Proposed Updated Course Structure for

Ph.D. in Applied Mathematics

(Applicable from session 2022-2023)

20th Boardof Studies

(Held on 20-12-2022)

Department of Applied Mathematics

School of Vocational Studies and Applied Sciences

Gautam Buddha University

Greater Noida, UP-201312

Preamble

The Program Ph.D. In Applied Mathematics was started in 2012 since the inception of the Department of Applied Mathematics. The progression of students belonging to this course is excellent. In the development of this course, we considered various stakeholders e.g. Full time and working professionals. All research scholars will earn14 credits in course work to get this Ph.D. degree.

Selection Procedure

Candidates will be selected on the basis of GBU admission policy.

Table of Contents

Programme Structure

SemesterI

S. No.	Course Code	Course	Category	Hours			Credit
				L	T	P	
2	AS 601	Research Methodology	C	4	0	0	4
3	RPE 601	Research and Publication Ethics	C	2	0	0	2
4	DSE 1	From list of DSE	C	4	0	0	4
5	DSE 2	From list of DSE	C	4	0	0	4
	Total of Semester Credits						14

List of DSE

S. No.	Course Code	Course	Category	Hours			Credit
				L	T	P	
2	MA 617	Elliptic curves and cryptography	C	4	0	0	4
3	MA 615	Non- Liner Programming	C	4	0	0	4
4	MA 616	An introduction to quantum computing	C	4	0	0	4
5	MA 621	Advanced Mathematical Methods	C	4	0	0	4

Abbreviation DSE: Discipline Specific Elective, L-lecture,T-Tutorial

- *Other courses may be included as per research area of student and supervisor.

MA616: An Introduction to Quantum Computing **Credit: 4-0-0**

Unit 1:
Hilbert Space: An overview, Introductory Cryptology
Unit 2:
Basic notions of quantum mechanics: Hilbert spaces, postulates of quantum mechanics, qubits, density operator, entanglement,
Unit 3:
EPR and Bell inequality. Quantum gates, quantum circuits.Quantum Fourier transform.
Unit 4:
Quantum algorithms: Deutsch's, Deutsch-Jozsa, Grover`s and Shor's algorithms.
Unit 5:
Quantum cryptography: quantum key distribution, BB84, B92, and EPR protocols.
Reference:

[1] HidaryQuantum Computing: An Applied Approach.
[2] F Grasselli, Quantum Cryptography

MA617: Elliptic Curves and Cryptography **Credit: 4-0-0**

Unit 1:
Introduction of Cryptography. Cryptographic Primitives Protocols, Symmetric Cryptosystems, PKC, Digital Signature

Unit 2: The Geometry of Elliptic Curves: Weierstrass equations, The group law, j-invariants, Isogenies, The dual isogeny, The Tate module, The Weil pairing. The Formal Group of an Elliptic Curve: Expansion around 0, Formal groups, Groups associated to formal groups, The invariant differential, The formal logarithm, Formal Groups over discrete valuation rings.

Unit 3:
Elliptic Curves over Finite Fields: Number of rational points, The Weil conjectures, The Endomorphism rings, Calculating Hasse invariant.

Unit 4:
Elliptic curves over finite fields: Arithmetic of Elliptic Curves (over Finite Fields), group structure, Weil conjectures, Super singular curves, efficient implementation of elliptic curves, determining the group order, Schoof algorithm, the elliptic curve discrete logarithm problem, the Weil pairing, MOV attack.

Unit 5: Review of Recent Research Papers in Cryptography.

Reference:

[1] Joseph H. Silverman , John T. Tate, Rational Points on Elliptic Curves.
[2] Elliptic Curve Cryptography in Practice, https://eprint.iacr.org/2013/734.pdf
[3] Darrel Hankerson, Alfred Menezes, Scott Vanstone, Elliptic Curve Cryptography,
[4] Roberto M Avanzi, Handbook of elliptic and hyperelliptic curve cryptography

MA 621: Advanced Mathematical Method **Credit: 4-0-0**

Unit I:

Existence Theorems: Introductions to ODE, Lipschitz condition, Grownwall Integral Inequality, Integral Equations Equivalent to IVPs, Existence theorem, Nonlocal Existence theorem, Error bound for approximations and Uniqueness of the solution, Fixed Point theorem, Continuation of solutions, the dependence of the solutions on initial conditions.

Unit II:

Analytical Methods: Introduction, Existence theorem (Peano's Theorem), Extremal solutions, Lower and Upper solutions, Monotone iterative method, and Quasilinearization method, Bihari Integral Inequality.

Unit III:

Linear Systems: Introduction, Matrix Operations, Linear Systems in Vector-Matrix form, Homogeneous linear systems, Fundamental Matrix, Solutions of nonhomogeneous Linear Systems, homogeneous Linear Systems with constant coefficients, Periodic Solutions of Linear Systems.

Unit IV:

Adjoint Equations and Boundary Value Problems: Introduction, Adjoint Equations of order one and

order two, Sturm- Liouville Problems, Greens functions nonexistence of the solutions.

References Books:

[1] V.Dharmaiah: Introducation to theory of ordinary differential Equations, PHI publishing house.
[2] Francis B. Hildebrand: Methods of Applied Mathematics, Dover, New York. W. E. Boyce, R. C. DiPrima: Elementry Differential Equations and Boundary value Wiley.
[3] F.B. Hilderbrand: Advanced Calculus for Applications, PHI, New Delhi.
[4] Martin Braun: Differential Equations and Their Applications An Introduction to Applied Mathematics, Springer.N.Jacobson, Basic Algebra-I,2nd Edition, Dover Publication2009

MA 615(Non-linear Programming) **Credits (L-T-P): 4(3-0- 0)**

Unit 1:

Review of Linear Programming and dual linear programming, Nonlinear programming, Convex sets and Convex functions, definition and basic properties, Differentiable convex and concave functions, Minima and Maxima of Convex and Concave functions.

Unit 2: Search Techniques Line search for unimodal functions, Fibonacci method of search, Golden Section Search, Steepest descent method, conjugate direction, conjugate direction method.

Unit 3: The Fritz John and Karush-KuhnTucker Optimality Conditions, Quadratic programming with linear constraints, Wolfe's Algorithm, Complementary Pivot Algorithm.

Unit 4:

Separable Programming, Geometric Programming, Quadratic Interpolation Method. Unconstrained and constrained optimization problems and applications.

References Books:

[1] Ravindran, Phillips, Solberg, Opeartions Research: Principles and Practice, Willey, 2007.
[2] D. G. Luenberger, Yinyu Ye, Linear and nonlinear programming, Springer, 2008.
[3] O. L. Mangasarian, Nonlinear Programming, McGraw Hill, 1969.
[4] M. S. Bazaraa, H. D. Sherali, C. M. Shetty, Nonlinear Programming: Theory and Algorithms, John Wiley and Sons, 2006