**B.Tech III Year I Semester**

# JNTUA COLLEGE OF ENGINEERING (AUTONOMOUS) PULIVENDULA

## 19ABS22-NUMBER THEORY

**(Open Elective -I)**

| L | T | P | C |
|---|---|---|---|
| 3 | 0 | 0 | 3 |

**Course Objectives:** This course aims at providing the basic knowledge

- To understand basic concepts of Number theory and
- To analyze the applications of Riemann Zeta Function and Dirichlet L Function of Number theory related to real word problems of engineering, biological science etc.

### UNIT – 1: Divisibility and Primes & Congruences 9 Hrs

**Divisibility and Primes:**

Division algorithm, Euclid's algorithm for the greatest common divisor- Linear Diophantine equations - Prime numbers, fundamental theorem of arithmetic, infinitude of primes- Distribution of primes, twin primes, Goldbach conjecture - Fermat and Mersenne primes - Primality testing and factorization.

**Congruences:**

Modular arithmetic- Linear congruences- Simultaneous linear congruences, Chinese Remainder Theorem- An extension of Chinese Remainder Theorem (with non-coprime moduli).

**Learning Outcomes:**

At the end of this unit, the student will be able to

- Learn Division algorithm, Euclid's algorithm etc. L2
- Analyze linear congruences- Simultaneous linear congruences, and Chinese Remainder Theorem. L3

### UNIT – II: Congruences with a Prime-Power Modulus, Euler's Function and RSA Cryptosystem, and Units Modulo an Integer

**Congruences with a Prime-Power Modulus:**

Arithmetic modulo p, Fermat's little theorem, Wilson's theorem - Pseudo-primes and Carmichael numbers- Solving congruences modulo prime powers.

**Euler's Function and RSA Cryptosystem:**

Definition of Euler function, examples and properties - Multiplicative property of Euler's function - RSA cryptography.

**Units Modulo an Integer:**

The group of units modulo an integer, primitive roots- Existence of primitive roots.

**Learning Outcomes:**

At the end of this unit, the student will be able to

- Analyze the Congruences with a Prime-Power Modulus L3
- Analyze the Euler's Function, RSA Cryptosystem and Units Modulo an Integer L4

### UNIT – III: Quadratic Residues and Quadratic Forms

Quadratic residues, Legendre symbol, Euler's criterion- Gauss lemma, law of quadratic reciprocity- Quadratic residues for prime-power moduli and arbitrary moduli- Binary quadratic forms, equivalent forms- Discriminant, principal forms, positive definite forms, indefinite forms- Representation of a number by a form, examples- Reduction of positive definite forms, reduced forms- Number of proper representations, automorph, class number.

**Learning Outcomes:**

At the end of this unit, the student will be able to

- Analyze the Quadratic residues L3
- Analyze the Quadratic Forms L4

### UNIT – IV: Sum of Powers, Continued Fractions and Pell's Equation

**Sum of Powers:**

Sum of two squares, sum of three squares, Waring's problem- Sum of four squares-Fermat's Last Theorem.

**Continued Fractions and Pell's Equation:**

Finite continued fractions, recurrence relation, Euler's rule- Convergents, infinite continued fractions, representation of irrational numbers- Periodic continued fractions and quadratic irrationals- Solution of Pell's equation by continued fractions.

**Learning Outcomes:**

At the end of this unit, the student will be able to

- Compute sum of powers and learn Fermat's last theorem. **L3**
- Solve Pell's equation by continued fractions **L4**

### UNIT – V: Arithmetic Functions, The Riemann Zeta Function and Dirichlet L Function

**Arithmetic Functions:**

Definition and examples, multiplicative functions and their properties- Perfect numbers, Mobius function and its properties- Mobius inversion formula- Convolution of arithmetic functions.

**The Riemann Zeta Function and Dirichlet L Function:**

Historical background for the Riemann Zeta function, Euler product formula, convergence. - Applications to prime numbers- Dirichlet L-functions, Products of two Dirichlet L functions, Euler product formula.

**Learning Outcomes:**

At the end of this unit, the student will be able to

- Analyze the arithmetic functions **L3**
- Analyze the Riemann Zeta function and its Applications to prime numbers **L4**

**Text Books:**

1. G. A. Jones & J.M. Jones, Elementary Number Theory, Springer UTM, 2007.
2. Niven, H. S. Zuckerman & H.L. Montgomery, Introduction to the Theory of Numbers, Wiley, 2000.
3. D. Burton; Elementary Number Theory, McGraw-Hill, 2005

**Reference Books:**

1. Tom M. Apostol, Introduction to Analytical Number theory, Narosa Publishing house, 1998.
2. Elementary number theory and its applications, BEL laboratories.

**Course Outcomes:**

At the end of this Course the student will be able to

- Understand the basic concepts such as Learn Division algorithm, Euclid's algorithm etc. **L1**
- Analyze the Congruences with a Prime-Power Modulus and RSA Cryptosystem. **L2**
- Analyze the Quadratic residues and Quadratic forms. **L3**
- Solve Pell's equation by continued fractions **L4**
- Analyze the real word problem through the technique of Number theory. **L5**

*****