A) + n(B) + n(C) – n(A∩B) – n(A∩C) – n(B∩C) + n(A∩B∩C)

Q.1 Among a group of students, 49 study Physics, 37 study English and 21 study Biology. If 9 of these students study Physics and English, 5 study English and Biology, 4 study Physics and Biology and 3 study Physics, English and Biology, find the number of students in the group.

Solution:

Let P represent the number of students who study Physics, E represent the number of students who study English and B represent the number of students who study Biology.

Number of students in the group = n (P∪E∪B)

Given

$n(P) = 49, n(E) = 37, n(B) = 21, n(P \cap E) = 9, n(E \cap B) = 5, n(P \cap B) = 4, n(P \cap E \cap B) = 3$

$n(P \cup E \cup B) = n(P) + n(E) + n(B) – n(P \cap E) – n(E \cap B) – n(P \cap B) + n(P \cap E \cap B)$

$= 49 + 37 + 21 – 9 – 5 – 4 + 3$

$= 92$

Q.2 In a renowned software development company of 240 computer programmers 102 employees are proficient in Java, 86 in C#, 126 in Python, 41 in C# and Java, 37 in Java and Python, 23 in C# and Python, and just 10 programmers are proficient in all three languages. How many computer programmers are there those are not proficient in any of these three languages?

Solution

Let U denote the set of all employed computer programmers and let J, C and P denote the set of programmers proficient in Java, C# and Python, respectively.

So, $|U| = 240, |J| = 102, |C| = 86, |P| = 126, |J \cap C| = 41, |J \cap P| = 37, |C \cap P| = 23$ and

$|J \cap C \cap P| = 10$.

The number of computer programmers that are not proficient in any of these three languages is said to be same as the cardinality of the complement of the set $J \cup C \cup P$.

First, we have to calculate $|J \cup C \cup P| = 102 + 86 + 126 – 41 – 37 – 23 + 10 = 223$.

Now calculate $|\overline{J \cup C \cup P}| = |U| – |J \cup C \cup P| = 240 – 223 = 17$.

17 programmers are not proficient in any of the three languages.\

1.6 COMPUTER REPRESENTATION OF SET

Assume that the universal set U is finite (and of reasonable size so that the number of elements of U is not larger than the memory size of the computer being used). First, specify an arbitrary ordering of the elements of U, for instance a_1, a_2,...,a_n. Represent a subset A of U with the bit string of length n, where the i^{th} bit in this string is 1 if a_i belongs to A and is 0 if a_i does not belong to A.

Example:

a. Let U = {1, 2, 3, 4, 5, 6, 7, 8, 9, 10}, and the ordering of elements of U has the elements in increasing order; that is, a_i = i. What bit strings represent the subset of all odd integers in U, the subset of all even integers in U, and the subset of integers not exceeding 5 in U?

Solution:

(a) The bit string that represents the set of odd integers in U, namely, {1, 3, 5, 7, 9}, has a one bit in the first, third, fifth, seventh, and ninth positions, and a zero elsewhere. It is

10 1010 1010

(b) The bit string that represents the set of all even integers in U, namely, {2, 4, 6, 8, 10}, by the string

01 0101 0101

(c) The bit string that represents the set of all integers in U that do not exceed 5, namely, {1, 2, 3, 4, 5}, is represented by the string

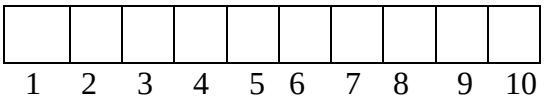
11 1110 0000

SET OPERATIONS USING BIT STRING LOGIC:

The following are some common set operations that can be performed using bit string logic:

Let, U={1,2,3,4,5,6,7,8,9,10}, A = {2, 4, 6} and B= {3, 4}

Length of bit = 10



- **Union:** To compute the union of two sets A and B represented as bit strings, we perform a bitwise OR operation between the two bit strings. In above given example:

  A = 0101010000 and B = 0011000000, A∪B = 0111010000

- **Intersection:** To compute the intersection of two sets A and B represented as bit strings, we perform a bitwise AND operation between the two bit strings. In above given example: A = 0101010000 and B = 0011000000, A∩B = 0001000000

- **Complement:** To compute the complement of a set A represented as a bit string, we perform a bitwise NOT operation on the bit string. In above given example:

  A = 0101010000, $\overline{\boldsymbol{A}}$ = 1010101111

- **Difference:** To compute the difference of two sets A and B represented as bit strings, we perform a bitwise AND operation between the bit string representing A and the complement of the bit string representing B. In above given example:

  A = 0101010000, $\overline{\boldsymbol{B}}$ = 1100111111, A-$\overline{\boldsymbol{B}}$ = 0100010000

- **Symmetric difference:** To compute the symmetric difference of two sets A and B represented as bit strings, we perform a bitwise XOR operation between the two bit strings. In above given example:

  A = 0101010000 and B = 0011000000, A⊕B = 0110010000

2. NUMBER THEORY

Number theory (or arithmetic or higher arithmetic in older usage) is a branch of pure mathematics devoted primarily to the study of the integers and integer-valued functions. German mathematician Carl Friedrich Gauss (1777–1855) said, "Mathematics is the queen of the sciences—and number theory is the queen of mathematics."

2.1 DIVISIBILITY OF INTEGER

DIVISION:

If **a** and **b** are integers with **a ≠0**, we say that **a** divides **b** if there is an integer **c** such that **b=ac.** When **a** divides **b** we say that **a** is a factor or divisor of **b**, and that **b** is a multiple of **a**. The notation **a | b** denotes that **a** divides **b**. We write **a ∤ b** when **a** does not divide **b.**

We can express a | b using quantifiers as ∃c (ac = b), where the universe of discourse is the set of integers.

Q.1 let n and d be positive integers. How many positive integers not exceeding n are divisible by d?

Solution:

The positive integers divisible by d are all the integers of the form dk, where k is a positive integer. Hence, the number of positive integers divisible by d that do not exceed n equals the number of integers k with $0 < dk \leq n$, or with $0 < k \leq n/d$. Therefore, there are $\lfloor n/d \rfloor$ positive integers not exceeding n that are divisible by d.

THEOREM: 1

Let a, b, and c be integers, where $a \neq 0$. Then

(i) if a | b and a | c, then a | (b + c);

(ii) if a | b, then a | bc for all integers c;

(iii) if a | b and b | c, then a | c.

COROLLARY: If a, b, and c are integers, where $a \neq 0$, such that a | b and a | c, then a | mb+nc whenever m and n are integers.

Proof: We have if a | b, then a | bc for all integers c; we see that a | mb and a | nc whenever m and n are integers. Also if a | b and a | c, then a | (b + c); it follows that a | mb + nc.

Q.1 Show that if a | b and b | a, where a and b are integers, then a=b or a=-b.

Solution:

If a | b then there exist integer c such that b=ac-----(i)

If b | a then there exist integer d such that a = bd----(ii)

Now, from (i) and (ii),

a = acd

cd = 1 i.e either c=1 and d=1 or c=-1 and d=-1. This follows that either a=b or a=-b.

THEOREM 2: THE DIVISION ALGORITHM

Let **a** be an integer and **d** a positive integer. Then there are unique integers **q** and **r**, with **0 ≤ r<d**, such that **a = dq + r.**

In the equality given in the division algorithm, **d** is called the divisor, **a** is called the dividend, **q** is called the quotient, and **r** is called the remainder. This notation is used to express the quotient and remainder: **q = a div d, r = a mod d.**

Q.1 What are the quotient and remainder when 101 is divided by 11?

Solution

The quotient when 101 is divided by 11 is 9 =101 div 11, and the remainder is 2 =101 mod 11.

$$101 = 11.\ 9 + 2$$

Q.2 What are the quotient and remainder when −11 is divided by 3?

Solution

The quotient when −11 is divided by 3 is −4 = −11 div 3, and the remainder is 1 = −11 mod 3.

Note that the remainder cannot be negative. Consequently, the remainder is not −2, even though −11 = 3(−3) − 2, because r = −2 does not satisfy $0 \leq r < 3$.

CONGRUENT MODULO:

Two integers 'a' and 'b' are congruent modulo to 'm' iff they have same remainder when divided by 'm'. Notation: $a \equiv b \pmod{m}$ [a is congruent modulo to b mod m]

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.

Example: 17 is congruent to 5 modulo 6

Here, a=17, b=5, m=6

a-b=17-5=12 which is divisible by 6. Therefore, $17 \equiv 5 \pmod{6}$

THEOREM: 3

Let 'm' be a positive integer. The integers 'a' and 'b' are congruent modulo 'm' if and only if there is an integer k such that a = b + km**.**

Proof:

If a ≡ b (mod m), by the definition of congruence, we know that m | (a − b). This means that there is an integer k such that a − b = km, so that a = b + km. Conversely, if there is an integer k such that a = b + km, then km = a − b. Hence, m divides a − b, so that a ≡ b (mod m).

THEOREM: 4

Let 'm' be a positive integer. If a ≡ b (mod m) and c ≡ d (mod m), then a + c ≡ b + d (mod m) and ac ≡ bd (mod m).

Proof:

If a ≡ b (mod m), then we can write, a=b + km------(i), for some integer k.

If c ≡ d (mod m), then we can write, c=d + lm------(i), for some integer l.

Now, to show: a + c ≡ b + d (mod m) we need to prove that m | (a+c) - (b+d).

(a+c) – (b + d) = [b +km + d +lm] - (b + d) ----------from (i) and (ii)

= b +km + d +lm - b – d

=km + lm

= (k + l) m, which is divisible by m.

i.e. a + c ≡ b + d (mod m)

Now, to show: ac ≡ bd (mod m) we need to prove that m | (ac) - (bd).

(a+c) – (b + d) = [(b +km) (d +lm)] - (bd) ----------from (i) and (ii)

= bd +blm + dkm + klm^2 - bd

= (bl + dk + kl)m, which is divisible by m.

i.e. ac ≡ bd (mod m).

2.2 PRIME NUMBERS

An integer ‘p’ greater than 1 is called prime if the only positive factors of ‘p’ are 1 and p. A positive integer that is greater than 1 and is not prime is called composite.

The integer n is composite if and only if there exists an integer a such that a | n and 1 <a<n.

THEROREM 1: THE FUNDAMENTAL THEOREM OF ARITHMETIC

Every integer greater than 1 can be written uniquely as a prime or as the product of two or more primes where the prime factors are written in order of non-decreasing size.

Example: The prime factorizations of 100, 641, 999, and 1024 are given by

$100 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 5^2$

641 = 641,

$999 = 3 \cdot 3 \cdot 3 \cdot 37 = 3^3 \cdot 37$

$1024 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^{10}$.

THEROREM 2:

If n is a composite integer, then n has a prime divisor less than or equal to √n.

Proof:

If n is composite, by the definition of a composite integer, we know that it has a factor ‘a’ with 1 <a<n. Hence, by the definition of a factor of a positive integer, we have n = ab---- (i), where 1 <b<n.

Let’s suppose a>√n and b>√n. then,

ab>√n. √n

ab>n, which is contradiction to (i).Hence,

a≤ √n or b≤√n.

Because both ‘a’ and ‘b’ are divisors of n, we see that n has a positive divisor not exceeding √n. This divisor is either prime or, by the fundamental theorem of arithmetic, has a prime divisor less than itself.

Example: Show that 101 is prime.

The only primes not exceeding √101 are 2, 3, 5, and 7. Because 101 is not divisible by 2, 3, 5, or 7 (the quotient of 101 and each of these integers is not an integer), it follows that 101 is prime.

THEROREM 3: EUCLID'S THEOREM

There are infinitely many prime numbers.

Proof:

Let's assume there are finitely many prime numbers, say, N prime numbers, N Ɛ Z^+

$\{P_1 , P_2 , P_3 , P_4 , \ldots\ldots\ldots\ldots\ldots P_n\}$

Let, $Q= P_1P_2P_3P_4\ldots\ldots P_n + 1$

$Q>P_1 , Q>P_2 , Q>P_3 , \ldots\ldots Q>P_n$ i.e $Q>P_i$

Therefore Q is greater than the biggest prime number which implies Q is a composite number. Since, Q is composite it is divisible by at least one prime number.

Let Q is divisible by P_1 such that (Q/P_1) Ɛ Z^+,

$$\frac{Q}{p_1} = \frac{p_1p_2p_3\ldots\ldots\ldots p_n+1}{p_1}$$

$$\frac{Q}{p_1} = p_2p_3 \ldots\ldots\ldots p_n + \frac{1}{p_1}$$

$$\frac{Q}{p_1} \notin Z^+$$

Similar Q is not divisible by $P_2, P_3, \ldots\ldots P_n$. Therefore Q is a prime number which is contradiction.

Hence, there are infinitely many prime numbers.

MERSENNE PRIMES: Mersenne primes are prime numbers of the form 2^p - 1, where p is also a prime number. The first few Mersenne primes are:

3 (corresponding to p=2)

7 (corresponding to p=3)

31 (corresponding to p=5)

127 (corresponding to p=7)

8191 (corresponding to p=13)

Mersenne primes are relatively rare, and only 51 of them are currently known.

TWIN PRIME: Twin primes are pairs of prime numbers that differ by 2. In other words, two prime numbers p and q are twin primes if q = p + 2. For example, (3, 5), (5, 7), (11, 13), and (17, 19) are all twin primes.

GOLDBACH'S CONJECTURE: Goldbach's Conjecture is a famous unsolved problem in number theory. The conjecture states that every even integer greater than 2 can be expressed as the sum of two prime numbers.

For example, 4 can be written as 2+2, 6 as 3+3, 8 as 3+5, 10 as 3+7 or 5+5, and so on. The conjecture suggests that there is always a way to express any even integer as the sum of two prime numbers.

2.3 GREATEST COMMON DIVISORS

Let 'a' and 'b' be integers, not both zero. The largest integer 'd' such that d | a and d | b is called the greatest common divisor of 'a' and 'b'. The greatest common divisor of a and b is denoted by gcd(a, b).

Q. What is the greatest common divisor of 24 and 36?

Solution:

The positive common divisors of 24 and 36 are 1, 2, 3, 4, 6, and 12. Hence,

$$\gcd(24, 36) = 12$$

Q. What is the greatest common divisor of 17 and 22?

Solution:

The integers 17 and 22 have no positive common divisors other than 1, so that

$$\gcd(17, 22) = 1$$

RELATIVELY PRIME: The integers 'a' and 'b' are relatively prime if their greatest common divisor is 1. In above example 17 and 22 are relatively prime.

PAIRWISE RELATIVELY PRIME: The integers $a_1, a_2,\ldots,a_n$ are pairwise relatively prime if $\gcd(a_i, a_j) = 1$ whenever $1 \leq i < j \leq n$.

Q. Determine whether the integers 10, 17, and 21 are pairwise relatively prime and whether the integers 10, 19, and 24 are pairwise relatively prime.

Solution:

Because gcd(10, 17) = 1, gcd(10, 21) = 1, and gcd(17, 21) = 1, we conclude that 10, 17, and 21 are pairwise relatively prime.

Because gcd(10, 24) = 2 > 1, we see that 10, 19, and 24 are not pairwise relatively prime.

Another way to find the greatest common divisor of two positive integers is to use the prime factorizations of these integers. Suppose that the prime factorizations of the positive integers 'a' and 'b' are

$$a = P_1^{a1} \cdot P_2^{a2} \cdot \ldots\ldots\ldots P_n^{an}$$

$$b = P_1^{b1} \cdot P_2^{b2} \cdot \ldots\ldots\ldots\ldots P_n^{bn}$$

Then gcd(a, b) is given by

$$\gcd(a, b) = P_1^{\min(a1, b1)} \cdot P_2^{\min(a2, b2)} \ldots\ldots\ldots P_n^{\min(an, bn)}$$

Q. What is the greatest common divisor of 120 and 500?

Solution

The prime factorizations of $120 = 2^3 \cdot 3 \cdot 5$

The prime factorizations of $500 = 2^2 \cdot 5^3$

The greatest common divisor is $\gcd(120, 500) = 2^{\min(3, 2)} \cdot 3^{\min(1, 0)} \cdot 5^{\min(1, 3)}$

$$= 2^2 3^0 5^1$$

$$= 20$$

LEAST COMMON MULTIPLE (LCM)

The least common multiple of the positive integers 'a' and 'b' is the smallest positive integer that is divisible by both 'a' and 'b'. The least common multiple of 'a' and 'b' is denoted by LCM (a, b).

Q. What is the Least common multiple of 3 and 15?

Solution:

The LCM of 3 and 5 is 15, because 15 is the smallest positive integer that is both a multiple of 3 and a multiple of 5.Hence, LCM (3, 15) = 15

Another way to find the least common multiple of two positive integers is to use the prime factorizations of these integers. Suppose that the prime factorizations of the positive integers 'a' and 'b' are

$a = P_1^{a1}.\ P_2^{a2}\cdot\ldots\ldots P_n^{an}$

$b = P_1^{b1}.\ P_2^{b2}\cdot\ldots\ldots\ldots P_n^{bn}$

Then LCM(a, b) is given by

$$\gcd(a, b) = P_1^{\max(a1, b1)}.\ P_2^{\max(a2, b2)}\ldots\ldots P_n^{\max(an, bn)}$$

Q. What is the least common multiple of 120 and 500?

Solution

The prime factorizations of $120 = 2^3 \cdot 3 \cdot 5$

The prime factorizations of $500 = 2^2 \cdot 5^3$

The greatest common divisor is LCM (120, 500) $= 2^{\max(3, 2)}. 3^{\max(1, 0)}. 5^{\max(1, 3)}$

$$= 2^3 3^1 5^3$$

$$= 3000$$

THEOREM 1:

Let 'a' and 'b' be positive integers. Then $ab = \gcd(a, b) \cdot \text{lcm}(a, b)$

Proof:

To prove this theorem, we can use the fact that any positive integer can be uniquely expressed as a product of prime factors.

Let $a = p_1^{e1} * p_2^{e2} * \ldots * p_k^{ek}$ and $b = p_1^{f1} * p_2^{f2} * \ldots * p_l^{fl}$ be the prime factorization of a and b

The gcd of a and b is given by,

$$\gcd(a, b) = p_1^{\min(e1, f1)} * p_2^{\min(e2, f2)} * \ldots * p_k^{\min(ek, fk)}$$

The lcm of a and b is given by,

$$\text{lcm}(a, b) = p_1^{\max(e1, f1)} * p_2^{\max(e2, f2)} * \ldots * p_k^{\max(ek, fk)}$$

Multiplying these two expressions gives:

$$\gcd(a, b) * \text{lcm}(a, b) = p_1^{(\min(e1, f1) + \max(e1, f1))} * p_2^{(\min(e2, f2) + \max(e2, f2))} * \ldots * p_k^{(\min(ek, fk) + \max(ek, fk))}$$

Now, note that for any integers x and y, we have $\min(x, y) + \max(x, y) = x + y$. Applying this rule to the exponents in the above expression, we get:

$$\gcd(a, b) * \text{lcm}(a, b) = p_1^{(e1 + f1)} * p_2^{(e2 + f2)} * \ldots * p_k^{(ek + fk)}$$

This is just the product of the prime factorizations of 'a' and 'b', which is equal to 'ab'. Thus, we have shown that $\gcd(a, b) * \text{lcm}(a, b) = ab$

THEOREM 2: THE EUCLIDEAN ALGORITHM

Computing the greatest common divisor of two integers directly from the prime factorizations of these integers is inefficient. The reason is that it is time-consuming to find prime factorizations. There is more efficient method of finding the greatest common divisor, called the Euclidean algorithm.

The algorithm works as follows:

1. Given two integers 'a' and 'b', where 'a' is greater than or equal to 'b', divide 'a' by 'b' and get the remainder 'r'.
2. If 'r' is equal to 0, then the GCD of 'a' and 'b' is equal to 'b'.
3. If 'r' is not equal to 0, then replace 'a' with 'b' and 'b' with 'r', and repeat step 1 & 2.

For example, let's find the GCD of 84 and 60:

a=84 divided by b=60 gives a remainder of r=24.

a=60 divided by b=24 gives a remainder of r=2.

a=24 divided by b=12 gives a remainder of r=0.

Since the remainder is now 0, the GCD of 84 and 60 is the final value of 12.

Q. Find the greatest common divisor of 414 and 662 using the Euclidean algorithm

Solution:

Here let, a=662and b=414

a	b	r= a%b
662	414	662%414 = 248
414	248	414%248 = 166
248	166	248%166 = 82
166	82	166%82 = 2
82	2	82 %2 = 0

Since the remainder is now 0, the GCD of 662 and 414 is the final value of 2.

The Euclidean algorithm is based on the following lemma about greatest common divisors and the division algorithm.

Let a = bq + r, where a, b, q, and r are integers. Then gcd (a, b) = gcd (b, r)

THEOREM 3: BÉZOUT'S THEOREM

If 'a' and 'b' are positive integers, then there exist integers 's' and 't' such that:
gcd(a, b) = sa + tb**(Bézout's identity).** In other words, gcd(a, b) can be expressed as a linear combination with integer coefficients of a and b. Here 's' and 't' are called **Bézout coefficients.** 's' and 't' are not necessarily positive.

Q. Express gcd(252, 198) = 18 as a linear combination of 252 and 198.

Solution:

a	b	q=r/b	r = a%b	a=bq + r
252	198	252/198=1	252%198 = 54	252 = 1 · 198 + 54 ----------(i)
198	54	198/54 = 3	198%54 = 36	198 = 3 · 54 + 36 ----------(ii)
54	36	54/36=1	54%36=18	54 = 1 · 36 + 18 ----------(iii)
36	18	36/18=2	36%18 = 0	36 = 2 · 18 + 0 ----------(iv)

From (iii) we have,

$$54 = 1 \cdot 36 + 18$$

$$18 = 54 - 1 \cdot 36$$

Substituting value of 36 from (ii),

$$18 = 54 - 1 \cdot (198 - 3 \cdot 54)$$

$$18 = 54 - 1 \cdot 198 + 1 \cdot 3 \cdot 54$$

$$18 = 4 \cdot 54 - 1 \cdot 198$$

Substituting value of 54 from (i),

$$18 = 4 \cdot (252 - 1 \cdot 198) - 1 \cdot 198$$

$$18 = 4 \cdot 252 - 4 \cdot 1 \cdot 198 - 1 \cdot 198$$

$$18 = 4 \cdot 252 - 5 \cdot 198$$

$$\mathbf{18 = (4) \cdot 252 + (-5) \cdot 198}$$

THEOREM 4: THE EXTENDED EUCLIDEAN ALGORITHM

The extended Euclidean algorithm is an extension of the Euclidean algorithm, which is used to find the greatest common divisor (GCD) of two integers. The extended Euclidean algorithm finds not only the GCD of two integers, but also the coefficients that can be used to express the GCD as a linear combination of the two integers.

More formally, given two integers 'a' and 'b', the extended Euclidean algorithm finds the GCD d = gcd (a, b), and two integers 's' and 't' such that: sa + tb = d

The extended Euclidean algorithm steps are:

1. Initialize two pairs of numbers: (r0, s0, t0) = (a, 1, 0) and (r1, s1, t1) = (b, 0, 1).
2. Compute the remainder r2 = r0 mod r1, and compute the quotient q = r0 / r1.
3. Compute the new triple (r2, s2, t2), where:

   r2 = r0 - q * r1
   s2 = s0 - q * s1
   t2 = t0 - q * t1
4. Set (r0, s0, t0) = (r1, s1, t1), and set (r1, s1, t1) = (r2, s2, t2).
5. Repeat steps 2-4 until r2 = 0.
6. The GCD of 'a' and 'b' is given by d = r1, and the Bézout coefficients are given by s = s1 and t = t1

Q. Find the GCD of 56 and 15, and express it as a linear combination of 56 and 15.

Solution:

q=r0/r1	r0	s0	t0	r1	s1	t1	r2= r0 - q * r1	s2= s0 - q * s1	t2 =t0 - q * t1
3	56	1	0	15	0	1	11	1	-3
1	15	0	1	11	1	3	4	-1	4
2	11	1	3	4	-1	4	3	3	-11
1	4	-1	4	3	3	-11	1	-4	15
3	3	3	-11	1	-4	15	0		

The GCD of 56 and 15 is given by d = r1 = 1, and the Bézout coefficients are given by s = s1=-4 and t = 15 i.e $1= (-4)\cdot 56 + (15)\cdot 15$

3. MATRIX

A matrix is a rectangular array of numbers. A matrix with m rows and n columns is called an m × n matrix.

The matrix $\begin{bmatrix} 1 & 1 \\ 0 & 2 \\ 1 & 3 \end{bmatrix}$ is 3*2 matrix.

Let 'm' and 'n' be positive integers and let

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}$$

The (i, j)th element or entry of A is the element a_{ij} , that is, the number in the ith row and jth column of A. The convenient shorthand notation for expressing the matrix A is to write A = $[a_{ij}]$, which indicates that A is the matrix with its (i, j)th element equal to a_{ij}.

3.1 MATRIX ARITHMETIC

a. TRANSPOSE:

The transpose of an m × n matrix A = $[a_{ij}]$ is defined as the n × m matrix B = $[b_{ij}]$, with $b_{ij} = a_{ji}$ for $1 \leq i \leq m$ and $1 \leq j \leq n$. The transpose of A is denoted by A^t .

$$\text{For example, if } A = \begin{bmatrix} 1 & 4 & 5 \\ 0 & 1 & 2 \end{bmatrix} \text{ then } A^t = \begin{bmatrix} 1 & 0 \\ 4 & 1 \\ 5 & 2 \end{bmatrix}$$

- ***A matrix A is called symmetric if $A^t = A$ and skew-symmetric if $A^t = -A$***
- ***A matrix A is said to be orthogonal if $AA^t = A^tA = I$.***

Example 1. Let $A = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 4 & -1 \\ 3 & -1 & 4 \end{bmatrix}$ and $B = \begin{bmatrix} 0 & 1 & 2 \\ -1 & 0 & -3 \\ -2 & 3 & 0 \end{bmatrix}$. Then A is a symmetric matrix and B is a skew-symmetric matrix.

The following theorem gives some basic properties of Transpose:

- $(A^t)^t = A$
- $(A + B) = A^t + B^t$
- $(AB)^t = B^tA^t$

b. ADDITION:

Let $A = [a_{ij}]$ and $B = [b_{ij}]$ be m × n matrices. The sum of A and B, denoted by A + B, is the m × n matrix that has $a_{ij} + b_{ij}$ as its $(i, j)^{th}$ element. In other words, $A + B = [a_{ij} + b_{ij}]$.

$$\begin{bmatrix} 1 & 0 & -1 \\ 2 & 2 & -3 \\ 3 & 4 & 0 \end{bmatrix} + \begin{bmatrix} 3 & 4 & -1 \\ 1 & -3 & 0 \\ -1 & 1 & 2 \end{bmatrix} = \begin{bmatrix} 4 & 4 & -2 \\ 3 & -1 & -3 \\ 2 & 5 & 2 \end{bmatrix}$$

The following theorem gives some basic properties of matrix addition:

i. A + B = B + A

ii. (A + B) + C = A + (B + C)

A + 0 = 0 + A = A

(The matrix whose all elements are zero is called zero matrix and denoted by 0)

c. MULTIPLICATION:

Let A be an m × k matrix and B be a k × n matrix. The product of A and B, denoted by AB, is the m × n matrix with its $(i, j)^{th}$ entry equal to the sum of the products of the corresponding elements from the i^{th} row of A and the j^{th} column of B. In other words, if $AB = [c_{ij}]$, then $c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \cdots + a_{ik}b_{kj}$.

For example, if $A = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 4 & 1 \end{bmatrix}$ and $B = \begin{bmatrix} 1 & 2 & 1 \\ 0 & 0 & 3 \\ 1 & 0 & 4 \end{bmatrix}$ then

$$AB = \begin{bmatrix} 1+0+3 & 2+0+0 & 1+6+12 \\ 2+0+1 & 4+0+0 & 2+12+4 \end{bmatrix} = \begin{bmatrix} 4 & 2 & 19 \\ 3 & 4 & 18 \end{bmatrix}.$$

Identity Matrix:

A square matrix $A = [a_{ij}]$ with $a_{ij} = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j \end{cases}$ is called the identity matrix, denoted by I_n.

For example, $I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, and $I_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$.

The following theorem gives some basic properties of Matrix multiplication:

- A(BC) = (AB)C
- A(B + C) = AB + AC
- (A+B)C = AC + BC
- If A is an n × n matrix then $AI_n = I_nA = A$.

Multiplicative Inverse: If A and B are two n*n matrix then we say B is the inverse of A if $AB=I_n$ and $BA =I_n$, where I_n is the identity matrix of order n*n.

3.2 BOOLEAN MATRIX OPERATIONS

A matrix all of whose entries are either 0 or 1 is called a zero–one matrix or Boolean/bit matrix.

JOIN: Let A = $[a_{ij}]$ and B = $[b_{ij}]$ be m × n zero–one matrices. Then the join of A and B is the zero–one matrix with $(i, j)^{th}$ entry $a_{ij} \vee b_{ij}$. The join of A and B is denoted by $A \vee B$.

$$\mathbf{A} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}, \qquad \mathbf{B} = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \end{bmatrix}.$$

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

MEET: Let A = $[a_{ij}]$ and B = $[b_{ij}]$ be m × n zero–one matrices. Then the meet of A and B is the zero–one matrix with $(i, j)^{th}$ entry $a_{ij} \wedge b_{ij}$. The join of A and B is denoted by $A \wedge B$.

$$\mathbf{A} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}, \qquad \mathbf{B} = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \end{bmatrix}.$$

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

BOOLEAN PRODUCT OF TWO MATRICES: Let A = $[a_{ij}]$ be an m × k zero–one matrix and B = $[b_{ij}]$ be a k × n zero–one matrix. Then the Boolean product of A and B, denoted by A (.) B, is the m × n matrix with $(i, j)^{th}$ entry c_{ij} where,

$$c_{ij} = (a_{i1} \wedge b_{1j}) \vee (a_{i2} \wedge b_{2j}) \vee \cdots \vee (a_{ik} \wedge b_{kj})$$

The Boolean product of A and B is obtained in an analogous way to the ordinary product of these matrices, but with addition replaced with the operation ∨ and with multiplication replaced with the operation ∧.

$$\mathbf{A} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 0 \end{bmatrix}, \qquad \mathbf{B} = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}.$$

The Boolean product $\mathbf{A} \odot \mathbf{B}$ is given by

$$\begin{aligned} \mathbf{A} \odot \mathbf{B} &= \begin{bmatrix} (1 \wedge 1) \vee (0 \wedge 0) & (1 \wedge 1) \vee (0 \wedge 1) & (1 \wedge 0) \vee (0 \wedge 1) \\ (0 \wedge 1) \vee (1 \wedge 0) & (0 \wedge 1) \vee (1 \wedge 1) & (0 \wedge 0) \vee (1 \wedge 1) \\ (1 \wedge 1) \vee (0 \wedge 0) & (1 \wedge 1) \vee (0 \wedge 1) & (1 \wedge 0) \vee (0 \wedge 1) \end{bmatrix} \\ &= \begin{bmatrix} 1 \vee 0 & 1 \vee 0 & 0 \vee 0 \\ 0 \vee 0 & 0 \vee 1 & 0 \vee 1 \\ 1 \vee 0 & 1 \vee 0 & 0 \vee 0 \end{bmatrix} \\ &= \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix}. \end{aligned}$$

Let A, B, C are Boolean matrices of compatible sizes, then

1. (a) $\mathbf{A} \vee \mathbf{B} = \mathbf{B} \vee \mathbf{A}$.
   (b) $\mathbf{A} \wedge \mathbf{B} = \mathbf{B} \wedge \mathbf{A}$.
2. (a) $(\mathbf{A} \vee \mathbf{B}) \vee \mathbf{C} = \mathbf{A} \vee (\mathbf{B} \vee \mathbf{C})$.
   (b) $(\mathbf{A} \wedge \mathbf{B}) \wedge \mathbf{C} = \mathbf{A} \wedge (\mathbf{B} \wedge \mathbf{C})$.
3. (a) $\mathbf{A} \wedge (\mathbf{B} \vee \mathbf{C}) = (\mathbf{A} \wedge \mathbf{B}) \vee (\mathbf{A} \wedge \mathbf{C})$.
   (b) $\mathbf{A} \vee (\mathbf{B} \wedge \mathbf{C}) = (\mathbf{A} \vee \mathbf{B}) \wedge (\mathbf{A} \vee \mathbf{C})$
4. $(\mathbf{A} \odot \mathbf{B}) \odot \mathbf{C} = \mathbf{A} \odot (\mathbf{B} \odot \mathbf{C})$.

4. BASIS OF COUNTING

In discrete mathematics, counting is the process of determining the number of possible outcomes of a given set of objects or events.

THE PRODUCT RULE: Suppose that a procedure can be broken down into a sequence of two tasks. If there are n_1 ways to do the first task and for each of these ways of doing the first task, there are n_2 ways to do the second task, then there are n_1n_2 ways to do the procedure.

- **Suppose you have 3 shirts and 4 pairs of pants. How many different outfits can you create by selecting one shirt and one pair of pants?**

Solution:

Using the product rule, we can count the number of possible outfits by multiplying the number of choices for the shirt and the number of choices for the pants. Since we have 3 choices for the shirt and 4 choices for the pants, the total number of outfits is:

Number of outfits = 3 x 4 = 12

Therefore, there are 12 different outfits that can be created by selecting one shirt and one pair of pants from the given options.

An extended version of the product rule is often useful. Suppose that a procedure is carried out by performing the tasks T_1, T_2... T_m in sequence. If each task T_i, $i = 1, 2,...,n$, can be done in n_i ways, regardless of how the previous tasks were done, then there are $n_1 \cdot n_2 \cdot \cdots \cdot n_m$ ways to carry out the procedure

- **Suppose you want to create a password using a combination of four uppercase letters and two digits. How many possible passwords can you create?**

Solution:

Since we want to create a password with four uppercase letters and two digits, we have a total of 6 characters to choose.

First, let's consider the number of choices for each uppercase letter. We have 26 letters in the English alphabet, and each letter can be only uppercase. Therefore, there are 26 possible choices for each letter.

Next, let's consider the number of choices for each digit. We have 10 digits, from 0 to 9. Therefore, there are 10 possible choices for each digit.

Using the product rule, the total number of possible passwords is:

Number of passwords = 26*26*26*26*10*10= 45,697,600

Therefore, there are 45,697,600 possible passwords that can be created using a combination of four uppercase letters and two digits.

THE SUM RULE: If a task can be done either in one of n_1 ways or in one of n_2 ways, where none of the set of n_1 ways is the same as any of the set of n_2 ways, then there are $n_1 + n_2$ ways to do the task.

- **Suppose you are planning a trip to a city with two different modes of transportation available: car and train. There are two different car rental companies and three different train companies to choose from. How many ways can you choose your mode of transportation?**

Solution:

Using the sum rule of counting, we can add the number of choices for each mode of transportation to find the total number of ways to choose:

Number of ways to choose mode of transportation = number of ways to choose a car + number of ways to choose a train

Number of ways to choose a car = number of car rental companies = 2

Number of ways to choose a train = number of train companies = 3

Therefore, the total number of ways to choose your mode of transportation is:

Number of ways to choose mode of transportation = number of ways to choose a car + number of ways to choose a train = 2 + 3 = 5

Therefore, there are 5 ways to choose the mode of transportation: we can rent a car from either of the two car rental companies, or we can take a train from any of the three train companies.

- **Suppose you want to choose a shirt to wear today from a selection of 5 different shirts in your closet. Additionally, you want to choose a pair of pants to wear today from a selection of 3 different pairs of pants in your closet. How many different outfit choices do you have?**

Solution:

Using the sum rule of counting, we can count the total number of possible outfit choices by adding the number of choices for the shirt and the number of choices for the pants. Since we have 5 choices for the shirt and 3 choices for the pants, the total number of outfit choices is:

Number of outfit choices = number of choices for shirt + number of choices for pants = 5 + 3 = 8

Therefore, there are 8 different outfit choices that can be created by selecting one shirt and one pair of pants from the closet.

Q.1 Each user on a computer system has a password, which is six to eight characters long, where each character is an uppercase letter or a digit. Each password must contain at least one digit. How many possible passwords are there?

Solution:

Let P be the total number of possible passwords, and let P6, P7, and P8 denote the number of possible passwords of length 6, 7, and 8, respectively.

By the sum rule, P = P6 + P7 + P8.

We will now find P6, P7, and P8. Finding P6 directly is difficult. To find P6 it is easier to find the number of strings of uppercase letters and digits that are six characters long, including those with no digits, and subtract from this the number of strings with no digits.

By the product rule,

The number of strings of six characters is 36^6, and the number of strings with no digits is 26^6. Hence, P6 = $36^6 - 26^6$ = 2,176,782,336 − 308,915,776 = 1,867,866,560.

Similarly, we have P7 = $36^7 - 26^7$ = 78,364,164,096 − 8,031,810,176 = 70,332,353,920 and P8 = $36^8 - 26^8$ = 2,821,109,907,456 − 208,827,064,576 = 2,612,282,842,880.

Consequently, P = P6 + P7 + P8 = 2,684,483,063,360.

Q.2 How many strings of eight uppercase English letters are there

a) If letters can be repeated?

b) If no letter can be repeated?

c) That start with X, if letters can be repeated?

d) That start with X, if no letter can be repeated?

e) That start and end with X, if letters can be repeated?

f) That start with the letters BO (in that order), if letters can be repeated?

g) That start and end with the letters BO (in that order), if letters can be repeated?

h) That start or end with the letters BO (in that order), if letters can be repeated?

Solution:

a) If letters can be repeated, then there are 26 choices for each of the 8 positions. Therefore, the total number of strings of eight uppercase English letters is:

26^8 = 208,827,064,576

b) If no letter can be repeated, then there are 26 choices for the first position, 25 choices for the second position (*since one letter has already been used*), 24 choices for the third position (*since two letters have already been used*), and so on. Therefore, the total number of strings of eight uppercase English letters with no repetition is:

26 * 25 * 24 *23 *22 *21 *20 *19 = 10,068,347,520

c) If the strings must start with X and letters can be repeated, then there is only one choice for the first position, which must be X, and 26 choices for each of the remaining 7 positions.

Therefore, the total number of strings of eight uppercase English letters that start with X and allow repetition is:

$1 * 26^7 = 2{,}116{,}551{,}424$

d) If the strings must start with X and no letter can be repeated, then there is only one choice for the first position, which must be X, and 25 choices for the second position (*since X has already been used*), 24 choices for the third position, and so on. Therefore, the total number of strings of eight uppercase English letters that start with X and have no repetition is:

$1 * 25 * 24 * 23 * 22 * 21 * 20 * 19 = 30{,}062{,}880$

e) If the strings must start and end with X and letters can be repeated, then there is only one choice for the first and last positions, which must be X, and 26 choices for each of the remaining 6 positions. Therefore, the total number of strings of eight uppercase English letters that start and end with X and allow repetition is:

$1 * 26^6 * 1 = 308{,}915{,}776$

f) If the strings must start with the letters BO (in that order) and letters can be repeated, then there is only one choice for the first two positions, which must be BO, and 26 choices for each of the remaining 6 positions. Therefore, the total number of strings of eight uppercase English letters that start with BO and allow repetition is:

$1 * 26^6 = 308{,}915{,}776$

g) If the strings must start and end with the letters BO (in that order) and letters can be repeated, then there is only one choice for the first and last two positions, which must be BO, and 26 choices for each of the remaining 4 positions. Therefore, the total number of strings of eight uppercase English letters that start and end with BO and allow repetition is:

$1 * 26^4 * 1 = 456{,}976$

h) If the strings must start or end with the letters BO (in that order) and letters can be repeated, then we can use the sum rule of counting to add the number of strings that start with BO and the number of strings that end with BO. From the previous parts, we know that the number of strings that start with BO and allow repetition is 26^6, and the number of strings that end with

BO and allow repetition is also 26^6. Therefore, the total number of strings of eight uppercase English letters that start or end with BO and allow repetition is:

$26^6 + 26^6 = 617,831,552$

THE SUBTRACTION RULE(principle of inclusion–exclusion): If a task can be done in either n1 ways or n2 ways, then the number of ways to do the task is n1 + n2 minus the number of ways to do the task that are common to the two different ways.

$$A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|$$

- **How many bit strings of length eight either start with a 1 bit or end with the two bits 00?**

Solution:

To count the number of bit strings of length eight that either start with a 1 bit or end with the two bits 00, we can use the principle of inclusion-exclusion.

Let A be the set of bit strings of length eight that start with a 1 bit, and let B be the set of bit strings of length eight that end with the two bits 00. We want to count the number of bit strings that are in either A or B, or both.

The number of bit strings in A is simply $1*2^7$, since the first bit is fixed to be 1 and the remaining 7 bits can be either 0 or 1.

The number of bit strings in B is also easy to count. We fix the last two bits to be 00, and the remaining 6 bits can be any combination of 0s and 1s, so there are $2^6 *1*1$ such bit strings.

However, we have double-counted the bit strings that both start with a 1 bit and end with the two bits 00. These are the bit strings of the form 1_ _ _ _ _ 00.

There are $1*2^5*1*1$ such bit strings, since we can choose whether each of the remaining 5 bits is 0 or 1.

Therefore, the total number of bit strings of length eight that either start with a 1 bit or end with the two bits 00 is:

$|A \cup B| = |A| + |B| - |A \cap B| = 2^7 + 2^6 - 2^5 = 192.$

4.1 THE PIGEONHOLE PRINCIPLE:

It states that if there are more pigeons than pigeonholes, then at least one pigeonhole must contain more than one pigeon.

In other words, if we have ‘n’ objects to be placed into ‘m’ containers and ‘n > m’, then at least one of the containers must contain more than one object.

Example:

- In a group of 367 people, at least two people must have the same birthday. This is because there are only 366 possible birthdays (including February 29th in a leap year), so if there are 367 people, at least two of them must share a birthday.

Q.1 Show that if any five numbers from 1 to 8 are chosen, then two of them will add to 9?

Solution:

We divide the set of numbers from 1 to 8 into four pigeonholes as follows:

- Pigeonhole 1: {1, 8}
- Pigeonhole 2: {2, 7}
- Pigeonhole 3: {3, 6}
- Pigeonhole 4: {4, 5}

Each of five chosen must belong to one of these pigeonhole. Since, there are only four sets, by the pigeonhole principle, at least two of the chosen numbers must fall into the same pigeonhole.

Q.2 Show that if any eight positive integers are chosen two of them will have same remainder when divided by 7.

Solution:

We can divide the set of positive integers into 7 pigeonholes according to their remainder when divided by 7:

- Pigeonhole 0: Positive integers that leave a remainder of 0 when divided by 7.
- Pigeonhole 1: Positive integers that leave a remainder of 1 when divided by 7.
- Pigeonhole 2: Positive integers that leave a remainder of 2 when divided by 7.
- Pigeonhole 3: Positive integers that leave a remainder of 3 when divided by 7.
- Pigeonhole 4: Positive integers that leave a remainder of 4 when divided by 7.
- Pigeonhole 5: Positive integers that leave a remainder of 5 when divided by 7.
- Pigeonhole 6: Positive integers that leave a remainder of 6 when divided by 7.

Since there are 8 positive integers chosen, by the pigeonhole principle, at least two of them must fall into the same pigeonhole. That is, if we choose any 8 positive integers, there must be at least one pair of integers that leave the same remainder when divided by 7.

To see why, suppose that each of the 8 chosen positive integers leaves a different remainder when divided by 7. Then there can be at most one integer in each of the 7 pigeonholes, and the 8th integer must be in a new pigeonhole. But this would mean that we have created 8 distinct pigeonholes, which is impossible since there are only 7 possible remainders when dividing by 7.

THE GENERALIZED PIGEONHOLE PRINCIPLE: If N objects are placed into k boxes, then there is at least one box containing at least $\lceil N/k \rceil$ objects.

Q.1 Find the minimum number of students in a class to be sure that four of them are born in the same month.

Solution

There are 12 months in a year, so we can consider each month as a pigeonhole i.e. k=12.

We want to find the minimum number of students i.e. N such that at least 4 of them fall into the same pigeonhole (month). Then by generalized pigeonhole principle,

$\lceil N/k \rceil \geq 4$

$\lceil N/12 \rceil \geq 4$

The smallest integer N such that $\lceil N/12 \rceil \geq 4$ is $N = 12 \cdot 3 + 1 = 37$

Therefore there should be minimum of 37 student in a class.

Q.2 How many cards must be selected from a standard deck of 52 cards to guarantee that
a) At least three cards of the same suit are chosen?
b) At least three cards of same value are selected?

Solution

A standard deck of 52 cards has 13 kinds of cards, with four cards of each of kind, one in each of the four suits, hearts, diamonds, spades, and clubs.

(a) Let us consider each suit as a pigeonhole i.e. k=4

We want to find the minimum number of cards i.e. N such that at least 3 of them fall into the same pigeonhole (suit). Then by generalized pigeonhole principle,

$\lceil N/k \rceil \geq 3$

$\lceil N/4 \rceil \geq 3$

The smallest integer N such that $\lceil N/4 \rceil \geq 3$ is $N = 2 \cdot 4 + 1 = 9$

Therefore minimum of 9 cards must be drawn such that at least three cards are of same suit.

(b) There are 13 values in a deck of cards: ace, 2, 3, 4, 5, 6, 7, 8, 9, 10, jack, queen, and king. Let us consider each value as a pigeonhole i.e. k= 13

We want to find the minimum number of cards i.e. N such that at least 3 of them fall into the same pigeonhole (value). Then by generalized pigeonhole principle,

$\lceil N/k \rceil \geq 3$

$\lceil N/13 \rceil \geq 3$

The smallest integer N such that $\lceil N/13 \rceil \geq 3$ is $N = 3 \cdot 13 + 1 = 40$

Therefore minimum of 40 cards must be drawn such that at least three cards are of same value.

4.2 PERMUTATION:

A permutation is a way of arranging a set of objects in a specific order. It is like shuffling a deck of cards or arranging a set of books on a shelf.

For example, if you have three objects labeled A, B, and C, the six possible permutations are: ABC, ACB, BAC, BCA, CAB, CBA.

Each permutation is a unique arrangement of the objects. The order in which the objects are arranged matters, so ABC is different from BAC, and so on.

If 'n' and 'r' are integers with $0 \leq r \leq n$, then P (n, r) = $\frac{n!}{(n-r)!}$

Q.1 How many 'words' of three distinct letters can be formed from the letters of the word MAST?

Solution:

The number is P (4, 3) = $\frac{4!}{(4-3)!}$ = 4! = 24

Q.2 How many permutations of the letters ABCDEFG contain

a) The string BCD?
b) The string CFGA?
c) The strings BA and GF?
d) The strings ABC and DE?
e) The strings ABC and CDE?

Solution:

a) The string BCD has three distinct letters, which we can consider as a single letter. There are then four other distinct letters left to arrange. Therefore, the number of permutations of the letters ABCDEFG that contain the string BCD is P (5, 5) = 120.

b) Similarly, the string CFGA can be considered as a single letter, leaving the remaining three distinct letters to arrange. Therefore, the number of permutations of the letters ABCDEFG that contain the string CFGA is P (4, 4) = 24.

c) To count the number of permutations that contain both BA and GF, we can consider BA and GF as two distinct objects that must be placed among the remaining three letters (C, D, and E). Therefore, the number of permutations of the letters ABCDEFG that contain both BA and GF is P (5, 5) = 120.

d) To count the number of permutations that contain both ABC and DE, we can consider ABC and DE as two distinct objects that must be placed among the remaining two letters (F, G). Therefore, the number of permutations of the letters ABCDEFG that both ABC and DE is P (4, 4) = 24.

e) To count the number of permutations that contain both ABC and CDE, we can consider ABC and CDE as two distinct objects that must be placed among the remaining one letters (F). Therefore, the number of permutations of the letters ABCDEFG that contain both ABC and CDE is P (3, 3) = 6.

The number of distinguishable permutations that can be formed from a collection of 'n' objects where the first object appears k_1 times, second object k_2 times and so on is: $\frac{n!}{k_1!k_2!\ldots k_t!}$

where $k_1+k_2+\ldots\ldots+k_t = n$

Q.3 how many distinguishable permutations of the letters in the word BANANA are there?

Solution:

$$= \frac{6!}{1!3!2!} = 60$$

4.3 COMBINATION:

A combination is a way of selecting items from a group without considering the order in which they are chosen. In other words, a combination is a collection of items that can be selected from a larger set, where the order in which the items are selected doesn't matter.

For example, suppose we have a set of three letters {A, B, C}. The possible combinations of two letters that can be chosen from this set are {AB, AC, BC}. Notice that each combination has two letters, but the order in which the letters appear doesn't matter. Therefore, {AB} and {BA} are considered the same combination.

The number of r-combinations of a set with 'n' elements, where 'n' is a nonnegative integer and 'r' is an integer with 0 ≤ r ≤ n, equals C (n, r) = $\frac{n!}{r!(n-r)!}$

Q.1 In how many ways can a committee of 3 people be selected from a group of 10?

Solution:

The problem involves finding the number of combinations of 3 people that can be chosen from a group of 10. We can use the formula for combinations:

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

Where n is the total number of items, r is the number of items to be selected

Using this formula, we can plug in the values n=10 and r=3:

10 C 3 = 10! / (3! (10-3)!) = 120

Therefore, there are 120 different ways to select a committee of 3 people from a group of 10.

Q.2 How many different seven-person committees can be formed each containing 3 women from an available set of 20 women and 4 men from an available set of 30 men?

Solution:

To form a committee with 3 women from a set of 20 women and 4 men from a set of 30 men, we need to select 3 women from 20 and 4 men from 30. We can do this separately and then multiply the results to get the total number of committees.

The number of ways to select 3 women from 20 is:

C (20, 3) = (20!)/ (3! *17!) = 1140

The number of ways to select 4 men from 30 is:

C (30, 4) = (30!)/ (4!*26!) = 27405

Therefore, the total number of different seven-person committees that can be formed, each containing 3 women from an available set of 20 women and 4 men from an available set of 30 men, is:

C (20, 3) * C (30, 4) = 1140 x 27405 = 31,231,700

So there are 31,231,700 different seven-person committees that can be formed with these requirements.

Q. 3 A microcomputer manufacturer who is designing an advertising campaign is considering six magazines, three newspaper, two television stations and four radio stations. In how many ways can six advertisements be run if :

(a) all six are to be in magazines?

(b) two are to be in magazines, two are to be in newspapers, one is to be on television and one is to be on radio?

Solution:

(a) If all six advertisements are to be in magazines, then there are 6 magazines to choose from, and we need to choose all 6 of them. This is a combination problem, and the number of ways to choose 6 magazines out of 6 is:

C (6, 6) = 1

Therefore, there is only 1 way to run all six advertisements in magazines.

(b) If two advertisements are to be in magazines, two are to be in newspapers, one is to be on television, and one is to be on radio, then we need to choose 2 magazines out of 6, 2 newspapers out of 3, 1 television station out of 2, and 1 radio station out of 4.

The number of ways to choose 2 magazines out of 6 is: C (6, 2) = 15

The number of ways to choose 2 newspapers out of 3 is: C (3, 2) = 3

The number of ways to choose 1 television station out of 2 is: C (2, 1) = 2

The number of ways to choose 1 radio station out of 4 is: C (4, 1) = 4

Therefore, the total number of ways to run the six advertisements as specified is:

C (6, 2) * C (3, 2) * C (2, 1) * C (4, 1) = 15 * 3 * 2 * 4 = 360

Therefore, there are 360 ways to run the six advertisements if two are to be in magazines, two are to be in newspapers, one is to be on television, and one is to be on radio.

Q.4 How many bit strings of length 10 contain:

a) Exactly four 1s?

b) At most four 1s?

c) At least four 1s?

d) An equal number of 0s and 1s?

Solution:

(a) To count the number of bit strings of length 10 with exactly four 1s is:

C (10, 4) = 210

Therefore, there are 210 bit strings of length 10 that contain exactly four 1s.

(b) To count the number of bit strings of length 10 with at most four 1s, we need to count the bit strings with zero, one, two, three, or four 1s. We can do this by adding up the number of bit strings with each of these possibilities:

- Bit strings with zero 1s: C(10, 0) = 1
- Bit strings with one 1: C(10, 1) = 10
- Bit strings with two 1s: C(10, 2) = 45
- Bit strings with three 1s: C(10, 3) = 120
- Bit strings with four 1s: C(10, 4) = 210

The total number of bit strings of length 10 with at most four 1s is the sum of the above values:

$$1 + 10 + 45 + 120 + 210 = 386$$

Therefore, there are 386 bit strings of length 10 that contain at most four 1s.

(c) To count the number of bit strings of length 10 with at least four 1s, we can count the complement, i.e., the number of bit strings with at most three 1s: C (10, 0) + C (10, 1) + C (10, 2) + C (10, 3) = 176

The number of bit strings with at least four 1s is: 2^{10} - 176 = 848

Therefore, there are 848bit strings of length 10 that contain at least four 1s.

(d) To count the number of bit strings of length 10 with an equal number of 0s and 1s, we need to have five 0s and five 1s in some order. C (10, 5) = 252

Therefore, there are 252 bit strings of length 10 that contain an equal number of 0s and 1s.

Q.5 A coin is flipped 10 times where each flip comes up either heads or tails. How many possible outcomes

a) Are there in total?

b) Contain exactly two heads?

c) Contain at most three tails?

d) Contain the same number of heads and tails?

Solution:

(a) There are two possible outcomes for each coin flip, so there are 2 options for the first flip, 2 options for the second flip, and so on, up to the 10^{th} flip. Therefore, the total number of possible outcomes is = 2^{10} = 1024

Therefore, there are 1024 possible outcomes.

(b) To count the number of outcomes with exactly two heads, we need to choose 2 of the 10 coin flips to be heads, and the other 8 flips must be tails.

$$C (10, 2) = 45$$

Therefore, there are 45 possible outcomes that contain exactly two heads.

(c) To count the number of outcomes with at most three tails, we need to count the number of outcomes with zero, one, two, or three tails. We can count these separately:

- Outcomes with zero tails: C(10, 0) = 1
- Outcomes with one tail: C(10, 1) = 10
- Outcomes with two tails: C(10, 2) = 45
- Outcomes with three tails: C(10, 3) = 120

The total number of outcomes with at most three tails is the sum of the above values:

$$1 + 10 + 45 + 120 = 176$$

Therefore, there are 176 possible outcomes that contain at most three tails.

(d) To count the number of outcomes with the same number of heads and tails, we need to have exactly 5 heads and 5 tails in some order. Therefore, there are: C (10, 5) = 252 possible outcomes with the same number of heads and tails.

CHAPTER: II

RELATIONS & FUNCTIONS

1. RELATIONS

CARTESIAN PRODUCT: The Cartesian product of two sets A and B, denoted as A x B, is the set of all ordered pairs (a, b) where a is an element of A and b is an element of B. In other words,

$$A \times B = \{(a, b) \mid a \quad A \text{ and } b \in B\}$$

For example, if A = {1, 2} and B = {a, b}, then their Cartesian product A x B would be:

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

For any two finite, nonempty sets A and B, $\lvert AxB\rvert = \lvert A\rvert\lvert B\rvert$

RELATION: Let A and B be sets. A binary relation from A to B is a subset of A × B. In notation, we can write: R ⊆ A x B.

If R ⊆ A x B and (a, b) ∈R, we say that a is related to b by R i.e. aRb.

Example 1: Let A = {1, 2, 3} and B = {6, 7, 8}. The relation R between A and B is defined as follows: R = {(a, b) | a is an even number and b is an even number}

A x B = {(1, 6), (1, 7), (1, 8), (2, 6), (2, 7), (2, 8), (3, 6), (3, 7), (3, 8)}
R = {(2, 6), (2, 8)} *[2R6, 2R8]*

Example 2: Let A = {1, 2, 3} and B = {6, 7, 8}. The relation R between A and B is defined as follows: R = {(a, b) | a divides b}

A x B = {(1, 6), (1, 7), (1, 8), (2, 6), (2, 7), (2, 8), (3, 6), (3, 7), (3, 8)}

R = {(1, 6), (1, 7), (1, 8), (2, 6), (2, 8), (3, 6)}

1.1 REPRESNTING RELATIONS:

i. The Matrix of a Relation: Suppose we have a relation R between sets A and B. Let a_1, a_2, ..., a_n be the elements of set A, and let b_1, b_2, ..., b_m be the elements of set B. We can represent the relation R as a matrix M_R with n rows and m columns, where the (i, j) entry of the matrix is 1 if (a_i, b_j) is in R, and 0 otherwise.

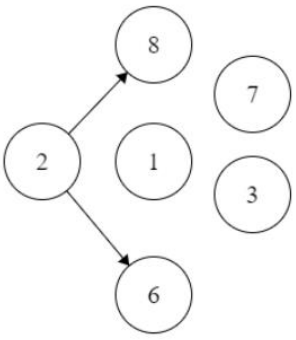
R	6	7	8
1	0	0	0
2	1	0	1
3	0	0	0

(M_R) Relation matrix of Example: 1

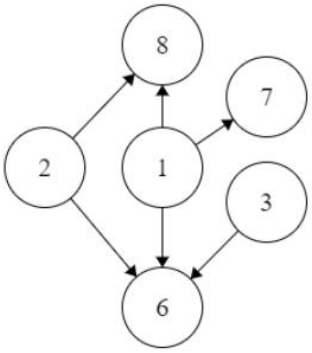
R	6	7	8
1	1	1	1
2	1	0	1
3	1	0	0

(M_R) Relation matrix of Example: 2

ii. The Digraph of a Relation: A relation between two sets can also be represented by a directed graph, which is called a digraph. To construct a digraph for a relation R between sets A and B, we first draw a node for each element in A and a node for each element in B. Then, for each ordered pair (a, b) in R, we draw a directed edge from the node corresponding to 'a' to the node corresponding to 'b'.



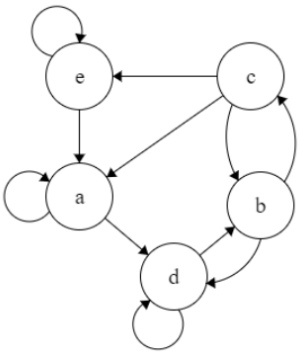
Diagraph of Example: 1



Diagraph of Example: 2

The Boolean operations join and meet can be used to find the matrices representing the union and the intersection of two relations.

Q. Let A= {a, b, c, d, e} and let R be given by the digraph below. Find M_R and R.



Solution:

M_R =

A x A	a	b	c	d	e
a	1	0	0	1	0
b	0	0	1	1	0
c	1	1	0	0	1
d	0	1	0	1	0
e	1	0	0	0	1

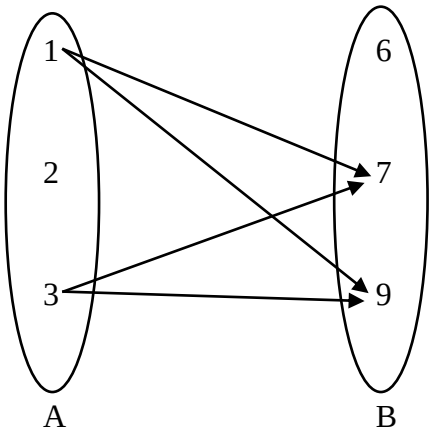
Relation, R = {(a, a), (a, d) , (b, c) , (b, d) , (c, a) , (c, b) , (c, e) , (d, b) , (d, d) , (e, a) , (e, e)}

DOMAIN, RANGE AND CODOMAIN:

Let A = {1, 2, 3} and B = {6, 7, 9}. The relation R between A and B is defined as follows: R = {(a, b) | a is odd and b is odd}

A x B = {(1, 6), (1, 7), (1, 9), (2, 6), (2, 7), (2, 9), (3, 6), (3, 7), (3, 9)}

R = {(1, 7), (1, 9), (3, 7), (3, 9)}



DOMAIN: The set which contains all the first elements of all ordered pairs of relation 'R' is known as Domain of relation. If we have two set A and B, R is a relation from A to B then,

$$Dom(R) = \{a \in A : (a, b) \in R \text{ for some } b \in B\}$$

In above example Domain, Dom(R) = {1, 3}

RANGE: The set which contains all the second elements of all ordered pairs of relation 'R' is known as Range of relation. If we have two set A and B, R is a relation from A to B then,

$$Ran(R) = \{b \in B : (a, b) \in R \text{ for some } a \in A\}$$

In above example Range, Ran(R) = {7, 9}

CODOMAIN: The codomain of R is the set of all elements b in B such that there is at least one element a in A such that (a, b) is an ordered pair in R.

In above example Codomain = {6, 7, 9}

1.2 TYPES OF RELATIONS:

1. INVERSE RELATION: The inverse of a relation is a new relation that results from swapping the order of the elements in each ordered pair of the original relation. The inverse of a relation R is denoted by R^{-1} and can be defined as:

$$\mathbf{R^{-1} = \{(b, a): (a, b) \in R\}}$$

Example, let R = {(1,2), (2,3), (3,4)} be a relation from the set A ={1,2,3} to the set B = {2,3,4}. The inverse relation R^{-1} is obtained by swapping the elements in each ordered pair of R, which gives: R^{-1}= {(2, 1), (3, 2), (4, 3)}

2. COMPLEMENT RELATION: The complement of R is the set of all possible ordered pairs from A × B that are not in R. The complement of R is denoted by R' or sometimes by R^c. Formally, the complement of a relation R can be defined as:

$$\mathbf{R' = \{(a, b): a \in A, b \in B, \text{and } (a, b) \notin R\}}$$

For example, let A = {1, 2, 3} and B = {4, 5, 6}, and let R = {(1, 4), (2, 5), (3, 6)} be a relation from A to B. The complement of R is given by:

R' = {(1,5), (1,6), (2,4), (2,6), (3,4), (3,5), (1,3), (2,3), (3,5), (3,4), (1,5), (2,4)}

3. IDENTITY RELATION: The identity relation on a set A is a special type of relation that relates every element of A to itself. Formally, the identity relation on a set A is defined as: **I = {(a, a): a ∈ A}.** In other words, the identity relation is the set of all ordered pairs (a, a) such that a belongs to A.

For example, let A = {1, 2, 3}. The identity relation on A is: I = {(1, 1), (2, 2), (3, 3)}

4. UNIVERSAL RELATION: The universal relation on a set A is a relation that relates every element of A to every other element of A. Formally, the universal relation on a set A is defined as: **U = {(a, b): a, b ∈ A}.** In other words, the universal relation is the set of all possible ordered pairs (a, b) such that a and b belong to A.

For example, let A = {1, 2, 3}. The universal relation on A is:

U = {(1,1), (1,2), (1,3), (2,1), (2,2), (2,3), (3,1), (3,2), (3,3)}

5. VOID (EMPTY) RELATION: The empty relation, also called the void or empty set relation, is a relation between two sets A and B that contains no ordered pairs. Formally, the empty relation between two sets A and B is defined as: **$\emptyset$ = {}.** In other words, the empty relation is the set of all ordered pairs that satisfy no conditions.

For example, let A = {1, 2, 3} and B = {4, 5, 6}.
The relation from A to B is defined as: R= {(a, b): a + b=0} is an empty relation.

1.3 PROPERTIES OF RELATION:

1. REFLEXIVE AND IRREFLEXIVE RELATIONS:

Reflexive Relations: A reflexive relation is a relation on a set A where every element of A is related to itself. In other words, for all a ∈ A, the ordered pair (a, a) belongs to the relation. Formally, a relation R on a set A is reflexive if for all a ∈ A, (a, a) ∈ R.

In the context of matrix R is reflexive if and only if diagonal elements of M_R =1.

Let, A = {1, 2, 3}

A x A	**1**	**2**	**3**
1	11	12	13
2	21	22	23
3	31	32	33

R = φ (*not reflexive*)

R = {(1, 1), (2, 2), (3, 3)} (*reflexive*)

R = {(1, 1), (2, 3), (3, 3)} (*not reflexive*)

R = {(1, 1), (2, 2), (3, 3), (3, 2)} (*reflexive*)

R = A x A (*reflexive*)

Irreflexive Relations: A relation R on a set A is irreflexive if for all a in A, (a, a) ∉ R.

In the context of matrix R is irreflexive if and only if diagonal elements of M_R =0.

.

R = φ (i*rreflexive*)

R = {(1, 1), (2, 3), (3, 3)} (*neither reflexive nor irreflexive*)

R = {(3, 2), (3, 1), (2, 3)} (*irreflexive*)

2. SYMMETRIC, ASYMETRIC AND ANTI-SYMETRIC RELATIONS:

Symmetric Relations: A relation R on a set A is said to be symmetric if for all (a, b) ∈ A and (a, b) ∈ R then (b, a) ∈ R.

In the context of matrix R is symmetric if and only if $M_R = M_R^T$.

Let, A = {1, 2, 3}

A x A	**1**	**2**	**3**
1	11	12	13
2	21	22	23
3	31	32	33

R = {(1, 2), (2, 1)} (*symmetric*)

R = {(2, 3), (3, 2), (2, 2), (3, 3)} (*symmetric*)

R = φ (*symmetric*)

R = A x A (*symmetric*)

R = {(1, 2), (2, 3), (1, 3)} (*not symmetric*)

Anti-symmetric Relations: A relation R on a set A is said to be anti-symmetric if for all (a, b) ∈ A and (a, b) ∈ R and (b, a) ∈ R then a=b.

In the context of matrix R is anti-symmetric if $m_{ij}=1$ *with* $i \neq j$, *then* $m_{ji}=0$.

R = {(1, 2), (2, 3), (1, 3)} (*anti-symmetric*)

R = {(1, 2), (1, 1), (2, 2)} (*anti-symmetric*)

R = {(1, 1), (2, 2), (3, 3)} (*symmetric and anti-symmetric*)

R = {(1, 2), (2, 1), (2, 3), (3, 1)} (*Neither symmetric nor anti-symmetric*)

R = φ (*symmetric*)

R = A x A (*not anti-symmetric*)

Asymmetric Relations: A relation R on a set A is said to be asymmetric if for all (a, b) ∈ A and (a, b) ∈ R then (b, a) ∉ R.

In the context of matrix R is asymmetric if $m_{ij}=1$ *then* $m_{ji}=0$.

R = {(1, 2), (2, 3), (3, 1)} (*asymmetric*)

R = {(1, 2), (2, 3), (3, 2)} (*not asymmetric*)

R = {(1, 1), (2, 2), (3, 3)} (*not asymmetric*)

R = φ (*asymmetric*)

R = A x A (*not asymmetric*)

3. TRANSITIVE RELATIONS:

A relation R on a set A is said to be transitive if for all (a, b) ∈ A and (a, b) ∈ R and (b, a) ∈ R then (a, c) ∈ R.

Let, A = {1, 2, 3}

A x A	**1**	**2**	**3**
1	11	12	13
2	21	22	23
3	31	32	33

R = {(1, 2), (2, 1), (1, 1), (2, 2)} (*Transitive*)

R = {(1, 1), (2, 2), (3, 3)} (*Transitive*)

R = {(1, 2), (1, 3)} (*Transitive*)

R = {(1, 2), (3, 1)} (*Transitive*)

R = {(3, 1), (2, 3)} (*not Transitive*)

Q.1 Let A = Z, the set of integers and let, R = {(a, b) ∈ A x A | a<b}. Is R symmetric, asymmetric or anti-symmetric?

Solution:

- The relation R = {(a, b) ∈ A x A | a<b} is not symmetric. A relation R is symmetric if for every (a, b) in R, (b, a) is also in R. However, this is not true for the relation R defined above. For example, (1, 2) is in R, but (2, 1) is not in R. Therefore, R is not symmetric.

- The relation R = {(a, b) ∈ A x A | a<b} is asymmetric. To prove this, we need to show that if (a, b) is in R, then (b, a) is not in R. Let's assume that (a, b) is in R, which means that a<b. If (b, a) were also in R, then we would have b<a, which contradicts the fact that a<b. Therefore, (b, a) cannot be in R, and R is asymmetric.

- The relation R = {(a, b) ∈ A x A | a<b} is antisymmetric. To show this, we need to prove that if (a, b) and (b, a) are both in R, then a = b. Let's assume that (a, b) and (b, a) are both in R. This means that a<b and b<a, which is a contradiction. Therefore, it cannot be the case that both (a, b) and (b, a) are in R. Hence, the relation R is antisymmetric.

1.4 CLOSURES OF RELATION:

The closure of a relation refers to the process of adding all the necessary elements to a relation in order to make it satisfy a certain property.

Let R be a relation on a set A. The closure of R with respect to a certain property P is a new relation denoted by R' that satisfies the following conditions:

i. R' contains all the pairs that are related by R.

ii. R' satisfies property P.

iii. R' is the smallest relation that satisfies conditions i and ii.

1. REFLECTIVE CLOSURE: For any relation R on A, reflexive closure of R is formed by adding to R all pairs of the form (a, a) with a ∈ A, not already in R i.e. R ∪ D, where D = {(a, a) | a ∈ A} is the diagonal relation on A.

Example:

Let R be the relation on the set {1, 2, 3, 4} containing the ordered pairs (1,2), (1,3), (2,2), (2, 4), (3,1), (3,2), (3, 4), and (4, 4) .find reflexive closure.

Solution:

We have R = {(1, 2), (1, 3), (2, 2), (2, 4), (3, 1), (3, 2), (3, 4), (4, 4)} and

D = {(1, 1), (2, 2), (3, 3), (4, 4)}

So, R ∪ D = {(1, 1), (1, 2), (1, 3), (2, 2), (2, 4), (3, 1), (3, 2), (3, 3), (3, 4), (4, 4)} is the reflexive closure of R.

2. SYMMETRIC CLOSURE: The symmetric closure of a relation can be constructed by taking the union of a relation with its inverse, that is, $R \cup R^{-1}$ is the symmetric closure of R, where $R^{-1} = \{(b, a) \mid (a, b) \in R\}$.

Example:

Let R be the relation on the set {1, 2, 3, 4} containing the ordered pairs (1,2), (1,3), (2,2), (2, 4), (3,1), (3,2), (3, 4), and (4, 4). Find symmetric closure.

Solution:

We have R = {(1, 2), (1, 3), (2, 2), (2, 4), (3, 1), (3, 2), (3, 4), (4, 4)}

R^{-1}= {(2, 1), (3, 1), (4, 2), (1, 3), (2, 3), (4, 3)}

So, R ∪ R^{-1} = {(1,2), (1,3), (2,1), (2,2), (2,3), (2,4), (3,1), (3,2), (3,4), (4,2), (4,3), (4,4)} is the symmetric closure of R.

3. TRANSITIVE CLOSURE: Let R be a relation on set A. Then R^{∞} is the transitive closure of R where, $R^{\infty} = R^1 \cup R^2 \cup R^3 \cup ..... \cup R^n$. (n= |A|)

> .. suppose that A, B, and C are sets, R is a relation from A to B, and S is a relation from B to C. We can then define a new relation, the **composition** of R and S, written $S \circ R$. The relation $S \circ R$ is a relation from A to C and is defined as follows. If a is in A and c is in C, then $a(S \circ R)c$ if and only if for some b in B

Example:

Let R be the relation on the set A= {1, 2, 3} containing the ordered pair (1, 2), (2, 3), (3, 1) Find Transitive closure.

Here, R = {(1, 2), (2, 3), (3, 1)}

R^2 = R o R = {(1, 2), (2, 3), (3, 1)} o {(1, 2), (2, 3), (3, 1)}

= {(1, 3), (2, 1), (3, 2)}

R^3 = R^2 o R = {(1, 3), (2, 1), (3, 2)} o {(1, 2), (2, 3), (3, 1)}

= {(1, 1), (2, 2), (3, 3)}

R^4 = R^3 o R = {(1, 1), (2, 2), (3, 3)} o {(1, 2), (2, 3), (3, 1)}

= {(1, 2), (2, 3), (3, 1)}

R^{∞} = $R^1 \cup R^2 \cup R^3 \cup R^4$

= {(1, 2), (2, 3), (3, 1)} ∪ {(1, 3), (2, 1), (3, 2)} ∪ {(1, 1), (2, 2), (3, 3)} ∪ {(1, 2), (2, 3), (3, 1)}

= {(1, 2), (2, 3), (3, 1), (1, 3), (2, 1), (3, 2), (1, 1), (2, 2)}

WARSHALL'S ALGORITHM:

Let A= {1, 2, 3, 4} and let R = {(1, 2), (2, 3), (3, 4), (2, 1)}. Find the transitive closure of R.

Solution:

Construct relation matrix M_R (W_0):

W_0 =

R	1	2	3	4
1	0	1	0	0
2	1	0	1	0
3	0	0	0	1
4	0	0	0	0

Step: 1 (1st column and 1st row of W_0)

W_0 has entry 1 on position 2 at column 1. C= {2}

W_0 has entry 1 on position 2 at row 1. R= {2}

C x R = {(2, 2)}

Now construct W_1 where entry on position(2, 2) is 1 and rest same entry as W_0.

W_1 =

R	1	2	3	4
1	0	1	0	0
2	1	1	1	0
3	0	0	0	1
4	0	0	0	0

Step: 2 (2nd column and 2nd row of W_1)

W_1 has entry 1 on position 1 and 2 at column 2. C= {1, 2}

W_1 has entry 1 on position 1, 2 and 3 at row 2. R= {1, 2, 3}

C x R = {(1, 1), (1, 2), (1, 3), (2, 1), (2, 2), (2, 3)}

Now construct W_2 where entry on every position of C x R is 1 and rest same entry as W_1.

W_2 =

R	1	2	3	4
1	1	1	1	0
2	1	1	1	0
3	0	0	0	1
4	0	0	0	0

Step: 3 (3rd column and 3rd row of W_2)

W_2 has entry 1 on position 1 and 2 at column 3. C= {1, 2}

W_2 has entry 1 on position 4 at row 3. R= {4}

C x R = {(1, 4), (2, 4)}

Now construct W_3 where entry on every position of C x R is 1 and rest same entry as W_2.

W_3 =

R	**1**	**2**	**3**	**4**
1	1	1	1	1
2	1	1	1	1
3	0	0	0	1
4	0	0	0	0

Step: 4 (4th column and 4th row of W_3)

W_3 has entry 1 on position 1, 2 and 3 at column 4. C= {1, 2, 3}

W_3 has no any entry 1 at row 4. R= { }

C x R = { }

Now construct W_4 where entry on every position of C x R is 1 and rest same entry as W_3.

W_4 =

R	**1**	**2**	**3**	**4**
1	1	1	1	1
2	1	1	1	1
3	0	0	0	1
4	0	0	0	0

W_4 is the required transitive closure.

1.5 EQUIVALENCE RELATIONS:

A relation R on a set A is called an equivalence relation if it is reflexive, symmetric, and transitive.

Example: Let, A= {a, b, c}

R_1 = { } (*not equivalence relation*)
R_2 = {(a, a), (b, b), (c, c)} (*equivalence relation also smallest possible equivalence relation*)
R_3 = {(a, a), (b, b), (c, c), (b, a)} (*not equivalence relation)*
R_4 = {(a, a), (a, c), (b, a), (c, a)} (*not-equivalence relation)*
R_5 = {(a, a), (b, b), (c, c), (a, b), (a, c), (b, a), (c, a)} (*equivalence relation)*
R_6 = A x A (*equivalence relation also largest possible equivalence relation*)

Q.1 Let R be the relation on the set of real numbers such that aRb if and only if a − b is an integer. i.e. R = {(a, b) | a –b ∈ Z}.Is R an equivalence relation?

Solution:

To determine whether R is an equivalence relation, we need to check whether it satisfies three properties: reflexivity, symmetry, and transitivity.

- **Reflexivity:** To prove reflexivity, we need to show that aRa holds for any real number a. This is true because a − a = 0, which is an integer. Therefore, R satisfies reflexivity.
- **Symmetry:** To prove symmetry, we need to show that if aRb holds, then bRa also holds. If aRb holds, then a − b is an integer. This implies that b – a = − (a − b) is also an integer. Therefore, bRa holds and R satisfies symmetry.
- **Transitivity:** If aRb and bRc, then a - b and b - c are integers. Therefore, a – c = (a - b) + (b - c) is also an integer. Hence, aRc is true, and R is transitive.

Since R satisfies all three properties of an equivalence relation, R is an equivalence relation.

Q.2 Let m be an integer with m > 1. Show that the relation R = {(a, b) | a ≡ b (mod m)} is an equivalence relation on the set of integers.

Solution:

To show that R = {(a, b) | a ≡ b (mod m)} is an equivalence relation, we need to show that it satisfies three properties: reflexivity, symmetry, and transitivity.

- **Reflexivity:** For any integer a, a ≡ a (mod m) since a - a = 0 is divisible by m. Therefore, (a, a) is in R for any integer a, and R is reflexive.
- **Symmetry:** If (a, b) is in R, then a ≡ b (mod m), which means that a − b = km, where k is an integer. It follows that b − a = (−k) m, so b ≡ a (mod m). Therefore, (b, a) is also in R, and R is symmetric.
- **Transitivity:** If (a, b) and (b, c) are in R, then a ≡ b (mod m) and b ≡ c (mod m). Then m divides both a − b and b − c. Therefore, there are integers k and l with a − b = km and b − c = lm. Adding these two equations shows that a − c = (a − b) + (b − c) = km + lm = (k + l) m. Thus, a ≡ c (mod m). Therefore, R is transitive.

Since R satisfies all three properties of an equivalence relation, R is an equivalence relation.

EQUIVALENCE CLASSES:

Let R be an equivalence relation on a set A. The set of all elements that are related to an element 'a' of A is called the equivalence class of a. The equivalence class of 'a' with respect to R is denoted by $[a]_R$. In other words, if R is an equivalence relation on a set A, the equivalence class of the element a is $[a]_R = \{s \mid s \in A \text{ and } (a, s) \in R\}$.

Example:

Let, A= {a, b, c, d, e}

R = {(a, a), (b, b), (c, c), (d, d), (e, e), (a, b), (b, a), (d, e), (e, d)}

$[a]_R$ = {a, b}

$[b]_R$ = {a, b}

$[c]_R$ = {c}

$[d]_R$ = {d, e}

$[e]_R$ = {d, e}

(Partitions) **P_1= {a, b} P_2 ={c} P_3= {d, e}**

$P_1 \cup P_2 \cup P_3 \cup \ldots\ldots\ldots \cup P_k = A$

$P_1 \cap P_2 \cap P_3 \cap \ldots\ldots\ldots \cap P_k = \varphi$

Q.1 List the ordered pairs in the equivalence relation R produced by the partition P_1 = {1, 2, 3}, P_2 = {4, 5}, and P_3 = {6} of A = {1, 2, 3, 4, 5, 6}.

Solution:

To list the ordered pairs in R, we can simply list all pairs of elements in each set P_1, P_2, and P_3 that belong to the same set:

- For P_1 = {1, 2, 3}, the pairs are (1, 1), (1, 2), (1, 3), (2, 1), (2, 2), (2, 3), (3, 1), (3, 2), and (3, 3).
- For P_2 = {4, 5}, the pairs are (4, 4), (4, 5), (5, 5), (5, 4).
- For P_3 = {6}, the pair is (6, 6).

Therefore, the ordered pairs in the equivalence relation R are:
{(1, 1), (1, 2), (1, 3), (2, 1), (2, 2), (2, 3), (3, 1), (3, 2), (3, 3), (4, 4), (4, 5), (5, 5), (5, 4), (6, 6)}.

Q.2 Let A= {1, 2, 3, 4}, R= {(a, b)| a+b is even}. find equivalence classes.

Solution:

First we need to prove that R is an equivalence relation.

- **Reflexivity**: For all a ∈ A, (a, a) ∈ R, since a + a = 2a is always even. Thus, R is reflexive.
- **Symmetry**: For all a, b ∈ A, if (a, b) ∈ R, then (b, a) ∈ R. This is because a + b is even if and only if b + a is even. Thus, R is symmetric.
- **Transitivity:** For all a, b, c ∈ A, if (a, b) ∈ R and (b, c) ∈ R, then (a, c) ∈ R. This is because a + b and b + c are both even, and the sum of two even numbers is even. Thus, a + b + b + c = a + c + 2b is also even, so (a, c) ∈ R. Thus, R is transitive.

The equivalence class [1] is the set of all elements that is related 1 under R. Since 1 + 1 = 2 is even, 1 + 3 = 4 is even, 1 + 5 = 8 is even we have

$[1]_R$ = {1, 3, 5}

Similarly, we can find the other equivalence classes:

$[2]_R$ = {2, 4}

$[3]_R$ = {1, 3, 5}

$[4]_R$ = {2, 4}

$[5]_R$ = {1, 3, 5}

Partitions are: P_1 = {2, 4} P_2 = {1, 3, 5}

1.6 PARTIAL ORDERING:

A relation R on a set S is called a partial ordering or partial order if it is reflexive, antisymmetric, and transitive.

Example: Let, A= {a, b, c}

R_1 = { } (*not partial order relation*)

R_2 = {(a, a), (b, b), (c, c)} (*partial order relation*)

R_3 = {(a, a), (b, b), (c, c), (a, b), (b, a)} (*not partial order relation)*

R_4 = {(a, a), (b, b), (c, c), (a, c), (b, c)} (*partial order relation)*

R_5 = {(a, a), (a, b), (b, c), (a, c)} (*not partial order relation)*

R_6 = A x A (*not partial order relation*)

POSET (Partially Ordered Set): A set S together with a partial ordering R is called a partially ordered set, or poset, and is denoted by (S, R). Members of S are called elements of the poset.

Example:

i.**R = {(a, b) | a, b ∈ Z, a≥b} in poset form: (Z, ≥)**

ii. **R = {(a, b) | a, b ∈ Z, a|b} in poset form: (Z, |)**

Q.1 Show that the "greater than or equal" relation (≥) is a partial ordering on the set of integers or show that (Z, ≥) is poset.

Solution:

R = {(a, b) | a, b ∈ Z, a≥b}

We need to verify the three properties:

- **Reflexivity:** For any integer 'a', a ≥ a, since 'a' is greater than or equal to itself.
- **Antisymmetric:** For any integers 'a' and 'b', if a ≥ b and b ≥ a, then a = b. This is because if a ≥ b, then 'a' is either greater than 'b' or equal to 'b'. Similarly, if b ≥ a, then 'b' is either greater than 'a' or equal to 'a'. If 'a' and 'b' are equal, then it satisfies antisymmetric property. Otherwise, if 'a' is greater than 'b' (i.e. a > b), and 'b' is greater than 'a' (i.e. b >

a), then this is a contradiction, since two different numbers cannot be both greater than each other. Therefore, a must equal b.

- **Transitivity:** For any integers ‘a’, ‘b’, and ‘c’, if a ≥ b and b ≥ c, then a ≥ c. This is because if a ≥ b, then ‘a’ is either greater than ‘b’ or equal to ‘b’, and if b ≥ c, then ‘b’ is either greater than ‘c’ or equal to ‘c’. If ‘a’ is greater than or equal to ‘b’, and ‘b’ is greater than or equal to ‘c’, then ‘a’ is either greater than ‘c’ or equal to ‘c’. In either case, we have a ≥ c.

Therefore, we have shown that the "greater than or equal" relation (≥) is a partial ordering on the set of integers, since it satisfies the three properties of a Partial Ordering.

Q.2 Show that the the divisibility relation | is a partial ordering on the set of integers or show that (Z, |) is a poset.

Solution:

$$\mathbf{R = \{(a, b) \mid a, b \in Z, a|b\}}$$

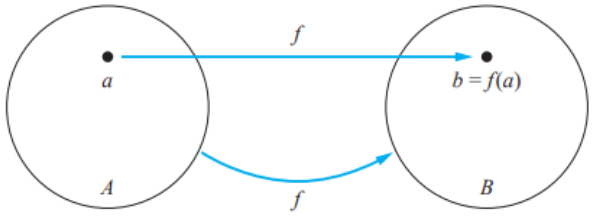
We need to verify the three properties of a POSET:

- **Reflexivity:** For any positive integer a, a | a, since a is divisible by itself.
- **Antisymmetric:** For any positive integers a and b, if a | b and b | a, then a = b. Thus, we have a = b, and the relation is antisymmetric.
- **Transitivity:** For any positive integers a, b, and c, if a | b and b | c, then a | c. This is because if a | b, then b is a multiple of a, and if b | c, then c is a multiple of b. Therefore, c is also a multiple of a (since c is a multiple of b and b is a multiple of a), and so a | c.

Therefore, the divisibility relation | is a partial ordering on the set of positive integers, since it satisfies the three properties of a POSET.

2. FUNCTIONS:

Let A and B be non-empty sets. A function f from A to B is an assignment of exactly one element of B to each element of A. We write f (a) = b if b is the unique element of B assigned by the function f to the element a of A. If f is a function from A to B, we write f: A → B.



The Function *f* Maps *A* to *B*.

If f is a function from A to B, we say that A is the domain of f and B is the codomain of f. If f (a) = b, we say that 'b' is the image of 'a' and 'a' is a preimage of 'b'. The range, or image, of f is the set of all images of elements of A. Also, if f is a function from A to B, we say that f maps A to B.

Example:

a.

Let $A = \{1, 2, 3\}$ and $B = \{x, y, z\}$. Consider the relations

$R = \{(1, x), (2, x)\}$ and $S = \{(1, x), (1, y), (2, z), (3, y)\}$.

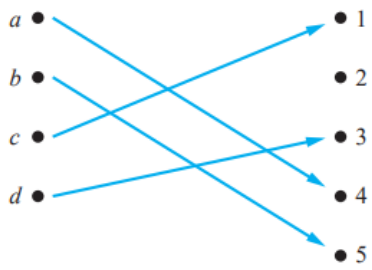
The relation S is not a function since $S(1) = \{x, y\}$. The relation R is a function with $\text{Dom}(R) = \{1, 2\}$ and $\text{Ran}(R) = \{x\}$.

b. Let f: Z → Z assign the square of an integer to this integer. Then, $f(x) = x^2$, where the domain of f is the set of all integers, the codomain of f is the set of all integers, and the range of f is the set of all integers that are perfect squares, namely, {0, 1, 4, 9,...}.

2.1 INJECTIVE, SURJECTIVE AND BIJECTIVE FUNCTIONS:

ONE-TO-ONE FUNCTION (INJECTIVE FUNCTION): A function f from set A to set B, f: A→B is said to be one to one if no two elements in A are mapped to same element in B. We can express that f is one-to-one using quantifiers as $\forall_a \forall_b [(a \neq b) \rightarrow (f(a) \neq f(b))]$ **or** $\forall_a \forall_b (f(a) = f(b) \rightarrow a = b)$, where the universe of discourse is the domain of the function.

If A and B are finite set, then one to one function from A→B is possible if |A|≤|B|.



A One-to-One Function

Q.1 Determine whether the function f (x) = x^2 from the set of integers to the set of integers is one-to-one.

Solution:

The function f (x) = x^2 is not one-to-one because, for instance, f (1) = f (−1) = 1.

Q.2 Determine whether the function f (x) = x + 1 from the set of real numbers to itself is one-to one.

Solution:

To determine whether the function is one-to-one, we need to check if each distinct input value maps to a distinct output value.

Suppose we have two distinct inputs a and b such that f(a) = f(b). Then, we have:

a + 1 = b + 1

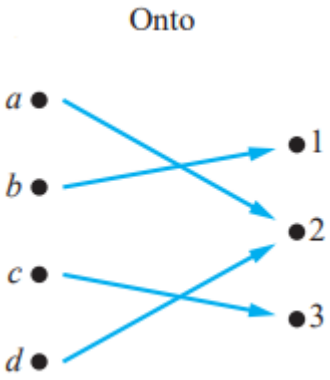
Simplifying this expression, we get:

a = b

This shows that if two inputs have the same output, then they must be the same input. Therefore, the function f(x) = x + 1 is one-to-one, since each input is mapped to a unique output.

ONTO FUNCTION (SURJECTIVE FUNCTION): A function f from set A to set B, f: A→B is said to be onto if an only if every element of B is mapped by at least one element of A. We can express that f is onto using quantifiers as **$\forall_b \exists_a$ [f (a) = b],** where the domain of x is the domain of function and domain of y is the codomain of function.

If A and B are finite set, then onto function from f: A→B is possible if |B|≤|A|.



Q.1 Is the function f (x) = x^2 from the set of integers to the set of integers onto?

Solution:

To show that a function is onto, we need to show that for every y in the range of the function, there exists an x in the domain such that f(x) = y. In this case, the function f(x) = x^2 maps each integer x to its square, so the range of the function consists of all non-negative integers (i.e., the set {0, 1, 2, 3, ...}).

However, there is no integer x such that f(x) = -1, for example. In fact, for any negative integer y, there is no integer x such that f(x) = y, since the square of an integer is always non-negative.

Therefore, the function f(x) = x^2 from the set of integers to the set of integers is not onto.

Q.2 Is the function f (x) = x + 1 from the set of integers to the set of integers onto?

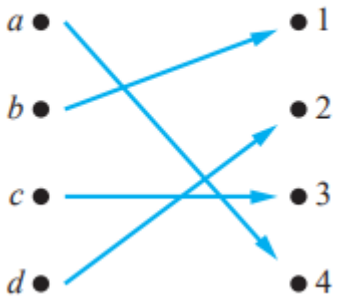
Solution:

To see that this function is onto, let y be any integer in the range. Then, we can find an integer x in the domain such that f(x) = y by setting x = y - 1. Then, f(x) = f(y - 1) = (y - 1) + 1 = y, which shows that f is onto.

Therefore, the function f(x) = x + 1 from the set of integers to the set of integers is onto.

ONE-TO-ONE-CORRESPONDENCE FUNCTION (BIJECTIVE / INVERTIBLE FUNCTION): A function f from set A to set B, f: A→B is said to be injective if 'f' is both one to one and onto.

If A and B are finite set, then one to one correspondence function from f: A→B is possible if |A| = |B|.



Q. Determine whether a function f(x) = 2x + 3 from the set of real numbers to the set of real numbers is bijective?

Solution:

To show that a function is bijective, we need to show that it is both injective (one-to-one) and surjective (onto).

To show that f(x) = 2x + 3 is injective, we assume that $f(x_1) = f(x_2)$ for some x_1 and x_2 in the domain of the function. Then,

$2x_1 + 3 = 2x_2 + 3$

Simplifying this equation, we get:

$2x_1 = 2x_2$

Dividing both sides by 2, we get:

$x_1 = x_2$

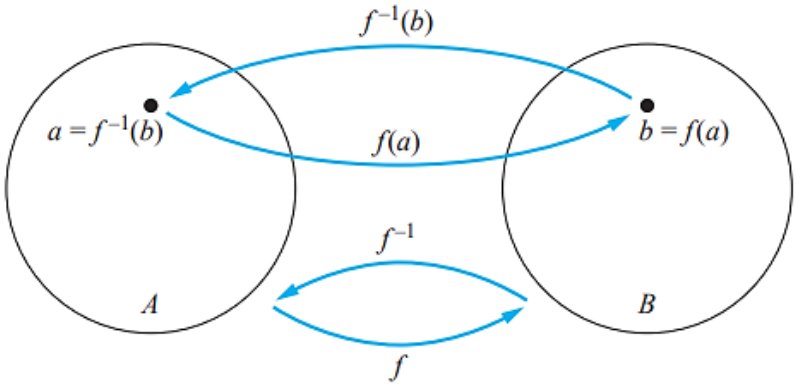
This shows that f(x) = 2x + 3 is injective.

To show that f(x) = 2x + 3 is surjective, we need to show that every real number y can be written in the form f(x) for some x in the domain. Let y be any real number. Then, we can find an x in the domain such that f(x) = y by setting x = (y - 3)/2. Then, f(x) = f((y-3)/2) = 2((y-3)/2) + 3 = y, which shows that f is surjective.

Since f(x) = 2x + 3 is both injective and surjective, it is bijective.

2.2 INVERSE AND COMPOSITE FUNCTIONS:

INVERSE FUNCTION: Let f be a one-to-one correspondence (Bijective) from the set A to the set B. The inverse function of 'f' is denoted by f^{-1} such that $f^{-1}(b) = a$ when $f(a) = b$.



The Function f^{-1} Is the Inverse of Function f

Q. Let a function f(x) = 2x + 3 from the set of real numbers to the set of real numbers. Find its inverse.

Solution:

Since f is bijective function its inverse exist.

To find the inverse of f(x) = 2x + 3, we can follow these steps:

- Replace f(x) with y: y = 2x + 3
- Solve for x in terms of y:

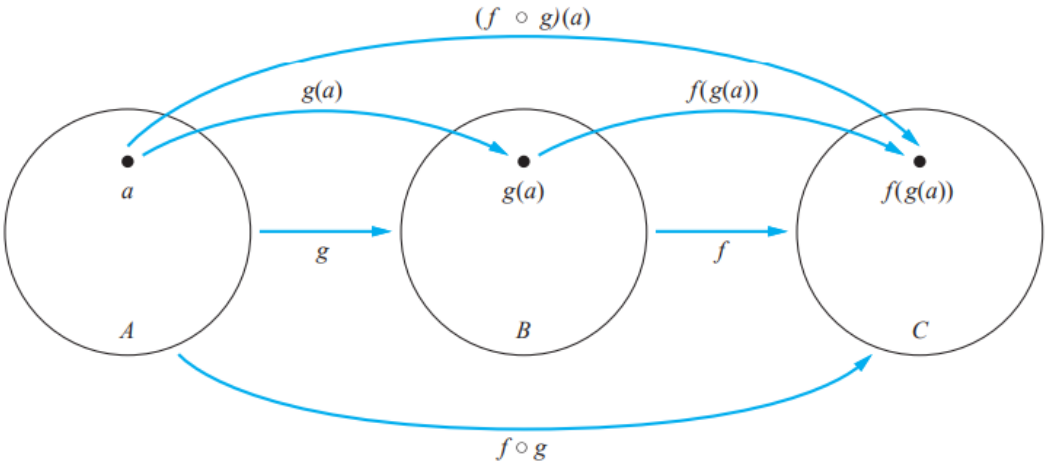
  y = 2x + 3

  y - 3 = 2x

  x = (y - 3)/2
- Replace x with $f^{-1}(y)$: $f^{-1}(y) = (y - 3)/2$

So the inverse function of f(x) = 2x + 3 is $f^{-1}(y) = (y - 3)/2$.

COMPOSITIONS OF FUNCTIONS: Let 'g' be a function from the set A to the set B and let 'f' be a function from the set B to the set C. The composition of the functions f and g, denoted for all a ∈ A by f ◦ g, is defined by: (f ◦ g) (a) = f (g (a)).



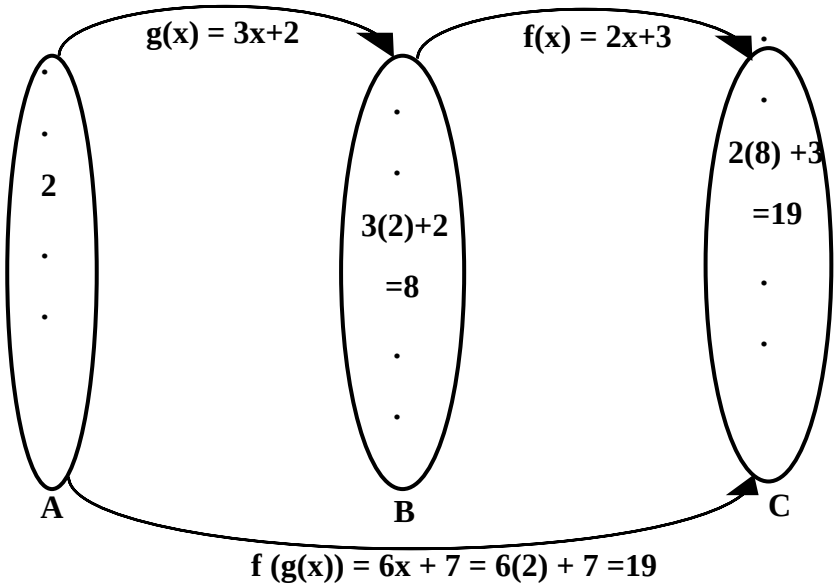
The Composition of the Functions *f* and *g*.

Q. Let f and g be the functions from the set of integers to the set of integers defined by f (x) = 2x + 3 and g(x) = 3x + 2. What is the composition of f and g? What is the composition of g and f?

Solution:

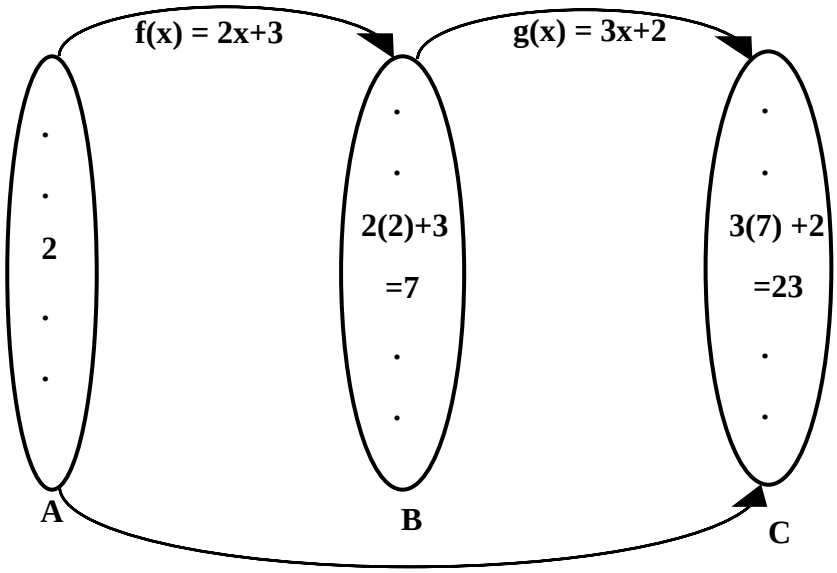
(a) Composition of f and g i.e. (f ◦ g) (x) = f (g(x)).

(f ◦ g)(x) = f (g(x)) = f (3x + 2) = 2(3x + 2) + 3 = 6x + 7



(b) Composition of g and f i.e. $(g \circ f)(x) = g(f(x))$.

$(g \circ f)(x) = g(f(x)) = g(2x + 3) = 3(2x + 3) + 2 = 6x + 11$



g(f(x)) = 6x + 11 = 6(2) + 11 = 23

Identity function: *Let A be a set. The identity function on A is the function I_A: $A \rightarrow A$, where $I_A(x) = x$ for all $x \in A$. In other words, the identity function I_A is the function that assigns each element to itself. The function I_A is one-to-one and onto, so it is a bijection.*

When the composition of a function and its inverse is formed, in either order, an identity function is obtained.

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

$(f \circ f^{-1})(b) = f(f^{-1}(b)) = f(a) = b.$

2.3 FUNCTIONS FOR COMPUTER SCIENCE:

FLOOR FUNCTION: The floor function assigns to the real number x the largest integer that is less than or equal to x. The value of the floor function at x is denoted by⌊x⌋.

CEILING FUNCTION: The ceiling function assigns to the real number x the smallest integer that is greater than or equal to x. The value of the ceiling function at x is denoted by⌈x⌉.

These are some values of the floor and ceiling functions:

$$\lfloor \tfrac{1}{2} \rfloor = 0,\ \lceil \tfrac{1}{2} \rceil = 1,\ \lfloor -\tfrac{1}{2} \rfloor = -1,\ \lceil -\tfrac{1}{2} \rceil = 0,\ \lfloor 3.1 \rfloor = 3,\ \lceil 3.1 \rceil = 4,\ \lfloor 7 \rfloor = 7,\ \lceil 7 \rceil = 7.$$

TABLE 1 Useful Properties of the Floor and Ceiling Functions.
(n is an integer, x is a real number)

(1a)	$\lfloor x \rfloor = n$ if and only if $n \le x < n + 1$
(1b)	$\lceil x \rceil = n$ if and only if $n - 1 < x \le n$
(1c)	$\lfloor x \rfloor = n$ if and only if $x - 1 < n \le x$
(1d)	$\lceil x \rceil = n$ if and only if $x \le n < x + 1$
(2)	$x - 1 < \lfloor x \rfloor \le x \le \lceil x \rceil < x + 1$
(3a)	$\lfloor -x \rfloor = -\lceil x \rceil$
(3b)	$\lceil -x \rceil = -\lfloor x \rfloor$
(4a)	$\lfloor x + n \rfloor = \lfloor x \rfloor + n$
(4b)	$\lceil x + n \rceil = \lceil x \rceil + n$

Q.1 Prove that if x is a real number, then ⌊2x⌋ =⌊x⌋+⌊x + 1/2⌋

Solution:

Case 1: x is an integer

If x is an integer, then ⌊2x⌋ = 2x since 2x is already an integer.

Moreover, ⌊x⌋ = x and ⌊x + 1/2⌋ = x + ⌊0.5⌋ = x

Now, ⌊2x⌋ =⌊x⌋+⌊x + 1/2⌋

2x = x + x

2x = 2x (LHS = RHS)

Case 2: x is not an integer

If x is not an integer, then we can write x = n + r, where n is the largest integer less than x and r is the fractional part of x, i.e., 0 < r < 1. Then we have:

$\lfloor 2x \rfloor = \lfloor 2n + 2r \rfloor = 2n + \lfloor 2r \rfloor$ (since 2n is an integer)

$\lfloor x \rfloor = \lfloor n + r \rfloor = n + \lfloor r \rfloor = n + 0 = n$ (since r<1)

$\lfloor x + 1/2 \rfloor = \lfloor n + r + 1/2 \rfloor = n + \lfloor r + 1/2 \rfloor$

Now, $\lfloor 2x \rfloor = \lfloor x \rfloor + \lfloor x + 1/2 \rfloor$

$2n + \lfloor 2r \rfloor = n + n + \lfloor r + 1/2 \rfloor$

$2n + \lfloor 2r \rfloor = 2n + \lfloor r + 0.5 \rfloor$

- When $0<r<0.5$, then $0<2r<1$ such that $\lfloor 2r \rfloor = 0$ and $0<(r+0.5)<1$ such that $\lfloor r + 0.5 \rfloor = 0$

  $2n + 0 = 2n + 0$

  $2n = 2n$ (LHS = RHS)

- When $0.5 \leq r<1$, then $1 \leq 2r<2$ such that $\lfloor 2r \rfloor = 1$ & $1 \leq (r+0.5)<1.5$ such that $\lfloor r + 0.5 \rfloor = 1$

  $2n + 1 = 2n + 1$

  $2n = 2n$ (LHS = RHS)

Q.2 SHOW THAT $\lceil n^2/4 \rceil = (n^2+3)/4$

BOOLEAN FUNCTION: A Boolean function can be mathematically defined as a function $f: B^n \rightarrow B$, where B = {0, 1} is the set of Boolean values, and 'n' is a positive integer representing the number of Boolean inputs. In other words, a Boolean function takes 'n' Boolean inputs and produces a single Boolean output.

EXPONENTIAL FUNCTION: The exponential function is a mathematical function of the form $f(x) = a^x$, where 'a' is a positive constant and 'x' is the variable. The constant 'a' is called the base of the exponential function, and 'x' is the exponent.