with effect from :2024-25 (R-23)

VASAVI COLLEGE OF ENGINEERING (AUTONOMOUS)

9-5-81, Ibrahimbagh, Hyderbad-500031, Telangana State

DEPARTMENT OF MATHEMATICS

NUMBER THEORY& BOOLEAN ALGEBRA (OE) for B.E., III - Semester – CBCS

(For CSE, AIML & IT only)

Instruction :2 Hours per week	**Semester End Exam Marks: 40**	**Subject Reference Code: U23OE320MA**
Credits: 2	**Sessional Marks: 60**	**Duration of Semester End Exam: 3 Hrs.**

Course Description: This course is designed to explain the basics and applications of number theory for the students of Computer Science & Information Technology. The core courses of these branches encounter with concepts like prime factorization, modular arithmetic, Congruences, Primitive roots and Boolean function in number theory. The students will also learn how number theory is used in public key cryptography to securely transmit information over the internet.

COURSE OBJECTIVES	COURSE OUTCOMES
The course will enable the students to:	*At the end of the course students will be able to:*
1. ***Study*** Fundamental Theorem of Arithmetic and GCD using Euclidean Algorithm and also Linear Diophantine Equations and their solutions. 2. ***Understand*** the concepts of number theory such Congruences and proofs of Fermat's and Wilson's theorem. 3. ***Identify*** Primitive roots for primes and their existence and also to outline the Euler's theorem and Lagrange's theorem. 4. ***Familiarise*** with properties of Boolean algebra and to understand Normal Forms**.**	**1.** ***Calculate*** GCD using Euclidean algorithm and also solve Linear Diophantine Equations in order to implement in RSA encryption. **2.** ***Use*** Fermat's Little Theorem & Wilson's theorem to prove that RSA works correctly and accurately and also in discrete log cipher of Cryptography. **3.** ***Apply*** primitive roots in the Diffie-Hellman key exchange protocol and ElGamal encryption of Cryptography **4.** ***Design*** secure hash functions, encryption schemes, and authentication protocols using Boolean functions which are the building blocks of symmetric cryptographic systems, which are used to design all types of digital security systems.

UNIT – I (6 Hours)

Theory of Numbers: The Integers and Division- Prime and Composite Numbers -Division Algorithm- Fundamental Theorem of Arithmetic –GCD and their properties- Euclidean Algorithm- Modular Arithmetic- Linear Diophantine Equations and their solutions.

UNIT – II (8 Hours)

Congruences: Introduction to Congruences, Linear Congruence. Chinese Remainder Theorem - Polynomial Congruences- System of Linear Congruences in two variables- The Pollard Rho Factoring Method- Fermat's Little Theorem, Wilsons Theorem and its converse

UNIT – III (5 Hours)
Primitive Roots: Euler's phi-function - Euler's theorem -The order of an integer modulo n, Primitive roots for primes - Lagrange's Theorem - Existence of Primitive roots.

UNIT – IV (6 Hours)
Boolean Algebra: Axiomatic definition of Boolean Algebra, Basic theorems and Properties of Boolean Algebra, Boolean Functions, Minterms and Maxterms, Disjunctive normal form and conjunctive normal form.

Text Books:

1. K.H. Rosen: Elementary Number Theory & its Applications, Pearson Addition Wesley
2. Elementary Number Theory | 7th Edition by David Burton, Mc Graw Hill Education
3. Discrete mathematics for computer scientists and mathematicians / by Joe L. Mott, Abraham Kandel and Theodore P. Baker, Prentice Hall Of India Pvt.Ltd., 1986.Edition: 2nd edition, New Delhi.
4. Basic Number Theory by S.B. Malik,S. Chand publishers

Reference Books:

1. N. Koblitz; A course in Number theory and Cryptography; Springer.

.

2. Neville Robinns, Beginning Number Theory (2nd Edition), Narosa Publishing House Pvt. Limited, Delhi, 2007.
3. Elementary Number Theory with Applications, Thomas Koshy, 2nd edition, Academic Press, An Imprint of Elsevier, USA, 2007.
4. An introduction to the theory of number, Ivan Niven, Zuckerman, Montgomery, willy India edition
5. Arnold B. H.: Logic and Boolean Algebra, Prentice Hall, 1962.

Online Resources:

1. https://www.classcentral.com/course/openlearn-science-maths-technology-introduction-number-theory-95553
2. https://www.open.edu/openlearn/science-maths-technology/introduction-number-theory/content-section-0?intro=1
3. https://ocw.mit.edu/courses/6-042j-mathematics-for-computer-science-fall-2010/resources/lecture-4-number-theory-i/

Prof.N.Kishan	Prof.M.A.Srinivas	Dr.M.Raghavendra Sharma	Dr.B.Srivastsa
(OU Nominee)	(Subject Expert-JNTUH)	(Subject Expert)	(Industry Expert)

Dr.T. Sudhakar Rao
(Chairman, BOS)