Course Code:MATH-213Course Title:Number theoryCredit Hours:303Pre-requisite(s):None

**Course Objectives**: The focus of the course is to study of the fundamental properties of integers and to develop the skills to prove properties in an abstract way. The specific objectives include study of division algorithm, prime numbers, Euclidean algorithm, Congruence, Fermat and Euler's theorem, Diophantine equations etc.

## READING LIST:

- 1. K.H Rosen, "Elementary Number Theory and its Applications" 6<sup>th</sup> edition, Pearson, 2010.
- 2. T. KOSHY, "Elementary Number Theory with Applications", Academic Press, 2007.
- 3. D.M. Burton, "Elementary Number Theory", 7<sup>th</sup> edition, McGraw-Hill, 2010.

Lecture #	Торіс
L1	Introduction
L2-L4	Divisibility, Transitivity of divisibility ,Division of linear combination of integers
	and other related properties of divisibility
L5-L7	The Division Algorithm, Proof, and consequences of Division Algorithm
L8-L10	Prime Number, Prime divisors, infinitude of primes, Upper bound for a prime
	factor of composite integers, Sieve of Eratosthenes, Prime number theorem
L11-L13	Greatest Common Divisor, Properties of GCD(theorems),GCD of more than
	two integers
L14-L15	The Euclidean Algorithm for finding GCD: general, and examples
L16	The Fundamental Theorem of Arithmetic,
L17-L18	Least common multiple, Theorem relating GCD and LCM
L19-L21	Fibonacci numbers, GCD of successive Fibonacci numbers, and related
	properties.
L22-L23	Fermat Numbers, Lame's Theorem Fermat factorization, Prime divisors of
	Fermat number
L24	Mid Exam
L25-L27	Linear Diophantine Equation, Method to Linear Method to solve Diophantine
	Equation

## Lecture-wise Distribution of the Contents

L28-L30	Introduction to Congruences, Linear Congruences, Criterion for existence of
	solution and method of solution, System of linear congruences in one variable,
	Chinese Reminder theorem
L31-L33	Applications of congruences, Divisibility Tests, bar codes, bank cheque
	Calendar etc
L34-L38	System of linear congruencies in two or more than two variables, Matrix method for solution of the system, The Perpetual Calendar and Hashing Functions
L39-L42	Wilson's Theorem and Fermat's Little Theorem, Pseudo-prime, Euler phi-
	function, Euler Theorem
L43-L45	Arithmetic function, Multiplicative functions, Euler phi-function as
	Multiplicative function, Mobius function, Mobius inversion formula
L46-L48	Functions for The Sum and Number of Divisors, Perfect Numbers and
	Mersenne Primes