**Number theory**

***PREAMBLE***

This course is designed to explain the basics and applications of number theory for the students of Computer Science. The core courses of these branches encounter with concepts like prime factorization, modular arithmetic, and quadratic reciprocities in number theory. The first unit of the course provide a strong platform for such encounters and the other units focuses on applications of number theory.

**Course Objectives**

* To teach basic concepts of number theory focusing on Computational aspects.
* To teach the concepts of factorization of integers.
* To teach Format’s theorem and quadratic residues.
* To explain Chines remainder theorem and Euclidean algorithm.
* To explain polynomial arithmetic.

Unit 1

**Basic Concepts in Number Theory**: Topics in elementary number theory, Divisibility, Greatest Common Divisor, Euclidean Algorithm

**Learning Outcomes:**

After completion of this unit, student will be able to

* develop the basics of number theory: (L3)
* perceive the concept of divisibility: (L5)

Unit 2

Fundamental theorem of Arithmetic, Congruence, Properties of congruence, Linear congruences, Chinese remainder theorem

**Learning Outcomes:** After completion of this unit, student will be able to

* understand the basics of congruences: (L3)
* know some facts about remainders : (L5)

Unit 3

Fermat's theorem, Fermat's little theorem, Wilson’s theorem

**Learning Outcomes:**

After completion of this unit, student will be able to

* learn some theorems on number theory: (L3)
* perceive the concepts of factorization methods(L5)

Unit 4 : The functions , Euler Phi-function, Euler’s theorem, Some

properties of phi function

**Learning Outcomes:**

After completion of this unit, student will be able to

* learn some theorems on number theory: (L3)
* apply primality testing algorithm (L5)

Unit 5

The order of integer modulo m, Primitive roots for prime, Composite number having primitive roots

**Learning Outcomes:**

After completion of this unit, student will be able to

* learn primitive roots of prime numbers and composite numbers: (L3)
* perceive the computation of order of integer modulo m(L5)

**Text Book**

Elementary Number Theory | 7th Edition by David Burton, Mc Graw Hill Education

**References**

# Basic Number Theory by S.B. Malik,S. Chand publishers