GUJARAT TECHNOLOGICAL UNIVERSITY

Bachelor of Engineering Syllabus

Subject Code : 3144803

Subject Name : Number Theory

WEF Academic Year:	2023-24
Semester:	04
Category of the Course:	Basic Science

Prerequisite:	Basic algebra of numbers, mathematical logic, basic set theory, well ordering principles, the division algorithm, Euclidean algorithm, and unique factorization theorem for integers, equivalence relations, functions, mathematical induction and Binomial Theorem, abstract algebra.
Rationale:	Number theory explores the properties of numbers and the relationships between numbers. From understanding the relationship between different numbers to learning about the unique properties of prime or rational numbers. Number theory and its applications give a detailed understanding of how numbers work in real life. To enhance privacy, confidentiality, and the security of data vast knowledge of number theory is required.

Course Scheme:

Teaching Scheme			Total Credits	Assessment Pattern and Marks				Total Marks
				Theory		Practical		
L	T	PR	C	ESE (E)	PA(M)	ESE (V)	PA (I)	
03	00	02	04	70	30	30	20	150

Course Content:

Sr. No.	Course Content	No. of Hours	% of Weightage
1	**Introduction to Number Theory:** Divisibility , The Division Algorithm, The Greatest Common Divisor, The Euclidean Algorithm, Extended Euclidean Algorithm, The Diophantine equation $a\,x + b\,y = c$. **Primes and Their Distribution:** Primes, Prime Counting Function, Statement of Prime Number Theorem, The Fundamental Theorem of Arithmetic, The Sieve of Eratosthenes, Mersenne Primes, Fibonacci numbers, The Goldbach Conjecture. (All theorems and Corollaries statements included are without proof)	08	20%
2	**Theory of Congruence:** Congruence, Linear Congruence, Congruence Classes, Basic Properties of Congruence, Binary and Decimal Representation of Numbers, Special	08	20%

	Divisibility, Complete and Reduced Residue Systems, The Chinese Remainder Theorem. **Fermat's Theorem:** Fermat's Little Theorem, Pseudoprimes, Perfect Numbers, Pythagorean Triplets, Continued Fractions, Wilson's Theorem. The Fermat - Kraitchik Factorization Method. (All theorems and Corollaries statements included are without proof)		
3	**Number Theoretic Functions:** The Sum and Number of Divisors, The Greatest Integer Function, The Mobius Function(μ), The Divisor Functions (σ_k; for $k \geq 0$ integer), Properties of These Functions, Multiplicative Functions, The Functions σ and r, The Mobius Inversion Formula, An application to the Calendar. **Euler's Generalization of Fermat's Theorem:** Euler's Phi-function, Euler's Theorem, Some Properties of the Phi-function. (All theorems and Corollaries statements included are without proof)	08	20%
4	**Primitive Roots and Indices:** The Order of an Integer of an integer Modulo n, Primitive roots for Primes, Composite Numbers having Primitive Roots, The theory of Indices. **The Quadratic Reciprocity Law:** Euler's Criterion, Quadratic Residues, The Legendre Symbol and Its properties, Quadratic Reciprocity law, Quadratic Congruence with composite moduli, The Jacobi Symbol and Its Properties (All theorems and Corollaries statements included are without proof)	10	20%
5	**Introduction to Cryptography:** From Caesar Cipher to Public-Key Cryptography, The Knapsack Cryptosystem, An application of Primitive Roots to Cryptography, RSA cryptosystem, RSA encryption, RSA decryption and examples on them.	08	20%
	Total		**100**

Reference Books:

1. David M. Burton, Elementary Number Theory. 7th Edition, Tata McGraw Hill Edition, Indian reprint, 2023.
2. Hardy, G.H., and Edward M. Wright. An Introduction to the Theory of Numbers. Oxford University Press, 1960.
3. Neville Robinns, Beginning Number Theory, 2nd Edition, Indian Student Edition, Jones & Bartlett
4. Thomas Koshy, Elementary Number Theory with Applications, 2nd Edition, Academic Press, 2007.

5. Ireland, Kenneth F., and Michael I. Rosen. A Classical Introduction to Modern Number Theory. Springer, 1990.
6. James S. Kraft, Lawrence C. Washington, An Introduction to Number Theory with Cryptography, CRC Press, 2013.
7. William Stallings, Cryptography and Network security: Principles and Practice, Pearson Education, 2002.

Course Outcome:

After Completion of the Course, Student will able to:

No	Course Outcomes	RBT Level*
01	demonstrate knowledge and critical understanding of the well-established principles within Number Theory	RM, UN, AP
02	demonstrate the capability to use a range of established techniques and a reasonable level of skill in calculation and manipulation of the material to solve problems in the following areas: integers, prime numbers, congruences, arithmetic functions, quadratic residues, Diophantine equation	RM, UN, AP
03	apply the concepts and principles in Number Theory in well-defined contexts	RM, UN, AP
04	apply number theoretical algorithms to cryptography.	UN, AP, AN, EL
05	make appropriate use of different tools and techniques.	AN, EL,CR

*RM: Remember, UN: Understand, AP: Apply, AN: Analyze, EL: Evaluate, CR: Create

Suggested Course Practical List:

The practical on some of the following topics/subtopics/concepts may be given for hands-on practice.

1. division algorithm
2. primes and composite numbers
3. linear congruence, congruence classes
4. Wilson's theorem
5. Euclidean Algorithm, Extended Euclidean Algorithm
6. Chinese remainder theorem
7. Pythagorean triplets and continued fractions
8. various number-theoretic functions
9. primitive roots and indices
10. quadratic residues.
11. quadratic congruence with composite moduli
12. cryptography: Public-Key Cryptosystems, The Knapsack Cryptosystem
13. RSA cryptosystem
14. cryptography: RSA encryption, RSA decryption

List of Laboratory/Learning Resources Required:

1. https://nptel.ac.in/courses
2. https://nptel.ac.in/courses/111103020/
3. https://nptel.ac.in/courses/111101137
4. https://nptel.ac.in/courses/111104138
5. https://nptel.ac.in/courses/106103015
6. https://nptel.ac.in/courses/106105162
7. https://nptel.ac.in/courses/106106221
8. https://doc.sagemath.org/html/en/tutorial/

* * * * * * *