SECOND SEMESTER 2021-22
COURSE HANDOUT

Date: 17.01.2022

In addition to part I (General Handout for all courses appended to the Time table) this portion gives further specific details regarding the course.

Course Number : MATH F231
Course Title : Number Theory
Instructor-In-charge : DIVYUM SHARMA
Tutorial Instructor : DIVYUM SHARMA

1. **Course Description:** This is a course on number theory, one of the oldest branches of mathematics. The course will cover the basics of elementary number theory including some of the fundamental properties of integers, greatest common divisors, primes, congruences, Chinese remainder theorem, Fermat's Little theorem and similar results, integer functions, primitive roots, quadratic residues and solutions to certain Diophantine equations.

2. **Scope and Objective of the Course:** This course will introduce some basic mathematical notation and methods, covering properties of divisors, prime numbers, integer functions, equations in integers as well as some applications. 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, or the number theoretic RSA cryptography algorithms.

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

4. **Reference Books:**
(i) I. Niven, H. S. Zuckerman, H.L. Montgomery: An Introduction to the Theory of Numbers, Wiley, 1991.
(ii) W. Stein: Elementary Number Theory: Primes, Congruences, and Secrets, Springer, 2011.
(iii) Neal Koblitz: A Course in Number Theory and Cryptography, 2nd Edition, Springer, 1994.
(iv) Harold Davenport & J. H. Davenport, The Higher Arithmetic: An Introduction to the Theory of Numbers, 8th edition, Cambridge University Press, 2008.

5. **Lecture Plan:**

Module No.	Lecture Sessions	Reference	Learning Outcome
1	L1.1 Fundamental properties, the summation and product notation, Mathematical induction, recursion, the binomial theorem	1.1- 1.5	Understanding the fundamental properties of integers
2	L2.1-L2.3 The division algorithm, base b-representation	2.1-2.2	Students will be able to check the correctness of a division problem
3	L3.1-L3.4 Prime numbers, composite numbers, Fibonacci numbers, Lucas numbers and Fermat numbers	2.5 –2.7	Students will be able to explore various important classes of positive integers
4	L4.1-L4.2 Greatest common divisor	3.1	Students will be able to learn the fundamental operations on integers
5	L5.1-L5.2 The Euclidean algorithm.	3.2	Students will be able to find the greatest common divisor of two numbers from prime factorizations.
6	L6.1-L6.2 The fundamental theorem of arithmetic	3.3	Understanding the factorization of any positive integer
7	L7.1-L7.2 Least common multiple, linear Diophantine equations	3.4 –3.5	Solving linear Diophantine equations
8	L8.1-L8.3 Introduction to congruences, linear congruences, The Pollard Rho factoring method	4.1- 4.3	Understanding the fundamental properties of congruences and applications
	L9.1-L9.2 Chinese remainder theorem	6.1	Knowledge about four classical

9	L9.3 Wilson's theorem	7.1	milestone theorems in number theory
	L9.4 Fermat's Little theorem	7.2	
	L9.5-L9.6 Euler's theorem	7.4	
10	L10.1-L10.4 Euler's Phi function, The Tau and sigma functions, The Mobius function	8.1- 8.2, 8.5	Knowledge about multiplicative functions and their properties
11	L11.1-L11.4 The order of a positive integer, Primality tests, primitive roots for primes	10.1-10.3	Students will be able to find the order of an integer and primitive roots of a prime
12	L12.1-L12.2 Quadratic residues, The Legendre symbol L12.3-L12.5 Quadratic reciprocity, The Jacobi symbol	11.1-11.4	Understanding the quadratic residues and the famous law of quadratic reciprocity
13	L13.1-L13.2 Finite continued fractions	12.1	Understanding finite continued fractions and their use in solving linear Diophantine equations

6. Evaluation Scheme:

Component	Duration	Weightage (%)	Date & time	Remarks
Mid Term Exam	90 Min	30	As scheduled by AUGSD	Closed/Open Book
Class tests (2 Quizzes)	30 Min each	30 (15% each)	Exact date will be announced a week in advance	Closed/Open Book
Comprehensive Examination	3 Hours	40	17/05, 8:00-11:00	Closed/Open Book

7. Chamber consultation hours: : To be announced on NALANDA/Google Classroom

8. Notices: All notices related to the course will be put up on NALANDA/Google Classroom and/or information will be passed in the lectures/tutorials

9. Make up Policy: Make-up for the quiz/mid-semester/comprehensive examination will be given to genuine cases with prior permission only.

Instructor-In-Charge
MATH F231