BIRLA INSTITUTE OF TECHNOLOGY AND SCIENCE, PILANI
HYDERABAD CAMPUS
INSTRUCTION DIVISION
FIRST SEMESTER 2016 - 2017
Course Handout Part II

Date: 01.08.2016

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

Course No. **: MATH F231**
Course Title **: Number Theory**
Instructor-in-charge **: Dr JAGANMOHAN JONNALAGADDA**

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) Tom M. Apostol: Introduction to Analytic Number theory, Springer, 1976.
(ii) Kenneth H. Rosen: Elementary Number Theory and its Applications, Addison – Wesley publishing Company, 1986.
(iii) Neal Koblitz: A Course in Number Theory and Cryptography, 2nd Edition, Springer, 1994.

5. **Course Plan:**

Lecture No.	Learning Objectives	Topics to be Covered	Text Book Chapter/Section
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 - 3	To check the correctness of a division problem	The division algorithm	2.1
4 - 6	To explore various important classes of positive integers	Prime numbers, composite numbers, Fibonacci numbers, Lucas numbers, Fermat numbers	2.5 – 2.7
7	To learn 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 - 16	To introduce congruences and develop their fundamental properties	Introduction to congruences, linear congruences, the Pollard rho factoring method	4.1 – 4.3
17 - 18	To know the applications of congruences	Divisibility tests, check digits, round - robin tournaments, the perpetual calendar	5.1, 5.3, 5.5 – 5.6
19 - 24	To learn the four classical mile stone theorems in number theory	Chinese remainder theorem	6.1 – 6.3
		Wilson's theorem	7.1
		Fermat's little theorem	7.2
		Euler's theorem	7.4
25 - 28	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
29 - 31	To learn about perfect numbers and Mersenne primes	Perfect numbers, Mersenne primes	8.3 – 8.4
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
41 - 42	To know about continued fractions	Finite continued fractions, infinite continued fractions	12.1 – 12.2

6. **Evaluation Scheme:**

S. No.	Evaluation Component	Duration	Weightage (%)	Date & Time	Nature of Component
1.	Test I	1Hour	30	8/9, 2.30--3.30PM	Closed Book
2.	Test II	1Hour	30	25/10, 2.30--3.30PM	Open Book
4.	Comprehensive Exam.	3Hours	40	06/12 AN	Closed Book

7. **Make-up Policy**: Make-up for tests will be given only for very genuine cases and prior permission has to be obtained from Instructor In-charge.

8. **Chamber consultation hour:** To be announced by the respective Instructor.

9. **Notices:** The notices concerning this course will be displayed in CMS only.

Instructor-in-charge
MATH F231