Discrete Mathematics
R204GA05401

Narasimhulu M *M. Tech.*
Assistant Professor
Department of Computer Science & Engineering

Objectives

Narasimhulu M *M. Tech.*
Assistant Professor
Department of Computer Science & Engineering

Objectives

- This course will introduce and illustrate in the elementary discrete mathematics for computer science and engineering students.
- To equip the students with standard concepts like formal logic notation, methods of proof, induction, sets, relations, graph theory, permutations and combinations, counting principles.

Course Outcomes

Narasimhulu M ***M. Tech.***
Assistant Professor
Department of Computer Science & Engineering

Course Outcomes

1. Illustrate discrete mathematic components like statements, logic, sets, structures, numbers and combinatorics.
2. Evaluate and simplify propositional and predicate calculus using inference theory.
3. Perform the operations on Sets, Relations and functions and their properties.
4. Identify algebraic systems and use general properties on number theory.
5. Use combinatorics solving the counting problems.
6. Use graph algorithms for representing, identifying, generating and evaluating the Graphs.

Unit III
Algebraic Structures and Number Theory

Narasimhulu M *M. Tech.*
Assistant Professor
Department of Computer Science & Engineering

Unit III

Algebraic Structures: Algebraic Systems, Examples, General Properties, Semi Groups and Monoids, Homomorphism of Semi Groups and Monoids, Group, Subgroup, Abelian Group, Homomorphism, Isomorphism.

Number Theory: Properties of Integers, Division Theorem, The Greatest Common Divisor, Euclidean Algorithm, Least Common Multiple, Testing for Prime Numbers, The Fundamental Theorem of Arithmetic, Modular Arithmetic (Fermat's Theorem and Euler's Theorem)

Algebraic Structures

Narasimhulu M *M. Tech.*
Assistant Professor
Department of Computer Science & Engineering

Algebraic Structures

Algebraic Systems:

- A system consisting of a set and one or more n-ary operations on the set will be called an algebraic systems or simple an algebra.
- We denote an Algebraic system by $\langle S, f_1, f_2, \cdots \rangle$ where S is a set and $f_1, f_2, \cdots$ are operation on S.
- If You include additionally relations to the Algebraic systems then that system is called algebraic structures.

Examples:

Let I be an Integer, + and x are the operations:

Properties for Addition:

Addition holds commutative(A-1), Associative Property.(A-2)

A-3 0 is called Identity Element for Set I. Eg: a+0 = 0+a = a

A-4 -a is called Inverse Element for Set I. Eg: a + (-a) = 0

Algebraic Structures

Algebraic Systems:

Properties for Multiplication:

It also holds commutative(M-2), Associative Property.(M-1)

1 is called identity element.(M-3)

It has distributive property over addition(D)

It has Cancellation Property (C)

For a, b, c $\in I$ and $a \neq 0$

$$a \times b = a \times c \implies b = c$$

For Algebraic system (R, +, X) and (N, +, X) (A-4)

Algebraic Structures

Algebraic Systems:

Some simple Algebraic systems and General Properties;

- **Composition of Functions**

EXAMPLE 2 Let $X = \{a, b\}$ and S denote the set of all mappings from X to X. Let us write $S = \{f_1, f_2, f_3, f_4\}$ where

$$f_1(a) = a \quad f_1(b) = b \quad f_2(a) = a \quad f_2(b) = a$$
$$f_3(a) = b \quad f_3(b) = b \quad f_4(a) = b \quad f_4(b) = a$$

Table 3-1.1

$\circ$	f_1	f_2	f_3	f_4
f_1	f_1	f_2	f_3	f_4
f_2	f_2	f_2	f_2	f_2
f_3	f_3	f_3	f_3	f_3
f_4	f_4	f_3	f_2	f_1

Algebraic Structures

Algebraic Systems:

Some simple Algebraic systems and General Properties;

EXAMPLE 3 Let $X = \{1, 2, 3, 4\}$ and $f: X \to X$ be given by

$$f = \{\langle 1, 2\rangle, \langle 2, 3\rangle, \langle 3, 4\rangle, \langle 4, 1\rangle\}$$

Let the identity mapping on X be denoted f^0. If we form the composite functions $f \circ f = f^2$, $f^2 \circ f = f^3$, $f^3 \circ f = f^4$, and so on, we find that $f^4 = f^0$. Let us denote f by f^1 and consider the set $F = \{f^0, f^1, f^2, f^3\}$. It is clear that the set F is closed under the operation of composition and that $\langle F, \circ\rangle$ is an algebraic system. The operation $\circ$ is both commutative and associative. Also the element f^0 is the identity element with respect to the operation of composition. The result of composition of any two functions of F is given by Table 3-1.2.

Table 3-1.2

$\circ$	f^0	f^1	f^2	f^3
f^0	f^0	f^1	f^2	f^3
f^1	f^1	f^2	f^3	f^0
f^2	f^2	f^3	f^0	f^1
f^3	f^3	f^0	f^1	f^2

Algebraic Structures

Algebraic Systems:

Some simple Algebraic systems and General Properties;

EXAMPLE 3 Let $X = \{1, 2, 3, 4\}$ and $f: X \to X$ be given by

$$f = \{\langle 1, 2\rangle, \langle 2, 3\rangle, \langle 3, 4\rangle, \langle 4, 1\rangle\}$$

Let the identity mapping on X be denoted f^0. If we form the composite functions $f \circ f = f^2$, $f^2 \circ f = f^3$, $f^3 \circ f = f^4$, and so on, we find that $f^4 = f^0$. Let us denote f by f^1 and consider the set $F = \{f^0, f^1, f^2, f^3\}$. It is clear that the set F is closed under the operation of composition and that $\langle F, \circ\rangle$ is an algebraic system. The operation $\circ$ is both commutative and associative. Also the element f^0 is the identity element with respect to the operation of composition. The result of composition of any two functions of F is given by Table 3-1.2.

Table 3-1.2

$\circ$	f^0	f^1	f^2	f^3
f^0	f^0	f^1	f^2	f^3
f^1	f^1	f^2	f^3	f^0
f^2	f^2	f^3	f^0	f^1
f^3	f^3	f^0	f^1	f^2

Algebraic Structures

Algebraic Systems:

Some simple Algebraic systems and General Properties;

EXAMPLE 4 An equivalence relation called "congruence modulo m" on the set of integers was defined in Sec. 2-3.5. Let $m = 4$ and $\mathbf{Z}_4$ denote the set of equiv-

Table 3-1.3

$+_4$	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

alence classes generated, so that

$$\mathbf{Z}_4 = \{[0], [1], [2], [3]\}$$

where $[j]$ denotes the set of all those integers which are equivalent to j. Let us define an operation $+_4$ on $\mathbf{Z}_4$ given by

$$[i] +_4 [j] = [(i + j) \pmod 4]$$

Algebraic Structures

Algebraic Systems:

Some simple Algebraic systems and General Properties:

From the above examples we notice Some similarities between two tables. These similarities leads to several general properties of Algebraic systems.

Homomorphism:

Definition 3-1.1 Let $\langle X, \circ \rangle$ and $\langle Y, * \rangle$ be two algebraic systems of the same type in the sense that both $\circ$ and $*$ are binary (n-ary) operations. A mapping $g: X \to Y$ is called a *homomorphism*, or simply morphism, from $\langle X, \circ \rangle$ to $\langle Y, * \rangle$ if for any $x_1, x_2 \in X$

$$g(x_1 \circ x_2) = g(x_1) * g(x_2) \qquad (2)$$

If such a function g exists, then it is customary to call $\langle Y, * \rangle$ a homomorphic image of $\langle X, \circ \rangle$, although we must note that $g(X) \subseteq Y$.

Algebraic Structures

Algebraic Systems:

Some simple Algebraic systems and General Properties:

Definition 3-1.2 Let g be a homomorphism from $\langle X, \circ \rangle$ to $\langle Y, * \rangle$. If $g: X \to Y$ is onto, then g is called an *epimorphism*. If $g: X \to Y$ is one-to-one, then g is called a *monomorphism*. If $g: X \to Y$ is one-to-one onto, then g is called an *isomorphism*.

Definition 3-1.3 Let $\langle X, \circ \rangle$ and $\langle Y, * \rangle$ be two algebraic systems of the same type. If there exists an isomorphic mapping $g: X \to Y$, then $\langle X, \circ \rangle$ and $\langle Y, * \rangle$ are said to be *isomorphic*.

Definition 3-1.4 Let $\langle X, \circ \rangle$ and $\langle Y, * \rangle$ be two algebraic systems such that $Y \subseteq X$. A homomorphism g from $\langle X, \circ \rangle$ to $\langle Y, * \rangle$ in such a case is called an *endomorphism*. If $Y = X$, then an isomorphism from $\langle X, \circ \rangle$ to $\langle Y, * \rangle$ is called an *automorphism*.

Algebraic Structures

Algebraic Systems:

Some simple Algebraic systems and General Properties:

Definition 3-1.5 Let $\langle X, \circ \rangle$ be an algebraic system and E be an equivalence relation on X. The relation E is called a *congruence relation* on $\langle X, \circ \rangle$ if E satisfies the substitution property with respect to the operation $\circ$.

$$(x_1 \, E \, x_1') \wedge (x_2 \, E \, x_2') \Rightarrow (x_1 \circ x_2) \, E \, (x_1' \circ x_2')$$

cation (3) states th

PROPERTIES 451

Definition 3-1.6 Let $\langle X, \circ \rangle$ be an algebraic system and $Y \subseteq X$ which is closed under the operation $\circ$. Then $\langle Y, \circ \rangle$ is called a *subalgebra* of $\langle X, \circ \rangle$.

Algebraic Structures

Algebraic Systems:

Some simple Algebraic systems and General Properties:

Definition 3-1.7 Let $\langle X, \circ \rangle$ and $\langle Y, * \rangle$ be two algebraic systems of the same type. The algebraic system $\langle X \times Y, \oplus \rangle$ is called the *direct product* of the algebras $\langle X, \circ \rangle$ and $\langle Y, * \rangle$ provided the operation $\oplus$ is defined for any $x_1, x_2 \in X$ and $y_1, y_2 \in Y$ as

$$\langle x_1, y_1 \rangle \oplus \langle x_2, y_2 \rangle = \langle x_1 \circ x_2, y_1 * y_2 \rangle$$

The algebraic systems $\langle X, \circ \rangle$ and $\langle Y, * \rangle$ are called the *factor algebras* of $\langle X \times Y, \oplus \rangle$.

Algebraic Structures

Algebraic Systems:

Semi Groups and Monoids:

Definition 3-2.1 Let S be a nonempty set and $\circ$ be a binary operation on S. The algebraic system $\langle S, \circ \rangle$ is called a *semigroup* if the operation $\circ$ is associative. In other words $\langle S, \circ \rangle$ is a semigroup if for any $x, y, z \in S$,

$$(x \circ y) \circ z = x \circ (y \circ z)$$

Definition 3-2.2 A semigroup $\langle M, \circ \rangle$ with an identity element with respect to the operation $\circ$ is called a *monoid*. In other words, an algebraic system $\langle M, \circ \rangle$ is called a monoid if for any $x, y, z \in M$,

$$(x \circ y) \circ z = x \circ (y \circ z)$$

and there exists an element $e \in M$ such that for any $x \in M$

$$e \circ x = x \circ e = x$$

Algebraic Structures

Algebraic Systems:

Homomorphism of Semi Groups and Monoids:

Definition 3-2.3 Let $\langle S, * \rangle$ and $\langle T, \Delta \rangle$ be any two semigroups. A mapping $g: S \rightarrow T$ such that for any two elements $a, b \in S$,

$$g(a * b) = g(a) \; \Delta \; g(b) \qquad (1)$$

is called a *semigroup homomorphism*.

Definition 3-2.4 Let $\langle M, *, e_m \rangle$ *and* $\langle T, *, e_T \rangle$ be any two moniods. A mapping g: M → T such that for any two elements a , b $\in M$

$$\mathbf{g(a * b) = g(a) \Delta g(b)}$$

and $\mathbf{g(e_M) = e_T}$

is called a monoid homomorphism.

Algebraic Structures

Algebraic Systems:

Group:

Let G be a non-empty set with a binary operation * that assigns to each ordered pair (a, b) of elements of G an element of G denoted by a * b. We say that G is a group under the binary operation * if the following three properties are satisfied**:**

1) Associativity: The binary operation * is associative i.e. $a*(b*c)=(a*b)*c$, $\forall\ a,b,c \in G$

2) Identity: There is an element e, called the identity, in G, such that $a*e=e*a=a$, $\forall\ a \in G$

3) Inverse: For each element a in G, there is an element b in G, called an inverse of a such that $a*b=b*a=e$, $\forall\ a, b \in G$

Algebraic Structures

Algebraic Systems:

Group:

The set of $N \times N$ non-singular matrices form a group under matrix multiplication operation.

The product of two $N \times N$ non-singular matrices is also an $N \times N$ non-singular matrix which holds closure property.

Matrix multiplication itself is associative. Hence, associative property holds.

The set of $N \times N$ non-singular matrices contains the identity matrix holding the identity element property.

As all the matrices are non-singular they all have inverse elements which are also nonsingular matrices. Hence, inverse property also holds.

Algebraic Structures

Algebraic Systems:

Sub Group:

A **subgroup** H is a subset of a group G (denoted by $H \leq G$) if it satisfies the four properties simultaneously – **Closure, Associative, Identity element**, and **Inverse**.

A subgroup H of a group G that does not include the whole group G is called a proper subgroup (Denoted by $H < G$). A subgroup of a cyclic group is cyclic and a abelian subgroup is also abelian.

Algebraic Structures

Algebraic Systems:

Sub Group:

Let a group $G = \{1, i, -1, -i\}$

Then some subgroups are $H_1 = \{1\}, H_2 = \{1, -1\}$,

This is not a subgroup – $H_3 = \{1, i\}$ because that $(i)^{-1} = -i$ is not in H_3

Algebraic Structures

Algebraic Systems:

Abelian Group:

An abelian group G is a group for which the element pair $(a,b) \in G$ always holds commutative law. So, a group holds five properties simultaneously - i) Closure, ii) Associative, iii) Identity element, iv) Inverse element, v) Commutative.

Algebraic Structures

Algebraic Systems:

Abelian Group:

The set of positive integers (including zero) with addition operation is an abelian group. $G = \{0, 1, 2, 3, \ldots\}$

Here closure property holds as for every pair $(a,b) \in S, (a+b)$ is present in the set S. [For example, $1 + 2 = 2 \in S$ and so on]

Associative property also holds for every element $a, b, c \in S, (a+b)+c = a+(b+c)$ [For example, $(1+2)+3 = 1+(2+3) = 6$ and so on]

Identity property also holds for every element $a \in S, (a \times e) = a$ [For example, $(2 \times 1) = 2, (3 \times 1) = 3$ and so on]. Here, identity element is 1.

Commutative property also holds for every element $a \in S, (a \times b) = (b \times a)$ [For example, $(2 \times 3) = (3 \times 2) = 3$ and so on]

Algebraic Structures

Algebraic Systems:

Homomorphism:

A homomorphism is a mapping f: G→ G' such that f (xy) =f(x) f(y), ∀ x, y ∈ G. The mapping f preserves the group operation although the binary operations of the group G and G' are different. Above condition is called the homomorphism condition.

Kernel of Homomorphism: - The Kernel of a homomorphism f from a group G to a group G' with identity e' is the set {x∈ G | f(x) =e'}

Algebraic Structures

Algebraic Systems:

Isomorphism:

Let $(G_1,*)$ and $(G_2,0)$ be two algebraic system, where * and 0 both are binary operations. The systems $(G_1,*)$ and $(G_2,0)$ are said to be isomorphic if there exists an isomorphic mapping f: $G_1 \rightarrow G_2$

Algebraic Structures

Algebraic Systems:

Isomorphism:

Example: Let $(A_1, *)$ and $(A_2, \boxdot)$ be the two algebraic systems as shown in fig. Determine whether the two algebraic systems are isomorphic.

x	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

$\boxdot$	1	w	w^2
1	1	w	w^2
w	w	w^2	1
w^2	w^2	1	w

Number Theory

Properties of Integers :

The following simple rules concerning the addition and multiplication of these numbers are assumed (where a, b, c are arbitrary integers):

(a) Associative law for multiplication and addition:

$$(a+b)+c = a+(b+c) \quad \text{and} \quad (ab)c = a(bc)$$

(b) Commutative law for multiplication and addition:

$$a+b = b+a \quad \text{and} \quad ab = ba$$

(c) Distributive law:

$$a(b+c) = ab+ac$$

(d) Additive identity 0 and multiplicative identity 1:

$$a+0 = 0+a = a \quad \text{and} \quad a \cdot 1 = 1 \cdot a = a$$

(e) Additive inverse $-a$ for any integer a:

$$a+(-a) = (-a)+a = 0$$

Number Theory

Division Theorem:

- If a and b are integers with a ≠ 0, then a divides b if there exists an integer c such that b = ac.
  1. When a divides b we write a|b.
  2. We say that **a is a factor or divisor of b and b is a multiple of a.**
  3. If a|b then b=a is an integer (namely the c above).
  4. If a does not divide b, we write a ∤b.
- **Theorem:** Let a, b, c be integers, where a ≠ 0
  1. If a/b and a/c, then a/(b + c).
  2. If a/b , then a/bc for all integers c,
  3. If a/b and b/c then, a/c.

Number Theory

Division Theorem:

- When an integer is divided by a positive integer, there is a quotient and a remainder. This is traditionally called the "Division Algorithm", but it is really a theorem.
- **Theorem:** If a is an integer and d a positive integer, then there are unique integers q and r , with 0 <= r < d, such that a = dq + r.
  - a is called the dividend.
  - d is called the divisor.
  - q is called the quotient. q = a **div** d
  - r is called the remainder. r = a **mod** d

Number Theory

Greatest Common Divisor:

- Let a and b be integers, not both zero. The largest integer d such that a/d and b/d is called the greatest common divisor of a and b. The greatest common divisor of a and b is denoted by gcd(a, b).
- What is the greatest common divisor of 24 and 36?
- What is the greatest common divisor of 17 and 22?
- The integers a and b are relatively prime (coprime) iff gcd(a, b) = 1.
- 17 and 22. (Note that 22 is not a prime.)
- The integers a1,a2, ... , an are pairwise relatively prime iff
- gcd(ai , aj) = 1 whenever 1 <=i < j <= n.

Number Theory

Euclidean Algorithm:

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

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

Solution: Successive uses of the division algorithm give:

$$662 = 414 \cdot 1 + 248$$
$$414 = 248 \cdot 1 + 166$$
$$248 = 166 \cdot 1 + 82$$
$$166 = 82 \cdot 2 + 2$$
$$82 = 2 \cdot 41.$$

Hence, gcd(414, 662) = 2, because 2 is the last nonzero remainder.

Number Theory

Euclidean Algorithm:

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

ALGORITHM 1 The Euclidean Algorithm.

procedure *gcd*(*a*, *b*: positive integers)
$x := a$
$y := b$
while $y \neq 0$
    $r := x$ **mod** y
    $x := y$
    $y := r$
return x {gcd(*a*, *b*) is x}

j	r_j	r_{j+1}	q_{j+1}	r_{j+2}
0	662	414	1	248
1	414	248	1	166
2	248	166	1	82
3	166	82	2	2
4	82	2	41	0

Number Theory

Least Common Multiple :

- The **least common multiple** of the positive integers a and b is the smallest positive integer that is divisible by both a and b. It is denoted by lcm(a, b).
- lcm(45, 21) = 7 X 45 = 15 X 21 = 315.
- Formula for LCM is Prime Factorization:

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

Let a and b be positive integers. Then

$$ab = \gcd(a, b) \cdot \text{lcm}(a, b).$$

Number Theory

Testing for Prime Numbers:

- An integer p greater than 1 is called prime if the only positive factors of p are 1 and p. A positive integer that is greater than 1 and is not prime is called composite.
- **If n is a composite integer, then n has a prime divisor less than or equal to $\sqrt{n}$.**
- **By using above rule we perform trail division to test whether the given number is prime.**

Number Theory

The Fundamental Theorem of Arithmetic:

- Every positive integer greater than 1 can be written uniquely as a prime or as the product of its prime factors, written in order of nondecreasing size.

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

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

$$641 = 641,$$

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

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

Number Theory

Modular Arithmetic:

If a and b are integers and m is a positive integer, then a is congruent to b modulo m iff m|(a- b).

- The notation $a \equiv b \pmod{m}$ says that a is congruent to b modulo m.
- We say that $a \equiv b \pmod{m}$ is a congruence and that m is its modulus.
- Two integers are congruent mod m if and only if they have the same remainder when divided by m.
- If a is not congruent to b modulo m, we write $a \not\equiv b \pmod{m}$.

Number Theory

Modular Arithmetic:

Example: Determine

- Whether 17 is congruent to 5 modulo 6, and
- Whether 24 and 14 are congruent modulo 6.

Clicker

1. No and No.
2. No and Yes.
3. Yes and No.
4. Yes and Yes.

Solution: $17 \equiv 5 \pmod{6}$ because 6 divides $17 - 5 = 12$.

Number Theory

Modular Arithmetic:

FERMAT'S LITTLE THEOREM If p is prime and a is an integer not divisible by p, then

$$a^{p-1} \equiv 1 \pmod{p}.$$

Furthermore, for every integer a we have

$$a^p \equiv a \pmod{p}.$$

Find 7^{222} **mod** 11.

Solution: We can use Fermat's little theorem to evaluate 7^{222} **mod** 11 rather than using the fast modular exponentiation algorithm. By Fermat's little theorem we know that $7^{10} \equiv 1 \pmod{11}$, so $(7^{10})^k \equiv 1 \pmod{11}$ for every positive integer k. To take advantage of this last congruence, we divide the exponent 222 by 10, finding that $222 = 22 \cdot 10 + 2$. We now see that

$$7^{222} = 7^{22 \cdot 10 + 2} = (7^{10})^{22} 7^2 \equiv (1)^{22} \cdot 49 \equiv 5 \pmod{11}.$$

It follows that 7^{222} **mod** $11 = 5$. ◀

Number Theory

Modular Arithmetic:

FERMAT's Theorem:

If a is an integer and m is a prime then a^m mod m = a mod m

Number Theory

Euler's Theorem

In number theory, **Euler's theorem** (also known as the **Fermat–Euler theorem** or **Euler's totient theorem**) states that, if n and a are coprime positive integers, and $\varphi(n)$ is Euler's totient function, then a raised to the power $\varphi(n)$ is congruent to 1 modulo n; that is

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

In number theory, **Euler's totient function** counts the positive integers up to a given integer n that are relatively prime to n. It is written using the Greek letter phi as $\varphi(n)$ or $\phi(n)$, and may also be called **Euler's phi function**. In other words, it is the number of

Number Theory

Euler's Theorem

The theorem may be used to easily reduce large powers modulo n. For example, consider finding the ones place decimal digit of 7^{222}, i.e. $7^{222} \pmod{10}$. The integers 7 and 10 are coprime, and $\varphi(10) = 4$. So Euler's theorem yields $7^4 \equiv 1 \pmod{10}$, and we get

$$7^{222} \equiv 7^{4\times 55+2} \equiv (7^4)^{55} \times 7^2 \equiv 1^{55} \times 7^2 \equiv 49 \equiv 9 \pmod{10}.$$