



In addition to Part I (General Handout for all courses appended to the time table) portion here give specific details regarding the course.

**Course Number** : MATH F231  
**Course Title** : Number Theory  
**Instructor-In-charge** : ASHISH TIWARI

- 1. Course Description:** This course will cover basic properties of the integers, greatest common divisors, primes, congruences, Chinese remainder theorem, Fermat's Little theorem and similar results, integer functions, primitive roots, quadratic residues.
- 2. Scope and Objective of the Course:** This course will introduce basic mathematical notations and methods, covering properties of divisors, prime numbers, integer functions, equations in integers and 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, 2<sup>nd</sup> Edition, Springer, 1994.
- 5. Lecture Plan:**

Lec. No.	Learning Objectives	Topics to be Covered	Ref. to text Book: chap/Sec.
1	To study the fundamental properties of integers	Fundamental properties, the summation and product notations, Mathematical induction, recursion, the binomial theorem,	1.1 – 1.5
2 - 4	To check the correctness of a division problem, base b-representation	The division algorithm.	2.1-2.2





5 - 8	To explore various important classes of positive integers	Prime numbers, composite numbers, Fibonacci numbers, Lucas numbers and Fermat numbers	2.5 – 2.7
9 - 10	To learn the fundamental operations on integers	Greatest common divisor	3.1
11 - 12	To know how to find the greatest common divisor of two numbers having prime factorizations.	The Euclidean algorithm.	3.2
13 – 15	To know how to factorize any positive integer	The fundamental theorem of arithmetic	3.3
16 – 18	To learn linear Diophantine equations	Least common multiple, linear Diophantine equations	3.4 – 3.5
19 – 21	To introduce congruences and develop their fundamental properties	Introduction to congruences, linear congruences, The Pollard Rho factoring method	4.1 – 4.3
22 – 27	To learn the four classical mile stone theorems in number theory and their applications	Chinese remainder theorem	6.1
		Wilson's theorem	7.1
		Fermat's Little theorem	7.2
		Euler's theorem	7.4
28 – 31	To know about multiplicative functions and their properties	Euler's Phi function, The Tau and sigma functions, The Mobius function	8.1 – 8.2, 8.5
32 – 35	To discuss 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 – 40	To learn quadratic residues and the famous law of quadratic reciprocity	Quadratic residues, The Legendre symbol, Quadratic reciprocity, The Jacobi symbol,	11.1- 11.4





**6. Evaluation Scheme:**

Component	Duration	Weightage	Date	Time	Venue	Remarks
Mid Term Exam	90 Min	35%	18/3	9:00 - 10:30 AM	***	CB
Comprehensive Examination	3 Hours	45%	10/5	FN	***	CB/OB (details will be announced in class)
Quizzes/Assignments	20 Min	20%	***	***	***	CB/OB

\*\*\* To be announced later.

**7. Notices:** All notices regarding the course MATH F231 will be put on online notice (NALANDA) and Mathematics department notice board.

**8. Make up Policy:** For mid-semester and comprehensive examinations, make up will be given only in genuine cases and for that prior permission has to be obtained. For quizzes/assignments, there will be no make up in any circumstances.

**9. Chamber consultation hours:** To be announced in the class.

**Instructor-In-Charge  
MATH F231**

