Course Type	Course Code	Name of Course	L	T	P	Credit
DE	NCSD521	COMPUTATIONAL NUMBER THEORY	3	0	0	3

Course Objective
To give students a detailed description of the main modern algorithms in computational number theory.
Learning Outcomes
To use the modern algorithms in computational number theory for searching information in targeted areas such as cryptography, coding theory.

Unit No.	Topics to be Covered	Lecture Hours	Learning Outcome
1.	Introduction, Prime Number Theorem, Goldbach and Twin Primes conjectures, Fermat primes, Mersenne primes, Euler primes, Miller-Robinson primes.	6	Understanding the different prime numbers
2.	Euclid's algorithm, LCM, Theorem of arithmetic, Canonical prime factorization, Dirichlet's Theorem on primes in arithmetic progressions.	5	Understanding the Euclid's algorithm and others
3.	Algebraic Structure: Groups, Ring, Field, Extension field.	7	Understanding the different Algebraic Structure
4.	Modular arithmetic, Congruence: Linear congruence in one variable, CRT, Wilson theorem, Fermat's theorem, Pseudo primes, Carmichael numbers.	7	Understanding the modular arithmetic, Congruence related theorems
5.	Arithmetic functions: Multiplicative functions, Moebius function, Euler phi function, Perfect numbers, Legendre symbol, Jacobi symbol.	5	Understanding the various Arithmetic functions
6.	Continued Fractions.	2	Understanding the Continued Fractions
7.	Quadratic residue: Quadratic congruence with primes and composites, Exponentiation and Logarithm.	5	Understanding the Quadratic residues
8.	Elliptic Curves: Curve over real numbers and GF(2^n)	5	Understanding the Elliptic Curves
Total		42	

Text Books:

1. "Elementary Number Theory: Primes, Congruences, and Secrets: A Computational Approach," by William Stein, 1st Edition, Springer, 2009.
2. "A Computational Introduction to Number Theory and Algebra," by Victor Shoup, 2nd Edition, Cambridge University Press, 2008.
3. "Computational Number Theory and Modern Cryptography," by Song Y. Yan, 1st Edition, John Wiley & Sons, 2013.
4. "Elementary Number Theory with Applications," by Thomas Koshy, 2nd Edition, Academic Press, 2007.

Reference Books:

1. "Elementary Number Theory," By David M. Burton, 7th Edition, McGraw Hill, 2023.
2. "Elementary number theory and its applications," By K. H. Rosen, 6th Edition, Addison-Wesley, 2010.