Discrete Structures

Day 1

Syllabus

Unit-1	**Logic: Propositional logic and its applications; Propositional equivalences; Predicates and Quantifiers; Rules of inference; Introduction to Proofs; Proof Methods; Proof by Mathematical Induction (Weak and Strong).**
Unit-2	Set theory: Sets, operations on sets, cardinality, inductive definition of sets and proof by induction; Relations, representation of relations, properties of relations, equivalence relations and partitions; Partial orderings; Posets; Well-ordered sets.
Unit-3	Functions: Mappings; Injection and Surjection; Composition of functions; Inverse functions; Special functions; recursive function theory.
Unit-4	Algebraic Structures: Definition and elementary properties of groups; semigroups; monoids; rings; fields, vector spaces; lattices and Boolean Algebra.
Unit-5	Elementary combinatorics: Basic Counting Principles; Permutations and Combinations; Binomial Coefficients and Identities; Generalized Permutations and Combinations; Sterling's number of the second kind; Pigeon-hole Principle and its application; Inclusion-Exclusion Principle and its application; Recurrence Relations; Solving Linear Recurrence Relations; Generating Functions; Catalan Numbers; Fibonacci numbers.
Unit-6	Number Theory: Divisibility and Modular Arithmetic; Integer Representations and Algorithms; Prime numbers and related Theorems; Greatest Common Divisors; Euclid's Algorithm; Solving Congruence; Applications of Congruence, Fermat's Little Theorem, The Chinese Remainder Theorem; Applications in Cryptography.

1. K. H. Rosen , *Discrete Mathematics and Applications,* TMH

Number Theory

- **Divisibility and Modular Arithmetic**

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

THEOREM 1

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

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

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

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

- **THEOREM 2**
- **THE DIVISION ALGORITHM** Let a be an integer and d a positive integer. Then there are unique integers q and r, with $0 \le r < d$, such that $a = dq + r$.

- What are the quotient and remainder when −11 is divided by 3. Which one is correct?

$$-11 = 3(-3) - 2$$

$$-11 = 3(-4) + 1.$$

Modular Arithmetic

- In some situations we care only about the remainder of an integer when it is divided by some specified positive integer.

Q. what time it will be (on a 12-hour clock) 50 hours from now (Assume 3:30 pm)

- If ‘*a*’ and ‘*b*’ are integers and ‘*m*’ is a positive integer, then ‘*a*’ is congruent to ‘*b*’ modulo ‘*m*’ if m divides $a - b$. We use the notation $a \equiv b \pmod{m}$ to indicate that a is congruent to b modulo m.
- If a and b are not congruent modulo m, we write $a \not\equiv b \pmod{m}$.

THEOREM 3: Let ‘a’ and ‘b’ be integers, and let m be a positive integer. Then a ≡ b (mod m) if and only if a **mod** m = b **mod** m.

Eg: 2 ≡ 9 (mod 7)   2 mod 7= 2   9 mod 7 =2

THEOREM 4: 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.

Eg: 13 ≡ 3 (mod 5)   13 = 3 + 2 × 5, k = 2

2 ≡ 9 (mod 7)   k=?

PROPERTIES

1. $(a+b) mod\, n = [(a\, mod\, n) + (b\, mod\, n)]\, mod\, n$
2. $(a-b) mod\, n = [(a\, mod\, n) - (b\, mod\, n)]\, mod\, n$
3. $(a \times b) mod\, n = [(a\, mod\, n) \times (b\, mod\, n)]\, mod\, n$

- $4^3 mod\ 11$: easy to compute as the values are small
- **Modular Exponentiation**

Find $a^n mod\ m$ efficiently, where a, n, and m are large integers.

- **ALGORITHM (Modular Exponentiation)**
  - a: integer, $n = (b_{k-1}b_{k-2}...b_1b_0)_2$ (binary representation), m: positive integers

```
x := 1
power := a mod m
for i := 0 to k − 1
    if $b_i = 1$
        then x := (x · power) mod m
    power := (power · power) mod m
return x {x equals $a^n mod\ m$ }
```

Q. Solve $23^{35} mod\ 19$ = ?

$4^3 mod\ 11$

$3=(11)_2$

$\boldsymbol{x} = 1$; power $= \boldsymbol{4\ mod\ 11 = 4}$

i=0			
i=1			

$23^{35} mod\ 19$

- $23^{35} mod\ 19$

$35 = (100011)_2$

$\boldsymbol{x}$ =1; power $= \boldsymbol{23\ mod\ 19 = 4}$

Representations of Integers

THEOREM: Let *b* be an integer greater than 1. Then if *n* is a positive integer, it can be expressed uniquely in the form

$$\boldsymbol{n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0}$$

where *k* is a nonnegative integer, $\boldsymbol{a_0}$, $\boldsymbol{a_1}$,…, $\boldsymbol{a_k}$ are nonnegative integers less than *b*, and $\boldsymbol{a_k \neq 0}$.

BINARY EXPANSIONS:

Q. What is the decimal expansion of the integer that has $(10101110)_2$ as its binary expansion?

Q. What is the decimal expansion of the number with hexadecimal expansion $(2AE0C)_{16}$

Binary addition

```
   1110        1011
 + 1011       +1101
 11001         1111
               0101
                ?
```

Binary multiplication

```
 110
 101
 110
    000x
  110xx
  11110
```

- Multiplicative inverse

In Z_n, two numbers ‘a’ and ‘b’ are multiplicative inverse of each other if $a \times b \equiv 1\, mod\, n$.

Eg If the modulus is 10, the multiplicative inverse of 3 is 7.

$3 \times 7 \equiv 1\, mod\, 10$.

Finding multiplicative inverse:

The extended Euclidean algorithm finds the multiplicative inverses of b in $Z_n$where ‘n’ and ‘b’ are given and gcd (n, b) = 1

Q. Find the multiplicative inverse of 11 in Z_{26} $x \equiv \frac{1}{11} mod\ 26$

First check, gcd(26, 11) = 1

2	26	11	4	0	1	-2
2	11	4	3	1	-2	5
1	4	3	1	-2	5	-7
3	3	1	0	5	-7	26
	1	0		**-7**	26	

Stop when $\boldsymbol{r_2}$ = 0

$-7\ mod\ 26 = 19$

$x = 19$ [Check: $19 \times 11\ mod\ 26 = 209\ mod\ 26 = 1$]

Q. Find the multiplicative inverse of 23 in Z_{100}

Q. $x \equiv \frac{-3}{13} mod\ 7$

Thank you