

With effect from :2025-26(R-24)

VASAVI COLLEGE OF ENGINEERING (AUTONOMOUS)

Accredited by NAAC with A++ Grade

9-5-81, Ibrahimbagh, Hyderabad-500031

DEPARTMENT OF MATHEMATICS

NUMBER THEORY & BOOLEAN ALGEBRA

(OPEN ELECTIVE)

For B.E., III - Semester – CBCS

(Common to CSE, AIML & IT Branches)

Instruction :3 Hours per week	Semester End Exam Marks: 40	Subject Reference Code: U24OE320MA
Credits: 2	Sessional Marks: 60	Duration of Semester End Exam: 3 Hours

COURSE OBJECTIVES	COURSE OUTCOMES
<i>The course will enable the students to :</i>	<i>At the end of the course students should be able to:</i>
1. <i>Study</i> Fundamental Theorem of Arithmetic and GCD using Euclidean Algorithm and also Linear Diophantine Equations and their solutions.	1. <i>Calculate</i> GCD using Euclidean algorithm and also solve Linear Diophantine Equations in order to implement in RSA encryption.
2. <i>Understand</i> the concepts of number theory such Congruences and proof of Chinese Remainder theorem.	2. <i>Apply</i> Chinese Remainder theorem for optimizing cryptographic processes, such as accelerating RSA decryption and the Pollard Rho method to assess and demonstrate the factorization of composite numbers used in cryptographic keys.
3. <i>Identify</i> Primitive roots for primes and their existence and also to outline the Euler's theorem and Lagrange's theorem.	3. <i>Use</i> Fermat's Theorem & Wilson's theorem to prove that RSA works accurately and also in discrete log cipher of Cryptography. Also primitive roots in the Diffie-Hellman key exchange protocol of Cryptography
4. <i>Familiarize</i> with properties of Boolean algebra and to understand Normal Forms.	4. <i>Design</i> secure hash functions, encryption schemes, and authentication protocols using Boolean functions which are the building blocks of symmetric cryptographic systems.

UNIT – I (6 Hours)

THEORY OF NUMBERS: The Integers and Division- Prime and Composite Numbers -Division Algorithm- Fundamental Theorem of Arithmetic(without proof) –GCD and their properties- Euclidean Algorithm- Linear Diophantine Equations and their solutions.

UNIT – II (8 Hours)

CONGRUENCES: Modular Arithmetic- Introduction to Congruences, Linear Congruence. Chinese Remainder Theorem - System of Linear Congruences in two variables- The Pollard Rho Factoring Method.

UNIT – III (5 Hours)

SOME SPECIAL CONGRUENCES: Fermat's Little Theorem- Wilson's Theorem and its converse Euler's phi-function - Euler's theorem -The order of an integer modulo n , Primitive roots for primes.

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 Addison 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. Discrete Mathematics, R.K.Bisht and H.S.Dhami, Oxford Higher Education.


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. Basic Number Theory by S.B. Malik, S. Chand publishers
5. Arnold B. H.: Logic and Boolean Algebra, Prentice Hall, 1962.

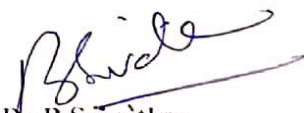
Online Resources:

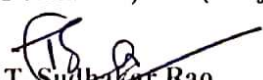
1. <https://www.classcentral.com/course/openlearn-science-maths-technology-introduction-number-theory-95553>
2. <https://www.open.edu/openlearn/science-maths-technology/introduction-number-theory/content-section-0?intro=1>
3. <https://ocw.mit.edu/courses/6-042j-mathematics-for-computer-science-fall-2010/resources/lecture-4-number-theory-i/>


Prof.N.Kishan
(OU Nominee)


Prof.M.A.Srinivas
(Subject Expert-JNTUH)


Dr.J.Jagannathan Mohan
(Subject Expert-BITS, Hyd)


Dr.B.Srivathsa
(Industry Expert)


Dr.T. Sudhakar Rao
(Chairman, BOS)