- S. Lang, Linear Algebra, Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1989.
- P. Lax, Linear Algebra, John Wiley & Sons, New York,. Indian Ed. 1997
- H.E. Rose, Linear Algebra, Birkhauser, 2002.
- S. Lang, Algebra, 3rd Ed., Springer (India), 2004.
- O. Zariski and P. Samuel, Commutative Algebra, Vol. I, Springer, 1975.

### MA 403 Real Analysis I 3 1 0 8

Review of basic concepts of real numbers: Archimedean property, Completeness.

*Metric spaces, compactness, connectedness, (with emphasis on*  $\mathbb{R}^{n}$ ).

Continuity and uniform continuity.

Monotonic functions, Functions of bounded variation; Absolutely continuous functions. Derivatives of functions and Taylor's theorem.

Riemann integral and its properties, characterization of Riemann integrable functions. Improper integrals, Gamma functions.

Sequences and series of functions, uniform convergence and its relation to continuity, differentiation and integration. Fourier series, pointwise convergence, Fejer's theorem, Weierstrass approximation theorem.

Texts / References

T. Apostol, Mathematical Analysis, 2nd ed., Narosa Publishers, 2002.

K. Ross, Elementary Analysis: The Theory of Calculus, Springer Int. Edition, 2004.

W. Rudin, Principles of Mathematical Analysis, 3<sup>rd</sup> ed., McGraw-Hill, 1983.

#### MA 419 Basic Algebra 3 1 0 8

Review of basics: Equivalence relations and partitions, Division algorithm for integers, primes, unique factorization, congruences, Chinese Remainder Theorem,
Euler φ-function.

Permutations, sign of a permutation, inversons, cycles and transpositions.

Rudiments of rings and fields, elementary properties, polynomials in one and several variables, divisibility, irreducible polynomials, Division algorithm, Remainder Theorem, Factor Theorem, Rational Zeros Theorem, Relation between the roots and coefficients, Newton's Theorem on symmetric functions, Newton's identities, Fundamental Theorem of Algebra, (statement only), Special cases: equations of

degree 4, cyclic equations.

Cyclotomic polynomials, Rational functions, partial fraction decomposition, unique factorization of polynomials in several variables, Resultants and discriminants.

Groups, subgroups and factor groups, Lagrange's Theorem, homomorphisms, normal subgroups. Quotients of groups, Basic examples of groups (including symmetric groups, matrix groups, group of rigid motions of the plane and finite groups of motions).

Cyclic groups, generators and relations, Cayley's Theorem, group actions, Sylow Theorems.

Direct products, Structure Theorem for finite abelian groups.

Texts / References

M. Artin, Algebra, Prentice Hall of India, 1994.

D.S. Dummit and R. M. Foote, Abstract Algebra, 2nd Ed., John Wiley, 2002.

J.A. Gallian, Contemporary Abstract Algebra, 4<sup>th</sup> ed., Narosa, 1999.

K.D. Joshi, Foundations of Discrete Mathematics, Wiley Eastern, 1989.

T.T. Moh, Algebra, World Scientific, 1992.

S. Lang, Undergraduate Algebra, 2nd Ed., Springer, 2001.

S. Lang, Algebra, 3<sup>rd</sup> ed., Springer (India), 2004.

J. Stillwell, Elements of Algebra, Springer, 1994.

## MA 406 General Topology 3 1 0 8

Prerequiste: MA 403 Real Analysis

Topological Spaces: open sets, closed sets, neighbourhoods, bases, subbases, limit points, closures, interiors, continuous functions, homeomorphisms.

Examples of topological spaces: subspace topology, product topology, metric topology, order topology.

Quotient Topology: Construction of cylinder, cone, Moebius band, torus, etc.

Connectedness and Compactness: Connected spaces, Connected subspaces of the real line, Components and local connectedness, Compact spaces, Heine-Borel Theorem, Local -compactness.

Separation Axioms: Hausdorff spaces, Regularity, Complete Regularity, Normality, Urysohn Lemma, Tychonoff embedding and Urysohn Metrization Theorem, Tietze Extension Theorem.

Tychnoff Theorem, One-point Compacti-fication.

Complete metric spaces and function spaces, Characterization of compact metric spaces, equicontinuity, Ascoli-Arzela Theorem, Baire Category Theorem. Applications: space filling curve, nowhere differentiable continuous function.

Optional Topics:

- 1. Topological Groups and orbit spaces.
- 2. Paracompactness and partition of unity.
- 3. Stone-Cech Compactification.
- 4. Nets and filters.

Texts / References

M. A. Armstrong, Basic Topology, Springer (India), 2004.

K.D. Joshi, Introduction to General Topology, New Age International, New Delhi, 2000.

J.L. Kelley, General Topology, Van Nostrand, Princeton, 1955.

J.R. Munkres, Topology, 2nd Ed., Pearson Education (India), 2001.

G.F. Simmons, Introduction to Topology and Modern Analysis, McGraw-Hill, New York, 1963.

### MA 408 Measure Theory 3 1 0 8

Prerequisite: MA 403 Real Analysis

Semi-algebra, Algebra, Monotone class, Sigma-algebra, Monotone class theorem. Measure spaces.

Outline of extension of measures from algebras to the generated sigma-algebras: Measurable sets; Lebesgue Measure and its properties.

Measurable functions and their properties; Integration and Convergence theorems.

Introduction to  $L^p$ -spaces, Riesz-Fischer theorem; Riesz Representation theorem for  $L^2$  spaces. Absolute continuity of measures, Radon-Nikodym theorem. Dual of  $L^p$ -spaces.

Product measure spaces, Fubini's theorem.

Fundamental Theorem of Calculus for Lebesgue Integrals (an outline).

Texts / Referenes

P.R. Halmos, Measure Theory, Graduate Text in Mathematics, Springer-Verlag, 1979.

Inder K. Rana, An Introduction to Measure and Integration (2<sup>nd</sup> ed.), Narosa Publishing House, New Delhi, 2004.

H.L. Royden, Real Analysis, 3<sup>rd</sup> ed., Macmillan, 1988.

#### MA 410 Multivariable Calculus 2 1 0 6

Prerequisites: MA 403 Real Analysis,

MA 401 Linear Algebra

Functions on Euclidean spaces, continuity, differentiability; partial and directional derivatives, Chain Rule, Inverse Function Theorem, Implicit Function Theorem.

Riemann Integral of real-valued functions on Euclidean spaces, measure zero sets, Fubini's Theorem.

Partition of unity, change of variables.

Integration on chains, tensors, differential forms, Poincare Lemma, singular chains, integration on chains, Stokes' Theorem for integrals of differential forms on chains. (general version). Fundamental theorem of calculus.

Differentiable manifolds (as subspaces of Euclidean spaces), differentiable functions on manifolds, tangent spaces, vector fields, differential forms on manifolds, orientations, integration on manifolds, Stokes' Theorem on manifolds.

Texts / References

V. Guillemin and A. Pollack, Differential Topology, Prentice-Hall Inc., Englewood Cliffe, New Jersey, 1974.

W. Fleming, Functions of Several Variables, 2nd Ed., Springer-Verlag, 1977.

J.R. Munkres, Analysis on Manifolds, Addison-Wesley, 1991.

W. Rudin, Principles of Mathematical Analysis, 3rd ed., McGraw-Hill, 1984.

M. Spivak, Calculus on Manifolds, A Modern Approach to Classical Theorems of Advanced Calculus, W. A. Benjamin, Inc., 1965.

## MA 412 Complex Analysis 3 1 0 8

Complex numbers and the point at infinity. Analytic functions.

Cauchy-Riemann conditions. Mappings by elementary functions. Riemann surfaces. Conformal mappings.

Contour integrals, Cauchy-Goursat Theorem.

Uniform convegence of sequences and series. Taylor and Laurent series. Isolated singularities and residues. Evaluation of real integrals.

Zeroes and poles, Maximum Modulus Principle, Argument Principle, Rouche's theorem.

Texts / References

J.B. Conway, Functions of One Complex Variable, 2<sup>nd</sup> ed., Narosa, New Delhi, 1978.

T.W. Gamelin, Complex Analysis, Springer International Edition, 2001.

R. Remmert, Theory of Complex Functions, Springer Verlag, 1991.

A.R. Shastri, An Introduction to Complex Analysis, Macmilan India, New Delhi, 1999.

## MA 414 Algebra - I 3 1 0 8

Prerequiste: MA 401 Linear Algebra, MA 419

Basic Algebra

Simple groups and solvable groups, nilpotent groups, simplicity of alternating groups, composition series, Jordan-Holder Theorem. Semidirect products. Free groups, free abelian groups.

Rings, Examples (including polynomial rings, formal power series rings, matrix rings and group rings), ideals, prime and maximal ideals, rings of fractions, Chinese Remainder Theorem for pairwise comaximal ideals.

Euclidean Domains, Principal Ideal Domains and Unique Factorizations Domains. Poly-nomial rings over UFD's.

Fields, Characteristic and prime subfields, Field extensions, Finite, algebraic and finitely generated field extensions, Classical ruler and compass constructions, Splitting fields and normal extensions, algebraic closures. Finite fields, Cyclotomic fields, Separable and inseparable extensions.

Galois groups, Fundamental Theorem of Galois Theory, Composite extensions, Examples (including cyclotomic extensions and extensions of finite fields).

Norm, trace and discriminant.

Solvability by radicals, Galois' Theorem on solvability.

Cyclic extensions, Abelian extensions, Trans-cendental extensions.

Texts / References

M. Artin, Algebra, Prentice Hall of India, 1994.

D.S. Dummit and R. M. Foote, Abstract Algebra, 2nd Ed., John Wiley, 2002.

J.A. Gallian, Contemporary Abstract Algebra, 4th Ed., Narosa, 1999.

N. Jacobson, Basic Algebra I, 2nd Ed., Hindustan Publishing Co., 1984, W.H. Freeman, 1985.

# MA 417 Ordinary Differential Equations 3 1 0 8

Review of solution methods for first order as well as second order equations, Power Series methods with properties of Bessel functions and Legendre polynomials.

Existence and Uniqueness of Initial Value Problems: Picard's and Peano's Theorems, Gronwall's inequality, continuation of solutions and maximal interval of existence, continuous dependence.

Higher Order Linear Equations and linear Systems: fundamental solutions, Wronskian, variation of constants, matrix exponential solution, behaviour of solutions.

Two Dimensional Autonomous Systems and Phase Space Analysis: critical points, proper and improper nodes, spiral points and saddle points.

Asymptotic Behavior: stability (linearized stability and Lyapunov methods).

Boundary Value Problems for Second Order Equations: Green's function, Sturm comparision theorems and oscillations, eigenvalue problems.

Texts / References

M. Hirsch, S. Smale and R. Deveney, Differential Equations, Dynamical Systems and Introduction to Chaos, Academic Press, 2004

L. Perko, Differential Equations and Dynamical Systems, Texts in Applied Mathematics, Vol. 7, 2<sup>nd</sup> ed., Springer Verlag, New York, 1998.

M. Rama Mohana Rao, Ordinary Differential Equations: Theory and Applications. Affiliated East-West Press Pvt. Ltd., New Delhi, 1980.

D. A. Sanchez, Ordinary Differential Equations and Stability Theory: An Introduction, Dover Publ. Inc., New York, 1968.

## MA 503 Functional Analysis 3 1 0 8

Prerequisites: MA 401 Linear Algebra,

*MA 408 Measure Theory* 

Normed spaces. Continuity of linear maps. Hahn-Banach Extension and Separation Theorems. Banach spaces. Dual spaces and transposes.

Uniform Boundedness Principle and its applications. Closed Graph Theorem, Open Mapping Theorem and their applications. Spectrum of a bounded operator. Examples of compact operators on normed spaces.

Inner product spaces, Hilbert spaces. Orthonormal basis. Projection theorem and Riesz Representation Theorem.

Texts / References

- J.B. Conway, A Course in Functional Analysis, 2<sup>nd</sup> ed., Springer, Berlin, 1990.
- C. Goffman and G. Pedrick, A First Course in Functional Analysis, Prentice-Hall, 1974.
- E. Kreyzig, Introduction to Functional Analysis with Applications, John Wiley & Sons, New York, 1978.
- B.V. Limaye, Functional Analysis, 2<sup>nd</sup> ed., New Age International, New Delhi, 1996.
- A. Taylor and D. Lay, Introduction to Functional Analysis, Wiley, New York, 1980.

# MA 504 Operators on Hilbert Spaces 2 1 0 6

Prerequisite: MA 503 Functional Analysis

Adjoints of bounded operators on a Hilbert space, Normal, self-adjoint and unitary operators, their spectra and numerical ranges.

 $Compact\ operators\ on\ Hilbert\ spaces.\ Spectral\ theorem\ for\ compact\ self-adjoint\ operators.$ 

Application to Sturm-Liouville Problems.

Texts / References

J.B. Conway, A Course in Functional Analysis, 2<sup>nd</sup> ed., Springer, Berlin, 1990.

C. Goffman and G. Pedrick, First Course in Functional Analysis, Prentice Hall, 1974.

I. Gohberg and S. Goldberg, Basic Operator Theory, Birkhauser, 1981.

E. Kreyzig, Introduction to Functional Analysis with Applications, John Wiley & Sons, New York, 1978.

B.V. Limaye, Functional Analysis, 2nd ed., New Age International, New Delhi, 1996.

## MA 505 Algebra- II 3 1 0 8

Prerequisite: MA 414 Algebra I

Modules, submodules, quotient modules and module homomorphisms.

Generation of modules, direct sums and free modules. Tensor products of modules. Exact sequences, projective modules.

Tensor algebras, symmetric and exterior algebras.

Finitely generated modules over principal ideal domains, invariant factors, elementary divisors, rational canonical forms. Applications to finitely generated abelian groups and linear trans-formations.

Noetherian rings and modules, Hilbert basis theorem, Primary decomposition of ideals in noetherian rings.

Integral extensions, Going-up and Going-down theorems, Extension and contraction of prime ideals, Noether's Normalization Lemma, Hilbert's Nullstellensatz.

Localization of rings and modules. Primary decompositions of modules.

Texts / References

M.F. Atiyah and I. G. Macdonald, Introduction to Commutative Algebra, Addison Wesley, 1969.

D.S. Dummit and R. M. Foote, Abstract Algebra, 2nd Ed., John Wiley, 2002.

N. Jacobson, Basic Algebra I and II, 2nd Ed., W. H. Freeman, 1985 and 1989.

S. Lang, Algebra, 3rd Ed., Springer (India), 2004.

O. Zariski and P. Samuel, Commutative Algebra, Vol. I, Springer, 1975.

#### MA 508 Mathematical Methods 3 1 0 6

Prerequisite: MA 515 Partial Differential

**Equations** 

Asymptotic expansions, Watson's lemma, method of stationary phase and saddle point method. Applications to differential equations. Behaviour of solutions near an irregular singular point, Stoke's phenomenon. Method of strained coordinates and matched asymptotic expansions.

Variational principles, Lax-Milgram theorem and applications to boundary value problems.

Calculus of variations and integral equations. Volterra integral equations of first and second kind.

Iterative methods and Neumann series.

Texts / References

C.M. Bender and S.A. Orszag, Advanced Mathematical Methods for Scientists and Engineers, McGraw-Hill Book Co., 1978.

R. Courant & D.Hilbert, Methods of Mathe-matical Physics, Vol. I & II, Wiley Eastern Pvt. Ltd. New Delhi, 1975.

J. Kevorkian and J.D. Cole, Perturbation Methods in Applied Mathematics, Springer Verlag, Berlin, 1985.

S.G. Mikhlin, Variation Methods in Mathe-matical Physics, Pergaman Press, Oxford 1964.

## MA 510 Introduction to Algebraic Geometry 2 1 0 6

Prerequisite: MA 414

Varieties: Affine and projective varieties, coordinate rings, morphisms and rational maps, local ring of a point, function fields, dimension of a variety.

Curves: Singular points and tangent lines, multiplicities and local rings, intersection multiplicities, Bezout's theorem for plane curves, Max Noether's theorem and some of its applications, group law on a nonsingular cubic, rational parametrization, branches and valuations.

Texts / References

S.S. Abhyankar, Algebraic Geometry for Scientists and Engineers, American Mathe-matical Society, 1990.

W. Fulton, Algebraic Curves, Benjamin, 1969.

J. Harris, Algebraic Geometry: A First Course, Springer-Verlag, 1992.

M. Reid, Undergraduate Algebraic Geometry, Cambridge University Press, Cambridge, 1990.

I.R. Shafarevich, Basic Algebraic Geometry, Springer-Verlag, Berlin, 1974.

R.J. Walker, Algebraic Curves, Springer-Verlag, Berlin, 1950.

# MA 515 Partial Differential Equations 3 1 0 8

Prerequisites:

MA 417 Ordinary Differential Equations.

MA 410 Multivariable Calculus

Cauchy Problems for First Order Hyperbolic Equations: method of characteristics, Monge cone.

Classification of Second Order Partial Differential Equations: normal forms and characteristics.

*Initial and Boundary Value Problems: Lagrange-Green's identity and uniqueness by energy methods.* 

Stability theory, energy conservation and dispersion.

Laplace equation: mean value property, weak and strong maximum principle, Green's function, Poisson's formula, Dirichlet's principle, existence of solution using Perron's method (without proof).

Heat equation: initial value problem, fundamental solution, weak and strong maximum principle and uniqueness results.

Wave equation: uniqueness, D'Alembert's method, method of spherical means and Duhamel's principle.

*Methods of separation of variables for heat, Laplace and wave equations.* 

Texts / References

E. DiBenedetto, Partial Differential Equations, Birkhauser, Boston, 1995.

L.C. Evans, Partial Differential Equations, Graduate Studies in Mathematics, Vol. 19, AMS, Providence, 1998.

F. John, Partial Differential Equations, 3<sup>rd</sup> ed., Narosa Publ. Co., New Delhi, 1979.

E. Zauderer, Partial Differential Equations of Applied Mathematics, 2<sup>nd</sup> ed., John Wiley and Sons, New York, 1989.

## MA 516 Algebraic Topology 3 1 0 8

Prerequiste: MA 406 General Topology

Paths and homotopy, homotopy equivalence, contractibility, deformation retracts.

Basic constructions: cones, mapping cones, mapping cylinders, suspension.

Cell complexes, subcomplexes, CW pairs.

Fundamental groups. Examples (including the fundamental group of the circle) and applications (including Fundamental Theorem of Algebra, Brouwer Fixed Point Theorem and Borsuk-Ulam Theorem, both in dimension two). Van Kampen's Theorem, Covering spaces, lifting properties, deck

transformations. universal coverings (existence theorem optional).

Simplicial complexes, barycentric subdivision, stars and links, simplicial approximation. Simplicial Homology. Singular Homology. Mayer-Vietoris Sequences. Long exact sequence of pairs and triples. Homotopy invariance and excision (without proof).

Degree. Cellular Homology.

Applications of homology: Jordan-Brouwer separation theorem, Invariance of dimension, Hopf's Theorem for commutative division algebras with identity, Borsuk-Ulam Theorem, Lefschetz Fixed Point Theorem.

Optional Topics:

Outline of the theory of: cohomology groups, cup products, Kunneth formulas, Poincare duality.

Texts / References

M.J. Greenberg and J. R. Harper, Algebraic Topology, Benjamin, 1981.

W. Fulton, Algebraic topology: A First Course, Springer-Verlag, 1995.

A. Hatcher, Algebraic Topology, Cambridge Univ. Press, Cambridge, 2002.

W. Massey, A Basic Course in Algebraic Topology, Springer-Verlag, Berlin, 1991.

J.R. Munkres, Elements of Algebraic Topology, Addison Wesley, 1984.

J.J. Rotman, An Introduction to Algebraic Topology, Springer (India), 2004.

H. Seifert and W. Threlfall, A Textbook of Topology, translated by M. A. Goldman, Academic Press, 1980.

J.W. Vick, Homology Theory, Springer-Verlag, 1994.

## MA 518 Spectral Approximation 2 1 0 6

Prerequisite: MA 503 Functional Analysis

Spectral decomposition. Spectral sets of finite type. Adjoint and product spaces.

Convergence of operators: norm, collectively compact and v convergence. Error estimates.

Finite rank approximations based on projections and approximations for integral operators.

A posteriori error estimates.

Matrix formulations for finite rank operators.

Iterative refinement of a simple eigenvalue.

Numerical examples.

Texts / References

M. Ahues, A. Largillier and B. V. Limaye, Spectral Computations for Bounded Operators, Chapman and Hall/CRC, 2000.

- F. Chatelin, Spectral Approximation of Linear Operators, Academic Press, 1983.
- T. Kato, Perturbation Theory of Linear Operators, 2<sup>nd</sup> ed., Springer-Verlag, Berlin, 1980.

# MA 521 Theory of Analytic Functions 2 1 0 6

Prerequisites: MA 403 Real Analysis,

MA 412 Complex Analysis.

Maximum Modulus Theorem. Schwarz Lemma. Phragmen-Lindelof Theorem.

Riemann Mapping Theorem. Weierstrass Factor-ization Theorem.

Runge's Theorem. Simple connectedness. Mittag-Leffler Theorem.

Schwarz Reflection Principle.

Basic properties of harmonic functions.

Picard Theorems.

Texts / References

L. Ahlfors, Complex Analysis, McGraw-Hill, 3<sup>rd</sup> ed., New York, 1979.

J.B. Conway, Functions of One Complex Varliable, 2<sup>nd</sup> ed., Narosa, New Delhi 1978.

T.W. Gamelin, Complex Analysis, Springer International, 2001.

R. Narasimhan, Theory of Functions of One Complex Variable, Springer (India), 2001.

W. Rudin, Real and Complex Analysis, 3<sup>rd</sup> ed., Tata McGraw-Hill, 1987.

# MA 522 Fourier Analysis and Applications 3 1 0 8

Prerequisite: MA 403 Real Analysis

Basic Properties of Fourier Series: Uniqueness of Fourier Series, Convolutions, Cesaro and Abel Summability, Fejer's theorem, Poisson Kernel and Dirichlet problem in the unit disc. Mean square Convergence, Example of Continuous functions with divergent Fourier series.

Distributions and Fourier Transforms: Calculus of Distributions, Schwartz class of rapidly decreasing functions, Fourier transforms of rapidly decreasing functions, Riemann Lebesgue lemma, Fourier Inversion Theorem, Fourier transforms of Gaussians.

Tempered Distributions: Fourier transforms of tempered distributions, Convolutions, Applications to PDEs (Laplace, Heat and Wave Equations), Schrodinger-Equation and Uncertainty principle.

Paley-Wienner Theorems, Poisson Summ-ation Formula: Radial Fourier transforms and Bessel's

functions. Hermite functions.

Optional Topics:

Applications to PDEs, Wavelets and X-ray tomography. Applications to Number Theory.

Texts / References:

R. Strichartz, A Guide to Distributions and Fourier Transforms, CRC Press.

E.M. Stein and R. Shakarchi, Fourier Analysis: An Introduction, Princeton University Press, Princeton 2003.

I. Richards and H. Youn, Theory of Distributions and Non-technical Approach, Cambridge University Press, Cambridge, 1990.

## MA 523 Basic Number Theory 2 1 0 6

Prerequisites: MA 419 Basic Algebra

Infinitude of primes, discussion of the Prime Number Theorem, infinitude of primes in specific arithmetic progressions, Dirichlet's theorem (without proof).

Arithmetic functions, Mobius inversion formula. Structure of units modulo n, Euler's phi function

Congruences, theorems of Fermat and Euler, Wilson's theorem, linear congruences, quadratic residues, law of quadratic reciprocity.

Binary quadratics forms, equivalence, reduction, Fermat's two square theorem, Lagrange's four square theorem.

Continued fractions, rational approximations, Liouville's theorem, discussion of Roth's theorem, transcendental numbers, transcendence of "e" and "pi".

Diophantine equations: Brahmagupta's equation (also known as Pell's equation), the Thue equation, Fermat's method of descent, discussion of the Mordell equation.

Optional Topics:

Discussion of Waring's problem.

Discussion of the Bhargava-Conway "fifteen theorem" for positive definite quadratic forms.

The RSA algorithm and public key encryption.

Primality testing, discussion of the Agrawal-Kayal-Saxena theorem.

Catalan's equation, discussion of the Gelfond-Schneider theorem, discussion of Baker's theorem.

Texts / References

W.W. Adams and L.J. Goldstein, Introduction to the Theory of Numbers, 3rd ed., Wiley Eastern, 1972.

A. Baker, A Concise Introduction to the Theory of Numbers, Cambridge University Press, Cambridge, 1984.

I. Niven and H.S. Zuckerman, An Introduction to the Theory of Numbers, 4th Ed., Wiley, New York, 1980.

#### MA 524 Algebraic Number Theory 2 1 0 6

Prerequisites: MA 505 Algebra - II (Exposure)

Algebraic number fields.

Localisation, discrete valuation rings.

Integral ring extensions, Dedekind domains, unique factorisation of ideals. Action of the galois group on prime ideals.

Valuations and completions of number fields, discussion of Ostrowski's theorem, Hensel's lemma, unramified, totally ramified and tamely ramified extensions of p-adic fields.

Discriminants and Ramification.

Cyclotomic fields, Gauss sums, quadratic reciprocity revisited.

The ideal class group, finiteness of the ideal class group, Dirichlet units theorem.

Texts / References

K. Ireland and M. Rosen, A Classical Introduction to Modern Number Theory, 2nd ed., Springer-Verlag, Berlin, 1990.

S. Lang, Algebraic Number Theory, Addison- Wesley, 1970.

D.A. Marcus, Number Fields, Springer-Verlag, Berlin, 1977.

## MA 525 Dynamical Systems 2 1 0 6

Prerequisite: MA 417 Ordinary Differential Equations

Review of stability for linear systems. Flow defined by nonlinear systems of ODEs, linearization and stable manifold theorem. Hartman-Grobman theorem. Stability and Lyapunov functions. Planar flows: saddle point, nodes, foci, centers and nonhyperbolic critical points. Gradient and Hamiltonian systems. Limit sets and attractors. Poincare map, Poincare Benedixson theory and Poincare index.

Texts / References

- V.I. Arnold, Ordinary Differential Equations, rentice Hall of India, New Delhi, 1998.
- M.W. Hirsch and S. Smale, Differential Equations, Dynamical Systems and inear Algebra, Academic Press, NY, 174.
- L. Perko, Differential Equations and Dynamical Systems, Springer Verlag, NY, 1991.
- S. Wiggins, Introduction to Applied Nonlinear Dynamical Systems and Chaos, TAM Vol.2, Springer-Verlag, NY, 1990.

### MA 526 Commutative Algebra 2 1 0 6

Prerequisites: MA 505 Algebra - II

Dimension theory of affine algebras: Principal ideal theorem, Noether normalization lemma, dimension and transcendence degree, catenary property of affine rings, dimension and degree of the Hilbert polynomial of a graded ring, Nagata's altitude formula, Hilbert's Nullstellensatz, finiteness of integral closure.

### Hilbert-Samuel polynomials of modules:

Associated primes of modules, degree of the Hilbert polynomial of a graded module, Hilbert series and dimension, Dimension theorem, Hilbert-Samuel multiplicity, associativity for-mula for multiplicity,

## Complete local rings:

Basics of completions, Artin-Rees lemma, associated graded rings of filtrations, completions of modules, regular local rings

## Basic Homological algebra:

Categories and functors, derived functors, Hom and tensor products, long exact sequence of homology modules, free resolutions, Tor and Ext, Koszul complexes.

## Cohen-Macaulay rings:

Regular sequences, quasi-regular sequences, Ext and depth, grade of a module, Ischebeck's theorem, Basic properties of Cohen-Macaulay rings, Macaulay's unmixed theorem, Hilbert-Samuel multiplicity and Cohen-Macaulay rings, rings of invariants of finite groups.

## Optional Topics:

- 1. Face rings of simplicial complexes, shellable simplicial complexes and their face rings.
- 2. Dedekind Domains and Valuation Theory.

## Text/References

- D. Eisenbud, Commutative Algebra (with a view toward algebraic geometry) Graduate Texts in Mathematics 150, Springer-Verlag, Berlin, 2003.
- H. Matsumura, Commutative ring theory, Cambridge Studies in Advanced Mathematics No. 8, Cambridge University Press, Cambridge, 1980.
- W. Bruns and J. Herzog, Cohen-Macaulay Rings, (Revised edition) Cambridge Studies in Advanced

Mathematics No. 39, Cambridge University Press, Cambridge, 1998.

## MA 530 Nonlinear Analysis 2 1 0 6

Prerequisites: MA 503 Functional Analysis.

Fixed Point Theorems with Applications: Banach contraction mapping theorem, Brouwer fixed point theorem, Leray-Schauder fixed point theorem.

Calculus in Banach spaces: Gateaux as well as Frechet derivatives, chain rule, Taylor's expansions, Implicit function theorem with applications, subdifferential.

Monotone Operators: maximal monotone operators with properties, surjectivity theorem with applications.

Degree theory and condensing operators with applications.

Texts / References

M.C. Joshi and R.K. Bose, Some Topics in Nonlinear Functional Analysis, Wiley Eastern Ltd., New Delhi, 1985.

E. Zeilder, Nonlinear Functional Analysis and Its Applications, Vol. I (Fixed Point Theory), Springer Verlag, Berlin, 1985.

## MA 532 Analytic Number Theory 2 1 0 6

Prerequisites: MA 414 Algebra - I

MA 412 Complex Analysis

The Wiener-Ikehara Tauberian theorem, the Prime Number Theorem.

Dirichlet's theorem for primes in an Arithmetic Progression.

Zero free regions for the Riemann-zeta function and other L-functions.

Euler products and the functional equations for the Riemann zeta function and Dirichlet L-functions.

Modular forms for the full modular group, Eisenstein series, cusp forms, structure of the ring of modular forms.

Hecke operators and Euler product for modular forms.

The L-function of a modular form, functional equations.

Modular forms and the sums of four squares.

Optional topics:

1. Discussion of L-functions of number fields and the Chebotarev Density Theorem.

- 2. Phragmen-Lindelof Principle, Mellin inversion formula, Hamburger's theorem.
- 3. Discussion of Modular forms for congruence subgroups.
- 4. Discussion of Artin's holomorphy conjecture and higher reciprocity laws.
- 5. Discussion of elliptic curves and the Shimura-Taniyama conjecture (Wiles' Theorem)

#### *Text / References:*

- S. Lang, Algebraic Number Theory, Addison-Wesley, 1970.
- J.P. Serre, A Course in Arithmetic, Springer-Verlag, 1973.
- T. Apostol, Introduction to Analytic Number Theory, Springer-Verlag, 1976

## MA 533 Advanced Probability Theory 2 1 0 6

Probability measure, probability space, construction of Lebesgue measure, extension theorems, limit of events, Borel-Cantelli lemma.

Random variables, Random vectors, distributions, multidimensional distributions, independence.

Expectation, change of variable theorem, convergence theorems.

Sequence of random variables, modes of convergence. Moment generating function and characteristics functions, inversion and uniqueness theorems, continuity theorems, Weak and strong laws of large number, central limit theorem.

Radon Nikodym theorem, definition and properties of conditional expectation, conditional distributions and expectations.

Texts / References

- P. Billingsley, Probability and Measure, 3<sup>rd</sup> ed., John Wiley & Sons, New York, 1995.
- J. Rosenthal, A First Look at Rigorous Probability, World Scientific, Singapore, 2000.
- A.N. Shiryayev, Probability, 2<sup>nd</sup> ed., Springer, New York, 1995.
- K.L. Chung, A Course in Probability Theory, Academic Press, New York, 1974.

## **Differential Equations 2 1 0 6**

Prerequisites: MA 503 Functional Analysis

MA 515 Partial Differential

Equations.

Theory of distributions: supports, test functions, regular and singular distributions, generalised derivatives.

Sobolev Spaces: definition and basic properties, approximation by smooth functions, dual spaces, trace and imbedding results (without proof).

Elliptic Boundary Value Problems: abstract variational problems, Lax-Milgram Lemma, weak solutions and wellposedness with examples, regularity result, maximum principles, eigenvalue problems.

Semigroup Theory and Applications: exponential map,  $C_0$ -semigroups, Hille-Yosida and Lummer-Phillips theorems, applications to heat and wave equations.

Texts / References

S. Kesavan, Topics in Functional Analysis Wiley Eastern Ltd., New Delhi, 1989.

M. Renardy and R.C. Rogers, An Introduction to Partial Differential Equations, 2<sup>nd</sup> ed., Springer Verlag International Edition, New York, 2004.

L.C. Evans, Partial Differential Equations, AMS, Providence, 1998.

# MA 538 Representation Theory of Finite Groups 2 1 0 6

Prerequisite : MA 414 Algebra I

Representations, Subrepresentations, Tensor products, Symmetric and Alternating Squares.

Characters, Schur's lemma, Orthogonality relations, Decomposition of regular represent-ation, Number of irreducible representations, canonical decomposition and explicit decompositions. Subgroups, Product groups, Abelian groups. Induced representations.

Examples: Cyclic groups, alternating and symmetric groups.

Integrality properties of characters, Burnside's

 $p^a q^b$  theorem. The character of induced representation, Frobenius Reciprocity Theorem, Meckey's irreducibility criterion, Examples of induced representations, Representations of supersolvable groups.

Texts / References

M. Burrow, Representation Theory of Finite Groups, Academic Press, 1965.

N. Jacobson, Basic Algebra II, Hindustan Publishing Corproation, 1983.

S. Lang, Algebra, 3<sup>rd</sup> ed. Springer (India) 2004.

J.P. Serre, Linear Representation of Groups, Springer-Verlag, 1977.

# MA 539 Spline Theory and Variational Methods 2 0 2 6

Even Degree and Odd Degree Spline Interpolation, end conditions, error analysis and order of convergence. Hermite interpolation, periodic spline interpolation. B-Splines, recurrence relation for B-splines, curve fitting using splines, optimal quadrature.

Tensor product splines, surface fitting, orthogonal spline collocation methods.

Texts / References

C. De Boor, A Practical Guide to Splines, Springer-Verlag, Berlin, 1978.

H.N. Mhaskar and D.V. Pai, Fundamentals of Approximation Theory, Narosa Publishing House, New Delhi, 2000.

P.M. Prenter, Splines and Variational Methods, Wiley-Interscience, 1989.

# MA 540 Numerical Methods for Partial Differential Equations 2 1 0 6

Prerequisite: MA 515 Partial Differential

**Equations** 

Finite differences: grids, derivation of difference equations. Elliptic equations, discrete maximum principle and stability, residual correction methods (Jacobi, Gauss-Seidel and SOR methods), LOD and ADI methods. Finite difference schemes for initial and boundary value problems: Stability (matrix method, von-Neumann and energy methods), Lax-Richtmyer equivalence Theorem. Parabolic equations: explicit and implicit methods (Backward Euler and Crank-Nicolson schemes) with stability and convergence, ADI methods. Linear scalar conservation law: upwind, Lax-Wendroff and Lax-Friedrich schemes and CFL condition.

Lab Component: Exposure to MATLAB and computational experiments based on the algorithms discussed in the course.

Texts / References

R. Mitchell and S. D. F. Griffiths, The Finite Difference Methods in Partial Differential Equations, Wiley and Sons, NY, 1980.

G.D. Smith, Numerical Solutions of Partial Differential Equations, 3rd Edition, Calrendorn Press, Oxford, 1985.

J.C. Strikwerda, Finite difference Schemes and Partial Differential Equations, Wadsworth and Brooks/ Cole Advanced Books and Software, Pacific Grove, California, 1989.

J.W. Thomas, Numerical Partial Differential Equations: Finite Difference Methods, Texts in Applied Mathematics, Vol. 22, Springer Verlag, NY, 1999.

J.W. Thomas, Numerical Partial Differential Equations: Conservation Laws and Elliptic Equations, Texts in Applied Mathematics, Vol. 33, Springer Verlag, NY, 1999.

#### MA 556 Differential Geometry 2 1 0 6

Prerequiste: MA 410 Multivariable Calculus

Graphs and level sets of functions on Euclidean spaces, vector fields, integral curves of vector fields, tangent spaces.

Surfaces in Euclidean spaces, vector fields on surfaces, orientation, Gauss map.

Geodesics, parallel transport, Weingarten map.

Curvature of plane curves, arc length and line integrals.

Curvature of surfaces.

Parametrized surfaces, local equivalence of surfaces.

Gauss-Bonnet Theorem, Poincare-Hopf Index Theorem.

Texts / References

M. doCarmo, Differential Geometry of Curves and Surfaces, Prentice Hall, 1976.

B. O'Neill, Elementary Differential Geo-metry, Academic Press, New York, 1966.

J.J. Stoker, Differential Geometry, Wiley-Interscience, 1969.

J.A. Thorpe, Elementary Topics in Differential Geometry, Springer (India), 2004.

# MA 562 Mathematical Theory of Finite Elements 2 1 0 6

Prerequisite: MA 515 Partial Differential

Equations

MA 503 Functional Analysis

Sobolev Spaces: basic elements, Poincare inequality. Abstract variational formulation and elliptic boundary value problem. Galerkin formulation and Cea's Lemma. Construction of finite element spaces. Polynomial approximations and interpolation errors.

Convergence analysis: Aubin-Nitsche duality argument; non-conforming elements and numerical integration; computation of finite element solutions.

Parabolic initial and boundary value problems: semidiscrete and completely discrete schemes with convergence analysis.

Lab component: Implementation of algorithms and computational experiments using MATLAB.

Texts / References

K.E. Brenner and R. Scott, The Mathematical Theory of Finite Element Methods, Springer-Verlang, Berlin, 1994.

P.G. Ciarlet, The Finite Element Methods for Elliptic Problems, North Holland, Amsterdam, 1978.

- C. Johnson, Numerical solutions of Partial Differential Equations by Finite Element Methods, Cambridge University Press, Cambridge, 1987.
- C. Mercier, Lectures on Topics in Finite Element Solution of Elliptic Problems, TIFR Lectures on Mathematics and Physics Vol. 63, Narosa Publ. House, New Delhi, 1979.

# MA 581 Elements of Differential Topology 2 1 0 6

Prerequisite: MA 410 Multivariable

Calculus

Differentiable Manifolds in  $\mathbb{R}^n$ : Review of inverse and implicit function theorems; tangent spaces and tangent maps; immersions; submersions and embeddings.

Regular Values: Regular and critical values; regular inverse image theorem; Sard's theorem; Morse lemma.

Transversality: Orientations of manifolds; oriented and mod 2 intersection numbers; degree of maps. Application to Fundamental theorem of Algebra.

\*Lefschetz theory of vector fields and flows: Poincare-Hopf index theorem; Gauss-Bonnet theorem.

\*Abstract manifolds: Examples such as real and complex projective spaces and Grassmannian varieties; Whitney embedding theorems.

(\* indicates expository treatment intended for these parts of the syllabus.)

Texts / References

- 1. A. Dubovin, A.T. Fomenko, S.P. Novikov, Modern Geometry Methods and Applications II, The Geometry and Topology of Manifolds, GTM 104, Springer-Verlag, Berlin, 1985.
  2.
- V. Guillemin and A Pollack, Differential Topology Prentice-Hall Inc., Englewood Cliffs, New Jersey, 1974.
- J. Milnor, Topology from the Differential View-point, University Press of Virginia, Charlottsville 1990.

### SI 421 Introduction to Mathematical Software 0 0 3 3

Introduction to following topics using mathematical softwares:

Linear Algebra: Solution of linear systems by elimination, Pivoting strategy, least squares problems, eigenvalue problem.

Euler's Method

The Second Order and Fourth Order Runge Kutta Methods

First Order differential equations; IVP for ODE systems of First Order equations.

Second Order differential equations

Predictor – Correction method

Combinatorics: Making lists of combinatorial objects, generating random combinatorial objects (like sets, permutations, partitions etc.), Tree Search, Graph search: Breadth and depth first search Mathematical packages such as MATLAB, MATHEMATICA, MAPLE etc. will be introduced to solve problems in Linear Algebra, Differential Equations, Numerical Analysis, Combinatorics etc.

#### **Texts / References**

Chapman, MATLAB programming for Engineers, Thomson Learning (3 Edition – 2005)
Wolfram, The MATHEMATICA book (5 Edition), Wolfram Media – 2003

rЛ

#### SI 402 Statistical Inference 3 1 0 8

*Prerequisite:SI 417 Introduction to* 

*Probability Theory* 

Distribution of functions of random variables, Order Statistics. Estimation - loss function, risk, minimum risk unbiased estimators, maximum likelihood estimation, method of moments, Bayes estimation. Sufficient Statistics, completeness, Basu's Theorem, exponential families, invariance and maximal invariant statistics.

Testing of Hypotheses - parametric and non-parametric problems, examples with data analytic applications.

Confidence Intervals.

#### **Texts / References**

G. Casella and B.L. Berger, Statistical Inference, Wadsworth and Brooks, Pacific Grove, 1990.

M.H. DeGroot, Probability and Statistics, Addison-Wesley, 1986

E.L.Lehmann and G. Casella, Theory of Point Estimation, Springer-Verlag, New York, 1998.

## SI 422 Regression Analysis 2 1 0 6

Prerequisites: SI 417 Introduction to

*Probability Theory* 

Simple and multiple linear regression models %G—%@ estimation, tests and confidence regions. Check for normality assumption. Likelihood ratio test, confidence intervals and hypotheses tests; tests for distributional assumptions. Collinearity, outliers; analysis of residuals, Selecting the \$(B!H(BBest\$(B!I(B regression equation, transformation of response variables. Ridge's regression.

Texts / Reference

B.L. Bowerman and R.T. O'Connell, Linear Statistical Models: An Applied Approach, PWS-KENT Pub., Boston, 1990

N.R Draper. And H. Smith., Applied Regression Analysis, John Wiley and Sons (Asia) Pvt. Ltd., Series in Probability and Statistics, 2003.

D.C. Montgomery, E.A. Peck, G.G. Vining, Introduction to Linear Regression Analysis, John Wiley, NY, 2003

A.A. Sen and M. Srivastava, Regression Analysis %G–%@ Theory, Methods & Applications, Springer-Verlag, Berlin, 1990.

## SI 417 Introduction to Probability Theory 3 1 0 8

Axioms of Probability, Conditional Prob-ability and Independence, Random variables and distribution functions, Random vectors and joint distributions, Functions of random vectors.

Expectation, moment generating functions and characteristic functions, Conditional expectation and distribution.

Modes of convergence, Weak and strong laws of large numbers, Central limit theorem.

## Text / References

- P. Billingsley, Probability and Measure, II Edition, John Wiley & Sons (SEA) Pvt. Ltd., 1995.
- P.G. Hoel, S.C. Port and C.J. Stone, Introduction to Probability, Universal Book Stall, New Delhi, 1998.
- J.S. Rosenthal, A First Look at Rigourous Probability Theory, World Scientific. 2000.
- M. Woodroofe, Probability with Applica-tions, McGraw-Hill Kogakusha Ltd., Tokyo, 1975.

#### SI 412 Algorithms 3 1 0 8

Prerequisite: None. For non-Math department students, consent of Instructor required to register. Tools for Analysis of Algorithms (Asymptotics, Recurrence Relations). Basic Data Structures (Lists, Stacks, Queues, Trees, Heaps) and applications.

Sorting, Searching and Selection (Binary Search, Insertion Sort, Merge Sort, QuickSort, Radix Sort, Counting Sort, Heap Sort etc.. Median finding using Quick-Select, Median of Medians). Basic Graph Algorithm (BFS, DFS, strong components etc.).

Algorithm Design Paradigms: Divide and Conquer. Greedy Algorithms (for example, some greedy scheduling algorithms, Dijkstra's Shortest Paths algorithm, Kruskal's Minimum Spanning Tree Algorithm). Dynamic Programming (for example, dynamic programming algorithms for optimal polygon triangulation, optimal binary search tree, longest common subsequence, matrix chain multiplication, all pairs shortest paths).

Introduction to NP-Completeness (polynomial time reductions, verification algorithms, classes P and NP, NP-hard and NP-complete problems).

## Texts / References

- R. Sedgewick, Algorithms in C++, Addison-Wesley, 1992.
- T. Cormen, C. Leiserson, R. Rivest and C. Stein, Introduction to Algorithms, MIT Press, 2001.
- M.A. Weiss, Data Structures and Algorithms Analysis in C++, Addison-Wesley, 1999.

#### SI 419 Combinatorics 2 1 0 6

Prerequisites: None. Non-math department students need the consent of the Instructor to register.

Algorithms and Efficiency. Graphs: Paths, Cycles, Trees, Coloring. Trees, Spanning Trees, Graph Searching (DFS, BFS), Shortest Paths. Bipartite Graphs and Matching problems. Counting on Trees and Graphs. Hamiltonian and Eulerian Paths.

Groups: Cosets and Lagrange Theorem, Cyclic Groups etc.. Permutation Groups, Orbits and Stabilizers. Generating Functions. Symmetry and Counting: Polya Theory. Special Topics (depending upon the instructor!)

Text / References

Normal L. Biggs, Discrete Mathematics, Oxford University Press, Oxford, 2002.

J. Hein, Discrete Structures, Logic and Computatibility, Jones and Barlett, 2002.

C.L.Liu, Elements of Discrete Mathematics, McGraw Hill, 1986

### SI 416 Optimization 2 0 2 6

Prerequisites: None. Non-math department students need the consent of the Instructor to register.

Unconstrained optimization using calculus (Taylor's theorem, convex functions, coercive functions). Unconstrained optimization via iterative methods (Newton's method, Gradient/conjugate gradient based methods, Quasi-Newton methods).

Constrained optimization (Penalty methods, Lagrange multipliers, Kuhn-Tucker conditions. Linear programming (Simplex method, Dual simplex, Duality theory). Modeling for Optimization.

Text / Reference

M. Bazarra, C. Shetty, Nonlinear Progra-mming, Theory and Algorithms, Wiley, 1979. Beale, Introduction to Optimization, John Wiley, 1988.

M.C. Joshi and K. Moudgalya, Optimization: Theory and Practice,
Narosa, New Delhi, 2004

# SI 418 Advanced Programming and Unix Environment 0 0 3 3

UNIX programming environment (file system and directory structure, and processes). Unix tools (shell scripting, grep, tar, compress, sed, find, sort etc). Graphical User Interface Programming using Java. Multithreaded programming in Java. Socket programming in Java.

Text / Reference

3. Eckel, Thinking In Java, <a href="http://www.bruceeckel.com/javabook.html">http://www.bruceeckel.com/javabook.html</a>

- B. Forouzan and R. Gilberg, Unix and Shell Programming: A Textbook, 3rd ed., Brooks/Cole, 2003.
- B.W. Kernighan and R. Pike, Unix Programming Environment, Prentice Hall, 1984.

## SI 404 Applied Stochastic Processes 2 1 0 6

Prerequisite: SI 417 Introduction to Probability Theory or MA 212

Stochastic processes: Description and definition. Markov chains with finite and countably infinite state spaces. Classification of states, irreduci-bility, ergodicity. Basic limit theorems.

Markov processes with discrete and continu-ous state spaces. Poisson process, pure birth process, birth and death process. Brownian motion.

Applications to queueing models and relia-bility theory.

Basic theory and applications of renewal processes, stationary processes. Branching processes. Markov Renewal and semi-Markov processes, regenerative processes.

Texts / References:

V.N. Bhat, Elements of Applied Stochastic Processes, Wiley, 1972.

V.G. Kulkarni, Modeling and Analysis of Stochastic Systems, Chapman and Hall, London, 1995.

- J. Medhi, Stochastic Models in Queueing Theory, Academic Press, 1991.
- R. Nelson, Probability, Stochastic Processes, and Queuing Theory: The Mathematics of Computer Performance Modelling, Springer-Verlag, New York, 1995.
- S. Ross, Stochastic Processes, 2<sup>nd</sup> ed., Wiley, New York, 1996.

## SI 501 Topics in Theoretical Computer Science 3 1 0 8

Introduction to Complexity Theory (P, NP, NP-hard, NP-complete etc.). Automata Theory and Formal Languages (finite automata, NFA, DFA, regular languages, equivalence of DFA and NFA, minimization of DFA, closure properties of regular languages, regular grammars, context free grammars, parse-trees, Chomsky Normal Form, top-down parsing).

Randomization and Computation (Monte Carlo and Las Vegas algorithms, Role of Markov and Chebyscheff's inequalities, Chernoff bounds in randomized algorithms, applications of probabilistic method).

Special Topics in Theoretical Computer Science, such as Approximation Algorithms, Number Theoretic Algorithms, Logic and Computability.

- G. Ausiello, P. Crescenzi, G. Gambosi, V. Kann, A. Marchetti-Spaccamela, Complexity and Approximation, Springer Verlag, Berlin, 1999.
- J. Hein, Discrete Structures, Logic and Computatibility, Jones and Barlett, 2002.
- P. Linz, An Introduction to Formal Languages and Automata, Narosa, New Delhi, 2004.

## SI 503 Categorical Data Analysis 3 1 0 8

Prerequisites: SI 422 Regression Analysis

Two-way contingency tables: Table structure for two dimensions. Ways of comparing proportions. Measures of associations. Sampling distributions. Goodness-of-fit tests, tests of independence. Exact and large sample inference. Three-way contingency tables.

Models for binary response variables. Logistic regression-dichotomous response. Logistic regression-polytomous response. Probit and extreme value models. Log-linear models for two and three dimensions. Fitting of logit and log-linear models. Log-linear models for ordinal variables.

Multi-category Logit Models.

Applications using SAS software.

Texts/ References:

- A. Agresti, Analysis of Categorical Data, Wiley, 1990.
- A. Agresti, An Introduction to Categorical Data Analysis, Wiley, New York, 1996.
- E.B. Andersen, The Statistical Analysis of Categorical Data, Springer-Verlag, Berlin, 1990.
- T.J. Santner and D. Duffy, The Statistical Analysis of Discrete Data, Springer-Verlag, Berlin, 1989.

## SI 505 Multivariate Analysis 3 1 0 8

Prerequisites: SI 402 statistical Inference

K-variate normal distribution. Estimation of the mean vector and dispersion matrix. Random sampling from multivariate normal distribution. Multivariate distribution theory. Discriminant and canonical analysis. Factor analysis. Principal components.

Distribution theory associated with the analysis.

Texts / References

- T.W. Anderson, An Introduction to Multivariate Statistical Analysis, 2<sup>nd</sup> Ed., Wiley, 1984.
- R. Gnanadesikan, Methods for Statistical Data Analysis of Multivariate Observations, John Wiley, New

R.A. Johnson and D.W. Wicheran, Applied Multivariate Statistical Analysis, Upper Saddle River, Prentice Hall, 1998.

M.S. Srivastava and E.M. Carter, An Introduction to Multivariate Statistics, North Holland, 1983.

## SI 507 Numerical Analysis 3 0 2 8

Principles of floating point computations and rounding errors.

Systems of Linear Equations: factorization methods, pivoting and scaling, residual error correction method.

Iterative methods: Jacobi, Gauss-Seidel methods with convergence analysis, conjugate gradient methods.

Eigenvalue problems: only implementation issues.

Nonlinear systems: Newton and Newton like methods and unconstrained optimization.

Interpolation: review of Lagrange interpolation techniques, piecewise linear and cubic splines, error estimates.

Approximation: uniform approximation by polynomials, data fitting and least squares approximation.

Numerical Integration: integration by interpolation, adaptive quadratures and Gauss methods

Initial Value Problems for Ordinary Differential Equations: Runge-Kutta methods, multi-step methods, predictor and corrector scheme, stability and convergence analysis.

Two Point Boundary Value Problems : finite difference methods with convergence results.

Lab. Component: Implementation of algorithms and exposure to public domain packages like LINPACK and ODEPACK.

Texts / References

K.E. Atkinson, An Introduction to Numerical Analysis, Wiley, 1989.

S.D. Conte and C. De Boor, Elementary Numerical Analysis %G–%@ An Algorithmic Approach, McGraw-Hill, 1981.

K. Eriksson, D. Estep, P. Hansbo and C. Johnson, Computational Differential Equations, Cambridge Univ. Press, Cambridge, 1996.

G.H. Golub and J.M. Ortega, Scientific Computing and Differential Equations: An Introduction to Numerical Methods, Academic Press, 1992.

J. Stoer and R. Bulirsch, Introduction to Numerical Analysis, 2nd ed., Texts in Applied Mathematics, Vol. 12, Springer Verlag, New York, 1993.

Recap of Linear Programming and duality. Transportation and Assignment. Maximum flow and minimum cut (duality, Ford and Fulkerson algorithm, polynomial time algorithms).

Minimum Cost Flows (cycle cancelling algorithms, successive path algorithms). Matching (bipartite matching, weighted bipartite matching, cardinality general matching).

Routing algorithms (Bellman Ford algorithm in computer networks, Dijkstra's algorithm in computer networks), Application of network models.

Text / Reference

R.K. Ahuja, T.L. Magnanti, J.B. Orlin, Network Flows, Prentice Hall, 1993

D. Bertsekas, Network Optimization: Continuos and Discrete Models, Athena Scientific, 1998

M.S. Bazaraa, J.J. Jarvis, H.D. Sherali, Linear Programming and Network Flows, Second Edition, 1990

## SI 509 Time Series Analysis 2 1 0 6

Prerequisites: SI 402 Statistical Inference

Stationary processes %G–%@ strong and weak, linear processes, estimation of mean and covariance functions. Wald decomposition Theorem.

Modeling using ARMA processes, estimation of parameters testing model adequacy, Order estimation.

Prediction in stationery processes, with special reference to ARMA processes. Frequency domain analysis %G-%(a) spectral density and its estimation, transfer functions.

ARMAX, ARIMAX models and introduction to ARCH models.

Multivariate Time Series, State Space Models.

Texts / References

P. Brockwell and R. Davis, Intoduction to Time Series and Forecasting, Springer, Berlin, 2000.

G.E.P. Box, G. Jenkins and G. Reinsel, Time Series Analysis-Forecasting and Control, 3<sup>rd</sup> ed., Pearson Education, 1994.

C. Chatfield, The Analysis of Time Series %G–%@ An Introduction, Chapman and Hall / CRC, 4<sup>th</sup> ed., 2004.

# SI 511 Computer-Aided Geometric Design 3 0 0 6

Polynomial curves: Bezier representation, Bernstein polynomials, Blossoming, de Castlijau algorithm. Derivatives in terms of Bezier polygon. Degree elevation. Subdivi-sion. Nonparametric Bezier curves.

Composite Bezier curves.

Spline curves: Definition and Basic properties of spline functions, B-spline curves, de Boor algorithm. Derivatives. Insertion of new knots. Cubic spline interpolation. Inter-pretation of parametric continuity in terms of Bezier polygon.

Geometric continuity. Frenet frame continuity. Cubic Beta splines and significance of the associated parameters.

Tensor product surfaces. Bezier patches. Tri-angular patch surfaces.

Texts / References:

G. Frain, Curves and Surfaces for Computer Aided Geometric Design: A Practical Guide, Academic Press, 1988.

L. Ramshaw, Blossoming: A Connect-the-Dots Approach to Splines, DEC systems Research Center, Report no. 19, 1987.

## SI 512 Finite Difference Methods for Partial Differential Equations

Description: Review of 2nd order PDEs: Classification, separation of variables and fourier transform techniques. Automatic mesh generation techniques: Structure mesh (transfinite interpolation), unstructured grids (triangulation for polygonal and non - polygonal domains). Finite difference Methods: Elliptic equations (SOR and conjugate gradient methods, ADI schemes), parabolic equations (explicit, back - ward Euler and Crank - Nicolson method, LOD), hyperbolic equations (Law - Wendroff scheme, Leapfrod method, CFL conditions), Stability, consistency and convergence results. Lab Component: Implementation of Algorithms developed in this course and exposure to software packages: ODEPACK and MATLAB.

Text/References: Gene H. Golub and James M. Ortega, Scientific Computing and Differential Equations: An Introduction to Numerical Methods, Academic Press, 1992.P. Knupp and S. Steinberg, Fundamentals of Grid Generation, CRC Press Inc., Boca Raton, 1994.A. R. Mitchell and D. F. Griffiths, The finite Difference Methods in Partial Differential Equations, Wiley, 1980.G. D. Smith, Numerical Solutions of Partial Differential Equations, Oxford Press, 1985.J. C. Stickwards, Finite Difference Schemes and PDEs, Chapman and Hall, 1989.J. F. Thompson, Z. U., A. Waarsi and C. W. MAstin, Numerical Grid Generations - Foundations and Applications, North Holland, 1985.Erich Zauderer, Partial Differential Equations of Applied Mathematics, 2nd ed., Wiley, 1989.

## SI 513 Theory of Sampling 2 1 0 6

Simple random sampling. Sampling for proportions and percentages.

Estimation of sample size. Stratified random sampling, Ratio estimators. Regression esti-mators. Systematic sampling. Type of sampling unit, Subsampling with units of equal and unequal size. Double sampling. Sources of errors in surveys.

A brief introduction to randomized response techniques and small area estimation

- 1. Chaudhuri and H. Stenger, Survey Sampling: Theory and Methods, Marcell Dekker, 1992.
- W.G. Cochran, Sampling Techniques, 3rd ed., Wiley Eastern, 1977.
- P. Mukhopadhyay, Theory and Methods of Survey Sampling, Prentice-Hall of India, New Delhi, 1998.

Des Raj, Sampling Theory, Tata McGraw-Hill, 1978.

## SI 514 Statistical Modeling 2 1 0 6

Prerequisites: SI 402 Statistical Inference

Nonlinear regression, Nonparametric regression, generalized additive models, Bootstrap methods, kernel methods, neural network, Artificial Intelligence, a few topics from machine learning.

Texts / References:

- T. Hastie, and R. Tibshirani, Generalized Additive Models, Chapman and Hall, London, 1990.
- G.A.F. Seber, and C.J. Wild, Nonlinear Regression, John Wiley & Sons, 1989.
- W. Hardle, Applied Nonparametric Regression, Cambridge University Press, London, 1990.

# SI 515 Statistical Techniques in Data Mining 2 1 0 6

Pre-requisite: p SI 402 Statistical Inference

Introduction to Data Mining and its Virtuous Cycle.

Cluster Analysis: Hierarchical and Non-hierarchical techniques. Classification and Discriminant Analysis Tools: CART, Random forests, Fisher's discriminant functions and other related rules, Bayesian classification and learning rules.

Dimension Reduction and Visualization Techniques: Multidimensional scaling, Principal Component Analysis, Chernoff faces, Sun-ray charts.

Algorithms for data-mining using multiple nonlinear and nonparametric regression.

Neural Networks: Multi-layer perceptron, predictive ANN model building using back-propagation algorithm. Exploratory data analysis using Neural Networks %G—%@ self organizing maps. Genetic Algorithms, Neuro-genetic model building.

Discussion of Case Studies.

*Texts/References:* 

L. Breiman, J.H. Friedman, R.A. Olschen and C.J. Stone, Classification of Regresion Trees, Wadsowrth Publisher, Belmont, CA, 1984.

D.J. Hand, H. Mannila and P. Smith, Principles of Data Minng, MIT Press, Cambridge, MA 2001.

M.H. Hassoun, Fundamentals of Artificial Neural Networks, Prentice-Hall of India, New Delhi 1998.

T. Hastie, R. Tibshirani & J. H. Friedman, The elements of Statistical Learning: Data Mining, Inference & Prediction, Springer Series in Statistics, Springer-Verlag, New York 2001.

R.A. Johnson and D.W. Wichern, Applied Multivariate Analysis, Upper Saddle River, Prentice-Hall, N.J. 1998.

S. James Press, Subjective and Objective Bayesian Statistics: Principles, Models, and Applications, 2nd Edition, Wiley, 2002.

## SI 525 Testing of Hypothesis 2 1 0 6

Prerequisites: SI 402 Statistical Inference

Statistical hypotheses, Neyman-Pearsaon fundmeantal lemma, Monotone likelihood ratio, confidence bounds, generalization of fundamental lemma, two-sided hypotheses.

Unbiased tests, UMP unbiased tests, applications to standard distributions, similarity and completion, Pemutation tests; most powerful permutation tests.

Symmetry and invariance, most powerful invariant tests, unbiased and invariance.

Tests with guaranteed power, maxi-min tests and invariance. Likelihood ratio tests and its properties.

Texts / References

E.L. Lehmann, Testing Statistical Hyp-otheses, 2<sup>nd</sup> ed. Wiley, 1986.

T.S. Ferguson, Mathematical Statistics: A Decision Theoretic Approach, Academic Press, New York, 1967.

G. Casella and R.L. Berger, Statistical Infwerence, Wordsworth & Brooks, California, 1990.

## SI 526 Experimental Designs 2 0 2 6

Prerequisites: SI 402 Statistical Inference

Linear Models and Estimators, Estimability of linear parametric functions. Gauss-Markoff Theorem. One-way classification and two-way classification models and their analyses. Standard designs such as CRD, RBD, LSD, BIBD. Analysis using the missing plot technique.

Fctorial designs. Confounding. Analysis using Yates' algorithm. Fractional factorial.

A brief introduction to Random Effects models and their analyses.

A brief introduction to special designs such as split-plot, strip-plot, cross-over designs.

Response surface methodology.

Applications using SAS software.

Texts / References

A.M. Kshirsagar, A First Course in Linear Models, Marcel Dekker, 1983.

D.C. Montgomery, Design and Analysis of Experiments, 3rd Ed., John Wiley & Sons, 1991. C.F.J. Wu and M. Hamada, Experiments: Planning Analysis, and Parameter Design Optimization, John Wiley & Sons, 2002.

## SI 527 Introduction to Derivatives Pricing 2 1 0 6

Prerequisites: SI 417 Introduction to

Probability Theory

Basic notions %G–%@ Cash flow, present value of a cash flow, securities, fixed income securities, types of markets.

Forward and futures contracts, options, properties of stock option prices, trading strategies involving options, option pricing using Binomial trees, Black %G–%@ Scholes model, Black %G–%@ Scholes formula, Risk-Neutral measure, Delta %G–%@ hedging, options on stock indices, currency options.

Texts / References

D.G. Luenberger, Investment Science, Oxford University Press, Oxford, 1998.

J.C. Hull, Options, Futures and Other Derivatives, 4<sup>th</sup> ed., Prentice-Hall, New York, 2000.

J.C. Cox and M. Rubinstein, Options Market, Englewood Cliffs, N.J.: Prentice Hall, 1985.

*C.P Jones, Investments, Analysis and Measurement,* 5<sup>th</sup> ed., John Wiley and Sons, New York, 1996. **SI 528 Biostatistics 2 1 0 6** 

Pre-requisite: SI 402 Statistical Inference

Introduction to clinical trials and other types of clinical research, bias and random error in clinical studies, overview of Phase I-IV trials, multi-center trials; randomized, controlled clinical trials; concept of blinding/masking in clinical trials.

Design of Phase 1-3 clinical trials: parallel vs. cross-over designs, cross-sectional vs. longitudinal

designs, review of factorial designs, objectives and endpoints of clinical trials, formulation of appropriate hypotheses (equivalence, non-inferiority, etc.); sample size calculation; design for bioequivalence/

bioavailability trials, sequential stopping in clinical trials.

Analysis of Phase 1-3 trials: Use of generalized linear models; analysis of categorical outcomes, Bayesian and non-parametric methods; analysis of survival data from clinical trials

Epidemiological studies: case-control and cohort designs; odds ratio and relative risk; logistic and multiple regression models.

## Texts/ References:

- S.C. Chow and J.P. Liu, Design and Analysis of Clinical Trials Concepts & Methodologies, John Wiley & Sons, NY, 1998.
- S.C. Chow and J.P. Liu, Design and Analysis of Bioavailability & Bioequivalence Studies, Marcel Dekker, 2000.
- W.W. Daniel, Biostatistics: A Foundation for Analysis in the Health Sciences (6th ed.), John Wiley, New York, 2002.
- J.L. Fleiss, The Design and Analysis of Clinical Experiments, John Wiley & Sons, 1986.
- D.W. Hosmer and S. Lemeshow, Applied Logistic Regression, John Wiley and Sons, NY, 1989.
- E. Vittinghoff, D.V. Glidden, S.C. Shiboski and C.E. McCulloch, Regression Methods in Biostatistics, Springer Verlag, 2005.
- J.G. Ibrahim, M-H Chen and D. Sinha, Bayesian survival analysis, Springer, NY, 2001.

## SI 530 Statistical Quality Control 2 1 0 6

Total quality control in an industry. Quality planning, quality conformance, quality ad-herence. Quality assurance and quality management functions.

Control charts and allied techniques. Concept of quality and meaning of control. Concept of inevitability of variation-chance and assign-able causes. Pattern of variation. Principles of rational sub-grouping.

Different types of control charts. Concept of process capability and its comparison with design specifications, CUSUM charts.

Acceptance sampling. Sampling inspection versus 100 percent inspection. Basic concepts of attributes and variables inspection. OC curve, Single, double, multiple and sequential sampling plans, Management and organisation of quality control.

## Texts / References:

- A.J. Duncan, Quality Control and Industrial Statistics, 5th ed., Richard D. Irwin, 1986.
- E.L. Grant and R. Levenworth, Statistical Quality Control, 6<sup>th</sup> ed., McGraw-Hill, 1988.
- J.M. Juran and F. M. Grayna, Quality Planning and Analysis, Tata McGraw-Hill, 1970.

- D.C. Montgomery, Introduction to Statistical Quality Control, Wiley, 1985.
- T.P. Ryan, Statistical Methods for Quality Improvement, Wiley, New York, 2000.

### SI 532 Statistical Decision Theory 2 1 0 6

Prerequisite: SI 402 Statistical Inference

Decision functions, Risk functions, utility and subjective probability, Randomization,

Optimal decision rules. Admissibility and completeness, Existence of Bayes Decision Rules, Existence of a Minimal complete class, Essential completeness of the class of non-randomized rules. The minimax theorem.

Invariant statistical decision problems. Multiple decision problems.

Sequential decision problems.

Texts / References

- J.O. Berger, Statistical Decision Theory: Foundations, Concepts and Methods, Springer-Verlag, 1980.
- J.O. Berger, Statistical Design Theory and Bayesian Analysis, 2<sup>nd</sup> ed., Springer-Verlag, 1985.
- T.S. Ferguson, Mathematical Statistics, Academic Press, New York, 1967.
- S.S. Gupta and D. Huang, Multiple Statistical Decision Theory, Springer-Verlag, New York, 1981.

## SI 534 Nonparametric Statistics 2 1 0 6

Prerequisite: SI 402, Statistical Inference

Kolmogorov-Smirnov Goodness-of %G-%@Fit Test.

The empirical distribution and its basic properties. Order Statistics. Inferences concerning Location parameter based on one-sample and two-sample problems. Inferences concerning Scale parameters. General Distribution Tests based on Two or More Independent Samples.

Tests for Randomness and equality of distributions. Tests for Independence. The one-sample regression problem.

Asymptotic Relative Efficiency of Tests. Confidence Intervals and Bounds

Texts / References

W.W. Daniel, Applied Nonparametric Statistics, 2<sup>nd</sup> ed., Boston: PWS-KENT, 1990.

M. Hollandor, and D.A. Wolfe, Non-parametric Statistical Inference, McGraw-Hill, 1973.

- E.L. Lehmann, Nonparametric Statistical Methods Based on Ranks, McGraw-Hill, 1975.
- J.D. Gibbons, Nonparametric Statistical Inference Marcel Dekker, NewYork, 1985

- R.H. Randles and D.A. Wolfe, Introduction to the Theory of Nonparametric Statistics, Wiley, New York, 1979.
- P. Sprent, Applied Nonparametric Statistical Methods, Chapman and Hall, London, 1989
- B.C. Arnold, N. Balakrishnan and H. N. Nagaraja, First Course in Order Statistics. John Wiley, NewYork, 1992
- J.K. Ghosh and R.V. Ramamoorthi, Bayesian Nonparametrics, Springer Verlag, NY, 2003.

# SI 540 Stochastic Programming and Applications 3 0 0 6

Quadratic and Nonlinear Programming solution methods applied to Chance Constrained Pro-gramming problems. Stochastic Linear and Non-linear Progra-mming Problems. Applications in inventory control and other industrial systems, opti-mization of queuing models of computer networks, information processing under uncertainty. Two stage and multi-stage solution techniques. Dynamic programming with Recourse. Use of Monte Carlo, probabilistic and heuristics algorithms. Genetic algorithms and Neural networks for adaptive optimization in random environment.

#### **Texts / References**

- J.R. Birge, and F. Louveaux: Introduction to Stochastic Programming. Springer, New York, 1997.
- V.V. Kolbin, Stochastic programming, D. Reidel Publications, Dordrecht, 1977
- S.S. Rao Engineering Optimization: Theory and Practice. 3rd Ed., John Wiley & Sons Inc., NY 1996/2002.
- J.K. Sengupta, Stochastic Optimizations and Economic Models. D. Reidel Publications, Dordrecht, 1986.
- K. Marti: Stochastic Optimization Methods. Springer, 2005
- Y. Ermoliev and R.J-B. Wets, Numerical Techniques for Stochastic Optimization, .Springer Verlag, Berlin, 1988.
- Z. Michaeleawicz, General Algorithms + Data Structures Evolution Program. Springer-Verlag, Berlin, 1992.
- R. J.-B. Wets and W. T. Ziemba (eds.): Stochastic Programming: State of the Art, 1998, Annals of Oper. Res. 85, Baltzer, Amsterdam, 1999.

# SI 542 Mathematical Theory of Reliability 2 1 0 6

Pre-requisites: SI 402 Statistical Inference

Coherent Structures, Reliability of systems of independent components, Bounds of system reliability, shape of the system reliability function, notion of ageing, parametric families of life distributions with monotone failure rate, classes of life distributions based on notions of ageing, classes of distributions in

replacement policies. Limit distributions for series and parallel systems. Statistical inferential aspects for (i) standard reliability models, (ii) parametric and non-parametric classes of aging distributions.

## Texts / References

- H. Ascher and H. Feingold, Repairable Systems Reliability: Modeling, Inference, Mis-conceptions and Their Causes, Marcel Dekker, 1984.
- L.J. Bain and M. Engelhardt, Statistical Analysis of Reliability and Life Testing Models: Theory and Methods, Marcel Dekker, New York, 1991.
- R.E. Barlow and F. Proschan, Statistical Theory of Reliability and Life Testing, Holt, Reinhart and Winston, 1975.
- J.D. Kalbfleisch and R.L. Prentice, The Statistical Analysis of Failure Time Data, Wiley, 1986.
- J.F. Lawless, Statistical Models and Methods for Life Time Data, John Wiley & Sons, 1982.
- S.K. Sinha, Reliability and Life Testing, Wiley Eastern, New Delhi, 1986.

# CS 101 Computer Programming & Utilization 2 0 2 6

Functional organization of computers, algorithms, basic programming concepts, FORTRAN language programming. Program testing and debugging, Modular programming subroutines: Selected examples from Numerical Analysis, Game playing, sorting/searching methods, etc.

## Texts / References

N.N. Biswas, FORTRAN IV Computer Programming, Radiant Books, 1979.

K.D. Sharma, Programming in Fortran IV, Affiliated East West, New Delhi, 1976.

#### CS 206 Formal Methods in CS 2 0 1 6

Propositional Logic and First Order Logic: Syntax and semantics. Proof systems such as Hilbert, Natural Deductions, Sequent and Resolution, Clasual Form, Herbrand Theorem, Unification and Resolution Theorem Proving, Applications of logic to Program Specification and Verification: specification of Abstract Data Types, Hoare logic, assertions, invariants, weakest preconditions, Formal models of programs: Complete partial orders as domains, continuous functions, domain constructors, fix point. Denotational semantic of a while-do language.

### *Text/References:*

- D. Gries, The Science of Programming, Springer-Verlag, 1977.
- R.C. Backhouse, Program Construction and Verification, Prentice Hall, 1986.
- W.K. Grassman and J.P. Tremblay, Logic and Discrete Mathematics %G–%@ a Computer Science Perspective, Prentice Hall, 1991.
- J. Loeckxm, H.D. Ehrich and M. Wolf, Specifications of Abstract Data Types, Wiley-Teubner, 1996.
- J. Gallier, Logic for Computer Science: Foundations of Automated Theorem Proving, Wiley, 1981. D.A. Schmidt, Denotational Semantics: A Methodology for Language Development, Allyn and Bacon,

*Inc.*, 1986.

M.J.C. Gordon, Programming Language Theory and its Implementations, Prentice Hall International, 1988.

N. Francez, Program Verification, Addison Wesley, 1992.

## EE 636 Matrix Computations 3 0 0 6

Basic iterative methods for solutions of linear systems and their rates of convergence. Generalized conjugate gradient, Krybov space and Lanczos methods. Iterative methods for symmetric, non-symmetric and generalized eigenvalue problems. Singular value decompositions. Fast computations for structured matrices. Polynomial matrix computations. Perturbation bounds for eigenvalues.

### Texts/Reference:

- O. Axelsson, Iterative Solution Methods, Cambridge University Press, Cambridge 1994.
- G. Meurant, Computer Solution of Large Linear Systems, North Holland, 1999.

Golub and C. Van Loan, Matrix Computations, John Hopkins Press, 1996.

G.W. Stewart and J. Sun, Matrix Perturbation Theory, Academic Press, New York, 1990.

### IT 640 Modern Information System 3 0 0 6

Introduction to Information Systems, Introduction to Database Management Systems, Software Engineering, Information Technology and basic of networking, Internet Technologies, Web and HTML, Distributed systems, Corporate Information systems.

### Texts/References:

N.L. Sada. Structured COBOL, programming with Business Applications, Pitamber Publ. Co., New Delhi, 1991.

- A. Silberschatz, H.F. Korth and S. Sudarshan, Database System Concepts, 3<sup>rd</sup> ed., McGraw-Hill, 1997.
- R.S. Pressman, Software Engineering %G–%@, A Practitioner's Approach, 4<sup>th</sup> ed., McGraw-Hill, 1995.

Object Oriented Modeling and Design, Prentice Hall, 1991.

# EE 649 Finite Fields and Their Applications 3 0 0 6

Basic of finite fields: Groups, rings, fields, polynomials, field extensions, characterization of finite fields, roots of irreducible polynomials, traces, norms, bases, roots of unity, cyclotomic polynomials, representation of elements of finite fields. Wedderbum's theorem, order of polynomials, primitive polynomials, construction of irreducible polynomials, linearized polynomials, binomials, trinomials. Applications to algebraic coding theory: Linear codes, cyclic codes, Goppa codes.

Texts/References:

- R. Lidl and H. Niederreiter, Finite Fields, Cambridge University Press, Cambridge, 1997.
- S. Roman, Coding and Information Theory, Springer Verlag, 1992.
- R. Lidl and H. Niederreiter, Introduction to Finite Fields and Their Applications, Cambridge University Press, 1986, Chapters 1 %G–%@ 3 and 8.

## EE 720 An Introduction to Number Theory and Cryptography 3 0 0 6

Some Topics In Elementary Number Theory: Time estimates for doing arithmetic. Divisibility and the Euclidean algorithm. Congruences. Some applications to factoring.

Finite Fields and Quadratic Residues:

Finite fields, Quadratic residues and reciprocity.

*Cryptography:* 

some simple cryptosystems. Enciphering matrices.

Public Key:

The idea of public key cryptography. RSA. Discrete log.

Elliptic Curves:

Basic facts. Elliptic curve cryptosystems.

Texts/References:

- N. Koblitz, A Course in Number and Theory and Cryptography, Graduate Texts in Mathematics, No.114, Springer-Verlag, New York/Berlin/Heidelberg, 1987.
- A. Baker, A Concise Introduction to the Theory of Numbers, Cambridge University Press, New York/Port Chester/Melbourne/Sydney, 1990.
- A.N. Parshin and I.R. Shafarevich (Eds.), Number Theory, Encyclopaedia of Mathe-matics Sciences, Vol. 49, Springer-Verlag, New York/Berlin/Heidelberg, 1995.
- J. Stillwell, Elements of Number Theory, Undergraduate Texts in Mathematics, Springer-Verlag, New York/Berlin/Heidelberg, 2003.
- H.C.A. van Tilborg, An Introduction to Cryptography, Kluwer Academic Publishers, Boston/Dordrecht/Lancaster, 1988.
- A. Weil, Number Theory for Beginners, Additional references.