Programme Name and Semester: B. Tech CSE (AIML), 3rd semester
Course Name (Course Code): Discrete Mathematics (BBS00008)
Academic Session: 2025-26

Study Material

Discrete Mathematics (BBS00008)

Table of Contents

Module I:
Introduction to Number Theory and Relations

Introduction:

Set theory is a foundational branch of mathematical logic that studies sets, which are collections of distinct objects. Developed in the late 19th and early 20th centuries, set theory provides a formal language and framework for describing and analyzing mathematical and logical concepts.

Sets: A set is a well-defined collection of distinct objects, considered as an object in its own right. The objects within a set are called elements. Sets are typically denoted by curly braces, and elements are listed inside. For example, if A is the set of natural numbers less than 5, it can be written as A={1,2,3,4}.

Some predefined notations of sets:

N – Set of natural numbers

Z or **I** – Set of integers

Q – Set of complex numbers

R – Set of real numbers

{}- null set

Representation of Sets:

A set is described in the following two ways:

- Roster or Tabulation or Enumeration method
- Set Builder or Rule or Property method.

1. Roster Form:

In Roster form, all the elements of a set are listed.

For example, the set of natural numbers less than 5.

Natural Number = 1, 2, 3, 4, 5, 6, 7, 8,….

Natural Number less than 5 = 1, 2, 3, 4

Therefore, the set is N = { 1, 2, 3, 4 }

2. Set Builder Form:

The general form is, A = { x : property }

Example: Write the following sets in set builder form: A={2, 4, 6, 8}

Solution:

2 = 2 x 1

4 = 2 x 2

6 = 2 x 3

8 = 2 x 4

So, the set builder form is A = {x: x=2n, n ∈ N and 1 ≤ n ≤ 4}

Also, Venn Diagrams are the simple and best way for visualized representation of sets.

Types of sets:

- **Null set or Empty set:** It is denoted by ϕ or{ }

  a. ϕ is unique

  b. ϕ is subset of every set

  c. ϕ is never written within brackets i.e., { ϕ } is not the null set.

- **Singleton set:** The set { ϕ } is a singleton set.

- **Finite set:** A = (a, e, i, o, u} is a finite set.

- **Infinite set:**

  A = (1, 2, 3, 4 } is an infinite set.

- **Equivalent set:**

  Two finite sets A and B are equivalent if n(A) = n(B)

- **Equal sets:**

  Two sets A and B are equal iff A = B

- **Universal set:** Superset of all the sets. It is usually denoted by Q or S or U or X.

- **Power set:** The family of all the subsets of set S is called the power set of S.

  It is denoted by P(S) i.e., P(S) = {T: T ⊆ S}

- **Subsets:** If A is subset of B, then

  A ⊆ B ⇒ a ∈ A ⇒ a ∈ B

  a. Every set is a subset of itself i.e.,

  A ⊆ A

b. ϕ is a subset of every set.

c. If A ⊆ B and B ⊆ C ⇒ A ⊆ C

d. A = B iff a ⊆ B and B⊆ A

Proper Subsets:

If A is a proper subset of B, then A ⊂ B.

a. If A ⊆ B, we may have B ⊆ A

b. But if A ⊂ B, we cannot have B ⊂ A.

Question: Find the power set of Z = {2, 7, 9} and a total number of elements.

Solution: Given, Z = {2, 7, 9}

Total number of elements in power set = 2^n

Here, n = 3 (number of elements in set Z)

So, $2^3 = 8$, which shows that there are eight elements of power set of Z

Therefore,

P(Z) = {{}, {2}, {7}, {9}, {2, 7}, {7, 9}, {2, 9}, {2, 7, 9}}

Operations on Sets:

- **Union of sets:** Let **A** and **B** be two sets. Then, A ∪ B= {x : x ∈ A or x ∈ B}.

  ∴A ⊆ A ∪ B, B ∪ A and A ∪ B = B ∪ A

- **Intersection of sets:** Intersection of two sets A and B is denoted by,

  A ∩ B= {x : x ∈ A and x ∈ B)

∴ A ∩ B ⊆ A, A ∩ B ⊆ B and A ∩ B = B ∩ A

- **Disjoint sets:** Two sets A and B are s.t.b disjoint if A ∩ B = ϕ
- **Difference of sets:** Let A and B be two sets, then A – B = {x : x ∈ A and x ∈ B} and B – A = {x : x ∈ B and x ∈ A)

a. A – B ≠ B – A
b. The sets A – B, B – A and A ∩ B are disjoint sets.
c. A – B ⊆ A and B – A ⊆ B
d. A – ϕ = A and A – A = ϕ

It is denoted by A – B or A ~ B or A\B or C_AB (complement of B in A).

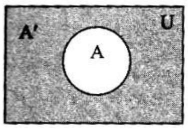
- **Symmetric difference of two sets:** is denoted by,

- $A \Delta B = (A - B) \cup (B - A) = (A \cup B) - (A \cap B)$

- **Complement of a set:**

  The complement of A with respect to U is denoted by A' or A^c or C(A) or U – A

  i.e., $A' = \{x \in U : x \notin A\}$



Note: If X is the universal set and A, B ⊆ X, then

i. $(A')' = A$

ii. $X' = \phi$

iii. $\phi' = X$

iv. $A \cap A' = \phi$

v. $A \cup A' = X$

vi. If $A \subseteq B$, then $B' \subseteq A'$

Distributive Properties of union and intersection:

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

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

Note: If A, B and C are any three sets, then

i. $A \cap (B - C) = (A \cap B) - (A \cap C)$

ii. $A \cap (B \Delta C) = (A \cap B) \Delta (A \cap C)$

iii. $P(A) \cap P(B) = P(A \cap B)$

iv. $P(A) \cup P(B) = P(A \cup B)$

If $P(A) = P(B) \Rightarrow A = B$ where, P(A) is the power set of A

De-Morgan's laws:

i. $(A \cup B)' = A' \cap B'$

ii. $(A \cap B)' = A' \cup B'$

iii. $A - (B \cap C) = (A - B) \cup (A - C)$

iv. $A - (B \cup C) = (A - B) \cap (A - C)$

Results on cardinal number of some sets:

If A, B and C are finite sets and U be the universal set, then

i. $n(A \cup B) = n(A) + n(B)$ if A and B are disjoint sets.

ii. $n(A \cup B) = n(A) + n(B) - n(A \cap B)$

iii. $n(A \cup B) = n(A - B) + n(B - A) + n(A \cap B)$

Cartesian Product of sets:

If set A and set B are two sets then the cartesian product of set A and set B is a set of all ordered pairs (a,b), such that a is an element of A and b is an element of B. It is denoted by A × B.

We can represent it in set-builder form, such as:

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

Example: set A = {1,2,3} and set B = {Bat, Ball}, then;

A × B = {(1,Bat),(1,Ball),(2,Bat),(2,Ball),(3,Bat),(3,Ball)}

Note: If A, B and C are three sets then,

i. $A \times (B\cup C) = (A \times B) \cup (A \times C)$

ii. $A \times (B \cap C) = (A \times B) \cap (A \times C)$

iii. $A \times (B - C) = (A \times B) - (A \times C)$

iv. If $A \subseteq B$, then $(A \times C) \subseteq (B\times C)$

v. If $A \subseteq B$, then $(A \times B) \cap (B\times A) = A^2$

vi. If $A \subseteq B$ and $C \subseteq D$ then $A \times C \subseteq B\times D$

vii. $(A \times B) \cap (S \times T) = (A \cap S) \times (B \cap T)$,

Relation:

If R is a relation from A to B then $R \subseteq A \times B$ ie, $R \subseteq \{(a,b): a \in A, b \in B\}$

Domain and Range of a Relation:

i. Domain of R = $(a: (a, b) \in R\}$

ii. Range of R = $\{b: (a, b) \in R\}$ If R is a relation from A to B,
then Dom (R) $\subseteq$ A and Range (R) $\subseteq$ B

(i.e., Co-domain)

Notes: Number of possible relations from A to B is = 2^{mn} [if o(A) = m and o(B) = n]

Inverse Relation:

The inverse of R, denoted by R^{-1} is a relation from B to A and is defined by,

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

Thus,

i. $(a, b) \in R \Leftrightarrow (b, a) \in R^{-1}\ \forall\, a \in A, b \in B$

ii. Dom (R^{-1}) = Range (R)

iii. Range (R^{-1}) = Dom (R)

iv. $(R^{-1})^{-1} = R$

Equivalence Relation:

A relation R on a set 'A' is said to be equivalence relation on a iff

1. It is reflexive i.e.,$(a, a) \in R\ \forall\, a \in A$

2. It is symmetric i.e., $(a, b) \in R \Rightarrow (b, a) \in R\ \forall\, a, b \in A$

3. It is transitive i.e., $(a, b) \in R$ and $(b, c) \in R \Rightarrow (a, c)$ e R $\forall$ a, b, c, $\in$ A.

Antisymmetric: A relation R on a set 'A' is said to antisymmetric i.e.,$(a, b) \in R$ and $(b, a) \in R$, then a = b.

Question: Let R be the relation on the set R of all real numbers defined by a R b if and only if $|a - b| \le 1$. Then check if R is reflexive, symmetric, anti-symmetric, or transitive.

Solution:

$|a - a| = 0 < 1$

Therefore, $a \, R \, a \; \forall \, a \in R$

Therefore, R is reflexive.

Again a R b, $|a - b| \leq 1 \Rightarrow |b - a| \leq 1 \Rightarrow b \, R \, a$

Therefore, R is symmetric.

Again 1 R [½] and [½] R1 but [½] ≠ 1

Therefore, R is not anti-symmetric.

Further, 1 R 2 and 2 R 3, but 1 R 3 is not possible, [Because, $|1 - 3| = 2 > 1$]

Hence, R is not transitive.

<u>Composition of two Relations</u>: If A, B and C are three sets such that $R \subseteq A \times B$ and $S \subseteq B \times C$, then $SoR \subseteq A \times C$ and $(SoR)^{-1} = R^{-1}oS^{-1}$. It is clear that aRb, bSc ⇒ a(SoR)c .

Partial Order Relations:

A relation R on a set A is called a partial order relation if it satisfies the following three properties:

1. Relation R is Reflexive, i.e. aRa ∀ a∈A.
2. Relation R is Antisymmetric, i.e., aRb and bRa ⟹ a = b.
3. Relation R is transitive, i.e., aRb and bRc ⟹ aRc.

<u>Question:</u> Show whether the relation (x, y) ∈ R, if, $x \geq y$ defined on the set of positive integers is a partial order relation.

<u>Solution:</u> Consider the set A = {1, 2, 3, 4} containing four positive integers. Find the relation for this set such as R = {(2, 1), (3, 1), (3, 2), (4, 1), (4, 2), (4, 3), (1, 1), (2, 2), (3, 3), (4, 4)}.

<u>Reflexive:</u> The relation is reflexive as for every a ∈ A. (a, a) ∈ R, i.e. (1, 1), (2, 2), (3, 3), (4, 4) ∈ R.

<u>Antisymmetric:</u> The relation is antisymmetric as whenever (a, b) and (b, a) ∈ R, we have a = b.

<u>Transitive:</u> The relation is transitive as whenever (a, b) and (b, c) ∈ R, we have (a, c) ∈ R.

Partial Order Set (POSET):

The set A together with a partial order relation R on the set A and is denoted by (A, R) is called a partial orders set or POSET.

Division Algorithm: Given integers a and d, with d > 0, there exists unique integers q and r, with $0 \leq r < d$, such that $a = qd + r$.

(Notation: We call a the dividend, d the divisor, q the quotient, and r the remainder.)

Proof. Suppose a and d are integers, and d > 0. We will use the well-ordering principle to obtain the quotient q and remainder r. Since we can take q = a if d = 1, we shall assume that d > 1. Let S be the set of all natural numbers of the form a−kd, where k is an integer. In symbols

S = {a – kd | k ∈ Z and a − kd ≥ 0}. If we can show that S is nonempty, then the well-ordering principle will give us a least element of S, and this will be the remainder r we are looking for. There are two cases.

Case 1: a ≥ 0. In this case, we can set k = 0 and get the element a − 0 · d = a ≥ 0 of S.

Case 2: a < 0. In this case, we can set k = a. Then a − kd = a − ad = a(1 − d). Since a < 0 and d > 1, a(1 − d) > 0; hence is an element of S. Thus, S 6= ∅, and so S has a least element r = a − qd for some integer q. Thus, a = qd + r and r ≥ 0. We are left to show (i) r < d and (ii) q and r are unique.

(i)Suppose r ≥ d. Then r = d + r 0 , where 0 ≤ r 0 < r. Then a = qd + r = qd + d + r 0 = (q + 1)d + r 0 , so that r 0 = a − (q + 1)d is an element of S smaller than r. This contradicts the fact that r is the least element of S. Thus, r < d.

(ii) Suppose integers q 0 and r 0 satisfy a = q 0d + r 0 and 0 ≤ r 0 < d. Without loss of generality, we may assume r 0 ≥ r, so that 0 ≤ r − r 0 < d. Since a = q 0d + r 0 = qd + r, r − r 0 = d(q 0 − q). This means that d divides r − r 0 , which implies either r − r 0 ≥ d or r − r 0 = 0. But but we know 0 ≤ r − r 0 < d. Thus, r 0 = r, which, in turn, implies q 0 = q. That is, q and r are unique.

Prime Number: If p is an integer greater than 1, then p is a prime number if the only divisors of p are 1 and p.

Composite Number: A positive integer greater than 1 that is not a prime number is called composite.

Fundamental Theorem of Arithmetic: Every positive integer greater than one can be written uniquely as a product of primes, where the prime factors are written in non-decreasing order

Greatest Common Divisor and Least Common Multiple:

Given integers a and b

(1) The greatest common divisor of a and b, denoted GCD (a, b), is the largest positive integer d such that d|a and d|b.

(2) The least common multiple of a and b, denoted LCM (a, b), is the smallest positive integer m such that a|m and b|m.

(3) a and b are called relatively prime if GCD (a, b) = 1.

(4) The integers a_1, a_2, a_3, . . . , an are called pairwise relatively prime if GCD(a_i , a_j) = 1 for 1 ≤ i < j ≤ n.

The Euclidean Algorithm:

Now we examine an alternative method to compute the gcd of two given positive integers a, b. The method provides at the same time a solution to the Diophantine equation: ax + by = gcd(a, b). It is based on the following fact: given two integers a ≥ 0 and b > 0, and r = a mod b, then gcd(a, b) = gcd(b, r).

Proof: Divide a by b obtaining a quotient q and a reminder r, then $a = bq + r$, $0 \leq r < b$. If d is a common divisor of a and b then it must be a divisor of $r = a-bq$. Conversely, if d is a common divisor of b and r then it must divide $a = bq + r$. So the set of common divisors of a and b and the set of common divisors of b and r are equal, and the greatest common divisor will be the same. The Euclidean algorithm is a follows. First we divide a by b, obtaining a quotient q and a reminder r. Then we divide b by r, obtaining a new quotient q0 and a reminder r0 . Next we divide r by r0 , which gives a quotient q00 and another remainder r00. We continue dividing each reminder by the next one until obtaining a zero reminder, and which point we stop. The last non-zero reminder is the gcd.

Example: Assume that we wish to compute gcd(500, 222). Then we arrange the computations in the following way:

$500 = 2 \cdot 222 + 56 \rightarrow r = 56$

$222 = 3 \cdot 56 + 54 \rightarrow r' = 54$

$56 = 1 \cdot 54 + 2 \rightarrow r'' = 2$

$54 = 27 \cdot 2 + 0 \rightarrow r''' = 0$

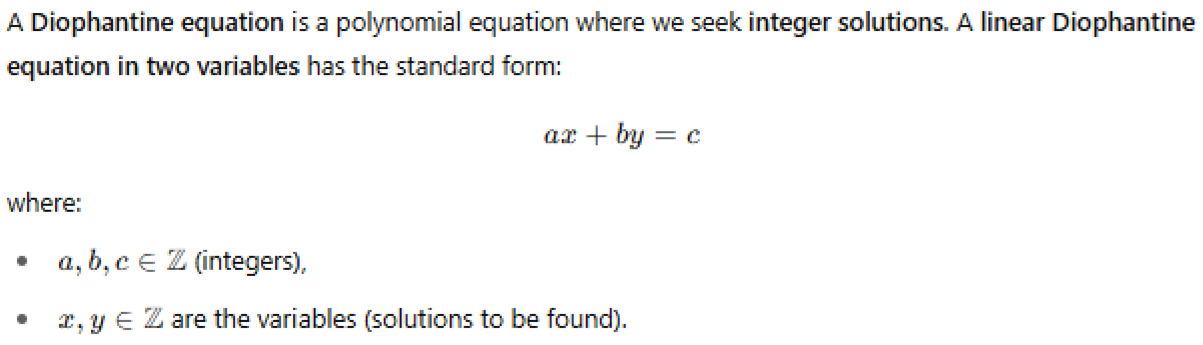
The last nonzero remainder is $r'' = 2$, hence gcd(500, 222) = 2.

Furthermore, if we want to express 2 as a linear combination of 500 and 222, we can do it by working backward:

$2 = 56 - 1 \cdot 54 = 56 - 1 \cdot (222 - 3 \cdot 56) = 4 \cdot 56 - 1 \cdot 222 = 4 \cdot (500 - 2 \cdot 222) - 1 \cdot 222 = 4 \cdot 500 - 9 \cdot 222$

Linear Diophantine Equation in Two Variables:

Introduction:



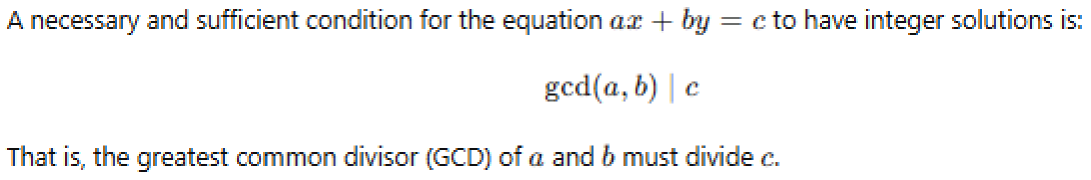
A **Diophantine equation** is a polynomial equation where we seek **integer solutions.** A **linear Diophantine equation in two variables** has the standard form:

$$ax + by = c$$

where:

- $a, b, c \in \mathbb{Z}$ (integers),
- $x, y \in \mathbb{Z}$ are the variables (solutions to be found).

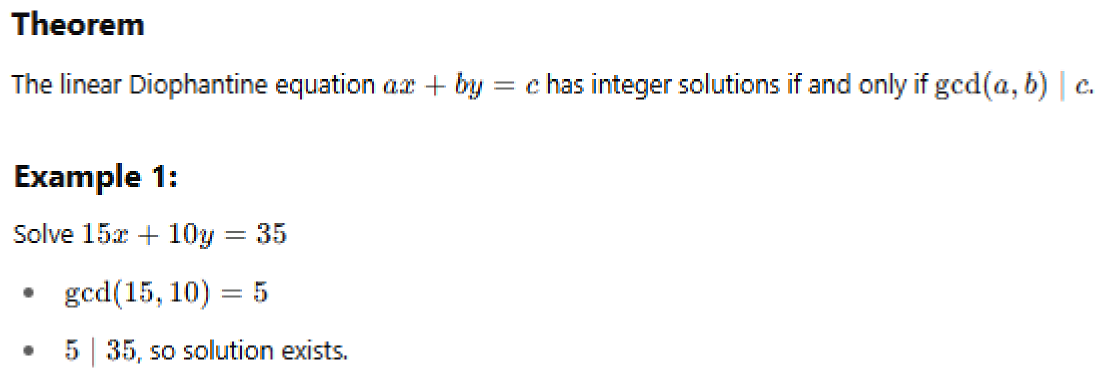
Existence of Solutions:



A necessary and sufficient condition for the equation $ax + by = c$ to have integer solutions is:

$$\gcd(a, b) \mid c$$

That is, the greatest common divisor (GCD) of a and b must divide c.



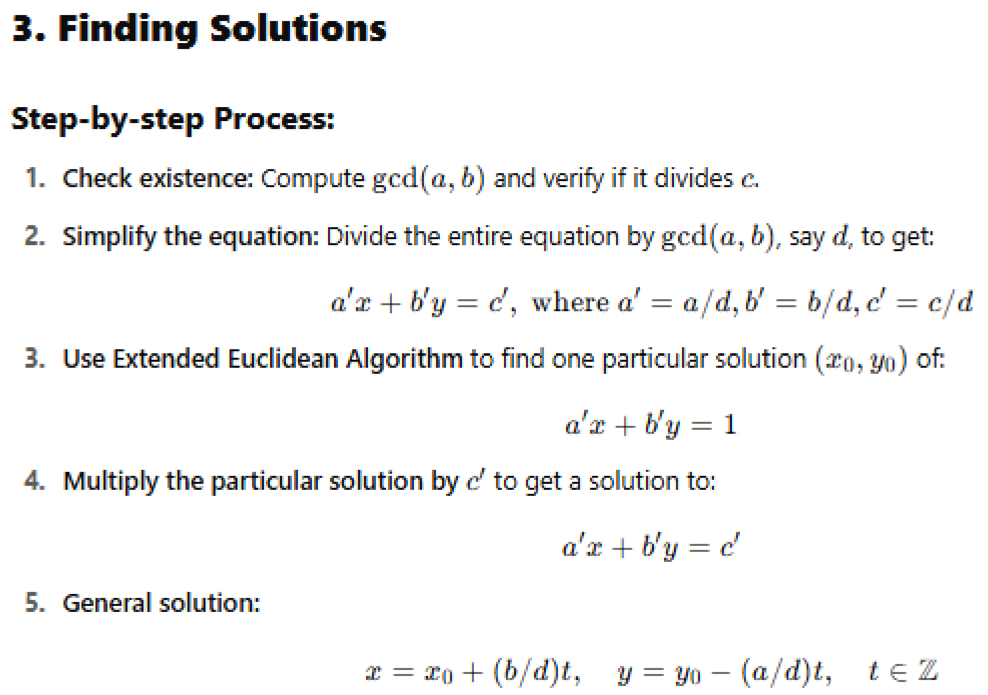
Theorem

The linear Diophantine equation $ax + by = c$ has integer solutions if and only if $\gcd(a, b) \mid c$.

Example 1:

Solve $15x + 10y = 35$

- $\gcd(15, 10) = 5$
- $5 \mid 35$, so solution exists.



3. Finding Solutions

Step-by-step Process:

1. **Check existence:** Compute $\gcd(a, b)$ and verify if it divides c.
2. **Simplify the equation:** Divide the entire equation by $\gcd(a, b)$, say d, to get:

$$a'x + b'y = c', \text{ where } a' = a/d, b' = b/d, c' = c/d$$

3. **Use Extended Euclidean Algorithm** to find one particular solution (x_0, y_0) of:

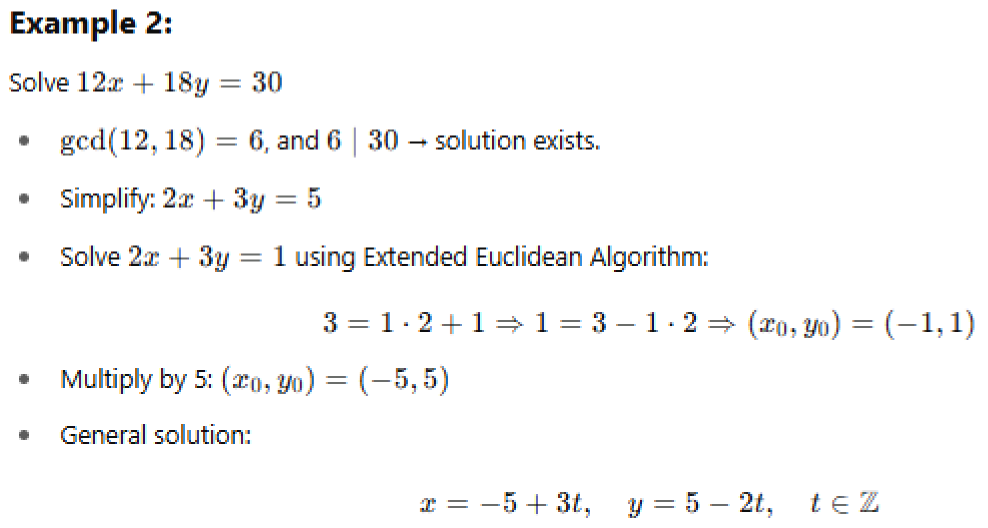
$$a'x + b'y = 1$$

4. **Multiply the particular solution by** c' to get a solution to:

$$a'x + b'y = c'$$

5. **General solution:**

$$x = x_0 + (b/d)t, \quad y = y_0 - (a/d)t, \quad t \in \mathbb{Z}$$



Example 2:

Solve $12x + 18y = 30$

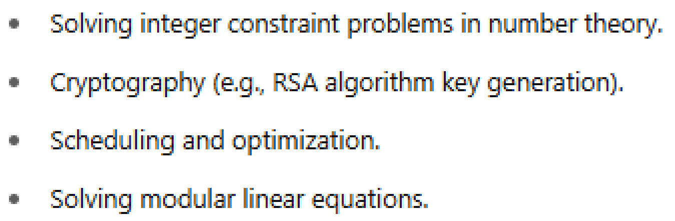
- $\gcd(12, 18) = 6$, and $6 \mid 30$ → solution exists.
- Simplify: $2x + 3y = 5$
- Solve $2x + 3y = 1$ using Extended Euclidean Algorithm:

$$3 = 1 \cdot 2 + 1 \Rightarrow 1 = 3 - 1 \cdot 2 \Rightarrow (x_0, y_0) = (-1, 1)$$

- Multiply by 5: $(x_0, y_0) = (-5, 5)$
- General solution:

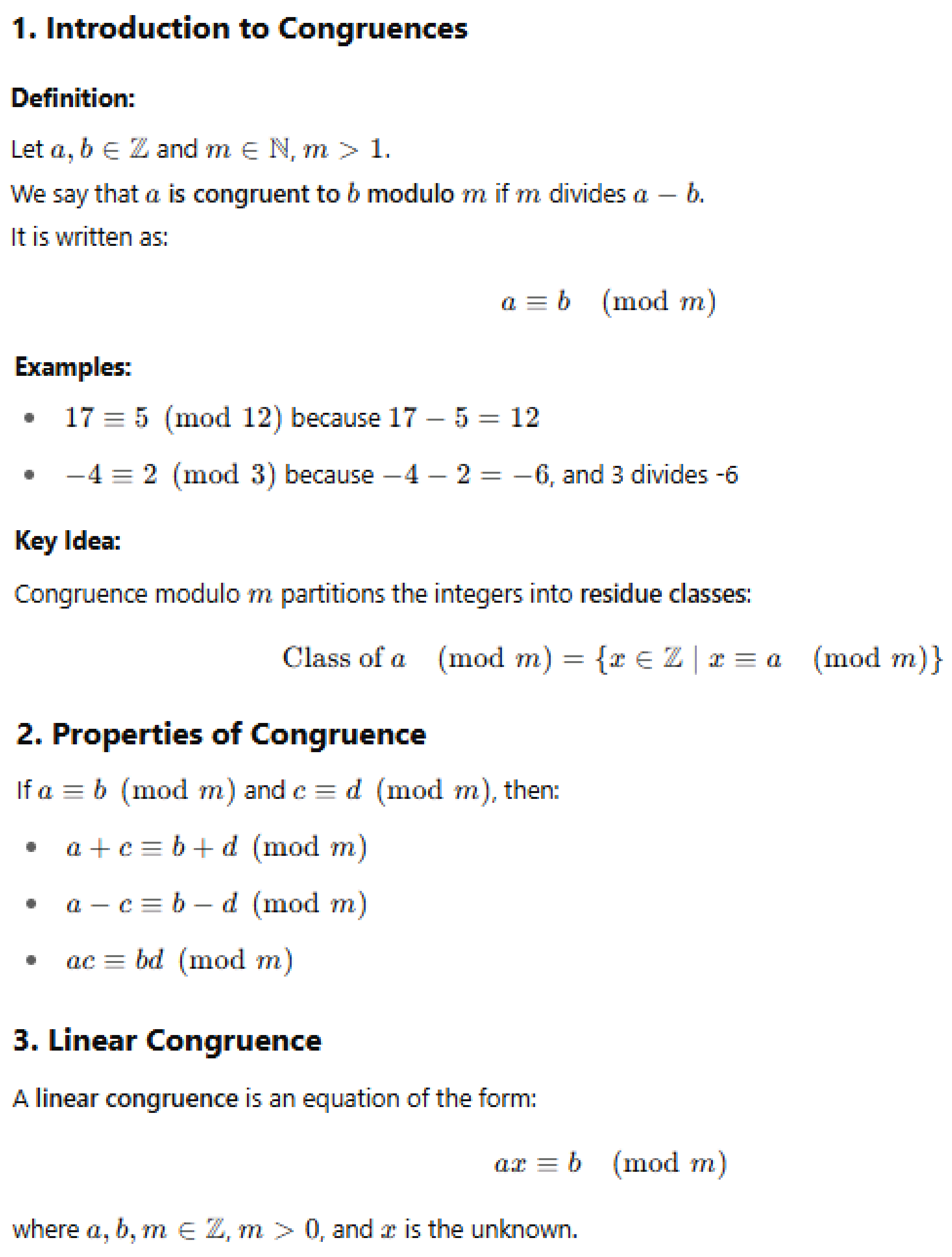
$$x = -5 + 3t, \quad y = 5 - 2t, \quad t \in \mathbb{Z}$$

Applications:



- Solving integer constraint problems in number theory.
- Cryptography (e.g., RSA algorithm key generation).
- Scheduling and optimization.
- Solving modular linear equations.

Introduction to Congruences and Solving Linear Congruences:



1. Introduction to Congruences

Definition:

Let $a, b \in \mathbb{Z}$ and $m \in \mathbb{N}$, $m > 1$.
We say that a **is congruent to** b **modulo** m if m divides $a - b$.
It is written as:

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

Examples:

- $17 \equiv 5 \pmod{12}$ because $17 - 5 = 12$
- $-4 \equiv 2 \pmod{3}$ because $-4 - 2 = -6$, and 3 divides -6

Key Idea:

Congruence modulo m partitions the integers into **residue classes**:

$$\text{Class of } a \pmod{m} = \{x \in \mathbb{Z} \mid x \equiv a \pmod{m}\}$$

2. Properties of Congruence

If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then:

- $a + c \equiv b + d \pmod{m}$
- $a - c \equiv b - d \pmod{m}$
- $ac \equiv bd \pmod{m}$

3. Linear Congruence

A **linear congruence** is an equation of the form:

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

where $a, b, m \in \mathbb{Z}$, $m > 0$, and x is the unknown.

4. Existence of Solutions

The linear congruence $ax \equiv b \pmod{m}$ has a solution if and only if:

$$\gcd(a, m) \mid b$$

5. Number of Solutions

- If $d = \gcd(a, m)$, and $d \mid b$, then the congruence has exactly d incongruent solutions modulo m.
- If $d \nmid b$, then there is **no solution**.

6. Solving Linear Congruences

Step-by-Step Method:

Step 1: Compute $d = \gcd(a, m)$.
If $d \nmid b$, no solution exists.

Step 2: Reduce the congruence:

$$\text{If } d \mid a, b, m \text{ then write: } a' = \frac{a}{d},\ b' = \frac{b}{d},\ m' = \frac{m}{d}$$

Now solve:

$$a'x \equiv b' \pmod{m'}$$

Step 3: Find the **modular inverse** of $a' \mod m'$, say a'^{-1}, such that:

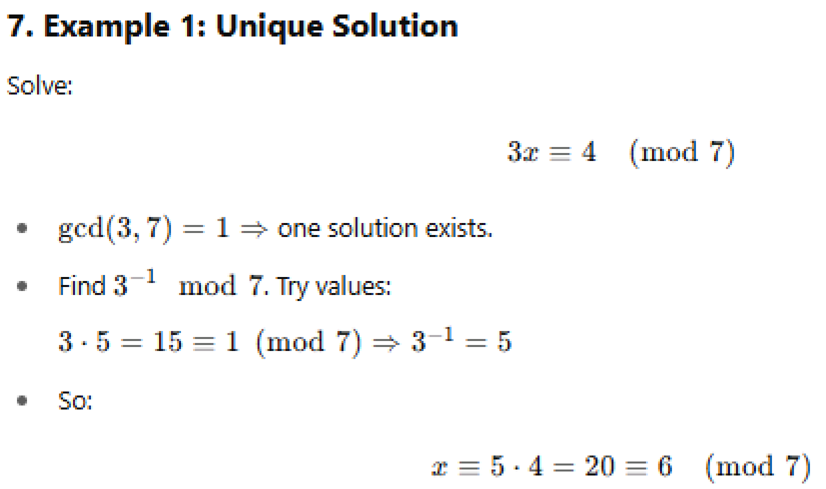
$$a'a'^{-1} \equiv 1 \pmod{m'}$$

Step 4: Multiply both sides by the inverse:

$$x \equiv a'^{-1}b' \pmod{m'}$$

Step 5: The general solution modulo m is:

$$x \equiv x_0 + k \cdot m' \pmod{m} \quad \text{for } k = 0, 1, \ldots, d - 1$$



7. Example 1: Unique Solution

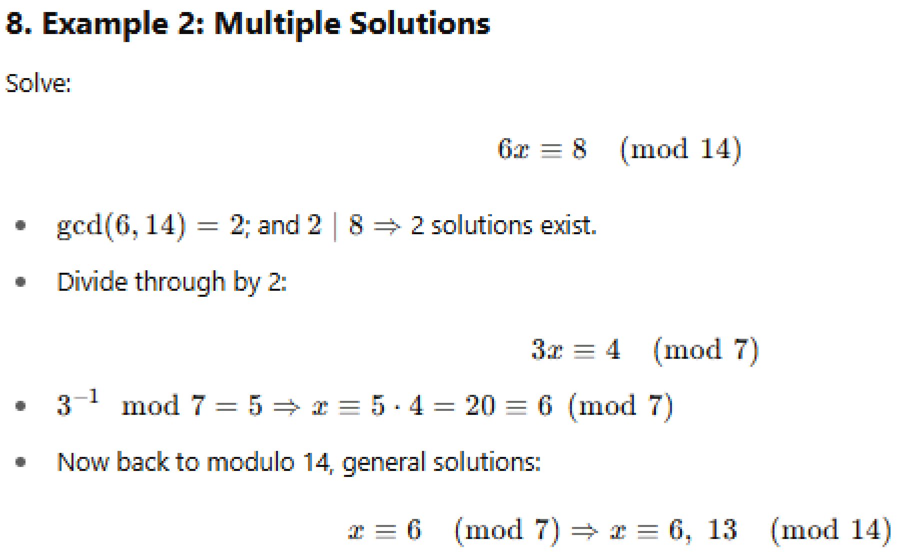
Solve:

$$3x \equiv 4 \pmod 7$$

- $\gcd(3,7) = 1 \Rightarrow$ one solution exists.
- Find $3^{-1} \mod 7$. Try values:

  $3 \cdot 5 = 15 \equiv 1 \pmod 7 \Rightarrow 3^{-1} = 5$
- So:

$$x \equiv 5 \cdot 4 = 20 \equiv 6 \pmod 7$$



8. Example 2: Multiple Solutions

Solve:

$$6x \equiv 8 \pmod{14}$$

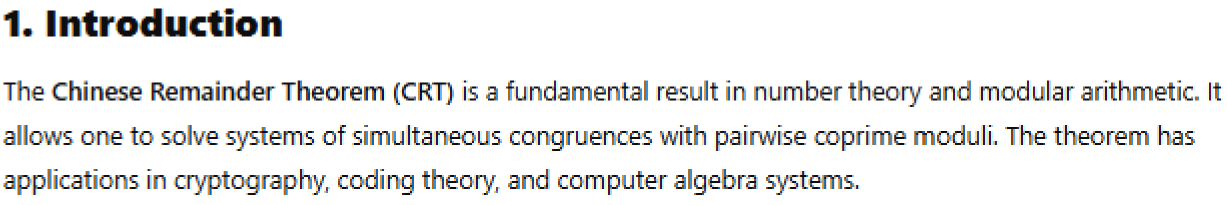
- $\gcd(6,14) = 2$; and $2 \mid 8 \Rightarrow$ 2 solutions exist.
- Divide through by 2:

$$3x \equiv 4 \pmod 7$$

- $3^{-1} \mod 7 = 5 \Rightarrow x \equiv 5 \cdot 4 = 20 \equiv 6 \pmod 7$
- Now back to modulo 14, general solutions:

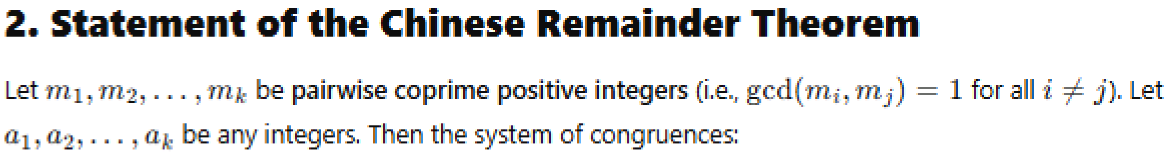
$$x \equiv 6 \pmod 7 \Rightarrow x \equiv 6,\ 13 \pmod{14}$$

The Chinese Remainder Theorem



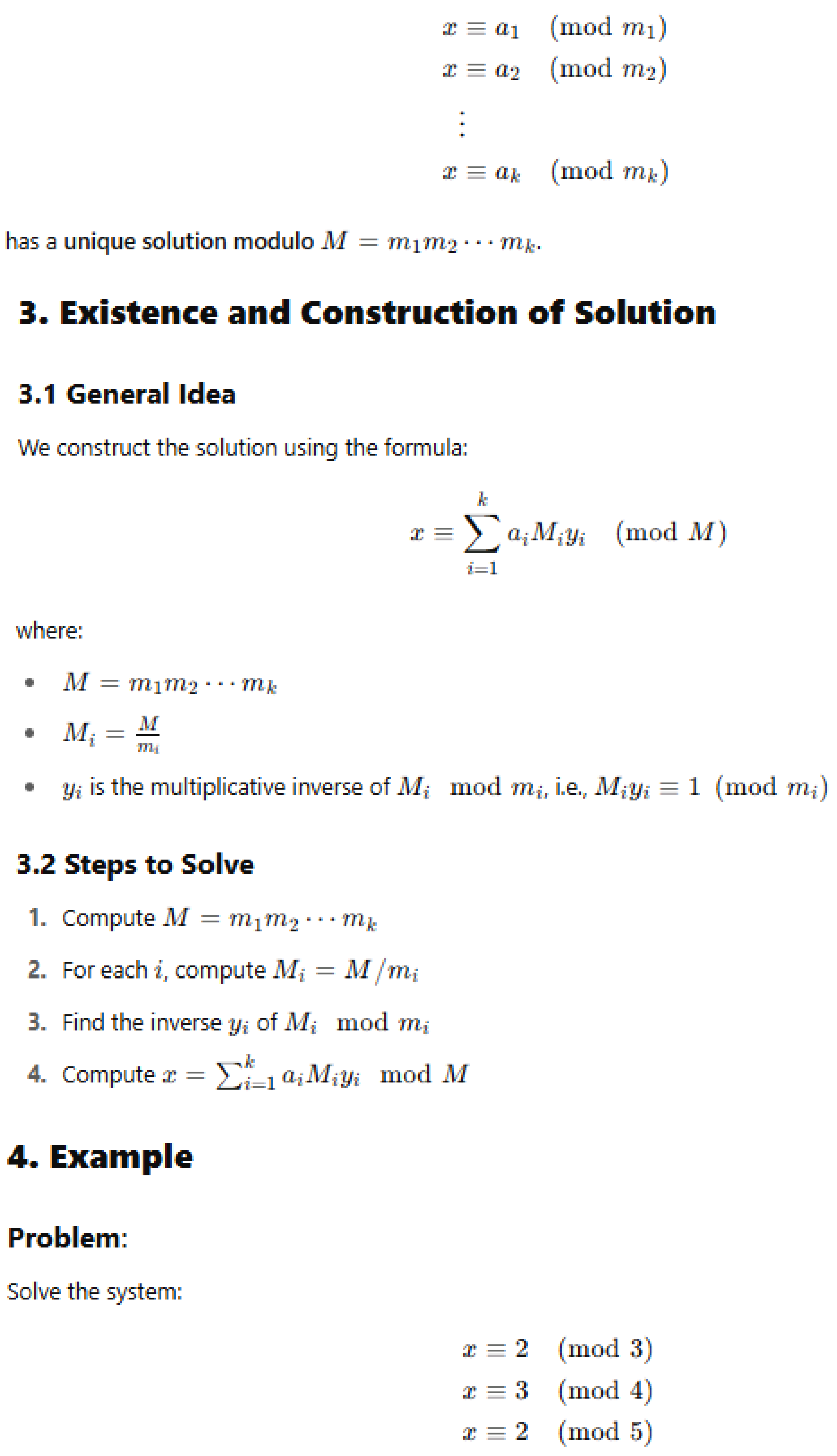
1. Introduction

The **Chinese Remainder Theorem (CRT)** is a fundamental result in number theory and modular arithmetic. It allows one to solve systems of simultaneous congruences with pairwise coprime moduli. The theorem has applications in cryptography, coding theory, and computer algebra systems.



2. Statement of the Chinese Remainder Theorem

Let $m_1, m_2, \ldots, m_k$ be **pairwise coprime positive integers** (i.e., $\gcd(m_i, m_j) = 1$ for all $i \neq j$). Let $a_1, a_2, \ldots, a_k$ be any integers. Then the system of congruences:



$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_k \pmod{m_k} \end{aligned}$$

has a **unique solution modulo** $M = m_1 m_2 \cdots m_k$.

3. Existence and Construction of Solution

3.1 General Idea

We construct the solution using the formula:

$$x \equiv \sum_{i=1}^{k} a_i M_i y_i \pmod{M}$$

where:

- $M = m_1 m_2 \cdots m_k$
- $M_i = \frac{M}{m_i}$
- y_i is the multiplicative inverse of $M_i \mod m_i$, i.e., $M_i y_i \equiv 1 \pmod{m_i}$

3.2 Steps to Solve

1. Compute $M = m_1 m_2 \cdots m_k$
2. For each i, compute $M_i = M / m_i$
3. Find the inverse y_i of $M_i \mod m_i$
4. Compute $x = \sum_{i=1}^{k} a_i M_i y_i \mod M$

4. Example

Problem:

Solve the system:

$$\begin{aligned} x &\equiv 2 \pmod{3} \\ x &\equiv 3 \pmod{4} \\ x &\equiv 2 \pmod{5} \end{aligned}$$

Solution:

- $m_1 = 3, m_2 = 4, m_3 = 5$, all pairwise coprime.
- $M = 3 \cdot 4 \cdot 5 = 60$
- $M_1 = 60/3 = 20, \quad M_2 = 60/4 = 15, \quad M_3 = 60/5 = 12$
- Find inverses:
  - y_1: $20y_1 \equiv 1 \pmod 3 \Rightarrow y_1 = 2$
  - y_2: $15y_2 \equiv 1 \pmod 4 \Rightarrow y_2 = 3$
  - y_3: $12y_3 \equiv 1 \pmod 5 \Rightarrow y_3 = 3$

Now:

$$x = 2 \cdot 20 \cdot 2 + 3 \cdot 15 \cdot 3 + 2 \cdot 12 \cdot 3 = 80 + 135 + 72 = 287$$

$$x \equiv 287 \mod 60 \Rightarrow x \equiv \boxed{47} \pmod{60}$$

5. Properties and Implications

- The solution is **unique modulo** M.
- The CRT can be extended to **non-coprime moduli**, but uniqueness and solvability require additional conditions.
- The theorem allows computation in **modular systems independently**, which is highly useful in **parallel computing** and **RSA encryption**.

Practice Problem:

1. Solve:

$$x \equiv 1 \pmod 5, \quad x \equiv 2 \pmod 7, \quad x \equiv 3 \pmod 9$$

2. Show that if $x \equiv a \mod m$ and $x \equiv a \mod n$, and $\gcd(m, n) = d$, then $x \equiv a \mod \operatorname{lcm}(m, n)$.

Questions for Practice.

A. MCQ Answer Type Questions:

1.	Select the correct option from the following that is **not** true for a partial order relation.	
	a. It must be antisymmetric	b. It must be symmetric
	c. It must be transitive	d. It must be reflexive

2.	Illustrate the Cartesian product of A = {1, 2} and B = {a, b}.	
	a. {(1, 1), (2, 2), (a, a), (b, b)}	b. {(1, a), (2, a), (1, b), (2, b)}
	c. {(1, a), (1, b), (2, a), (b, b)}	d. {(1, 1), (a, a), (2, a), (1, b)}
3.	Consider the set $\boldsymbol{A} = \{\mathbf{1}, \mathbf{2}, \mathbf{3}\}$ and the relation $\boldsymbol{R} = \{(\mathbf{1}, \mathbf{1}), (\mathbf{2}, \mathbf{2}), (\mathbf{3}, \mathbf{3}), (\mathbf{1}, \mathbf{2}), (\mathbf{2}, \mathbf{3}), (\mathbf{1}, \mathbf{3})\}$. Select the correct option.	
	a. it is not reflexive	b. it is not transitive
	c. it is a partial order	d. it is not antisymmetric
4.	Select the correct option. Let R be a symmetric and transitive relation on a set A. Then	
	a. R is reflexive and hence a partial order	b. R is reflexive and hence a equivalence relation
	c. R is not reflexive and hence a equivalence relation	d. None of these
5.	Let $A = \{1,2,3\}$ **and the relation** $R = \{(1,1), (2,2), (3,3), (1,2), (2,1), (2,3)\}$**. Then select the correct one.**	
	a. it is equivalence relation	b. it is symmetric
	c. it is not transitive	d. it is not reflexive
6.	Select the correct option from the following that defines a valid equivalence relation on the set of integers $\mathbb{Z}$.	
	a. $aRb \Leftrightarrow a + b$ is even	b. $aRb \Leftrightarrow a.b > 0$
	c. $aRb \Leftrightarrow a \equiv b \ (mod\ 3)$	d. $aRb \Leftrightarrow a < b$
7.	Select the correct option. The relation {(1,2), (1,3), (3,1), (1,1), (3,3), (3,2)} is	
	a. Reflexive	b. Symmetric
	c. Transitive	d. Asymmetric
8.	Select the correct option. The total number of reflexive relations on a set with n elements is…	
	a. $2^{n\,(n+1)\,/\,2}$	b. $2^{n(n\,-\,1)}$
	c. 2^n	d. 2^{n+2}
9.	Memorize the total number of symmetric relations possible on a set with n elements and it is	

	a. $2^{n\,(n+1)\,/\,2}$	b. $2^{n(n\,-\,1)}$
	c. 2^n	d. 2^{n+2}
10.	Select the correct option. Division Algorithm states	
	a. $a = qb + r$, where $0 \le r < b$	b. $a = qb + r$, where $0 < r < b$
	c. $a = qb + r$, where $r > b$	d. $a = qb + r$, where $r < 0$
11.	Select the correct option. If $S = \{\emptyset\}$ then power set of S is	
	a. $\{\emptyset\}$	b. $\emptyset$
	c. $\{\emptyset, \{\emptyset\}\}$	d. None of these
12.	Select the correct option. The Division Algorithm is applicable to the numbers	
	a. Only positive integers	b. All integers
	c. rational numbers	d. None of these
13.	Observe and find out the singleton set from the following.	
	a. $A = \{ x : 3x^2 - 27 = 0 , x \in Q \}$	b. $B = \{ x : x^2 - 1 = 0 , x \in R \}$
	c. $C = \{ x : 30x - 59 = 0 , x \in N \}$	d. $D = \{ x : x^2 - 1 = 0 , x \in N \}$
14.	If $a = -17$ and $b = 5$, then identify the quotient and remainder according to the Division Algorithm.	
	a. $q = -4, r = 3$	b. $q = -3, r = 2$
	c. $q = -5, r = 8$	d. $q = 3, r = 2$
15.	If A and B are sets and A∪ B= A ∩ B, then select the correct option.	
	a. A = Φ	b. B = Φ
	c. A = B	d. none of these
16.	Predict the number of elements in the power set of the set {a, b}.	
	a. 2	b. 4
	c. 6	d. 8
17.	Select the correct option. Let N be the set of natural numbers and R be the relation in N defined as R = {(a, b) : a = b – 2, b > 6}.	
	a. (2, 4) ∈ R	b. (8, 7) ∈ R
	c. (3, 8) ∈ R	d. (6, 8) ∈ R
18.	A survey shows that 70% of the Indian like mango whereas 82% like apple. Interpret the range of x if x% of Indian like both mango and apples.	

	a. $x=52$	b. $52\leq x\leq 70$
	c. $x=70$	d. $70\leq x\leq 82$
19.	Select the correct option. If $X\cup\{3,4\}=\{1,2,3,4,5,6\}$, then	
	a. Smallest set X = {1,2,5,6}	b. Smallest set X= {1,2,3,5,6}
	c. Smallest set X= {1,2,3,4}	d. Greatest set X= {1,2,3,4}
20.	If two sets A and B are having 43 elements in common, then select the number of elements in the set A∩ B	
	a. 43	b. 43^{2}
	c. 43^{43}	d. 2^{86}
21.	In a certain town 30% families own a scooter and 40% on a car 50% own neither a scooter nor a car 2000 families own both a scooter and car consider the following statements in this regard (1) 20% families own both scooter and car (2) 35% families own either a car or a scooter (3) 10000 families live in town Identify the correct statements from the above.	
	a. 2 and 3	b. 1 and 2
	c. 1 and 3	d. 1, 2 and 3
22.	If set A is an empty set then illustrate the value of $n\left[P\left[P\left[P(A)\right]\right]\right]=$	
	a. 6	b. 16
	c. 2	d. 4
23.	If $a\equiv 2\ (mod\ 5)$ and $b\equiv 3\ (mod\ 5)$, then identify the value of $(a+b)$ mod 5.	
	a. 0	b. 1
	c. 2	d. 3
24.	Identify the value of x for $25\equiv x\ (mod\ 7)$.	
	a. 4	b. 5
	c. 3	d. 111
25.	Let $A=\left\{(x,y):y=e^{x},x\in R\right\}$, $B=\left\{(x,y):y=e^{-x},x\in R\right\}$ then predict the correct option.	

	a. $A\cap B=\varphi$	b. $A\cap B\neq\varphi$
	c. $A\cup B=R$	d. $A\cup B=A$
26.	Let R be a reflexive relation of a finite set A having n elements and let there be m ordered pairs in R. Then observe the correct option.	
	a. $m\geq n$	b. $m\leq n$
	c. $m=n$	d. None of these
27.	Let R be a relation on N defined by $R=\left\{\left(1+x,1+x^2\right): x\leq 5, x\in N\right\}$. Select the correct option.	
	a. $R=\{(2,2),(3,5),(4,10),(5,17),(6,25)\}$	b. Domain of R = {2,3,4,5,6}
	c. Range of R = {2,5,10,17,26}	d. (b) and (c) are true
28.	Let R be the real line consider the following subsets of the plane $R\times R$, $S=\left\{(x,y): y=x+1 \text{ and } 0<x<2\right\}$, $T=\left\{(x,y): x-y \text{ is an integer}\right\}$. Then select the correct option from the following.	
	a. T is an equivalence relation on R but S is not.	b. Neither S nor T is an equivalence relation on R
	c. Both S and T are equivalence relations on R	d. S is an equivalence relation on R but T is not
29.	If A is the set of even natural numbers less than 8 and B is the set of prime numbers less than 7, then identify the number of relations from A to B.	
	a. 2^9	b. 9^2
	c. 3^2	d. 2^9-1
30.	For $m,n\in N$, $n\mid m$ means that *n* is a factor of *m*, then classify the relation | from the following.	
	a. Reflexive and symmetric	b. Transitive and symmetric
	c. Reflexive, transitive and symmetric	d. Reflexive, transitive and not symmetric
31.	Select the correct option. The relation ρ is defined on the set $A=\{1,2,3,4,5\}$ by $\rho=\left\{(x,y)\mid\left\|x^2-y^2\right\|<16\right\}$ is given by	
	a. {(1,1), (2,1), (3,1), (4,1), (2,3)}	b. {(2,2), (3,2), (4,2), (2,4)}

	c. $\{(3,3), (4,3), (5,4), (3,4)\}$	d. None of these
32.	If $\gcd(a,b) = d$, then select the correct option.	
	a. d divides both a and b	b. d is the largest number that divides both a and b
	c. $\gcd(b,a) = d$	d. All of the above
33.	Identify the GCD of 270 and 192 using the Euclidean Algorithm.	
	a. 12	b. 6
	c. 18	d. 24
34.	Given the relation $R=\{(a,b),(b,c)\}$ in the set $A=\{a,b,c\}$ then identify the minimum number of ordered pairs that need to be added to R make it an equivalence relation.	
	a. 5	b. 6
	c. 7	d. 8
35.	Let R be the relation over the set $N\times N$ and is defined by $(a,b)R(c,d)\Rightarrow a+d=b+c$ then classify the relation R.	
	a. Reflexive only	b. Symmetric only
	c. Transitive only	d. An equivalence relation
36.	Select the correct option. If S is defined on R by $(x,y)\in S \Leftrightarrow xy\geq 0$ then S is	
	a. An equivalence relation	b. Reflexive only
	c. Symmetric only	d. Transitive only
37.	Select the correct option. A linear Diophantine equation in two variables has the form:	
	a. $ax^2 + by = c$, where $a,b,c \in \mathbb{Z}$	b. $ax + by = c$, where $a,b,c \in \mathbb{Z}$
	c. $ax + by + cz = d$, where $a,b,c,d \in \mathbb{Z}$	d. $axy = c$, where $a,c \in \mathbb{Z}$
38.	Select the correct option. The linear Diophantine equation $4x + 6y = 14$ has:	
	a. No solution	b. A unique integer solution
	c. Infinitely many integer solutions	d. Exactly two integer solutions
39.	Identify the number of integer solutions of the equation $6y + 9y = 20$ is	
	a. 0	b. 1

	c. 2	d. Infinitely many
40.	Identify the condition for the equation $ax + by = c$ to have integer solutions.	
	a. c must be even	b. $a = b$
	c. $\gcd(a, b) / c$	d. ab / c
41.	Select the correct option. If $ax + by = c$ has one integer solution, then:	
	a. It has exactly one more	b. It has no more solutions
	c. It has infinitely many solutions	d. It has only complex solutions
42.	Select the correct option. For all odd integer a, gcd(3a,3a+2)=	
	a. 1	b. 2
	c. 3	d. None of these
43.	Select the correct option. The Euclidean algorithm is used to:	
	a. Solve equations	b. Find LCM
	c. Find GCD	d. Find roots of polynomials
44.	Identify the equation having **no** integer solution.	
	a. $8x + 6y = 10$	b. $2x + 4y = 6$
	c. $3x + 7y = 1$	d. $9x + 3y = 10$
45.	If $x \equiv 1 \ (mod\ 2)$ and $x \equiv 2 \ (mod\ 3)$, identify the smallest x.	
	a. 2	b. 4
	c. 5	d. 8
46.	Let $x \equiv 3 \ (mod\ 5)$ and $x \equiv 4 \ (mod\ 7)$. Identify the least positive x.	
	a. 24	b. 38
	c. 18	d. 10
47.	Let $x \equiv 4 \ (mod\ 6)$ and $x \equiv 3 \ (mod\ 8)$. Then choose the correct option from below if a solution is possible using Chinese Remainder Theorem.	
	a. Yes, always	b. No, since 6 and 8 are not coprime
	c. Yes, only if the remainders are the same	d. No, because 4 > 3

B. Short Answer Type Questions:

1. Identify all integer solutions of the equation 12x + 8y = 4.

2. Identify all integer solution to 15x + 21y = 6.

3. Identify the GCD of 252 and 105 using the Euclidean Algorithm.

4. Identify two integers u and v satisfying $63u + 55v = 1$.

5. Describe The Fundamental Theorem of Arithmetic.

6. Describe The Division algorithm.

7. Examine the relation R on Z defined by aRb if and only if $a - b$ is even, an equivalence relation.

8. Let $A = \{1,2,3\}$ and let $R = \{(1,1), (2,2), (3,3), (1,2), (2,1)\}$. Examine if R is an equivalence relation on A.

9. Let R on $\mathbb{Z}$ be defined as aRb if and only if $a \equiv b \ (mod\ 5)$. Show that R is an equivalence relation.

10. State the Chinese Remainder Theorem

C. Long Answer Type Questions:

1. State the partial order relation. Examine if the subset relation $\subseteq$ on power set $P(S)$ a partial order.

2. Show that congruence modulo n is an equivalence relation.

3. Identify the Hasse diagram for the power set of $\{a, b\}$ ordered by inclusion.

4. Discuss a linear Diophantine equation in two variables. Discuss the condition for its solvability. Also, identify all integer solutions of the equation $15x + 21y = 6$.

5. Examine if the relation R = {(p, q): |p-q| is even} is an equivalence relation on the set P= {3, 4, 5,6}.

6. Consider A = {2, 3, 4, 5} and R = {(5, 5), (5, 3), (2, 2), (2, 4), (3, 5), (3, 3), (4, 2), (4, 4)}, then examine if R is an Equivalence Relation.

7. Examine that cube of any integer can be written in the form 9k, 9k + 1 or 9k − 1 for some k ∈ Z, Z is the set of all integers.

8. Identify the solution of the linear congruence $4x \equiv 8\ (mod\ 8)$.

9. Identify the solution of the system of linear congruences using Chinese Remainder Theorem: $x \equiv 2\ (mod\ 3), x \equiv 3\ (mod\ 4), x \equiv 2\ (mod\ 5)$.

10. Identify the solution of the system of linear congruences using Chinese Remainder Theorem: $x \equiv 1\ (mod\ 7), x \equiv 2\ (mod\ 8), x \equiv 3\ (mod\ 9)$.

References:

1. “Discrete Mathematics and Its Applications”, Kenneth H. Rosen, McGraw-Hill.
2. “Discrete Mathematics with Applications”, Susanna S Epp, Wadsworth Publishing Co. Inc, 4th edition
3. “Elements of Discrete Mathematics: a computer oriented approach”, C L Liu and Mohapatra, McGraw Hill, 3rd edition.
4. “Discrete Mathematical Structures and its Application to Computer Science”, J P Trembley, R Manohar, TMG Edition, Tata McGraw-Hill.
5. “Discrete Mathematics”, Norman L Biggs, Oxford University Press, 2nd Edition.
6. “Discrete Mathematics”, Schaum’s Outlines Series, Semyour Lipschutz and Marc Lipson