GUJARAT TECHNOLOGICAL UNIVERSITY

Program Name: Bachelor of Engineering

Level: UG

Subject Code: BE04000291

Subject Name: Number Theory

w.e.f. Academic Year:	A.Y.2024-25
Semester:	4
Categor yof the Course:	Basic Science Course

Prerequisite:	Basic knowledge of Mathematics
Rationale:	The course focuses on mathematical foundation in AI and Security. It highlights the basics of number theory like, GCD, Divisibility, Prime number etc. This course includes algebraic structure for Groups, Discrete logarithms and Classification. Probability theory is important to understand the concept of probability and conditional probability. Coding theory is important for liner code, hamming code and syndrome decoding. Pseudorandom number is used for Next bit predictor and Blum-Blum-Shub Generator. All mathematical concepts are highly important for the mathematical foundation and calculation used for AI and Cyber Security.

Course Outcome:

After Completion of the Course, Student will be able to:

No	Course Outcomes	RBT Level
1	To learn about Number theory including Probability, Divisibility, Greatest common divisor and Prime numbers.	R, U
2	To understand and apply Euclidean algorithm, Fermat's theorem and Euler's theorem.	R, U
3	To understand the concept of Algebraic structure including Groups, Rings, Fields and Classifications.	R, U
4	To calculate probability based on Baye's theorem and for discrete random variables and continuous random variables	N
5	To apply the concept of Coding and Random number generation.	A

**Revised Bloom's Taxonomy(RBT)*

Teaching and Examination Scheme:

Teaching - Learning Scheme (in Hours per Semester)					Total Credits = TH/30	Assessment Pattern and Marks					Total Marks
						Theory		Tutorial / Practical			
L	T	P	PBL*	TH		ESE (E)	PA (M)	PA (I)	PBL (I)	ESE (V)	
45	0	30	15	90	03	70	30	20	30	50	200

* Problem Based Learning (PBL) aims to accommodate learning beyond syllabus as per clause 9.4 of NBA manual.

Course Content:

Unit No.	Content	No. of Hours	% of Weightage
1.	**Finite Fields** : Groups, Cyclic groups, Rings and Fields, Modular Arithmetic, Properties of Modular Arithmetic, The Euclidean Algorithm-for GCD, Finite Fields of the Form GF(p), Multiplicative inverse of GF(p), Polynomial Arithmetic, Finite Fields of the Form GF(2n)-modular polynomial arithmetic, finding multiplicative inverse, Extended Euclid algorithm, Generator.	8	20
2.	**Introduction to Number Theory** -Divisibility - Greatest common divisor –Prime numbers – Fermat's and Euler's Theorem, Euler Totient function, Testing for Primality-Miller Rabin Algorithm, The Chinese Reminder Theorem, Discrete Logarithms –Power of integer modulo n, Logarithm for modular arithmetic	8	20
3.	**Elliptic Curve Arithmetic:** Abelian groups, Elliptic curve over Real Numbers, Geometric Description of Addition, Algebraic Description of Addition, Elliptic curve over Zp, Elliptic curve over GF(2m)	7	15
4.	**Random Number Generation**: Use of random numbers, Pseudorandom Number Generation (PRNGs), Linear Congruential Generators, Cryptographically Generated Random numbers, Blum Blum Shub Generator, True Random Number Generators	6	15
5.	**Coding Theory** : Introduction - Basic concepts: codes, minimum distance, equivalence of codes, Linear codes - Generator matrices and parity-check matrices - Syndrome decoding – Hamming codes - Hadamard Code - Goppa codes.	8	15
6.	**Probability Theory** : Introduction – Concepts of Probability - Conditional Probability - Baye's Theorem - Random Variables – discrete and continuous- central Limit Theorem-Stochastic Process- Markov Chain.	8	15

Suggested Specification Table with Marks(Theory):

Distribution of Theory Marks (in%)					
RLevel	**ULevel**	**ALevel**	**NLevel**	**E Level**	**CLevel**
20	**40**	**20**	**20**	**--**	**-**

WhereR:Remember;U:Understanding;A:Application,N:AnalyzeandE:EvaluateC: Create (as per Revised Bloom's Taxonomy)

References/Suggested Learning Resources:

(a) Books:

1. Sheldon M Ross, "Introduction to Probability Models", Academic Press, 2003.
2. Joseph A. Gallian, ''Contemporary Abstract Algebra', Narosa, 1998. 04 10

3. Cryptography and Network Security by William Stallings 5th Edition Pearson Education
4. Ivan Niven, Herbert S. Zuckerman, and Hugh L. Montgomery, 'An introduction to the theory of numbers', John Wiley and Sons 2004.
5. C.L. Liu, 'Elements of Discrete mathematics', McGraw Hill, 2008.
6. Cryptography and Network Security by Behrouz A. Forouzan TMH Publication

(b) Open source software and website:

NPTELCourse:

1. A Basic Course In Number Theory**,** By Prof. Shripad Garge | IIT Bombay
2. Number Theory By Anupam Saikia Department of Mathematics Indian Institute of Technology Guwahati

Suggested Course Practical List:(List can be change according to Latest Development)

Sr	Aim
1	Find greatest common divisor for following: a. gcd (2, 4) b. gcd (6, 9) c. gcd (7, 5) d. gcd (8, 9) e. gcd (124, 72) f. gcd (748, 2024)
2	Determine multiplicative inverse of x^3+x+1 in GF(2^4), with $m(x)=x^4+x+1$.
3	Explain Fundamental of Modular arithmetic.
4	Using CRT (Chinese Remainder Theorem) to Simplify Modulo Computations Calculate 3299 mod 24
5	Using CRT to Simplify Modulo Computations Calculate 12345*12345 mod 35
6	Using Fermat's little theorem Solve 1117 mod 3
7	Explain properties of Group
8	Check for the Closure, Identity, Inverse and Associativity properties for following: a. $Z_3^+ = (\{0,1,2\}, +_{mod3})$ b. $Z_7^+ = (\{0,1,\ldots,6\}, +_{mod7})$ c. $Z_3 = (\{1,2\}, *_{mod3})$ d. $Z_7 = (\{1,\ldots,6\}, *_{mod7})$
9	Explain Conditional probability. What is the expected outcome of rolling a dice? Rolling a fair dice, what is the expectation of the square of the outcomes? What is the expected output about rolling a dice Twice?
10	Given 2 as a primitive root of 29, construct a table of descript logarithms and use it ot solve following congruences: a. $17x^2 \equiv 10 \pmod{29}$ b. $x^2-4x-16 \equiv 0 \pmod{29}$ c. $x^7 \equiv 17 \pmod{29}$

- **List of suggested activities for Problem Based Learning:**

Sl. No.	Name of the activity	No. of hours	Evaluation Criteria
1	Assignment writing. Numerical based assignment is preferable.	5 assignments of 3h each. Total = 15h	Based on the assignment submitted.
2	Problem solving/Coding using C, C++, Python, SCILAB, MATLAB, MS-EXCEL or any other relevant software	5 small coding-based problems of 3h each. Total = 15h	Based on the coding solution submitted.
3	Technical Video based learning related to the subject	Duration of video = 5h Report preparation & Presentation = 10h Total = 15h	Report /presentation based on the video learning outcomes.
4	Discussion on research paper based on relevant subject	3 research paper = 15h	Summarize research paper and evaluation critical parameters
5	Poster/chart/power point preparation on technical topics	Duration = 10 h	Based on poster/chart preparation and presentation skills
6	Application/Software development	Duration = 15 h	Depending on the complexity of the Application/Software
7	Group Discussion on emerging/trending technical topics based on subject	Duration = 1 h each	Based on performance in group discussion, technical depth, knowledge etc.
8	Seminar / Presentation	Duration for study and preparation=5h Report writing=3h Presentation=2h Total=10h	Topic can be selected technical content beyond syllabus
9	Real world case studies-based learning	Duration of data collection/study = 5h Report preparation = 10h Total = 15h	Based on in-depth study, technical depth, data collected, fact finding, etc.
10	Working/non-working model on technical topics	Working = 12 h Non- working = 8 h	Based on inter department/external evaluation
11	Self-learning on-line course	Minimum duration of the course should be 15h.	Examination based assessment at the end of course. Based on the certificate produced.
12	Complex problem solving	Maximum 3 problem. Study of the problem and solution finding, Total = 15h	Based on the depth of the solution submitted.

13	Industry/Research laboratory visit	Visit = 5h, Report preparation = 5h Total = 10h	Based on report submitted. Report should contain observations and calculations based on industry/ lab data.
14	Videos on Industrial safety aspects based on subject	Duration of video = 5h Report preparation = 5h Total = 10h	Based on quiz/report submitted
15	Industrial exposure for 2-3 days to observe and provide tentative solutions on society/environment /health/any other issue	Duration = 15 h for industrial exposure Problem identification and tentative solution = 10 h Total = 20 h	Based on evaluation of critical problems and solutions

Note:

- All the suggested activity should be related to the subject.
- Min 3 activities must be carried out as per the availability of faculties and students.
- The number of hours is suggestive. Faculty can sub-divide the number of hours based on the activity. However, total number of hours is fixed.
- Rubrics for the evaluation can be prepared by the faculty.