MTH7071 : Number Theory

Programme: M.Sc. **Year:** Second **Semester:** Forth
Course: Elective **Credits:** 4 **Hours:** 40 hours (Theory)

Course Context and Overview: Number Theory was studied for its long and rich history, its wealth of easily accessible and fascinating questions, and its intellectual appeal. But, in recent years Number Theory has been studied for both for the traditional reasons and for the compelling reason that number theory has become essential for Cryptology. Topics include the integers, divisibility, prime numbers, primality testing, factorization methods, congruences, Diophantine problems, arithmetical functions, Fermat's little theorem, primitive roots, quadratic reciprocity, Diophantine equations, Fermats's last theorem, arithmetical functions and so forth.

Prerequisites Courses: There are no formal prerequisites for the class, but some familiarity with proofs will be helpful.

Textbook:

- Niven, H. Zuckerman, H. Montgomery, An Introduction to the Theory of Numbers, 5th Edition, Wiley, ISBN 0471625469.

Alternative text:

- Kenneth H. Rosen: Number Theory and its applications, 5th edition..
- Burton, David M. Elementary Number Theory. Allyn and Bacon, 1976. ISBN: 9780205048144.
- Ireland, Kenneth F., and Michael I. Rosen. A Classical Introduction to Modern Number Theory. Springer, 1990. ISBN: 9780387973296

Additional References:

- NPTEL: Number Theory (Web): http://nptel.ac.in/courses/111103020/

Course outcomes (COs):

On completion of this course, the students will have the ability to:
CO1: The course provides an introduction to basic number theory, where the focus is on computational aspects with applications in cryptography.
Co2: Getting the basic idea of Primes, Divisibility and the Fundamental Theorem of Arithmetic, Greatest Common Divisor (GCD), Euclidean Algorithm
CO3: Understanding the concepts of Congruences, Chinese Remainder Theorem, Hensel's Lemma, Primitive Roots
CO4: Understanding the Theory of Quadratic Residues and Reciprocity

Course Topics

Contents		Lecture Hours	
UNIT – 1: Divisibility and Factorization			
1.1	Divisibility: Definition, properties, division algorithm, greatest integer function	2	12
1.2	Congruence and Modular Arithmetic.	1	
1.3	Primes: Definition, Euclid's Theorem, Prime Number Theorem (statement only), Goldbach and Twin Primes conjectures, Fermat primes, Mersenne primes	3	
1.4	The greatest common divisor: Definition, properties, Euclid's algorithm, linear combinations and the gcd	1	
1.5	The least common multiple: Definition and properties, The Fundamental Theorem of Arithmetic: Euclid's Lemma, canonical prime factorization, divisibility, gcd, and lcm in terms of prime factorizations	3	
1.6	Primes in arithmetic progressions: Dirichlet's Theorem on primes in arithmetic progressions (statement only)	2	
UNIT –2: Congruences			9
2.1	Definitions and basic properties, residue classes, complete residue systems, reduced residue systems	2	
2.2	Linear congruences in one variable, Euclid's algorithm	2	
2.3	Simultaneous linear congruences, Chinese Remainder Theorem	2	
2.5	Wilson's Theorem	1	
2.6	Fermat's Theorem, pseudoprimes and Carmichael numbers, Euler's Theorem	2	
UNIT-3: Arithmetic functions			
3.1	Arithmetic function, multiplicative functions: definitions and basic examples	2	10
3.2	The Moebius function, Moebius inversion formula	2	
3.3	The Euler phi function, Carmichael conjecture	2	
3.4	The number-of-divisors and sum-of-divisors functions	2	
3.5	Perfect numbers, characterization of even perfect numbers	2	
UNIT-4 : Quadratic residues			9
4.1	Quadratic residues and nonresidues	2	
4.2	The Legendre symbol: Definition and basic properties, Euler's Criterion	2	
4.3	Gauss' Lemma The law of quadratic reciprocity	1	
4.4	The order of an integer, Primitive roots: Definition and properties	2	
4.5	The Primitive Root Theorem: Characterization of integers for which a primitive root exists	2	

Evaluation Methods:

Component	Weightage (%)
Assignment	30%
Quiz	20%
End term	50%

Instructor
Dheerendra Mishra, PhD
Office Phone: (0141) 519-1719
Email: dheerendra.mishra@lnmiit.ac.in