Dept. of Mathematics

The Department of Mathematics offers excellent Graduate courses designed to meet the needs of students pursuing graduate work in mathematics and related areas leading students to professional excellence in mathematical research or applications of mathematics.

The Department of Mathematics offers programs leading to Master of Science (M.S.), the Doctor of Philosophy (Ph.D.) degrees, and Master's & Doctoral. Courses of study are available in algebra, analysis, topology, geometry, applied mathematics, cryptography, information mathematics, and probability theory.

The M.S. degree program is designed to prepare students for industrial, management or public service employment. It emphasizes the skills, attitudes, and knowledge needed for recognition, formulation and solution of real-world problems. It also encourages a more intensive program which emphasizes the skills needed for study of problems arising in areas related to mathematics. In addition, students are expected to undertake a project or problem-solving seminar as part of their studies.

The Ph.D. program consists of intensive course of study designed for the full-time student planning a career in research in academic or in a nonacademic setting. The program consists initially of the course work necessary to pass the Qualifying Examinations and then the research necessary to write an original piece of mathematics for a thesis and eventual publication in scholarly journals.

❑ **Mathematics Major**

❑ **Information Security Major**

☐ **Courses**

❑ **Core Courses**

· **Research Ethic & Thesis Study (3)**

Graduate students will acquire an appreciation of the reasons for conducting ethical review of research and an awareness of some of the international codes of research ethics that have been developed in response to scandals and abuses in research. Finally, they will understand the nature and definition of research ethics and an appreciation of the importance of good research.

· **Modern Algebra (3)**

Elementary algebraic structure of Groups, Rings, Fields, Vector Spaces, Fundamental concepts of Category and Functions.

· **Real Function Theory (3)**

This lecture concerns the Lebesgue measure in 1-dimensional real space, integration and differentiation, Riesz representation theory, and existence and uniqueness of regular measure.

· **Basic Topology (3)**

An introductory course of general topology. Fundamentals of point set topology with a brief introduction to the fundamental group and related topics, topological and metric spaces, compactness and connectedness, separation properties, local compactness, completeness, introduction to function spaces, and basic notions involving deformations of continuous paths.

· **Foundations of Geometry (3)**

Deals with basic theories in various areas of Geometry on 3 dimensional Euclidean space.

· **Mathematical Statistics (3)**

This course deals with Distribution theory of Random variables, estimation, statistical test, and nonparametric statistical methods.

· **Introduction to Applied Mathematics (3)**

Introductory course of applications of mathematical theories and methods in many areas of Science & Engineering.

· **Introduction to Information Security (3)**

Topics covered include need for security services in computer networks, basic concepts of cryptology, historical ciphers, modern symmetric ciphers(such as DES, IDEA, RC5), Advanced Encryption Standard(AES), public key cryptography(RSA, elliptic curve cryptosystem), hash functions, and digital signature algorithms.

· **Topics in Modern Algebra (3)**

A Study on the structure of groups, rings, fields and modules.

· **Real Analysis (3)**

In this course, we consider the Lebesgue measure in 1-dimensional real space, integration and differentiation, Banach space, functional space, general function theory, and integration and measure in abstract space.

· **Modern Differential Geometry (3)**

Deal with Tensor analysis, concept of the modern differential geometry and topological properties.

· **General Topology (3)**

Fundamentals of point set topology, topological and metric spaces. compactness, connectedness, separation properties, local compactness, completeness, topology of Euclidean spaces, winding number and applications, and the fundamental group and covering spaces.

· **Topics in Statistics and Probability (3)**

Seminar on topics of modern statistics and probability theory.

❑ **Mathematics Major Courses**

· **Probability Theory (3)**

This course deals with conditional probability, concept of probability process, Limit actions, Markov chain, and Markov process.

· **Topics in Abstract Algebra (3)**

Topics in abstract algebra.

· **Functional Analysis (3)**

We study the linear topological space, Banach-Steinhaus theorem, open mapping theory, closed graph theory, Hahn-Banach theorem, and duality in Banach space.

· **Topology (3)**

Topological and metric spaces, compactness and connectedness, separation properties, Euler characteristic, simplicial complexes, the classification of two-dimensional manifolds, vector fields, and introduction to three-dimensional topology.

· **Actuarial Mathematics (3)**

This course assumes basic theory of probability and deals with death rules, life insurance and annuity, reserve fund, continuous and discrete insurance theory.

· **Topics in Financial Mathematics (3)**

Derivatives and options in modern financial market based on probability and probability process, probability differential equations, Black-Scholes model, Hull-White models.

· **Topological Geometry (3)**

This lecture is an account of the elementary theory of topological spaces and of continuous and differentiable maps leading up to the smooth manifolds and their tangent spaces and Lie groups and Lie algebras. Here the geometric algebra provides numerous significant examples.

· **Topics in Topology (3)**

Studies on resent papers relative to the subject general topology, algebraic topology, combinatorial topology, and their applications.

· **Differential Geometry (3)**

Deal with theory of curve and surfaces and the basic of the transformation.

· **Differentiable Manifolds (3)**

Deal with Stokes theorem, Frobenius theorem, Affine connection, Lie group, Cohomology on manifold.

· **Topics in Geometry (3)**

Introduce the recent topics concerning papers.

· **Multivariate Statistical Analysis (3)**

Topics includes discriminant functions, factor analysis, principal components, canonical correlations, and cluster analysis. maximum likelihood and Baysian methods, robust estimation and survey sampling.

· **Theory of Probability (3)**

Deals with Random spaces, random variables, expectations, moment generating functions, and characteristic functions.

· **Topics in Numerical Analysis (3)**

Deals with numerical methods to find approximate solutions for mathematical problems in science or engineering.

· **Applied Differential Equations (3)**

We consider the applications of differential equations and related examples and their solutions in Engineering.

· **Topics in Scientific Computations (3)**

This course deals with computational theory and algorithms based on mathematical theory.

· **Theory of Field (3)**

Structure of Finite Fields, Polynomials over Finite Fields, Theoretical Applications of Finite Fields, Finite Extension Fields, Galois Theory, Ordered Fields, Theory of valuations, artin Schreier theory.

· **Commutative Algebra (3)**

Rings and ideals, modules, localizations, primary decomposition, integral dependence

and valuations, chain conditions, Noetherian Rings, Artin Rings, discrete valuation rings and Dedekind domains, completions, and dimension theory.

· **Algebraic Number Theory (3)**

Principal ideal rings, integral over a ring, integrally closed rings, norms and traces, Noetherian rings, Dedekind rings, ideal classes and the unit theorem, splitting of prime ideals in an extension field, Galois extensions of number fields.

· **Group Representation Theory (3)**

An introduction to group representations, character theory, modular representations, and integral representations.

· **Advanced Algebra (3)**

Topics covered include advanced algebraic theory of elliptic curve cryptosystem and cryptography over number-field for public key cryptosystems.

· **Complex Analysis (3)**

This lecture considers analytic function, infinite series, line integral, conformal mapping, Dirichlet problem, and elliptic functions in Complex analysis.

· **Partial Differential Equations (3)**

The purpose of this lecture is the classification, boundary value problems, initial value problems of second ordered partial differential equations as well as the existence and regularity of general linear partial differential equations.

· **Topological Vector Space (3)**

Local convexity, Hahn-Banach theorem, compactness, Klein-Milman theorem, conjugate space, and polar set.

· **Operator Theory (3)**

This course deals with Banach algebras, topology and density theorem in operator algebra, Von Neumann algebras.

· **Introduction to Inverse Problems (3)**

We study the concept of layer potential, Neumann and Dirichlet functions, and Generalized Polarization Tensors, and consider the detection algorithm of inhomogeneities embedded in a material by using the asymptotic expansion formula.

· **Topics in Inverse Problems (3)**

We consider the concept of Multiple Signal Classification(MUSIC) algorithm, linear sampling method, topological derivative, and Newton's method by using Frechet derivative in inverse problems, and study the method of numerical simulations.

· **Elements of Differential Geometry (3)**

Deal with Tensor analysis, classical and modern differential geometry.

· **Submanifold Theory (3)**

Deal with Riemannian manifold, submanifold, complex and contact manifold.

· **Differential Manifolds (3)**

Deal with the fiber bundle on manifolds, connection theory, Green theorem and the integral formula, geometric transformation, Laplace operator, complex and contact manifolds.

· **Riemannian Geometry (3)**

Deal with structure transformation, differential forms, and submanifold theory.

· **Topics in Differential Geometry (3)**

Deal with recent topics on the differential geometry concerning to the high level course.

· **Differential Topological Geometry (3)**

Deal with the differential structure using the topological property on differential geometry.

· **Algebraic Topology (3)**

An introductory course with emphasis on the algebraic topology of manifolds. Topics include singular homology theory, Eilenberg-Steenrod axioms, simplicial and cell complexes, elementary homotopy theory, Lefschetz fixed point theorem.

· **Homology Theory (3)**

This lecture is to present as a clearly and concisely as possible the basic techniques and application of homology theory. The subject matter includes singular homology, attaching spaces and CW complexes, cellular homology, cohomology, products, and fixed point theory for the topological manifolds.

· **Homotopy Theory (3)**

This lecture is an introductory course to the algebraic topology from the point of view of a homotopy theoriest. In first few sections are introductory in nature. These are followed by a discussion of the fundamental group, covering spaces, and Van Kampen's theorem. Many results which are most often state in the category of CW complexes are valid in this generality. The key result we used to make calculation is the Blakers_Massay theorem. This is strong enough to imply the suspension theorem and Serre exact sequences.

· **Differential Topology (3)**

We prove embedding, isotropy and transversality theorems, and discuss, as import techniques, Sard's Theorem, Morse functions, partition of unity, dynamical systems. We also consider connected sums tubular neighborhoods and so on.

· **Fuzzy Topology (3)**

This lecture is to present the basic techniques and application of fuzzy topology. The subject matter includes operations on lattices, fuzzy topological spaces and convergence theory, connectedness, separation and compactness. Metric spaces and relations between fuzzy topological spaces and locales are also included in the subject.

· **Theory of Discrete Distribution (3)**

Probability generating functions, Poisson distribution, mixed discrete distribution, multivariate discrete distribution.

· **Nonparametric Statistics (3)**

This course deals with locally most powerful rank tests, regression and analysis of variance using ranks, asymptotic power and efficiency, goodness of fit tests, permutation tests and randomization.

· **Analysis of Time Series (3)**

Decomposition of series, trends and regression as a special case of time series, cyclic components, smoothing techniques, stochastic difference equations autoregressive schemes, moving average, covariance structure and spectral densities.

· **Analysis of Regression (3)**

Correlation theory, distributions of correlation coefficients, Least square method, linear and nonlinear regression, optimal curves.

· **Statistical Decision Theory (3)**

Utility theory, Loss theory, Baysian analysis, minimum and maximum analysis.

· **Data Analysis and Statistics Laboratory (3)**

Deals with theories and methods for data analysis including linear and nonlinear regression, Time series analysis and Computer experiments.

· **Numerical Methods for Differential Equations (3)**

We study the numerical solution for ordinary differential equations of n-th order, Laplace, Heat, and wave equations with initial-boundary conditions.

· **Finite Difference Methods (3)**

This course deals with theories of finite difference methods focused on the stability, convergence and their applications in initial value problems or boundary value problems.

· **Introduction to Image Processing (3)**

Throughout the level set, calculus of variations, Euler-Lagrange equation, total variation minimization problems, regularization, and CFL conditions, we understand the structure of partial differential equations and theory of numerical analysis and study the application of image processing such as image denoising and segmentations.

· **Computational Fluid Dynamics (3)**

This course deals with theories of dynamical fluids and computational methods for models that can not be solved analytically.

· **Chaos and Dynamical Systems (3)**

This course deals with iterations, graphic analysis, chaos, and stability.

· **Topics in Mathematical Models (3)**

This course deals with theories, mathematical and numerical methods for various mathematical models.

· **Finite Element Methods (3)**

This course deals finite element methods in one and two dimension spaces and error analysis.

· **Option Pricing (3)**

Deals with evaluations of options, futures, swaps derived from Stocks, Bonds and VaR.

· **Mathematical Models for Computation (3)**

Deals with Finite automata, Pushdown automata, Turing machine, λ-calculus, μ -Recursive Functions and introduce various mathematical models for computation.

· **Queueing Theory (3)**

Deals with Single server queues, M/M/1, M/G/1, G/M/1, G/G/1, Heavy traffic, Networks of queues.

❑ **Information Security Major Courses**

· **Cryptomathematics (3)**

Topics covered include finite fields for information security. The structure of finite field, polynomials over finite field, factorization of polynomials, applications of finite

fields, ECC over finite fields.

- **Crypto-Algorithm (3)**

  Topics covered include classical cipher, stream cipher based on Shannon's theory, block cipher and their security issues.

- **Advanced Crypto-Algorithm (3)**

  Topics covered include the design and implementation of public key cryptosystem, symmetric key cryptosystem, digital signature schemes, and hash functions.

- **Logic of Information Flow (3)**

  Topics: languages and models of the first order, terminological representation languages, logical models for solving scheduling problems

- **Mathematics and Information (3)**

  Deals with uncertainty, Entropy, Coding Theory based on Statistics and Probability.

- **Information Security Protocol (3)**

  Topics covered include an introduction of information security protocol, key distribution, identification, message authentication code, secret sharing, pseudo-random number generation, zero-knowledge proof, electronic elections.

- **Key Management System (3)**

  Topics covered include the key generation, key management, and key recovery schemes.

- **Electronic Commerce Security (3)**

  Topics covered include information security schemes to protect the electronic commerce, especially electronic cash, electronic payment, electronic wallet.

- **Hash Function and Masseage Authentication (3)**

  Topics covered include the design principle of collision free hash functions and the generation of MAC.

- **Cryptanalysis of Public - Key Cryptosystem (3)**

  Topics covered include the cryptanalysis of public key cryptosystem based on the mathematical methods such as factorization of numbers, discrete logarithm problems.

- **Complexity and Algorithms (3)**

  Topics: running time analysis, efficient algorithms, the class P, the class NP, computability theory, and complete theories.

- **Provable Security (3)**

Deals with Computational complexity, Unconditional security, Complexity theoretic security, Provable security under assumptions, and Ad hoc security.

- **Steganography and its Applications (3)**

  We study the implementation Technology and Principle of Steganography, and Information Hiding Application Method, such as Watermarking and DRM, etc.

- **Networks Security (3)**

  Deals with Authentication systems, Entity authentication, Security handshake pitfalls, Strong password protocols, Kerberos system, Public key infrastructure, and IPsec.

- **Financial Information Security (3)**

  We study the information Security Technology in Financial Field, such as Electronic cash, Secure Electronic Transaction, and Internet Banking Systems, etc.

- **Topics in Symmetric Key Cryptanalysis (3)**

  We study the security analysis on the block ciphers and stream ciphers.

- **Implementation of Cryptographic S/W (3)**

  Acquire the software implementation technologies of international standard Symmetric Key Encryption Algorithm and public key Encryption Algorithm.

- **Implementation of Cryptographic H/W (3)**

  Studying about current technology for H/W structure and optimal implementation on crypto-device.

- **Evaluation and Validation of Cryptographic Module (3)**

  Studying about the knowledge necessary to perform the evaluation verification guideline on the basis of understanding for the Cryptographic Module Validation Program(CMVP).

- **Implementation of Parallel Cryptography (3)**

  Studying about the High Speed Implementation technology on crypto algorithm using the GPU or Parallel systems, and its applications.

- **Mobile Security (3)**

  Studying about the latest mobile networks security architecture and technology.

- **Wireless Security (3)**

  Studying about the latest wireless communications technology, and the security technology of the applications.

- **IT Convergence and Security (3)**

  Studying about Convergence Technology on IT field and other fields, and the

security technology of the applications.

· **Smartgrid Security (3)**

Studying about structure and security required for application on SmartGrid.

· **Internet Security (3)**

Studying about structure of Wired and wireless Internet, and its security technology.

· **Side Channel Attacks (3)**

Studying about physical security analysis of the smart devices.

· **Countermeasures of Side Channel Attacks (3)**

Secure implementation of the side channel attack countermeasures based on S/W and H/W.

· **Secure Multiparty Computation (3)**

Studying about technology that can protect the privacy of the participating entity under an environment that does not assume the existence of a trusted server.

· **Pseudorandomness (3)**

Studying about the theory of Pseudorandom Number which is a basic Security factor Of cryptographic algorithms, and the Method of Statistical Randomness Test.

☐ **Faculty Members**

Yi, Okyeon
Korea Univ., B.S.
Korea Univ., M.S.
Univ. of Kentucky, Ph. D.
Applied Algebra
oyyi@kookmin.ac.kr

Kim, Pok Son
Kookmin Univ., B.S.
Johann Wolfgang Goethe Universitaet Frankfurt am Main, M.S.
Johann Wolfgang Goethe Universitaet Frankfurt am Main, Ph. D.
Mathematical Information Theory
pskim@kookmin.ac.kr

Kang, Ju Sung
Korea Univ., B.S.
Korea Univ., M.S.
Korea Univ., Ph. D.
Applied Mathematics & Probability
jskang@kookmin.ac.kr

Han, Dong-Guk
Korea Univ., B.S.
Korea Univ., M.S.
Korea Univ., D.En.
Future Univ.-Hakodata, Japan, Post.Doc.
Information Security
christa@kookmin.ac.kr

Park, Won-Kwang
Kookmin Univ., B.S.
Yonsei Univ., M.S.
Ecole Polytechnique, Ph. D.
Applied Mathematics
parkwk@kookmin.ac.kr

Yeom, Yongjin
Seoul National Univ., B.S.
Seoul National Univ., M.S.
Seoul National Univ., Ph. D.
Cryptography, Information Security
salt@kookmin.ac.kr

Kim, Jongsung
Korea Univ., B.S.
Korea Univ., M.S.
Katholieke Universiteit Leuven, Belgium, Ph. D.
Information Security
jskim@kookmin.ac.kr

Kim, Dong-Chan
Sogang Univ., B.S.
Sogang Univ., M.S.
Sogang Univ., Ph. D.
Cryptography, Coding theory
dckim@kookmin.ac.kr

Seo, SeogChung
Ajou Univ., B.S.
GIST, M.S.
Korea Univ., Ph.D.
Information Security
scseo@kookmin.ac.kr

You, IlSun
Dankook Univ., B.S.
Dankook Univ., M.S.
Dankook Univ., Ph.D.
Kyushu Univ., Ph.D.
Information Security
isyou@kookmin.ac.kr