Course Code: MATH-213
Course Title: Number theory
Credit Hours:
Pre-requisite(s):

303
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 th edition, Pearson, 2010.
2. T. KOSHY, "Elementary Number Theory with Applications", Academic Press, 2007.
3. D.M. Burton, "Elementary Number Theory", $7^{\text {th }}$ edition, McGraw-Hill, 2010.

## Lecture-wise Distribution of the Contents

| Lecture \# | Topic |
| :--- | :--- |
| L1 | Introduction |
| L2-L4 | Divisibility, Transitivity of divisibility ,Division of linear combination of integers <br> 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 <br> factor of composite integers, Sieve of Eratosthenes, Prime number theorem |
| L11-L13 | Greatest Common Divisor, Properties of GCD(theorems), GCD of more than <br> 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 <br> properties. |
| L22-L23 | Fermat Numbers, Lame's Theorem Fermat factorization, Prime divisors of <br> Fermat number |
| L24 | Mid Exam |
| L25-L27 | Linear Diophantine Equation, Method to Linear Method to solve Diophantine <br> Equation |


| L28-L30 | Introduction to Congruences, Linear Congruences, Criterion for existence of <br> solution and method of solution, System of linear congruences in one variable, <br> Chinese Reminder theorem |
| :--- | :--- |
| L31-L33 | Applications of congruences, Divisibility Tests, bar codes, bank cheque <br> Calendar etc |
| L34-L38 | System of linear congruencies in two or more than two variables, Matrix method <br> 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- <br> function, Euler Theorem |
| L43-L45 | Arithmetic function, Multiplicative functions, Euler phi-function as <br> Multiplicative function, Mobius function, Mobius inversion formula |
| L46-L48 | Functions for The Sum and Number of Divisors, Perfect Numbers and <br> Mersenne Primes |

