Number Theory - Web course

COURSE OUTLINE

Division algorithm, Euclid's algorithm, linear Diophantine equations, prime numbers, fundamental theorem of arithmetic, distribution of primes, Fermat and Mersenne primes, primality testing and factorization.

Modular arithmetic, linear congruences, Chinese Remainder Theorem, arithmetic modulo p, pseudoprimes and Carmichael numbers, Euler function, RSA cryptography, group of units modulo an integer, primitive roots.

Quadratic residues, Legendre symbol, Gauss lemma, quadratic reciprocity.

Binary quadratic forms, equivalent forms, discriminant, positive definite forms, representation of a number by a form, reduction of positive definite forms, reduced forms, class number, sum of two and four squares.

Continued fractions, Convergents, Periodic continued fractions and quadratic irrationals, Pell's equation.

Arithmetic functions, Convolution, Mobius inversion formula.

Riemann Zeta function, Applications to prime numbers, Dirichlet L-fuctions, Euler product.

COURSE DETAIL

Module 1: Divisibility and Primes	
Lecture 1	Division algorithm, Euclid's algorithm for the greatest common divisor.
Lecture 2	Linear Diophantine equations.
Lecture 3	Prime numbers, fundamental theorem of arithmetic, infinitude of primes.
Lecture 4	Distribution of primes, twin primes, Goldbach conjecture.
Lecture 5	Fermat and Mersenne primes.
Lecture 6	Primality testing and factorization.
Module 2: Congruences	
Lecture 7	Modular arithmetic.

NP-TEL

NPTEL

http://nptel.iitm.ac.in

Mathematics

Additional Reading:

1. H. Davenport, The Higher Arithmetic, Cambridge University Press, 2008.

Coordinators:

Dr. Anupam Saikia
Department of MathematicsIIT Guwahati

Lecture 8	Linear congruences.
Lecture 9	Simultaneous linear congruences, Chinese Remainder Theorem.
Lecture 10	An extension of Chinese Remainder Theorem (with non-coprime moduli).
Module 3: Congruences with a Prime-Power Modulus	
Lecture 11	Arithmetic modulo p, Fermat's little theorem, Wilson's theorem.
Lecture 12	Pseudo-primes and Carmichael numbers.
Lecture 13	Solving congruences modulo prime powers.
Module 4: Euler's Function and RSA Cryptosystem	
Lecture 14	Definition of Euler function, examples and properties.
Lecture 15	Multiplicative property of Euler's function.
Lecture 16	RSA cryptography.
Module 5: Units Modulo an Integer	
Lecture 17	The group of units modulo an integer, primitive roots.
Lecture 18	Existence of primitive roots.
Module 6: Quadratic Residues and Quadratic Forms	
Lecture 19	Quadratic residues, Legendre symbol, Euler's criterion.
Lecture 20	Gauss lemma, law of quadratic reciprocity.
Lecture 21	Quadratic residues for prime-power moduli and arbitrary moduli.
Lecture 22	Binary quadratic forms, equivalent forms.
Lecture 23	Discriminant, principal forms, positive definite forms, indefinite forms.

Lecture 24	Representation of a number by a form, examples.
Lecture 25	Reduction of positive definite forms, reduced forms.
Lecture 26	Number of proper representations, automorph, class number.
Module 7: Sum of Powers	
Lecture 27	Sum of two squares, sum of three squares, Waring's problem.
Lecture 28	Sum of four squares.
Lecture 29	Fermat's Last Theorem.
Module 8: Continued Fractions and Pell's Equation	
Lecture 30	Finite continued fractions, recurrence relation, Euler's rule.
Lecture 31	Convergents, infinite continued fractions, representation of irrational numbers.
Lecture 32	Periodic continued fractions and quadratic irrationals.
Lecture 33	Solution of Pell's equation by continued fractions.
Module 9: Arithmetic Functions	
Lecture 34	Definition and examples, multiplicative functions and their properties.
Lecture 35	Perfect numbers, Mobius function and its properties.
Lecture 36	Mobius inversion formula.
Lecture 37	Convolution of arithmetic functions.
Module 10: The Riemann Zeta Function and Dirichlet L-Function	
Lecture 38	Historical background for the Riemann Zeta function, Euler product formula, convergence.

Lecture 39	Applications to prime numbers.
Lecture 40	Dirichlet L-functions, Products of two Dirichlet L-functions, Euler product formula.

References:

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.