Birla Institute of Technology & Science, Pilani
Hyderabad Campus

SECOND SEMESTER, 2024 - 2025
Course Handout Part II

Date: 06.01.2025

In addition to Part-I (General Handout for all courses appended to the timetable) this portion gives further specific details regarding the course.

Course Number : MATH F231
Course Title : Number Theory
Instructor In-charge : Sushil Bhunia

Scope and Objective of the Course:
In this course, we cover the basic mathematical notation and methods, properties of divisors, prime numbers, integer functions, equations in integers, and applications of some of the concepts. The main objective of this course is to understand the divisibility properties of integers and other related topics as a basis for studying more advanced topics in Number Theory, Modern Algebra, and number-theoretic cryptography algorithms.

Text Book:
Thomas Koshy: *Elementary Number Theory with Applications*, Second Edition, Academic Press, 2007.

Reference Books:
(i) David M. Burton: *Elementary Number Theory*, McGraw-Hill, 7th edition, 2011.
(ii) Tom M. Apostol: *Introduction to Analytic Number theory*, Springer, 1976.
(iii) I. Niven, H. S. Zuckerman, H. L. Montgomery: *An Introduction to the Theory of Numbers*, 5th edition, John Wiley & Sons, 1991.

Course Plan:

Lecture No.	Learning objectives	Topics to be covered	Chapter in the Text Book
1	To explain the fundamental properties of integers	Fundamental properties, the summation and product notations, mathematical induction, recursion, the binomial theorem	1.1 – 1.5
2 – 3	To examine the correctness of a division problem	The division algorithm	2.1

4 – 6	To classify the various classes of positive integers	Prime numbers, composite numbers, Fibonacci numbers, Lucas numbers, Fermat numbers	2.5 – 2.7
7	To list the fundamental operations on integers	Greatest common divisor	3.1
8 – 9	To know how to find the greatest common divisor of two numbers having prime factorizations.	The Euclidean algorithm	3.2
10	To know how to factorize any positive integer	The fundamental theorem of arithmetic	3.3
11 – 13	To learn linear Diophantine equations	Least common multiple, linear Diophantine equations	3.4, 3.5
14 – 15	To define what is congruence and explain its fundamental properties	Congruence, linear congruence	4.1, 4.2
16 – 17	To explain the applications of congruence	Divisibility tests, check digits	5.1 – 5.3
18 – 24	To explain the four classical milestone theorems in number theory	Chinese remainder theorem, Wilson's theorem, Fermat's little theorem, Euler's theorem	6.1 – 6.3, 7.1, 7.2, 7.4
25 – 28	To define the multiplicative functions and to explain their properties	Euler's phi function, the tau and sigma functions, the Mobius function	8.1 – 8.2, 8.5
29 – 31	To explain perfect numbers	Perfect numbers, Mersenne primes	8.3, 8.4
32 – 35	To define the order of an integer and primitive roots	The order of a positive integer, primality tests, primitive roots for primes	10.1 – 10.3
36 – 38	To define quadratic residues and to explain the famous law of quadratic reciprocity	Quadratic residues, the Legendre symbol, quadratic reciprocity, the Jacobi symbol	11.1 – 11.4
39 – 40	To explain the continued fractions	Continued fractions	12.1, 12.2

Evaluation Scheme:

Component	Duration	Weightage (%)	Date & Time	Nature of Component
Quiz 1	30 minutes	10	29/01 & 2-2:30 PM	Open Book
Quiz 2	30 minutes	10	24/02 & 2-2:30 PM	Open Book
Mid-Semester Test	90 minutes	25	07/03 9.30 - 11.00AM	Closed Book
Quiz 3	30 minutes	10	09/04 & 2-2:30 PM	Open Book
Comprehensive Exam	180 minutes	45	10/05FN	Closed Book

- **Total marks: 200**
- **Chamber consultation hour:** This will be announced in the class.
- **Notices:** The notices concerning this course will be displayed in LMS.
- **Make-up Policy**: Make-up will be given only in genuine cases, and prior permission from the IC must be obtained.
- **Academic Honesty and Integrity Policy:** All students are to maintain academic honesty and integrity throughout the semester, and no academic dishonesty is acceptable.

Instructor In-charge
MATH F231