Unit I: Basic Discrete Structures

Contents Overview

- Sets, Set Operations, Venn Diagram, Inclusion-Exclusion Principle and Computer representation of sets
- Basic Concept of Functions
- Integers and Division
- Matrices
- Basics of Counting

SETS

Sets

- **Definition**
  - Sets are used to group objects together
  - A set is any well-defined collection of objects called *elements* or *members* of sets
  - Example: collection of real numbers between 0 and 1, collection of even numbers from 0 to 100,

Sets

Representation

- Represent having finite number of sets by listing all elements of sets between braces

First method

Eg: {1,2,3}

- Ordering is not important. {1,3,2}, {2,1,3} is same.
- Example: set V of all vowels in English alphabet can be written as V={a,e,i,o,u}
- Uppercase letters such as A, B, C to denote sets and lowercase letters such as a, b, c,x to denote members or elements of sets

Second method

- $The\ notation\ a \epsilon A, denotes\ a\ is\ element\ of\ set\ A.$
- $a \notin A\ means\ a\ is\ not\ element\ of\ set\ A.$

Sets

Third method

- Some members of set are listed, and then ***ellipses*** (…) are used when general pattern of elements
- Example: set of positive integers less than 100 can be denoted by {1,2,3,…..,99}

Fourth method

- We use notation P(x) to denote sentence or statement P concerning variable object x. The set defined by P(x), written as {x | P(x)} is just collection of all objects x for which P is sensible and true. This is also called ***set builder*** notation.
- For example, set O of all odd positive integers less than 10 can be written as
- O={x|x is an odd positive integer less than 10}

Specifying universe as set of positive integers, as

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

where Z^+ is set of positive integers

This notation is generally used when it is impossible to list all elements of set

The set that has no elements in it is denoted either by {} or symbol ∅ is called empty set.

Examples for Sets

- $A = \varnothing$ "empty set/null set"
- $A = \{z\}$ Note: $z \in A$, but $z \neq \{z\}$
- $A = \{\{b, c\}, \{c, x, d\}\}$ set of sets
- $A = \{\{x, y\}\}$ Note: $\{x, y\} \in A$, but $\{x, y\} \neq \{\{x, y\}\}$
- $A = \{x \mid P(x)\}$ "set of all x such that P(x)"
- P(x) is the membership function of set A
- $\forall x\,(P(x) \rightarrow x \in A)$
- $A = \{x \mid x \in \mathbf{N} \wedge x > 7\} = \{8, 9, 10, \ldots\}$
  "set builder notation"

Sets

- **Exercise**

  The set of all positive rational numbers

  The set of Boolean numbers

Definition

Two sets are equal if and only if they have same elements. And we write A=B.

Two sets are equal if and only if $\forall x(x \in A \leftrightarrow x \in B)$

Eg: If A={1,2,3} and B={x|x is positive integer and x^2 <12}, then A=B

If A={BASIC, PASCAL, ADA} and B={ADA,BASIC, PASCAL}then A=B

Examples for Sets

- "Standard" Sets:
- Natural numbers **N** = {0, 1, 2, 3, …}
- Integers **Z** = {…, -2, -1, 0, 1, 2, …}
- Positive Integers $\mathbf{Z}^+$ = {1, 2, 3, 4, …}
- Real Numbers **R** = {47.3, -12, π, …}
- Rational Numbers **Q** = {1.5, 2.6, -3.8, 15, …}

Examples for Sets

- We are now able to define the set of rational numbers Q:
- $\mathbf{Q} = \{a/b \mid a \in \mathbf{Z} \wedge b \in \mathbf{Z}^{+}\}$, or
- $\mathbf{Q} = \{a/b \mid a \in \mathbf{Z} \wedge b \in \mathbf{Z} \wedge b \neq 0\}$

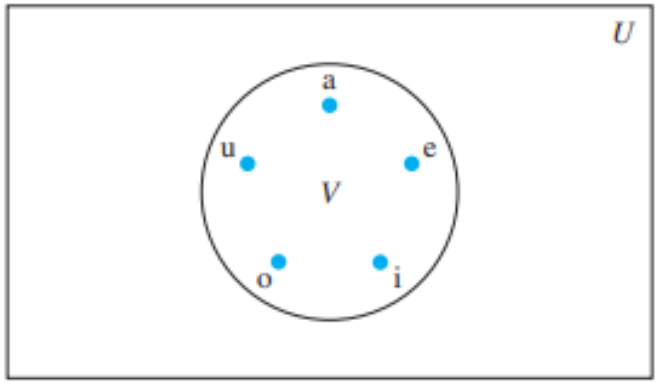
- And how about the set of real numbers R?

- $\mathbf{R} = \{r \mid r \text{ is a real number}\}$

That is the best we can do. It can neither be defined by enumeration nor builder function.

Venn Diagram

- Sets can be represented graphically using Venn diagrams
- In Venn diagrams, universal set U which contains all objects under consideration, is represented by rectangle
- Inside this rectangle, circles or other geometrical figures are used to represent sets
- Sometimes points are used to represent particular elements of sets
- Venn diagrams are often used to indicate relationships between sets



Sets

- Set A is called *finite* if it has n distinct elements. Here n is called *cardinality* of A and is denoted by |A|
- A set that is not finite is called *infinite*.
- If A is set, then set of all subsets of A is called *power set* of A and is denoted by P(A).

  Example: Let A={1,2,3}, Then P(A) consists of following subsets of A:
  {}, {1},{2},{3}, {1,2},{1,3},{2,3}, and {1,2,3}
- There is special set called empty set or null set and is denoted by {} or Ø
- Sets with just one element is called *singleton set*.
- $Empty\ set$ Ø is not {Ø} . {Ø} is singleton set
- Empty set can be thought as empty folder, and singleton set {Ø} can be thought of as folder with exactly one folder inside, that is empty folder

Cardinality of Sets

- If a set S contains n distinct elements, $n \in \mathbf{N}$, we call S a finite set with cardinality n.

- Examples:
- A = {Mercedes, BMW, Porsche}, $|A| = 3$

$B = \{1, \{2, 3\}, \{4, 5\}, 6\}$ $\quad |B| = 4$

$C = \cdot \emptyset$ $\quad |C| = 0$

$D = \{ x \in \mathbf{N} \mid x \leq 7000 \}$ $\quad |D| = 7001$

$E = \{ x \in \mathbf{N} \mid x \geq 7000 \}$ $\quad$ E is infinite!

The Power Set

- P(A) "power set of A" (also written as 2^A)
- P(A) = {B | B ⊆ A} (contains all subsets of A)

- Examples:

- A = {x, y, z}
- P(A) = {∅, {x}, {y}, {z}, {x, y}, {x, z}, {y, z}, {x, y, z}}

- A = ∅
- P(A) = {∅}
- Note: |A| = 0, |P(A)| = 1

The Power Set

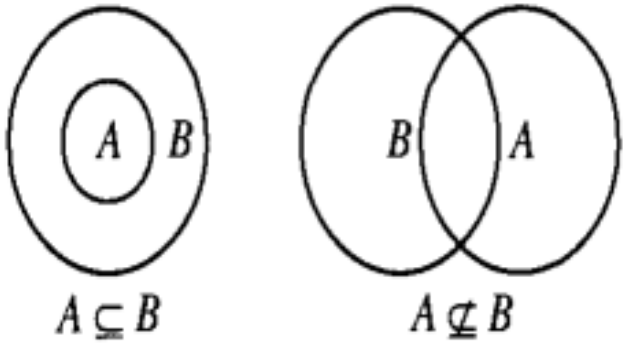
- Cardinality of power sets: $|P(A)| = 2^{|A|}$
- Imagine each element in A has an "on/off" switch
- Each possible switch configuration in A corresponds to one subset of A, thus one element in P(A)

A	1	2	3	4	5	6	7	8
x	x	x	x	x	x	x	x	x
y	y	y	y	y	y	y	y	y
z	z	z	z	z	z	z	z	z

- For 3 elements in A, there are 2□2□2 = 8 elements in P(A)

Subsets

- If every element of A is also an element of B, then A is subset of B.
- Example: set of A is men, set of B is human. So all men are human
- Representation:
  - If whenever $x \in A$ then $x \in B$, we say that A is subset of B or that A is contained in B.
  - $A \subseteq B$. "A is a subset of B"
  - $A \subseteq B$. if and only if every element of A is also an element of B.
  - We can completely formalize this:
  - $A \subseteq B \Leftrightarrow \forall x(x \in A \rightarrow x \in B)$
  - If A is not subset of B, we write $A \nsubseteq B$.
- Every set is subset of itself



Subsets

Examples

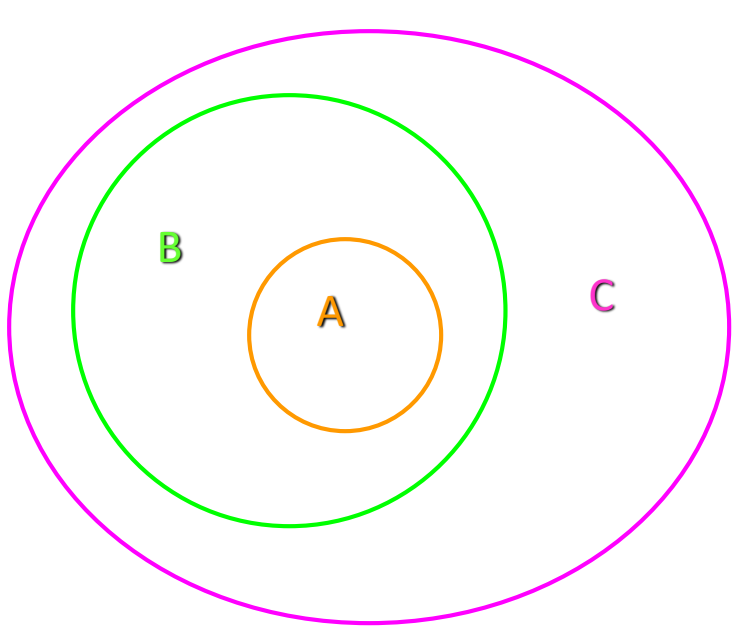
- A={3,9}, B={5,9,1,3} $A \subseteq B$?
- A={3,3,3,9}, B={5,9,1,3} $A \subseteq B$?
- A={1,2,3}, B={2,3,4} $A \subseteq B$?

Solutions

- True
- True
- False

Subsets

- Useful rules:
- $A = B \Leftrightarrow (A \subseteq B) \wedge (B \subseteq A)$
- $(A \subseteq B) \wedge (B \subseteq C) \Rightarrow A \subseteq C$ (see Venn Diagram)



Subsets

- Useful rules:
- $\emptyset \subseteq A$ for any set A
- (but $\emptyset \in A$ may not hold for any set A)
- $A \subseteq A$ for any set A

- Proper subsets:
- $A \subset B$ "A is a proper subset of B"
- $A \subset B \Leftrightarrow \forall x\,(x \in A \rightarrow x \in B) \wedge \exists x\,(x \in B \wedge x \notin A)$
- or
- $A \subset B \Leftrightarrow \forall x\,(x \in A \rightarrow x \in B) \wedge \neg\forall x\,(x \in B \rightarrow x \in A)$

Set Exercises

Let $A = \{1, 2, 4, a, b, c\}$. Identify each of the following as true or false.

(a) $2 \in A$ (b) $3 \in A$ (c) $c \notin A$

(d) $\varnothing \in A$ (e) $\{\} \notin A$ (f) $A \in A$

Let $A = \{x \mid x \text{ is a real number and } x < 6\}$.
Identify each of the following as true or false.

(a) $3 \in A$ (b) $6 \in A$ (c) $5 \notin A$

(d) $8 \notin A$ (e) $-8 \in A$ (f) $3.4 \notin A$

In each part, write the set in the form $\{x \mid P(x)\}$, where $P(x)$ is a property that describes the elements of the set.

(a) $\{2, 4, 6, 8, 10\}$ (b) $\{a, e, i, o, u\}$

(c) $\{1, 8, 27, 64, 125\}$ (d) $\{-2, -1, 0, 1, 2\}$

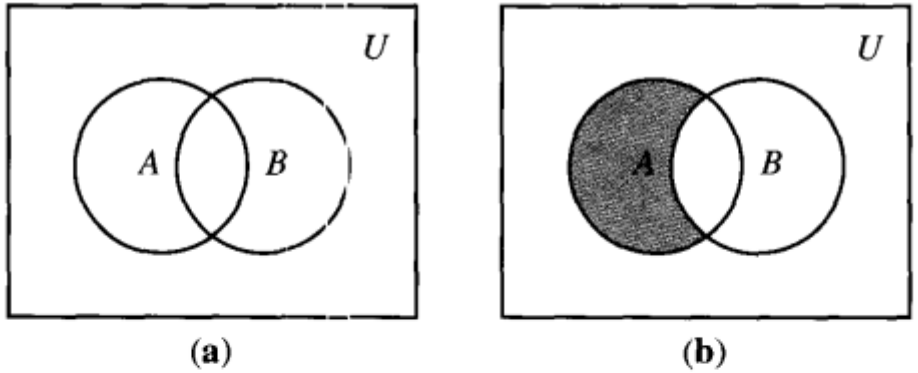
Set Operations

- **Union Operations**
  - Union set is set consisting of all elements that belong to A or B
  - Representation:
    - $A \cup B$
    - $\{x | x \in A \ or \ x \in B\}$
  - Example: A can be set of male students, B can set of female students, Union is set of students
- **Intersection**
  - Intersection set is set consisting of all elements that belong to both A and B
  - Representation
    - $\{x | x \in A \ and \ x \in B\}$
    - $A \cap B$

Set Operations

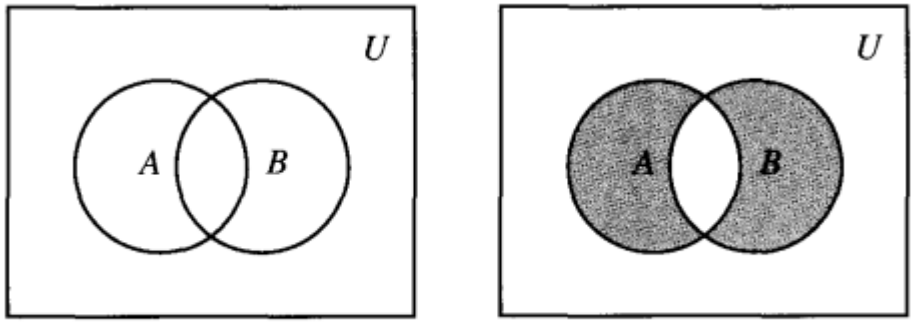
- **Complement of B with respect to A/Difference between two sets**
  - If A and B are two sets, we define complement of B with respect to A as set of all elements that belong to A but not to B
  - Representation:
    - $A - B$
    - $\{x | x \in A \; or \; x \notin B\}$
  - Example: Let A={a,b,c} and B={b,c,d,e} then A-B={a} and B-A= {d,e}
- **Complement of A**
  - If U is universal set containing A, then U-A is called complement of A.
  - Representation
    - $\{x | x \notin A\}$
    - $\bar{A}$

Exercise



Set Operations

- **Symmetric Difference**
  - If A and B are two sets, we define symmetric difference as set of all elements that belong to A or B but not to both A and B
  - Representation:
    - $A \oplus B$
    - $\{x | (x \in A \text{ and } x \notin B) \text{ or } (x \in B \text{ and } x \notin A\}$
    - $A \oplus B$ = (A-B)U(B-A)



(a) (b) $A \oplus B$

Algebraic Properties of Set Operations

Commutative properties

1. $A \cup B = B \cup A$
2. $A \cap B = B \cap A$

Associative properties

3. $A \cup (B \cup C) = (A \cup B) \cup C$
4. $A \cap (B \cap C) = (A \cap B) \cap C$

Distributive Properties

5. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
6. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

Idempotent properties

7. A ∪ A= A
8. A ∩ A =A

14 and 15 are also called DeMorgan's Laws

Properties of Complement

9. $(\bar{\bar{A}}) = A$
10. $A \cup \bar{A} = U$
11. . $A \cap \bar{A} = \emptyset$
12. $\overline{\emptyset} = U$
13. $\bar{U} = \emptyset$
14. $\overline{A \cup B} = \bar{A} \cap \bar{B}$
15. $\overline{A \cap B} = \bar{A} \cup \bar{B}$

Properties of Universal Set

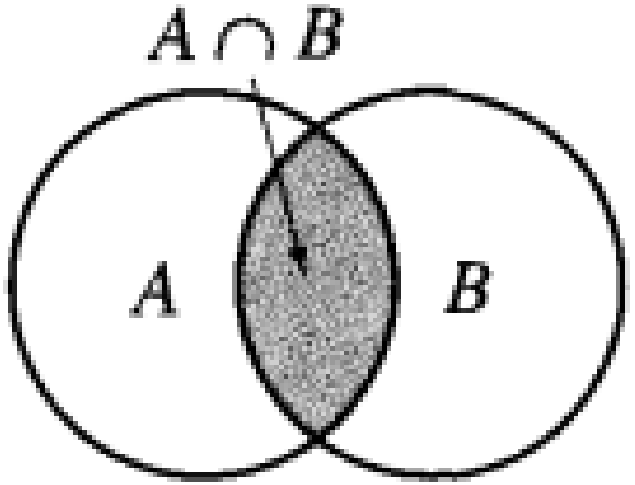
16. $A \cup U = U$
17. $A \cap U = A$

Properties of Empty Set

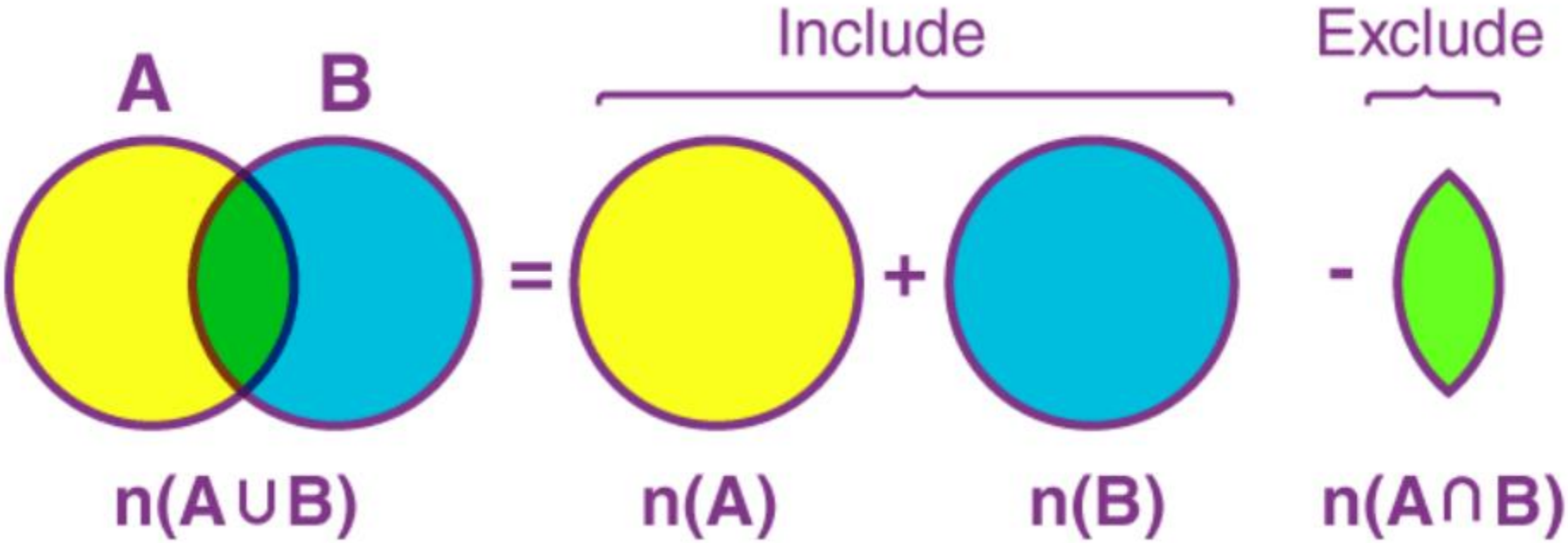
18. $A \cup \emptyset = A$
19. $A \cap \emptyset = \emptyset$

Inclusion Exclusion Principle/Addition Principle

- If A and B are finite sets, then $|A \cup B| = |A| + |B| - |A \cap B|$



Inclusion Exclusion Principle/Addition Principle



Computer Representation of Sets

- To represent set in computer, elements of set must be arranged in sequence.
- When universal set is finite, say $U=\{x_1,x_2,\ldots x_n\}$ and A is subset of U, then characteristic function f_A assigns 1 to an element x_i that belongs to A and 0 to a element that does not belong to A. Thus f_A can be represented by sequence of 0's and 1's of length n.
  - Example
  - Let U ={1,2,3,4,5,6}, A={1,2}, B={2,4,6} and C={4,5,6}. Then $f_A(x)$ has value 1 when x is 1 or 2 and 0 otherwise, Hence f_A corresponds to sequence 1,1,0,0,0,0.
  - f_B=? f_c=?
  - Complement of A??

FUNCTIONS

Definition of function

- A function f from a set A to a set B is an assignment of exactly one element of B to each element of A.

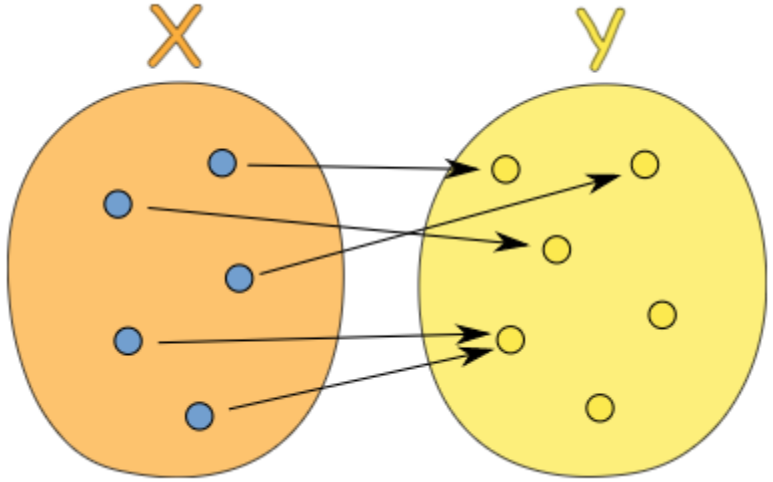
  We write

  f(a) = b

- If f is a function from A to B, we write

  f: A→B

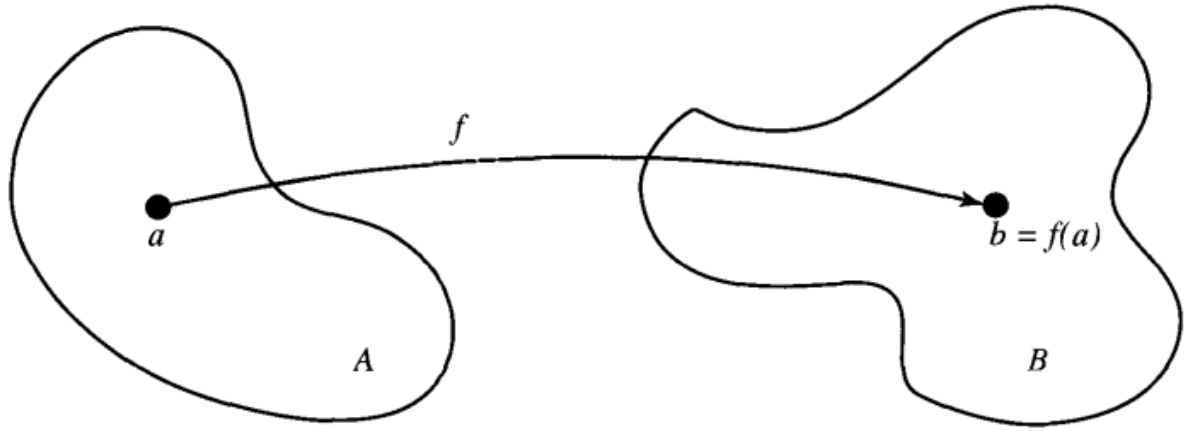
  (note: Here, "→" has nothing to do with if… then)



Functions

- Functions are also called mappings or transformations. We say that $f:A \to B$ maps A to B.
- If $f:A \to B$, 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/value of function for argument a and a is the pre-image/argument of b.

- The range of $f:A \to B$ is the set of all images of all elements of A.



Functions

- Let us take a look at the function $f:P \rightarrow C$ with
- P = {Linda, Max, Kathy, Peter}
- C = {Boston, New York, Hong Kong, Moscow}

- f(Linda) = Moscow
- f(Max) = Boston
- f(Kathy) = Hong Kong
- f(Peter) = New York

- Here, the range of f is C.

Functions

- Let us re-specify f as follows:

- f(Linda) = Moscow
- f(Max) = Boston
- f(Kathy) = Hong Kong
- f(Peter) = Boston

- Is f still a function? yes

What is its range? {Moscow, Boston, Hong Kong}

- The Codomain is the set of values that could **possibly** come out. The Codomain is actually **part of the definition** of the function.
- And The Range is the set of values that **actually do** come out.

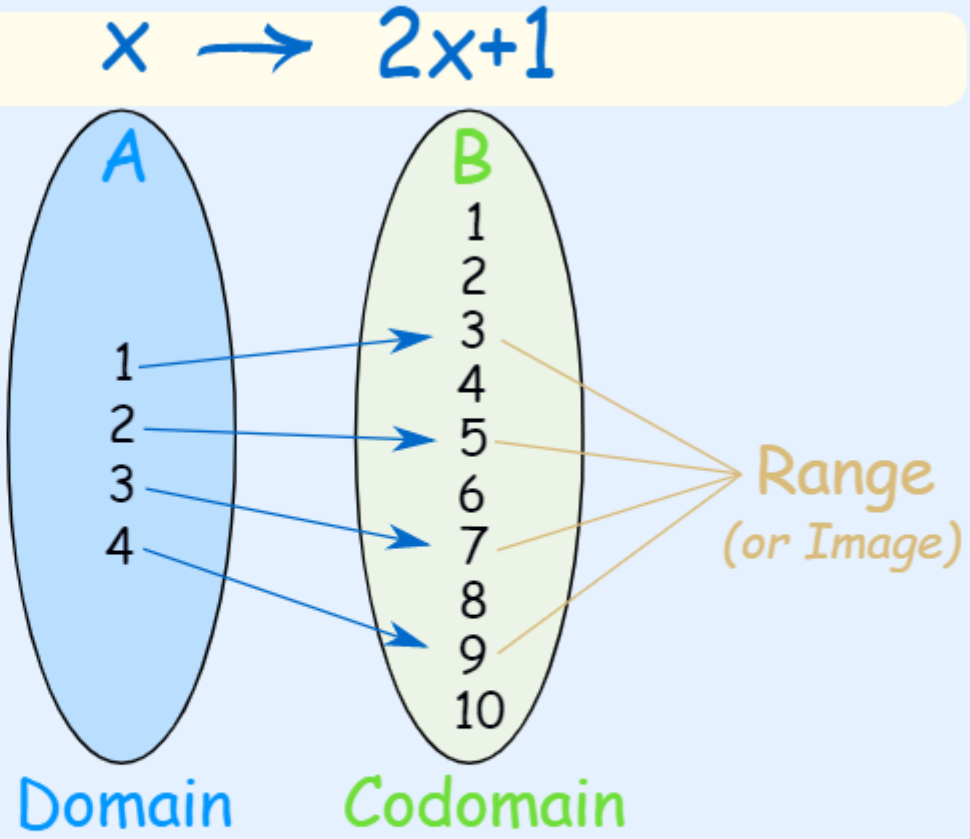
Domain, Codomain, Range

Example

- The set "A" is the **Domain**,
- The set "B" is the **Codomain**,
- And the set of elements that get pointed to in B (the actual values produced by the function) are the **Range**, also called the Image.

And we have:

- Domain: {1, 2, 3, 4}
- Codomain: {1, 2, 3, 4, 5, 6, 7, 8, 9, 10}
- Range: {3, 5, 7, 9}



Function Examples

- Let A={1,2,3,4} and B={a,b,c,d} and let

  f={(1,a),(2,a), (3,d),(4,c)}

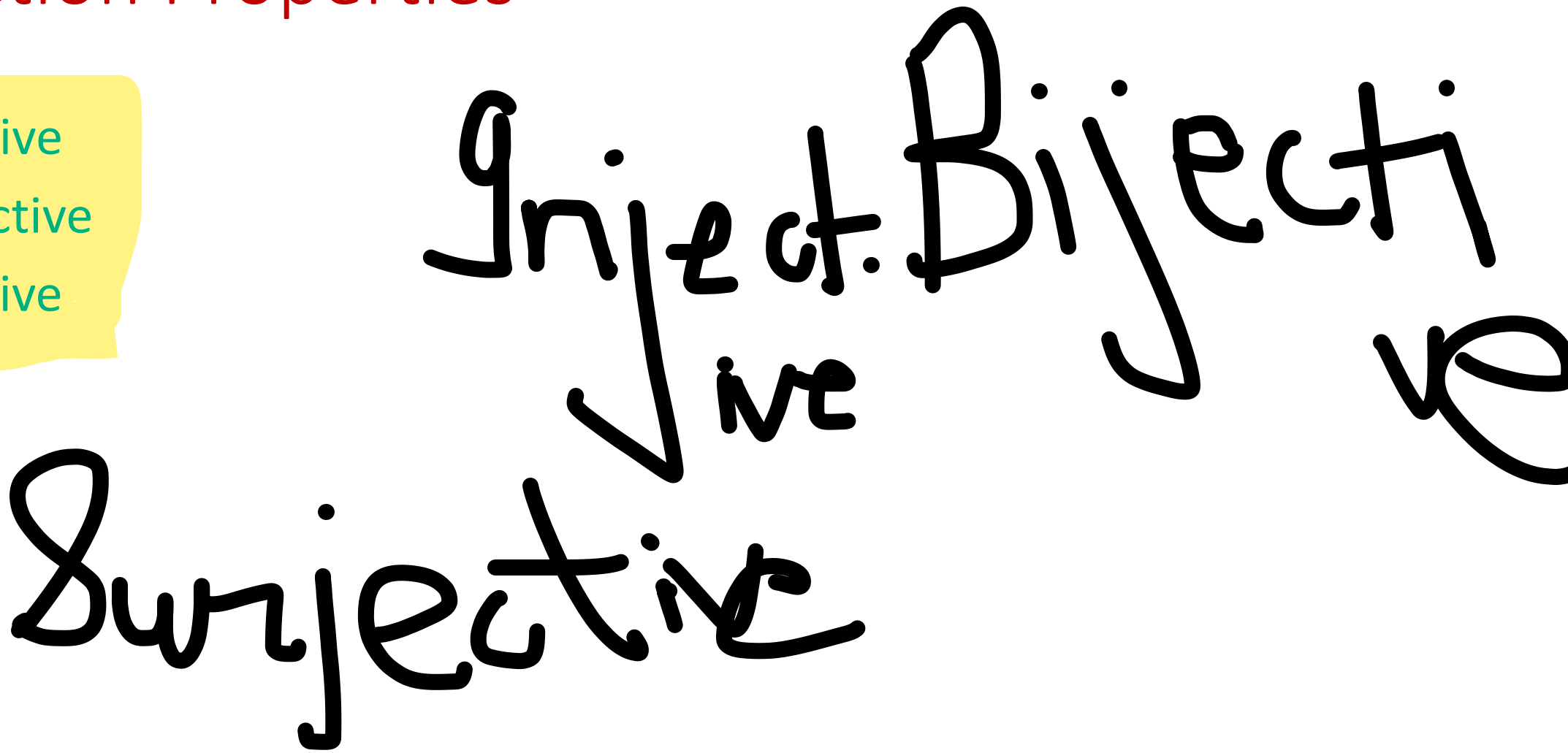
  Is f a function? What are its ranges? Codomain?
- Let A= {1,2,3} and B={x,y,z} and

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

  Are relation S and R functions?
- Is $f(x) \rightarrow x^2$ a function ?

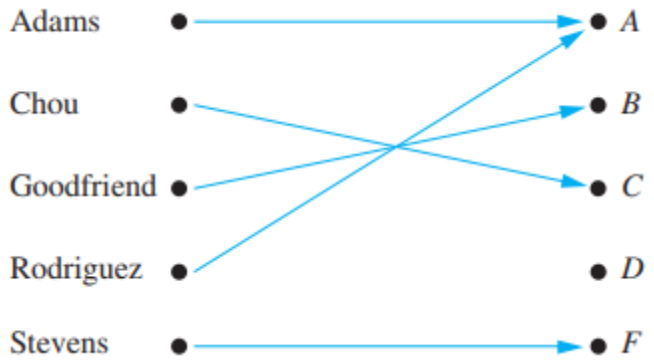
Function Properties

- Injective
- Surjective
- Bijective



Injective function or one to one function

- What are domain, codomain, and range of function that assign grades to students?
- Let R be relation consisting of ordered pairs (Abdul,22), (Brenda,24), (Carla,21), (Desire,22), (Eddie,24),(Felicia,22), where each pair consists of graduate student and age of this student. What is the function this relation determines?
- Let f be function that assigns the last two bits of a binary bit string of length 2 or greater to a string. For example, f (11010)=10. What is codomain of set?

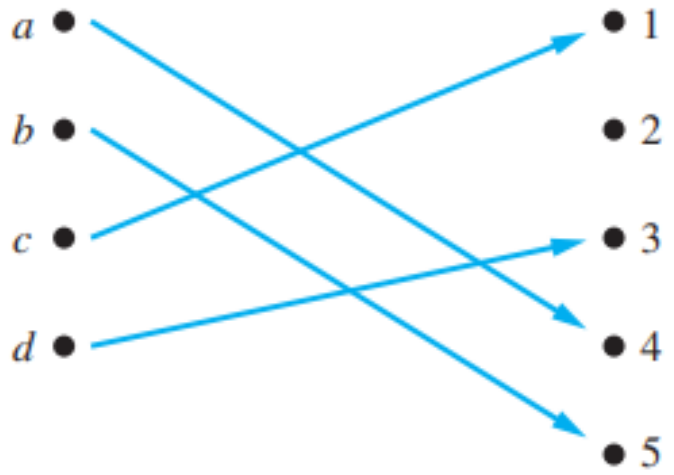


Properties of Functions

•A function f:A→B is said to be **one-to-one (or injective),** if and only if

- $\forall x, y \in A\ (f(x) = f(y) \rightarrow x = y)$
- If f(a)= f(a'), then a=a'

•In other words: f is one-to-one if and only if it does not map two distinct elements of A onto the same element of B.



Properties of Functions

- And again…
- f(Linda) = Moscow
- f(Max) = Boston
- f(Kathy) = Hong Kong
- f(Peter) = Boston

- Is f one-to-one?

- No, Max and Peter are mapped onto the same element of the image.

g(Linda) = Moscow
g(Max) = Boston
g(Kathy) = Hong Kong
g(Peter) = New York

Is g one-to-one?

Yes, each element is assigned a unique element of the image.

Injective

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

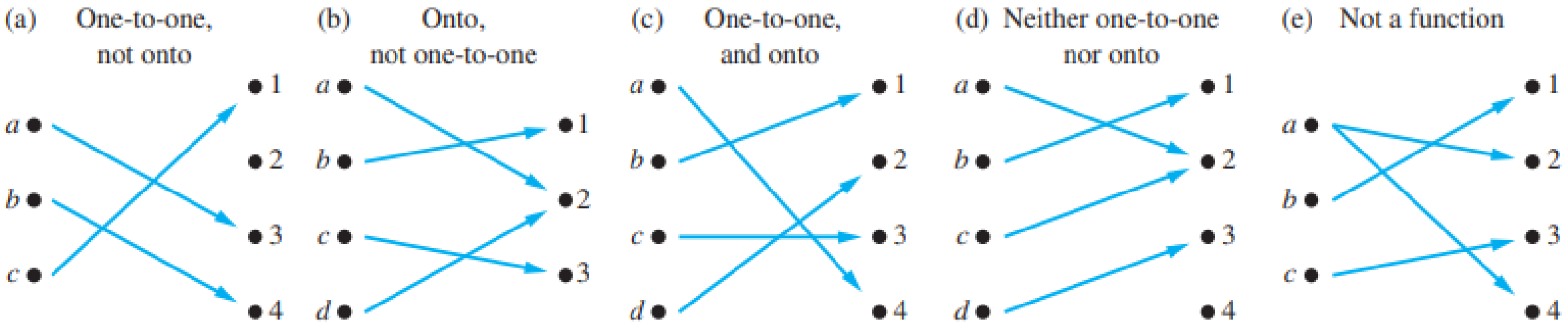
Properties of function

- For some functions, range and codomain are equal. That is every member of codomain is image of some element of domain Functions with this property are called onto functions
- A function f from A to B is called **onto, or a surjection**, if and only if for every element b ∈ B there is an element a ∈ A with f (a) = b. A function f is called surjective if it is onto

Properties of function

1. Let f be the function from {a, b, c, d} to {1, 2, 3} defined by f (a) = 3, f (b) = 2, f (c) = 1, and f (d) = 3. Is f an onto function?
2. Is the function f (x) = x2 from the set of integers to the set of integers onto?
3. Is the function f (x) = x + 1 from the set of integers to the set of integers onto?

Different functions



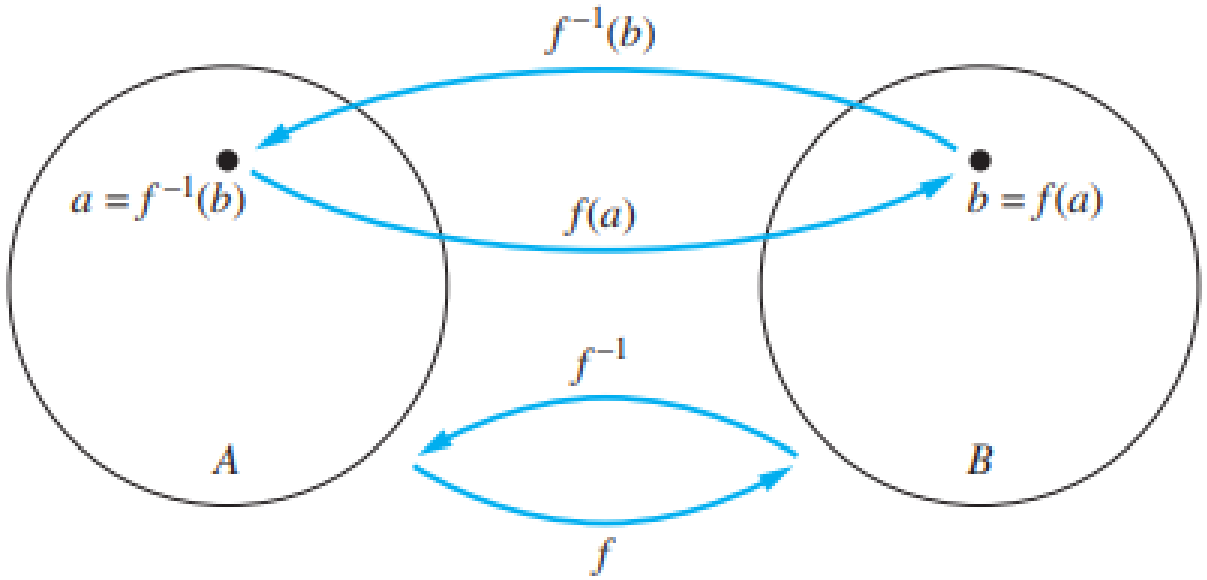
Bijective Function

- The function f is a **one-to-one correspondence, or a bijection**, if it is both one-to-one and onto. We also say that such a function is bijective
- Let f be the function from {a, b, c, d} to {1, 2, 3, 4} with f (a) = 4, f (b) = 2, f (c) = 1, and f (d) = 3. Is f a bijection?
- Let A be a set. The identity function on A is the function ιA : A → A, where $t_A(x)=x$. Is function is bijection?

Inverse function

- Let f be a one-to-one correspondence from the set A to the set B. The inverse function of f is the function that assigns to an element b belonging to B the unique element a in A such that f (a) = b. The inverse function of f is denoted by f^{-1}. Hence, $f^{-1}(b) = a$ when f (a) = b.
- Be sure not to confuse the function f^{-1} with the function 1/f , which is the function that assigns to each x in the domain the value 1/f (x). Notice that the latter makes sense only when f (x) is a non-zero real number
- A one-to-one correspondence is called invertible because we can define an inverse of this function. A function is not invertible if it is not a one-to-one correspondence, because the inverse of such a function does not exist

Inverse function



Inverse function

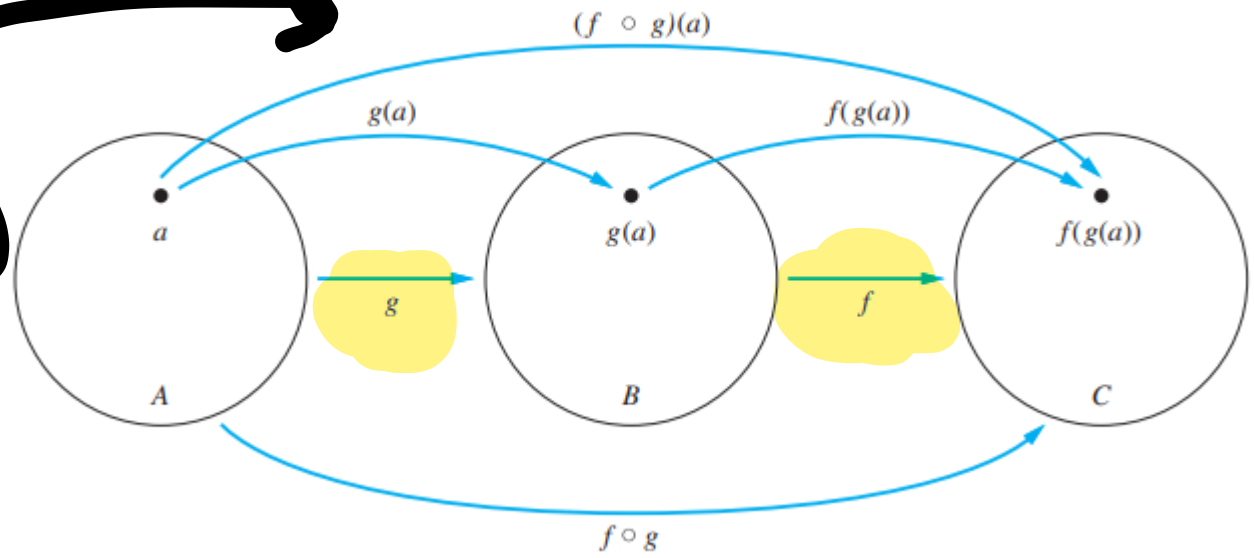
1. Let f be the function from {a, b, c} to {1, 2, 3} such that f (a) = 2, f (b) = 3, and f (c) = 1. Is f invertible, and if it is, what is its inverse?
2. Let f : Z → Z be such that f (x) = x + 1. Is f invertible, and if it is, what is its inverse?

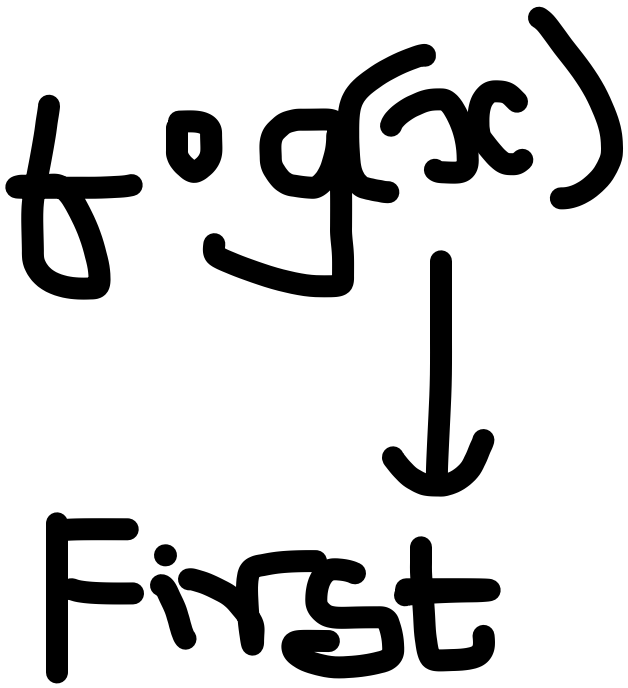
Inverse Function

- Show that if we restrict the function $f(x) = x^2$ from the set of all nonnegative real numbers to the set of all nonnegative real numbers, then f is invertible.
- Solution: The function $f(x) = x^2$ from the set of nonnegative real numbers to the set of nonnegative real numbers is one-to-one. To see this, note that if $f(x) = f(y)$, then $x^2 = y^2$, so $x^2 - y^2 = (x + y)(x - y) = 0$. This means that $x + y = 0$ or $x - y = 0$, so $x = -y$ or $x = y$. Because both x and y are nonnegative, we must have $x = y$. So, this function is one-to-one. Furthermore, $f(x) = x^2$ is onto when the codomain is the set of all nonnegative real numbers, because each nonnegative real number has a square root. That is, if y is a nonnegative real number, there exists a nonnegative real number x such that $x = \sqrt{y}$, which means that $x^2 = y$. Because the function $f(x) = x^2$ from the set of nonnegative real numbers to the set of nonnegative real numbers is one-to-one and onto, it is invertible. Its inverse is given by the rule $f^{-1}(y) = \sqrt{y}$

Composite Function

- 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)).





Composition

- The **composition** of two functions $g:A \to B$ and $f:B \to C$, denoted by $f \circ g$, is defined by

- $(f \circ g)(a) = f(g(a))$

- This means that
  - **first**, function g is applied to element $a \in A$, mapping it onto an element of B,
  - **then**, function f is applied to this element of B, mapping it onto an element of C.
  - **Therefore**, the composite function maps from A to C.

Composition Function

- Let g be the function from the set {a, b, c} to itself such that g(a) = b, g(b) = c, and g(c) = a. Let f be the function from the set {a, b, c} to the set {1, 2, 3} such that f (a) = 3, f (b) = 2, and f (c) = 1. What is the composition of f and g, and what is the composition of g and f ?
- Solution: f and g
  - $(f \circ g)(a) = f(g(a)) = f(b) = 2$, $(f \circ g)(b) = f(g(b)) = f(c) = 1$, and $(f \circ g)(c) = f(g(c)) = f(a) = 3$.
- Solution: g and f
  - Not defined..

Composition function

- 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: f and g
  - $(f \circ g)(x) = f(g(x)) = f(3x + 2) = 2(3x + 2) + 3 = 6x + 7$
- Solution: g and f
  - $(g \circ f)(x) = g(f(x)) = g(2x + 3) = 3(2x + 3) + 2 = 6x + 11$

- Remarks: Note that even though $f \circ g$ and $g \circ f$ are defined for the functions f and g , $f \circ g$ and $g \circ f$ are not equal. In other words, the commutative law does not hold for the composition of functions.

Composition

- Composition of a function and its inverse:

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

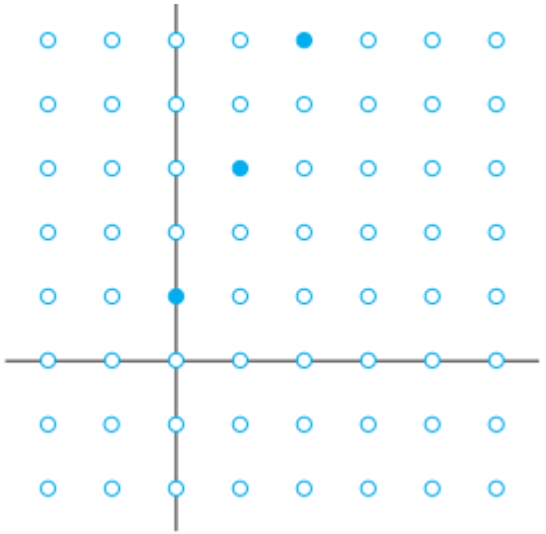
- The composition of a function and its inverse is the **identity function** $i(x) = x$.

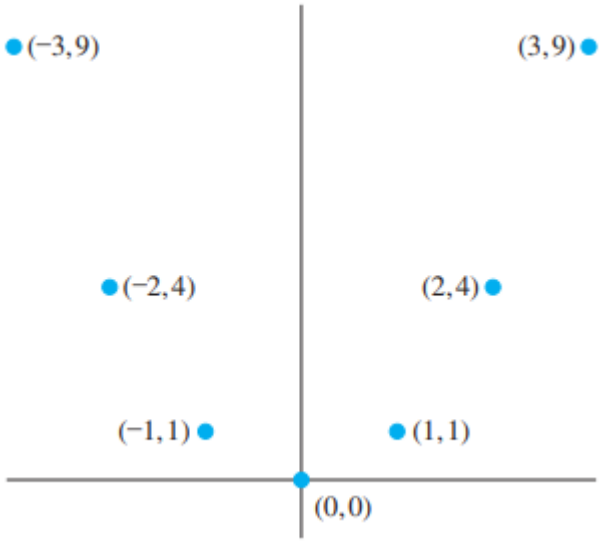
Graph

- The **graph** of a function $f:A \rightarrow B$ is the set of ordered pairs $\{(a, b) \mid a \in A$ and $f(a) = b\}$.
- The graph is a subset of $A \times B$ that can be used to visualize f in a two-dimensional coordinate system.
- Display the graph of the function f (n) = 2n + 1 from the set of integers to the set of integers.
- Display the graph of the function f (x) = x2 from the set of integers to the set of integers.

Graphs

- Solution: The graph of f is the set of ordered pairs of the form (n, 2n + 1), where n is an integer
- The graph of f is the set of ordered pairs of the form (x, f (x)) = (x, x^2), where x is an integer.





Functions for Computer Science

- Ceiling Function
- Floor function
- Boolean Function
- Exponential function
- Hashing function

Floor and ceiling function

- The floor function rounds x down to the closest integer less than or equal to x, and the ceiling function rounds x up to the closest integer greater than or equal to x.
- 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 $\lfloor x \rfloor$.
- 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 $\lceil x \rceil$.

Floor and ceiling function

- **Examples:** $\lfloor 2.3 \rfloor = 2, \lfloor 2 \rfloor = 2, \lfloor 0.5 \rfloor = 0, \lfloor -3.5 \rfloor = -4$
- **Examples:** $\lceil 2.3 \rceil = 3, \lceil 2 \rceil = 2, \lceil 0.5 \rceil = 1, \lceil -3.5 \rceil = -3$

Boolean Function

- Let B=[true,false]. Then a function from a set A to B is called Boolean function.
- Example: Let p(x):x is even and Q(y):y is odd. Then P(4) is true and Q(4) is false.

Exponential Function

- Let $A=B=Z^+$ and let $f:A \rightarrow B$ be defined by $f(z)=2^z$. We call f the base 2 exponential function.
- Let $A=B=R$ and let $f_n:A \rightarrow B$ be defined for each positive integer $n>1$ as $f_n(x)=\log_n(x)$, the logarithm to base n of x.

Hashing Function

- Read yourself

NUMBER THEORY

Number Theory

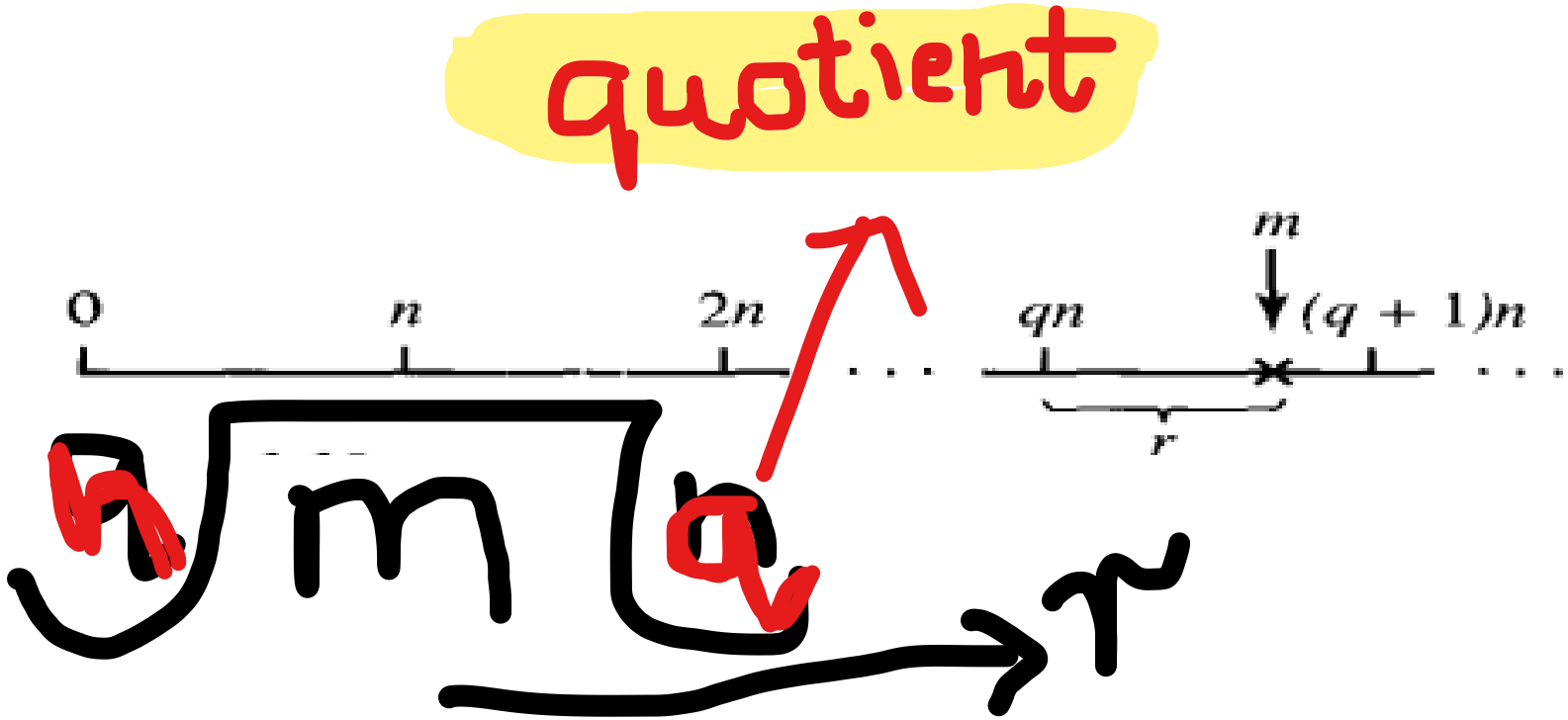
- Number theory is about integers and their properties
- Basic principles
  - Divisibility
  - Modular arithmetic
  - Greatest common divisors
  - Least common multipliers

A. Division Definition

- If a and b are integers with $a \neq 0$, we say that a divides b if there is an integer c so that $b = ac$.
- When a divides b we say that a is a factor of b and that b is a multiple of a.
- The notation $a \mid b$ means that a divides b.
- We write $a \nmid b$ when a does not divide b

Division in Integers

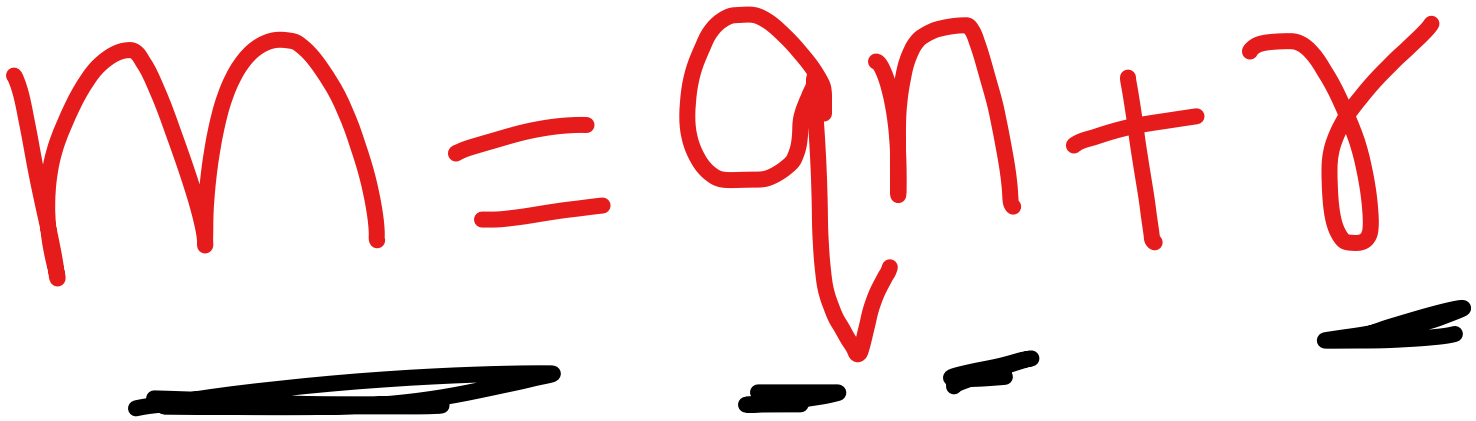
- If m and n are non-negative integers and n is not zero. We can write m=qn + r.
- If m is multiple of n, r=0 and if m is not multiple of n, r is not 0
- $0 \leq r < n$
- n is divisor
- m is dividend
- q is quotient
- r is remainder



Divisibility Algorithm

- THEOREM 1: If n≠ 0 and m are non-negative integers, we can write m=qn+r for some nonnegative integers q and r with $0 \leq r < n$.

- Example: if n is 3 and m is 16, then 16=5(3)+1, so q is 5 and r is 1
-



Theorem Properties

THEOREM 2: For integers a, b, and c it is true that

- if a | b and a | c, then a | (b + c)

Example: 3 | 6 and 3 | 9, so 3 | 15.

- if a | b, then a | bc for all integers c
- **Example**: 5 | 10, so 5 | 20, 5 | 30, 5 | 40, …
- if a | b and b | c, then a | c
- **Example**: 4 | 8 and 8 | 24, so 4 | 24
- if a | b and a | c, where b>c, then a | b-c

Example: 4 | 24 and 4 | 8, so 4 | (24-8=16)

Theorem Properties

- if a | b and a | c, then a | (b + c)
  - Proof
  - There are integers s and t. b=as, c=at
  - b+c=as+at=a(s+t)
  - Thus a divides (b+c)

  (Proof for other properties are homework)

Integer Division

1. What are quotient and remainder when 101 is divided by 11?
2. What are quotient and remainder when -11 is divided by 3?

Note : Remainder cannot be negative. Because r=-2 does not satisfy $0 \leq r < 3$.

B. Modular Arithmetic

- Let a be an integer and m be a positive integer.
We denote by **a mod m** the remainder when a is divided by m.

- **Examples:**

9 mod 4 = 1

9 mod 3 = 0

9 mod 10 = 9

-13 mod 4 = 3

Congruences

- Let a and b be integers and m be a positive integer. We say integers a and b are congruent modulo m, if they have same remainder on division by m.

- Example: 16, 21 are congruent on modulo 5.

- Or a **is congruent to b modulo m** if m divides a – b.

- **Representation**: We use the notation **a ≡ b (mod m)** to indicate that a is congruent to b modulo m.

Theorem::
a ≡ b (mod m) if and only if **a mod m = b mod m.**

Congruences

Theorem::

$a \equiv b \pmod{m}$ if and only if **a mod m = b mod m.**

- **Proof**
- **If** $a \equiv b \pmod{m}$, then there are integers q,q' and r,
  with a=qn+r
  and b=q'n+r.
  So a-b=(qn+r)-(q'n+r)
  =qn-q'n
  = (q-q')n

Congruence

- Determine whether 17 is congruent to 5 modulo 6 and whether 24 and 14 are congruent modulo 6.
- Solution
  - (17-5)=12 is divisible by 6 . Hence congruent
  - (24-14)=10 is not divisible by 6. Hence not congruent

Congruence

- **Theorem**: 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 $a \equiv b \pmod{m}$, then $m \mid (a-b)$.
- This means 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 $a \equiv b \pmod{m}$
- **The set of all integers congruent to an integer a modulo m is called congruence class of modulo m.**

Applications of congruence/

- Assigning memory locations to computer files
- Generation of pseudo random numbers
  - $X_{n+1}=(ax_n+c) \bmod m$
- cryptosystems

C.1 Prime Number

- Definition:
  - A prime is an integer greater than 1 that is divisible by 1 and by itself. A positive integer p greater than 1 is called prime if only positive factors of p are 1 and p. A positive integer that is greater than 1 and is not prime is called composite.
- Composite Definition:
  - The integer n is composite if and only if there exists an integer a such that a|n and 1 <a < n

Algorithm to find out prime???

C.1 Prime Number

- Theorem 1: Every positive integer greater than 1 can be written uniquely as prime or as product of two or more primes.
  - Find prime factorization of 100, 999
  - Example: $100=2.2.5.5=2^2 5^2$
  - $999=3.3.3.37=3^3.37$
- Theorem 2: If n is composite integer, then n has prime divisor less than or equal to $\sqrt{n}$.
  - It follows that an integer is prime if it is not divisible by any prime less than or equal to its square root.
  - Show that 101 is prime

C.1 Prime Number

- Twin prime: Twin primes are primes that differ by 2 such as 3 and 5, 7 and 9, 11 and 13
- Mersenne primes: 2^p-1 is also prime given p is prime

C.2 Greatest Common Divisors

Definition

- 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.

Representation

- The greatest common divisor of a and b is denoted by gcd(a, b).

- **Example 1:** What is gcd(48, 72) ?
- The positive common divisors of 48 and 72 are 1, 2, 3, 4, 6, 8, 12, 16, and 24, so gcd(48, 72) = 24.

- **Example 2:** What is gcd(19, 72) ?
- The only positive common divisor of 19 and 72 is 1, so gcd(19, 72) = 1.

C.2 Greatest Common Divisors

- **Using prime factorizations:**

- $a = p_1^{a_1} p_2^{a_2} \ldots p_n^{a_n}$, $b = p_1^{b_1} p_2^{b_2} \ldots p_n^{b_n}$,
- where $p_1 < p_2 < \ldots < p_n$ and $a_i, b_i \in \mathbf{N}$ for $1 \leq i \leq n$

- $\gcd(a, b) = p_1^{\min(a_1, b_1)} p_2^{\min(a_2, b_2)} \ldots p_n^{\min(a_n, b_n)}$

- **Example:**

$a = 60 = 2^2 3^1 5^1$

$b = 54 = 2^1 3^3 5^0$

$\gcd(a, b) = 2^1 3^1 5^0 = 6$

Relatively Prime Integers

- **Definition:**

Two integers a and b are **relatively prime** if gcd(a, b) = 1.

Examples:

- Are 15 and 28 relatively prime?
- Yes, gcd(15, 28) = 1.
- Are 55 and 28 relatively prime?
- Yes, gcd(55, 28) = 1.
- Are 35 and 28 relatively prime?
- No, gcd(35, 28) = 7.

Relatively Prime Integers

- **Definition:**
- The integers $a_1, a_2, \ldots, a_n$ are **pairwise relatively prime** if $\gcd(a_i, a_j) = 1$ whenever $1 \leq i < j \leq n$.
- **Examples:**
- Are 15, 17, and 27 pairwise relatively prime?
- No, because gcd(15, 27) = 3.
- Are 15, 17, and 28 pairwise relatively prime?
- Yes, because gcd(15, 17) = 1, gcd(15, 28) = 1 and gcd(17, 28) = 1.

D. Least Common Multiples

- **Definition:**
- The **least common multiple** of the positive integers a and b is the smallest positive integer that is divisible by both a and b.
- We denote the least common multiple of a and b by lcm(a, b).
- **Examples:**

lcm(3, 7) = 21

lcm(4, 6) = 12

lcm(5, 10) = 10

D. Least Common Multiples

- **Using prime factorizations:**

- $a = p_1^{a_1} p_2^{a_2} \dots p_n^{a_n}$, $b = p_1^{b_1} p_2^{b_2} \dots p_n^{b_n}$,
- where $p_1 < p_2 < \dots < p_n$ and $a_i, b_i \in \mathbf{N}$ for $1 \leq i \leq n$

- $\text{lcm}(a, b) = p_1^{\max(a_1, b_1)} p_2^{\max(a_2, b_2)} \dots p_n^{\max(a_n, b_n)}$

- **Example:**

a = 60 = $2^2 3^1 5^1$

b = 54 = $2^1 3^3 5^0$

lcm(a, b) = $2^2 3^3 5^1 = 4 \cdot 27 \cdot 5 = 540$

GCD and LCM

$a = 60 = 2^2 \; 3^1 \; 5^1$

$b = 54 = 2^1 \; 3^3 \; 5^0$

$\gcd(a, b) = 2^1 \; 3^1 \; 5^0 = 6$

$\text{lcm}(a, b) = 2^2 \; 3^3 \; 5^1 = 540$

Theorem: $a \cdot b = \gcd(a,b) \cdot \text{lcm}(a,b)$

Sieve of Eratosthenes Algorithm

1. To find out all primes under n, generate a list of all integers from 2 to n. (Note: 1 is not prime)
2. Start with a smallest prime number, ie p=2
3. Mark all the multiples of p which are less than n as composite. To do this, mark the value of the numbers (multiples of p) in the generated list as 0. Do not mark p itself as composite.
4. Assign the value of p to the next prime. The next prime is the next non-zero number in the list which is greater than p.
5. Repeat the process until $p \leq \sqrt{n}$.

Sieve of Eratosthenes Algorithm

- Create a list of integers from 2 to 10. list =[2,3,4,5,6,7,8,9,10]
- Start with p=2
- Since $2^2 \leq 10$, continue
- Mark all multiples fo 2 as composite by setting their value as 0 in the list. List=[2,3,0,5,0,7,0,9]
- Assign value of p to next prime i.e 3. Since $3^2 \leq 10$, continue
- Mark all multiples of 3 as composite by setting their value as 0 in the list
- Assign value of p to 5.
- Since $5^2 \nleq 10$, stop

The Euclidean Algorithm/Euclid's algorithm

- Finds GCD of two numbers efficiently
- Theorem
  - Let a=b+qr, where a,b,q,r are integers. Then gcd(a,b)=gcd(b,r)
- Base
  - if a | b and a | c, where b>c, then a | b-c
- Algorithm
  - Subtraction
    - If we subtract smaller number from larger one, GCD does not change
    - So if we keep subtracting repeatedly larger of two, we end up with GCD.
    - Eg: (287,91)
  - Division
    - Now instead of subtraction, if we divide smaller number, algorithm stops when we find remainder 0
    - repeatedly divide the divisor by the remainder until the remainder is 0. The gcd is the last non-zero remainder in this algorithm
    - Use division method (287,91)

The Euclidean Algorithm

- The **Euclidean Algorithm** finds the **greatest common divisor** of two integers a and b.
- For example, if we want to find gcd(287, 91), we **divide** 287 by 91:
- $287 = 91 \cdot 3 + 14$
- We know that for integers a, b and c,
if $a \mid b$ and $a \mid c$, then $a \mid (b + c)$.
- Therefore, any divisor (including their gcd) of 287 and 91 must also be a divisor of $287 - 91 \cdot 3 = 14$.
- Consequently, gcd(287, 91) = gcd(14, 91).

The Euclidean Algorithm

- In the next step, we divide 91 by 14:
- $91 = 14 \cdot 6 + 7$
- This means that gcd(14, 91) = gcd(14, 7).
- So we divide 14 by 7:
- $14 = 7 \cdot 2 + 0$
- We find that $7 \mid 14$, and thus gcd(14, 7) = 7.
- **Therefore, gcd(287, 91) = 7.**

The Euclidean Algorithm

- In **pseudocode**, the algorithm can be implemented as follows:

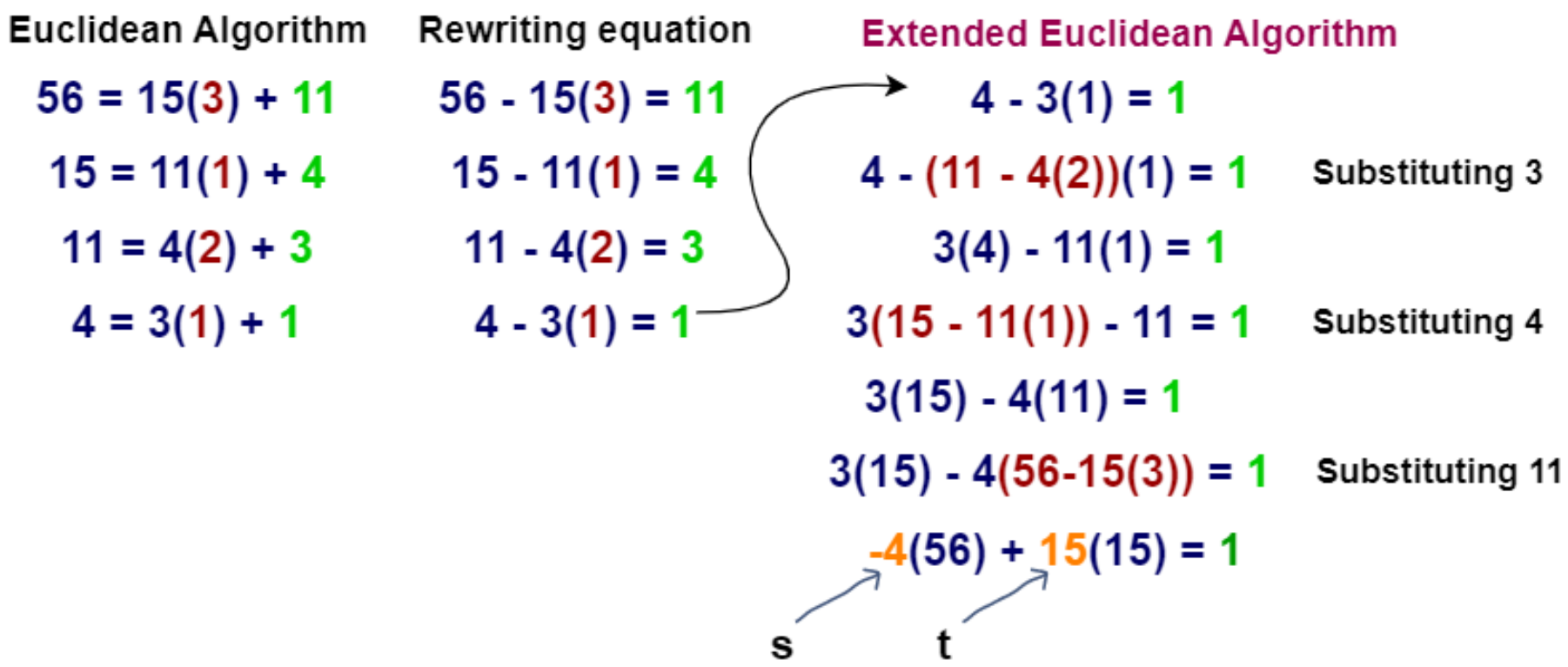
- **procedure** gcd(a, b: positive integers)
- x := a
- y := b
- **while** y ≠ 0
- **begin**
- r := x **mod** y
- x := y
- y := r
- **end** {x is gcd(a, b)}

Extended Euclidean algorithm

- In addition to computing GCD, Extended Euclidean Algorithm also finds integers *s* and *t* such that $as+bt=gcd(a,b)$.
- Bézout's Identity guarantees the existence of *s* and t
-

  Extended Euclidean Algorithm finds s and t by using back substitutions to recursively rewrite the division algorithm equation until we end up with the equation that is a linear combination of our initial numbers

Extended Euclidean algorithm



MATRIX

Matrix

- Definition:
  - A matrix is rectangular array of numbers. A matrix with m rows and n columns is called m x n matrix.
  - A matrix with same number of rows and columns is called square
  - Two matrices are equal if they have same number of rows and same number of columns and corresponding entries in every position are equal
  - The (i,j)th element of A is element a_{ij}, that represents ith row and jth column of A.

$$\begin{bmatrix} 1 & -6 \\ 4 & 13 \\ -3 & 5 \end{bmatrix}$$

3x2

$$\begin{bmatrix} 3 & -3 & 4 \\ 5 & 2 & 8 \end{bmatrix}$$

2x3

Sum of Two matrices

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

$$\begin{bmatrix} 2 & -3 & 7 \\ 3 & -2 & 1 \end{bmatrix} + \begin{bmatrix} 3 & 4 & 1 \\ 2 & 5 & 2 \end{bmatrix} = \begin{bmatrix} 5 & 1 & 8 \\ 5 & 3 & 3 \end{bmatrix}$$

Matrix Multiplication

Let A be an mxk matrix and B be a kxn matrix. The *product* of A and B, denoted by AB, is the mxn matrix with (i,j)th entry equal to the sum of the products of the corresponding elements from the ith row of A and the jth column of B. In other words, if AB = $[c_{ij}]$, then

$$c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \ldots + a_{ik}b_{kj} = \sum_{t=1}^{k} a_{it}b_{tj}$$

Matrix multiplication -- Example

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

3x2 2x3 3x3

Matrix multiplication -- Example

$$\begin{bmatrix} 3 & 2 \\ 1 & 5 \\ 3 & 0 \end{bmatrix} \begin{bmatrix} 2 & 1 & 0 \\ -1 & 3 & 4 \end{bmatrix} = \begin{bmatrix} 4 & 9 & 8 \\ -3 & 16 & 20 \\ 6 & 3 & 0 \end{bmatrix}$$

3×2 $\quad$ 2×3 $\quad$ 3×3

Matrix Multiplication- algorithm

```
procedure matrix
multiplication(A,B:matrices)
for i:=1 to m
begin
    for j:=1 to n
    begin
        c_ij := 0
        for q := 1 to k
            c_ij := c_ij + a_iq b_qj
    end
end
```

Identity Matrix

Exist as square matrices.

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

$$AI = IA = A$$

Transpose of matrix

The transpose of a square matrix **A** is labeled $\mathbf{A}^T$ and is found by interchanging rows and columns.

$$A = \begin{bmatrix} 3 & 6 & 8 \\ 4 & 5 & 2 \\ 1 & 9 & 7 \end{bmatrix} \qquad A^T = \begin{bmatrix} 3 & 4 & 1 \\ 6 & 5 & 9 \\ 8 & 2 & 7 \end{bmatrix}$$

Symmetric matrix

A square matrix A is called *symmetric* if $A = A^T$.

$$\begin{bmatrix} 3 & 4 & 8 & 7 \\ 4 & 9 & 1 & 4 \\ 8 & 1 & 3 & 5 \\ 7 & 4 & 5 & 0 \end{bmatrix}$$

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

Zero One Matrix

- A matrix with entries that are either 0 or 1 is called zero-one matrix
- What is difference between zero one matrix and identity matrix??

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

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

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

Operations of zero one matrix

- Join
- Meet

$$b_1 \wedge b_2 = \begin{cases} 1 & \text{if } b_1 = b_2 = 1 \\ 0 & \text{otherwise,} \end{cases}$$

$$b_1 \vee b_2 = \begin{cases} 1 & \text{if } b_1 = 1 \text{ or } b_2 = 1 \\ 0 & \text{otherwise.} \end{cases}$$

Join of two zero one matrices

Let $A = [a_{ij}]$ and $B = [b_{ij}]$ be $m \times n$ zero-one matrices. Then the join of A and B is the zero-one matrix with (i, j)th entry $a_{ij} \vee b_{ij}$

- Join of two A and B matrices is represented by AVB

Join of two zero one matrices

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

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

Meet of two zero one matrices

The *meet* of A and B is the zero-one matrix with (i, j)th entry $a_{ij} \wedge b_{ij}$.

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

Meet of two A and B matrices is represented by A∧B

Find join and meet of two matrices

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

Find join and meet of two matrices

- Join

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

  - Meet

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

Boolean product of matrix

- Let $A = [a_{ij}]$ be an $m \times k$ zero–one matrix and $B = [b_{ij}]$ be a $k \times n$ zero–one matrix.
- Then the Boolean product of A and B, denoted by $\mathbf{A} \odot \mathbf{B}$, is the $m \times n$ matrix with (i, j)th entry c_{ij} where
- $cij = (a_{i1} \wedge b_{1j}) \vee (a_{i2} \wedge b_{2j}) \vee \cdots \vee (a_{ik} \wedge b_{kj})$.

Find Boolean product of A and B

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

Find Boolean product of A and B

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

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

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

Boolean Power of matrix

- Let A be a square zero–one matrix and let r be a positive integer. The r^{th} Boolean power of A is the Boolean product of r factors of A. The r^{th} Boolean product of A is denoted by A[r] .
- Hence $A^{[r]} = \underbrace{A \odot A \odot A \cdots \odot A}_{\text{r times}}$

Boolean Power of matrix

Let $\mathbf{A} = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{bmatrix}$. Find $\mathbf{A}^{[n]}$ for all positive integers n.

Boolean Power of matrix

$$\mathbf{A}^{[2]} = \mathbf{A} \odot \mathbf{A} = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{bmatrix}$$

$$\mathbf{A}^{[3]} = \mathbf{A}^{[2]} \odot \mathbf{A} = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix}.$$

$$\mathbf{A}^{[4]} = \mathbf{A}^{[3]} \odot \mathbf{A} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix}$$

$$\mathbf{A}^{[5]} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}.$$

$\mathbf{A}^{[n]} = \mathbf{A}^{[5]}$ for all positive integers n with $n \geq 5$.

COUNTING

Combinatorics

- Combinatorics, study of arrangement of objects
- Count number of ways to put things together into various combinations

  e.g. If a password is 6-8 letters and/or digits, how many passwords can there be?
- Two main rules
  - Sum rule/Addition rule
  - Product rule

Sum Rule/Addition Rule

- Let us consider two tasks:
  - *m* is the number of ways to do **task 1**
  - *n* is the number of ways to do **task 2**
  - Tasks are independent of each other, i.e.,
    - Performing **task 1** does not accomplish **task 2** and vice versa.
- *Sum rule*: the number of ways that "**either** task 1 **or** task 2 can be done, but **not both**", is *m*+*n*.
- Generalizes to multiple tasks ...

Example

- A student can choose a computer project from one of three lists. The three lists contain 23, 15, and 19 possible projects respectively. How many possible projects are there to choose from?
- Solution:
  - The student can choose a project by selecting project from first list, second list or third list
  - By sum rule, there are 23 + 15 +19=57 ways

Example

- Suppose either member of mathematics faculty or student who is mathematics major is chosen as representative to university committee. How many different choices are there for this representative if there are 37 members of mathematics faculty and 83 mathematics major s and no one is both faculty member and student?
- If there are 10 both faculty member and student?

Set Theoretic Version

- If A is the set of ways to do task 1, and B the set of ways to do task 2, and if A and B are disjoint, then:

"the ways to do either task 1 or 2 are

$A \cup B$, and $|A \cup B| = |A| + |B|$"

Product Rule

- Let us consider two tasks:
  - *m* is the number of ways to do **task 1**
  - *n* is the number of ways to do **task 2**
  - Tasks are independent of each other, i.e.,
    - Performing task 1does not accomplish task 2 and vice versa.
- P*roduct rule*: the number of ways that "**both** tasks 1 and 2 can be done" in *mn*.
- Definition: Suppose that a procedure can be broken down into sequence of two tasks. IF there are n_1 ways to do first task and for each of these ways of doing first task, there are n_2 ways to do second task, then there are n_1n_2 ways to do procedure.
- Generalizes to multiple tasks ...

Example

- The chairs of an auditorium are to be labeled with a letter and a positive integer not to exceed 100. What is the largest number of chairs that can be labeled differently?
- A new company with two employees. Ram and Hari rents a floor of a building with 12 offices. How many ways are there to assign different offices to these two employees?

Set Theoretic Version

- If A is the set of ways to do task 1, and B the set of ways to do task 2, and if A and B are disjoint, then:
- The ways to do both task 1 and 2 can be represented as $A \times B$, and $|A \times B| = |A| \cdot |B|$

Extended Product function

- Lets a procedure is carried out by performing tasks $T_1, T_2, \ldots T_m$ in sequence. If task T_i, i=1,2,..n can be done in n ways, regardless of how previous tasks were done, then there are $n_1 . n_2 .. n_m$ ways to carry out procedure.
- **Example**
- How many different bit strings of length seven are there?

- How many different license plates are available if each plate contains a sequence of three letters followed by three digits(no sequence of letters are prohibited)

Examples Using both rules

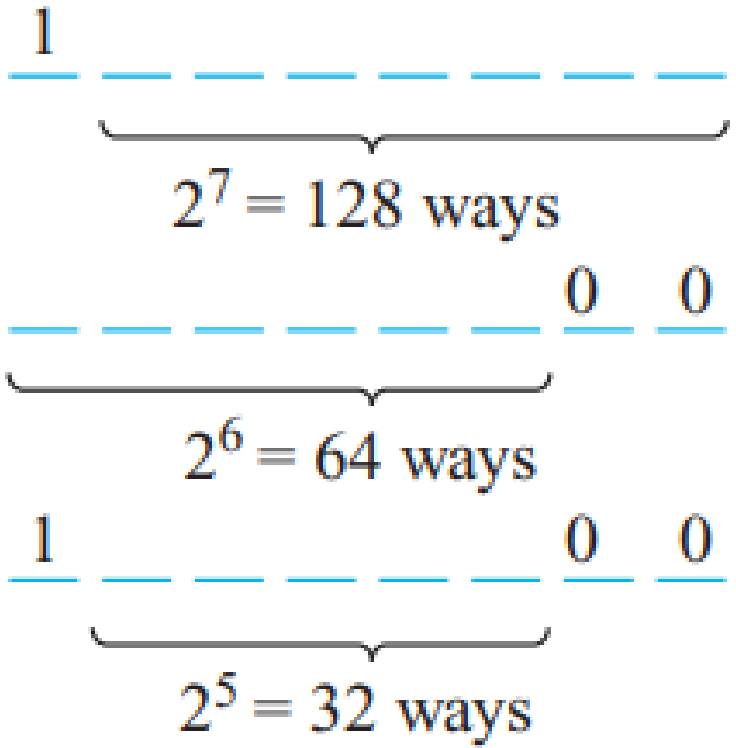
- In a version of computer language BASIC, the name of variable is a string of one or two alphanumeric characters, where uppercase and lowercase letters are not distinguished. More over, a variable name must begin with a letter and must be different from five strings of two characters that are reserved for programming use. How many different variable names are there in version of BASIC?

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

Inclusion-Exclusion Principle (relates to the "sum rule")

- Suppose that $k \leq m$ of the ways of doing task 1 also simultaneously accomplishes task 2. (And thus are also ways of doing task 2.)
- Then the number of ways to accomplish "Do either task 1 or task 2" is $m+n-k$.
- **Set theory:** If A and B are not disjoint, then $|A \cup B| = |A| + |B| - |A \cap B|$.

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

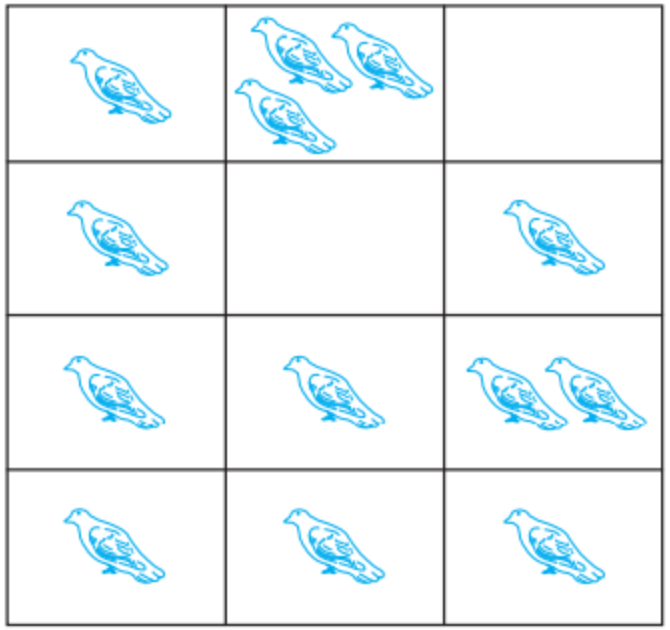


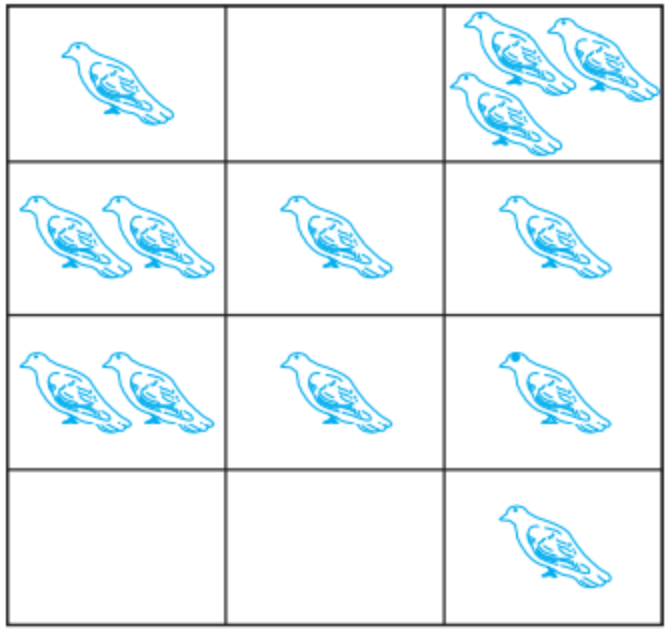
128 + 64 − 32 = 160.

- A computer company receives 350 applications from computer graduates for a job planning a line of new Web servers. Suppose that 220 of these applicants majored in computer science, 147 majored in business, and 51 majored both in computer science and in business. How many of these applicants majored neither in computer science nor in business?

Pigeonhole Principle/ Dirichlet drawer principle

- Suppose that a flock of 13 pigeons flies into a set of 12 pigeonholes to roost. Because there are 13 pigeons but only 12 pigeonholes, a least one of these 12 pigeonholes must have at least two pigeons in it.
- This illustrates a general principle called the pigeonhole principle, which states that if there are more pigeons than pigeonholes, then there must be at least one pigeonhole with at least two pigeons in it





Pigeonhole Principle

- Theorem:
  - If n pigeons are assigned to m pigeon-holes, and m <n, then at least one pigeonhole contains two or more pigoesn
- Proof:
  - Consider labelling, the m pigeonholes with the numbers 1 through m and the n pigeons with the numbers 1 through n. Now, beginning with pigeon 1, assign each pigeon in order to the pigeonhole with the same number. This assigns as many pigeons as possible to individual pigeonholes but because m<n, there are n-m pigeons that have not yet been assigned to pigeonhole. At least one pigeonhole will be assigned a second pigeon

- Suppose that none of k boxes contains more than one object. Then total number of objects would be at most k. This is contradiction, because there are at least k+1 objects

Examples

- If eight people are chosen in any way from some group, at least two of them will have been born on same day of the week.
- Solution: here each person (pigeon) is assigned to day of week (pigeonhole) on which he of she was born. Since there are eight people and only seven days of week, the pigeonhole principle tells us that at least two people must be assigned to same day of the week

- Show that if any five numbers from 1 to 8 are chosen, the two of them will add up to 9
- Solution:
  - Find set that add up to 9 [1,8], [2,7],[3,6],[4,5]
  - Only possibility that the numbers that do not add to 9 should be less than 5 numbers. When numbers reach to 5, any two of them will add to 9

- How many students must be in class to guarantee that at least two students receive same score on final exam, if exam is graded on a scale from 1 to 100 points?
- Solution
  - Grade 101
  - Students : at least 102

1. Show that if any 11 numbers are chosen from set {1,2,…,20} then one of them will be multiple of another
2. Show that for every integer n, there is multiple of n that has only 0s and 1s in its decimal expansion

Extended Pigeonhole principle

Theorem 2 (The Extended Pigeonhole Principle). *If n pigeons are assigned to m pigeonholes, then one of the pigeonholes must contain at least $\lfloor (n-1)/m \rfloor + 1$ pigeons.*

Proof (by contradiction): If each pigeonhole contains no more than $\lfloor (n-1)/m \rfloor$ pigeons, then there are at most $m \cdot \lfloor (n-1)/m \rfloor \leq m \cdot (n-1)/m = n - 1$ pigeons in all. This contradicts our assumptions, so one of the pigeonholes must contain at least $\lfloor (n-1)/m \rfloor + 1$ pigeons. ◆

Numerical examples

- Show that if any 30 people are selected, then we may choose a subset of 5 so that all 5 were born on same day of the week
- Solution:
  - Assign each person to day of the week on which she or he was born.
  - Then 30 pigeons are assigned to 7 pigeonholes. By extended pigeonhole principle with n=30 and m=7, at least $\lfloor(30-1)/7\rfloor+1$ or 5 people must have been born on same day of the week.

Permutations and Combinations

- permutation relates to the act of arranging all the members of a set into some sequence or order, r-permutation
- combination is a way of selecting items from a collection, such that (unlike permutations) the order of selection does not matter. R-combination
- **${}^{n}P_{r}$ = (n!) / (n-r)!**

$$ {}_nC_r = \binom{n}{r} = \frac{{}_nP_r}{r!} = \frac{n!}{r!(n-r)!} $$

Permutations and Combinations

Permutation	**Combination**
Arranging people, digits, numbers, alphabets, letters, and colours	Selection of menu, food, clothes, subjects, team.
Picking a team captain, pitcher and shortstop from a group.	Picking three team members from a group.
Picking two favourite colours, in order, from a colour brochure.	Picking two colours from a colour brochure.
Picking first, second and third place winners.	Picking three winners.

Example

- In how many ways can we select three students from a group of five students to stand in line for a picture? In how many ways can we arrange all five of these students in a line for a picture?
- How many different committees of three students can be formed from a group of four students?

Permutations and Combinations

- How many ways are there to pick a set of 3 people from a group of 6?
- There are 6 choices for the first person, 5 for the second one, and 4 for the third one, so there are $6 \cdot 5 \cdot 4 = 120$ ways to do this.
- This is not the correct result!
- For example, picking person C, then person A, and then person E leads to the **same group** as first picking E, then C, and then A.
- However, these cases are counted **separately** in the above equation.

Permutations and Combinations

- **Example:** Let S = {1, 2, 3}.
- The arrangement 3, 1, 2 is a permutation of S.
- The arrangement 3, 2 is a 2-permutation of S.

- The number of r-permutations of a set with n distinct elements is denoted by **P(n, r).**

- We can calculate P(n, r) with the product rule:
- $P(n, r) = n \cdot (n - 1) \cdot (n - 2) \cdot \ldots \cdot (n - r + 1)$.
- (n choices for the first element, (n – 1) for the second one, (n – 2) for the third one…)

Permutations and Combinations

- An **r-combination** of elements of a set is an unordered selection of r elements from the set.
- Thus, an r-combination is simply a subset of the set with r elements.

- **Example:** Let S = {1, 2, 3, 4}.
- Then {1, 3, 4} is a 3-combination from S.

- The number of r-combinations of a set with n distinct elements is denoted by C(n, r).

- **Example:** C(4, 2) = 6, since, for example, the 2-combinations of a set {1, 2, 3, 4} are {1, 2}, {1, 3}, {1, 4}, {2, 3}, {2, 4}, {3, 4}.

Permutations and Combinations

- **Example:**
- $P(8, 3) = 8 \cdot 7 \cdot 6 = 336$
- $= (8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1)/(5 \cdot 4 \cdot 3 \cdot 2 \cdot 1)$

- **General formula:**
- $P(n, r) = n!/(n - r)!$

- Knowing this, we can return to our initial question:
- How many ways are there to pick a set of 3 people from a group of 6 (disregarding the order of picking)?

Permutations and Combinations

- How can we calculate C(n, r)?
- Consider that we can obtain the r-permutation of a set in the following way:
- **First,** we form all the r-combinations of the set (there are C(n, r) such r-combinations).
- **Then,** we generate all possible orderings in each of these r-combinations (there are P(r, r) such orderings in each case).
- Therefore, we have:
- $P(n, r) = C(n, r) \cdot P(r, r)$