

COURSE NAME: NUMBER THEORY

COURSE CODE: MAT606

Course Credit: 4

SYLLABUS

Distribution of Primes and Theory of Congruencies

Divisibility theory, Linear Diophantine equation, Prime numbers, gcd, lcm, Prime counting function, Goldbach conjecture,

Twin-prime conjecture, Odd perfect numbers conjecture, Fermat and Mersenne primes, Congruence relation and its properties, Linear congruence and Chinese remainder theorem, Fermat's little theorem, Wilson's theorem.

Number Theoretic Functions

Number theoretic functions for sum and number of divisors, Multiplicative function, The Möbius inversion formula, Greatest integer function, Euler's ϕ -function and properties, Euler's theorem.

Primitive Roots

Order of an integer modulo n , Primitive roots for primes, Composite numbers having primitive roots, Perfect Number, Mersenne prime.

Definition of quadratic residue of an odd prime, Euler's criterion.

Quadratic Reciprocity Law

The Legendre symbol and its properties, Quadratic reciprocity Law, Quadratic congruencies with composite moduli.

Applications

Public key encryption, RSA encryption and decryption with applications in security systems.

References and Suggested Readings

1. **Burton, David M**, *Elementary Number Theory*. 7th ed., McGraw-Hill Education, 2011.
2. **Niven, Ivan, Herbert S. Zuckerman, and Hugh L. Montgomery**. *An Introduction to the Theory of Numbers*. 5th ed., Wiley, 1991.
3. **Pundir, Sudhir K., and Rajiv Pundir**, *Algebra and Number Theory*. Pragati Prakashan, 2010.
4. **Titu Andreescu, and Dorin Andrica**, *Number Theory: Structures, Examples, and Problems*. Birkhäuser, 2009.
5. **Hugh L. Montgomery and Robert C. Vaughan**, *Multiplicative Number Theory I: Classical Theory*, Cambridge University Press.
6. **H. Iwaniec and E. Kowalski**, *Analytic Number Theory*, American Mathematical Society, 2004.
7. **T. Koshy**, *Elementary Number Theory with Applications*, Academic Press.