Programme pour Auditeurs libres

Semestre d'été 2022-2023

DESCRIPTION DÉTAILLÉE | DETAILED DESCRIPTION | DETAILLIERTE BESCHREIBUNG

Faculté des Sciences, des Technologies et de Médecine

UNIVERSITÉ DU LUXEMBOURG

All courses offered in this Faculty :

Bachelor en Mathématiques :

- Analyse 1
- Analyse 3
- Structures mathématiques
- Algèbre
- Probabilités et statistiques 1
- Algèbre linéaire 1
- Topologie générale
- Reading Course 1 : Quiver Representations and root systems
- Modélisation des milieux continus
- Reading Course 2
- Reading Course 3

Bachelor in Physics :

- Experimental Physics 1a und 1b : Mechanics, Oscillations and Waves (CM, 1a) and TD(1b)
- Mathematical methods 1

Master in Mathematics :

- Partial Differential Equations i
- Discrete-time stochastic processes
- Lie Algebras and Lie Groups
- Combinatorial Geometry
- Stochastic Analysis
- Riemannian Geometry
- Probabilistic Models in Finance
- Scientific Python
- Arithmetic Geometry
- Numerical Analysis
- Algebraic Geometry
- Functional Analysis
- Stochastic Analysis and PDE
- Gaussian processes and applications
- American options : Optimal Stopping Theory and numerical methods
- Continuous-Time Stochastic Calculus and Interest Rate Models
- Numerical Methods in Finance
- Mathematical Modelling
- Advanced Discretization Methods
- Selected Topics in Industrial Mathematics 1
- Commutative Algebra
- Data Science
- Algorithmic Number Theory

Erasmus Mundus Joint Master in Cybersecurity (CYBERUS) :

- Cybersecurity and AI

- EU Digital sovereignty : Cyberthreats to the EU and Cyberactors
- Security of databases
- Security of Software defined networking
- Static and dynamic softwares security analysis
- Digital Wallets
- Security of Mobile computing

- EurIdentity Certificate

FSTM – Faculty of Science, Technology and Medicine

FSTM – Bachelor en Mathématiques

Analyse 1

Teacher(s)
Jean-Marc SCHLENKER, Abderrahim MESBAH, Viola GIOVANNI

Language
Français

Description

Les étudiants apprendront à connaître et à utiliser les bases de l'analyse : suites, fonctions réelles à une variable, développements de Taylor, et quelques bases sur des espaces métriques.
Par ailleurs le cours et les exercices les aideront à acquérir les bases du raisonnement mathématique.

- entiers, rationnels, nombres réels
- suites de nombres réels
- fonctions, limites de fonctions
- continuité et dérivées
- développements de Taylor
- espaces métriques, notions de topologie dans les espaces métriques

Analyse 3

Teacher(s)
Martin OLBRICH

Language
Français, English

Description

Dans ce cours, on diversifie et approfondit diverses connaissances et techniques de l'analyse mathématique. On s'intéresse à démontrer plusieurs théorèmes fondamentaux dans l'étude des fonctions de plusieurs variables, des équations différentielles et des suites de fonctions.

Programme

- Fonctions implicites et applications
- Théorie locale des équations différentielles ordinaires
- Convergence de suites de fonctions
- Série de puissances

- L'exponentielle matricielle
- Théorème d'approximation de Stone-Weierstrass

Structures mathématiques

Teacher(s)
Bruno TEHEUX, Alexandre LECESTRE, Charles-Philippe Manuel DIEZ

Language
Français

Description

Programme

- logique, ensembles, applications
- démonstrations (types et pratique)
- nombres naturels, entiers et rationnels
- groupes : définition, exemples, groupe symétrique, morphismes, sous-groupes, (sous-groupes distingués), (quotients)
- anneaux : définition, exemples, corps, morphismes, (sous-anneaux), (idéaux), (quotients), congruences, algorithme d'Euclide, Z/nZ

Algèbre

Teacher(s)
Pieter BELMANS, Alfio Fabio LA ROSA, Gianni PETRELLA

Language
Français, English

Description

Dans l'histoire on comprend par l'algèbre l'étude des équations. Au cours des 2000 ans de cette étude, les gens se sont aperçus que certaines structures revenaient très souvent, et en plus dans des contextes tout à fait différents ! Depuis, les algébristes s'occupent aussi de l'étude et du développement de ces structures, ainsi que, évidemment, de leurs applications dans d'autres domaines en sciences, ingénierie et mathématiques.

L'objet principal du cours sera l'étude des anneaux et des extensions algébriques des corps commutatifs. En particulier, la théorie de Galois sera développée et appliquée. Elle permet entre autres de démontrer que l'équation générale de degré au moins 5 ne peut pas être résolue en radicaux et de résoudre (parfois de manière négative) plusieurs problèmes classiques (provenant des anciens Grecs) de construction à la règle et au compas comme la trisection d'un angle et la quadrature du cercle.

Le cours couvrira les sujets suivants :

- théorèmes d'isomorphismes pour groupes et anneaux (sous-groupes distingués, idéaux, quotients)
- anneaux généraux: idéaux premiers et maximaux, quotients, corps des fractions d'un anneau intègre
- anneaux euclidiens et anneaux factoriels
- critères d'irréductibilité pour polynômes
- extensions algébriques de corps
- corps : caractéristique, clôture algébrique, corps de rupture, corps de décomposition, corps finis
- quelques constructions à la règle et au compas
- extensions de corps: normales, séparables, galoisiennes
- correspondance de Galois
- groupes solubles, (non-)solubilité d'équations polynomiales par radicaux, groupes de Galois de polynômes
- constructions à la règle et au compas
- (Hilbert 90 et Théorie de Kummer : caractérisation des extensions solubles)

Probabilités et statistiques 1

Teacher(s)
Ivan NOURDIN, Francesca PISTOLATO

Language
Français

Description
Le but de ce cours est de faire acquérir à l'étudiant une connaissance de base des principaux concepts en probabilité et statistique.

Programme
1. Espace de probabilité et variable aléatoire
   - Univers
   - Tribu et variable aléatoire
   - Probabilité
   - Cas où l'univers est fini ou dénombrable
   - Indépendance d'événements
   - Loi d'une variable aléatoire
   - Fonction de répartition
   - Lois discrètes vs continues
   - Variables aléatoires indépendantes
2. Lois classiques
   - Loi uniforme discrète
   - Loi de Bernoulli
   - Loi binomiale
   - Loi hypergéométrique
   - Loi géométrique
   - Loi de Poisson
   - Loi uniforme continue
   - Loi gaussienne
   - Loi exponentielle

- Loi de Cauchy

3. Espérance
   - Introduction
   - Espérance d'une variable positive
   - Moments, variance, écart-type
   - Espérance et variance des lois classique
   - Inégalité de Markov, Bienaymé-Tchebicheff et Jensen
   - Fonction génératrice
   - Fonction caractéristique
   - Covariance et coefficient de corrélation linéaire
4. Théorème limite
   - Loi faible des grands nombres
   - Théorème central limite
5. Estimation de paramètres (si le temps le permet)

Algèbre linéaire 1

Teacher(s)
Ivan NOURDIN, Leonardo MAINI, N.N.

Language
Français

Description

Au terme du cours, l'étudiant doit être à même de :

- comprendre le rôle central de l'algèbre linéaire dans les sciences mathématiques
- maîtriser les notions et les algorithmes fondamentaux de l'algèbre linéaire ainsi que les principaux outils développés pour l'étude générale des espaces vectoriels
- acquérir un raisonnement rigoureux et systématique, indispensable à l'analyse et à l'interprétation des objets de l'algèbre linéaire
- formuler et résoudre mathématiquement certains problèmes concrets modélisables au moyen de l'algèbre linéaire

Programme

- Matrices : définitions et opérations de base, matrices particulières, transposée, inverse, lien avec les systèmes linéaires et méthode du pivot
- Espaces vectoriels : définitions, premières propriétés, exemples, sous-espace vectoriel, bases, dimension, supplémentaire,
- Applications linéaires : définition, noyau, image, théorème du rang, matrice d'une application linéaire, changement de bases
- Déterminant : rappels sur le groupe symétrique, formes n-linéaires alternées, définition du déterminant, propriétés, applications, calculs, comatrice
- Géométrie dans le plan et l'espace : produit scalaire, bases orthonormées, procédé de Gram-Schmidt, orthogonal, isométrie et classification

Topologie générale

Teacher(s)
Bruno TEHEUX

Language
English, Français

Description
Apprendre les fondements de la topologie générale au travers des propriétés de base des espaces topologiques et des fonctions continues.

Programm

- Espaces topologiques, bases, intérieur, adhérence, frontière, application continue, topologie produit, topologie induite, espaces métriques
- Connexité, connexité par arcs, composantes connexes, points de coupures
- Compacité, axiomes de séparations, nombre de Lebesgue et applications
- Espaces quotients
- Lemme d'Urysohn, Théorème de Tietze et applications...

Reading Course 1 : Quiver Representationand root systems

Teacher(s)
Sarah SCHEROTZKE

Language
English

Description

Learn what the representation of a quiver is, how to classify simple representations of Dynkin quivers via their root system.

In this class, we will introduce the theory of representations of a quiver and their connection with root systems. We will learn some basics in representation theory, such as what a simple representations are. We will classify the simple representations of quivers of Dynkin type and show that their isomorphism classes are in bijection with the positive roots of the system.

Modélisation des milieux continus

Teacher(s)
Robert Lee KONSBRUCK

Language
Français

Description

Outre des compétences en mathématiques appliquées, ce cours permet de s'approprier des connaissances en analyse tensorielle, aussi bien du point de vue des mathématiques que de celui des applications, ainsi que dans le domaine de l'intégration des équations aux dérivées partielles.

Programme

Modélisation des systèmes continus, analyse tensorielle et équations aux dérivées partielles. La modélisation des fluides conduit à un bel exemple de modèle mathématique, basé sur deux notions fondamentales : les tenseurs et les équations aux dérivées partielles.

Le cours se situe à la frontière entre les mathématiques et la physique, ainsi qu'à celle entre les mathématiques pures et les mathématiques appliquées. Un objectif est de présenter un enseignement cohérent de la dynamique des milieux continus, en mettant l'accent sur les aspects mathématiques de cette théorie. Le cours se propose entre autres d'appliquer l'outillage mathématique connu à des problèmes concrets et, inversement, d'étudier les concepts mathématiques nouveaux qui se dégagent de ces études.

Reading Course 2

Teacher(s)
Serguei MERKOULOV

Language
English

Description

Students who successfully pass this course should know all relevant definitions, correct statements of the major theorems (including their hypotheses and limitations), and examples and non-examples of the various concepts covered in class. The students should be able to demonstrate their mastery by solving non-trivial problems related to these concepts, and by proving simple (but non-trivial) theorems about these concepts, related to, but not identical to, statements proven by the text or instructor.

Depending on the class, this may include the following concepts:

- affine space and algebraic sets;
- examples such as plane curves, quadrics, cubic surfaces
- Segre and Veronese embeddings
- the Hilbert basis theorem and applications;
- the Zariski topology on affine space;
- irreducibility and affine varieties;
- the Nullstellensatz;
- morphisms of affine varieties;
- projective varieties.

The aim of the course is to help students learn about a topic in algebraic geometry. We will begin with a rapid introduction to the basics of algebraic geometry. Further topics that may be covered, such as toric varieties or enumerative geometry, will depend on the registered/interested students.

Reading Course 3

Teacher(s)
N.N.

Language
English

Description
This course will focus on the probabilistic model of random walk. Students and the teacher will take turn to present in class particular properties of random walks.

The classical random walk is one the most fascinating model in probability. Its description is very simple: in dimension one, it can be seen as the sequence of successive gains in a game of heads or tails. Beyond the limit asymptotics given by the central limit theorem, we can study many properties of this model: return times, first visits, the gambler's ruin problem, approximation to Brownian motion, the law of titerated logarithm, recurrence and transience, etc. It is a good support to use probabilistic tools such as the characteristic function, Borel-Cantelli lemma, central limit theorems, moment generating function, etc. The mathematical tools used vary from probability to combinatorics and analysis. Some prerequisites will be teached during the first courses.

FSTM – Bachelor in Physics

Experimental Physics 1a and 1b: Mechanics, Oscillations and Waves (CM, 1a) and TD(1b)

Teacher(s)
Roland André SANCTUARY

Language
Français, English

Description
Motion of point masses/kinematics
Forces and Newton's laws of mechanics
Work and (potential and kinetic) energy
Relative motion (Galilei transformation, inertial system, Centrifugal and Coriolis forces)
Conservation principles (momentum, angular momentum, energy)
Dynamic properties of rigid bodies (center of mass, moment of inertia, Euler equations)
Oscillations and resonance (harmonic oscillator)
Wave equation and propagation of waves
Principle of Huygens
Interference phenomena
Diffraction of waves

Physique expérimentale 1a: Mécanique newtonienne, oscillations et ondes :
Le cours vise
- à familiariser l'étudiant avec les principes et lois de la mécanique newtonienne
- à l'apprendre à appliquer ces principes et lois à des phénomènes oscillatoires et ondulatoires
- et à fournir à l'étudiant de manière ciblée des outils mathématiques indispensables en physique.
Physique Expérimentale 1b: TD (Travaux Dirigés) :

L'étudiant est amené à
- résoudre d'une manière autonome des problèmes en physique
- appliquer les lois physiques
- manipuler correctement les outils mathématiques indispensables en physique

Mathematical methods 1

Teacher(s)
Aurélia CHENU, Christian WAGNER

Language
English, Deutsch

Description
Méthode Mathématiques de la Physique 1a:
L' étudiant(e) réussit à manipuler les outils mathématiques indispensables en mécanique et en électromagnétisme.

Méthode Mathématiques de la Physique 1a :
1. Vectors and Matrices
2. Complex Numbers
3. Differentiation and Integration
4. Taylor series
5. Differential equations
6. 3-dimensional differentiation and integration
7. Probability

Méthode Mathématiques de la Physique 1b: TD (Travaux Dirigés):
Homework exercises and their explanation in support of Physique expérimentale 4a : Optique

Partial Differential Equations I

Teacher(s)
Martin OLBRICH

Language
English

Description

On successful completion of the course the student should be able to:

- Apply methods of Fourier Analysis to the discussion of constant coefficient differential equations
- Work freely with the classical formulas in dealing with boundary value problems for the Laplace equation
- Prove acquaintance with the basic properties of harmonic functions (maximum principle, mean value property) and solutions of the wave equation (Huygens property)
- Solve Cauchy problems for the heat and the wave equations
- Give a pedagogic talk for peers on a related topic

Fourier transform, the classical equations, spectral theory of unbounded operators, distributions, fundamental solutions.

Discrete-time stochastic processes

Teacher(s)
N.N

Language
English

Description

On successful completion of the course, the student should be able to:

- Understand and use concepts of modern probability theory (e.g., filtrations, martingales, stopping times)
- Apply the notion of martingale to model random evolutions
- Know and apply classical martingale convergence theorems
- Describe and manipulate basic properties of Brownian motion

Radon-Nikodym Theorem, conditional expectations, martingales, stopping times, optional stopping theorems, Doob's inequalities, martingale convergence theorems, martingale central limit theorem, Brownian motion.

Lie Algebras and Lie Groups

Teacher(s)
Serguei MERKOULOV

Language
English

Description

On successful completion of the course, the student should be able to:

- Expound the mathematical foundation behind symmetries of solid bodies, dynamics of mechanical systems, and geometric structures in nature.
- Explain the deep interrelations between Lie groups and Lie algebras, as well as the technical tools behinds these interrelations.
- Simplify mathematical problems admitting symmetry Lie groups actions to problems admitting symmetry actions of their Lie algebras.
- Master applications to the theory of manifolds and representation theory, which in turn have applications in physics, engineering and mechanics.

The Lie algebra of a Lie group, the exponential map, the adjoint representation, actions of Lie groups and Lie algebras on manifolds, the universal enveloping algebra, basics of the representation theory.

Combinatorial Geometry

Teacher(s)
Hugo PARLIER, Kate VOKES

Language
English

Description

The course requires minimal prerequisites (some linear algebra, Euclidean geometry and basic topology) but aims to explore results that are at the limit of current known understanding. In particular, we'll discuss some open problems and try to illustrate the process of modern research. The subjects are chosen so that they can be treated with a hands-on approach, and this approach and experience are as important for this course as the actual content.

The course will cover a selection of themes from combinatorial aspects of geometry.
Themes include general theorems about convex sets in n dimensional real space (and Helly type theorems), Minkovski's first theorem for lattices, and Ramsey theory (graph coloring problems).

Riemannian Geometry

Teacher(s)
N.N.

Language
English

Description

On successful completion of the course, the student should be able to:

- compute with tensors, such as metrics and curvature, in coordinates or coordinate-free
- demonstrate detailed knowledge of the exponential map, including criteria for completeness, conjugate points, and Jacobi fields
- understand multiple interpretations of curvature, for example, as the obstruction to a local parallel framing, or how it influences the spreading of geodesics via the Jacobi equation

This foundational Master-level course is centered around the concepts of connection on a manifold and curvature. These are investigated in further depth in the setting of Riemannian or Lorentzian metrics, where the geometry of geodesics and its relation to curvature are studied.

Stochastic Analysis

Teacher(s)
Giovanni PECCATI, Charles-Philippe Manuel DIEZ

Language
English

Description

///

Probabilistic Models in Finance

Teacher(s)
Chiara AMORINO

Language
English

Description

///

Scientific Python

Teacher(s)
Jack HALE

Language
English

Description

///

Arithmetic Geometry

Teacher(s)
Gabor WIESE

Language
English

Description

This course leads from classical mathematics (real numbers, conics, “classical” geometry, plane curves) to some topics in modern number theory and geometry and underlines the continuity from classical geometry (as taught in school) and classical number theory to the modern points of view.

It covers p-adic numbers and more generally local fields as analogues of the real numbers, quadratic forms (arising from the study of conic sections) and elliptic curves (arising from the study of certain integrals), as well as some of their relevance for modern mathematics.
Having their origin in the study of conics, the theory of quadratic forms is a modern theory situated in both geometry and number theory with plenty of applications. It turns out that for a full classification of quadratic forms, one needs to introduce analogues for the real numbers: the so-called p-adic numbers, or, more generally, local fields. In the first part of the lecture, the theory of quadratic forms is introduced, number theory applications are treated, p-adic numbers are dealt with, and the classification theorem is fully proved.
The second part of the course is concerned with elliptic curves. These are curves arising from the study of certain integrals. They are relevant in everyday life for their fundamental role in Elliptic Curves Cryptography (e.g. used in ID cards, passports). In the language of modern geometry, they are curves of genus one with a rational point. For number theory, they appear in many of the most important questions of current research, e.g. the Birch-and-Swinnerton-Dyer conjecture, which is one of the 7 Millenium Problems. In the course, elliptic curves are introduced in modern geometric language, thus introducing this language, and several important number theoretic and geometric properties are proved, such as the addition law (making them into a group, a complicated generalisation of the integers), and statements on their rational points (number theoretic “Diophantine” question).
The course will be a classical lecture, complemented by integrated exercises and contributions by the students via short talks.
Students from the Master in Secondary Education will be asked to focus in their contributions on how to link the topics of their lectures with High School mathematics.

Numerical Analysis

Teacher(s)
Philippe MARCHNER

Language
English

Description

///

Algebraic Geometry

Teacher(s)
Sarah SCHEROTZKE

Language
English

Description
We will introduce basic notions of algebraic geometry starting with Hilbert's Nullstellensatz, algebraic sets, affine and projective varieties over algebraically closed fields. We will then introduce the modern language of sheaf theory and introduce schemes. We will then discuss divisors, line bundles and vector bundles on schemes.

Functional Analysis

Teacher(s)
Salah MEHDI, Guendalina PALMIROTTA

Language
English

Description
///

Stochastic Analysis and PDE

Teacher(s)
Anton THALMAIER

Language
English

Description
Upon successful completion of the course students should be able to

- evaluate functionals of Brownian motion and relate them to PDE;
- manipulate Feynman-Kac formulas;
- derive stochastic representations of classical initial value problems;
- derive stochastic representations of classical boundary value problems;
- calculate Monte-Carlo formulas for Greek parameters in financial models

Stochastic flows associated to second order differential operators, stochastic differential equations and L-diffusions, Feynman-Kac formulas and Dirichlet problems, boundary value problems (elliptic and parabolic), spectral problems of Schrödinger operators, differentiation of heat semigroups, computation of price sensitivities (Greeks).

Gaussian processes and applications

Teacher(s)
Ivan NOURDIN

Language
English

Description

On successful completion of the course, the student should be able to:

- Explain the language, basic concepts and techniques associated with Gaussian variables, vectors, and processes
- Identify, analyse, and prove relevant properties of models based on a Gaussian structure
- Solve exercises involving a Gaussian structure

- Gaussian random variables (characteristic function, CLT, stability properties, Stein's lemma)
- Gaussian random vectors (definition, characteristic function, existence, uniqueness in law, multivariate CLT, density, Hermite polynomials)
- Gaussian random processes (definition, modifications, uniqueness in law, function of positive type, existence, Brownian motion, continuity)
- Fractional Brownian motion (definition, existence, Hölder regularity).

American options: Optimal Stopping Theory and numerical methods

Teacher(s)
Gilles PAGES

Language
English

Description

On successful completion of the course, the student should be able to:

- Explain pricing and hedging of Vanilla' American options in a multi-asset Black-Scholes model using bi- or multinomial trees
- Extend multinomial tree methods to the pricing and hedging of American options in local volatility or stochastic volatility models (CEV, SABR, Heston…)
- Implement efficiently a regression method à la Longstaff-Schwarz' for solving multi-dimensional optimal stopping problems like the pricing and the hedging of multi-asset American options or energy derivatives like swing options (take-or-pay gas contracts)
- Implement an optimal quantization based numerical scheme to price and hedge multi-asset American style derivatives
- Analyze these numerical methods and their respective ranges of efficiency, especially compared to PDE methods

- Discrete time optimal stopping theory: Snell envelope, Rogers' dual representation, optimal stopping times
- Backward dynamical programming principle
- American options pricing and hedging in a complete market, with and without dividends

- Bermuda options (discrete time)
- Swing options on energy markets
- Numerical methods: variational inequality (PDE method), regression methods (Longstaff-Schwarz), Quantization methods with a priori error bounds
- Continuous time optimal stopping theory and applications to complete markets
- Réduites, variational inequalities, free boundary

Continuous-Time Stochastic Calculus and Interest Rate Models

Teacher(s)
Giovanni PECATTI

Language
English

Description

On successful completion of the course, the student should be able to:

- Calculate probabilities and expectations related to the semi-martingale models presented in the lectures
- Carry out calculations based on change of numéraire and no-arbitrage pricing
- Compute the prices of interest rate derivatives
- Apply stochastic volatility models to deal with implied volatility surfaces

Basic Notions of Fixed Income Markets; Semimartingale Modeling; Stochastic Differential Equations; No-Arbitrage Pricing; Change of Numéraire; Short Rate Models; Heath-Jarrow-Morton Framework; Market Models; Stochastic Volatility.

Numerical Methods in Finance

Teacher(s)
Agnès SULEM, Ludovic GOUDENÈGE

Language
English

Description

On successful completion of the course, the student should be able to:

- Explain and apply relevant numerical methods currently used in finance
- Carry out calculations based on Monte Carlo methods, especially in option pricing and portfolio optimization

First, we will introduce mathematical problems occurring in finance, mainly in option pricing and portfolio optimization in financial markets following stochastic models. These formulations call

upon partial differential equations, conditional expectation, optimal time, dynamic programming and control.
Next, we shall describe methods to approach numerical simulations of these objects.
Finally, in practical sessions, we will use recent software and Python programming to illustrate efficiency of these methods.
The course will be organized in three parts:

- PDE methods for option pricing and numerical methods in stochastic control: 15h (A. Sulem)
- Monte Carlo methods (tree method, regression, machine learning) : 8h (Ludovic Goudenège)
- Applied sessions with computer using the computational finance software "Premia" (www.premia.fr) and Python programming: 7h (Ludovic Goudenège)

Mathematical Modelling

Teacher(s)
Stéphane BORDAS

Language
English

Description
///

Advanced Discretization Methods

Teacher(s)
Stéphane BORDAS

Language
English

Description
On successful completion of the course the student should be able to:

- Explain the mathematical foundation of advanced discretization techniques for PDEs
- Master their concrete implementation on nontrivial engineering boundary-value problems
- Adapt them according to the problem under consideration

- Complements the Finite Element Method
- Finite difference schemes in space
- Finite difference schemes fort he discretization of time-dependent PDEs
- Introduction to integral equations

Selected Topics in Industrial Mathematics 1

Teacher(s)
Jack HALE

Language
English

Description
This course will review a selection of recent and classical topics in Industrial Mathematics by a process of student-led discussions around articles in the academic literature. The course will be run in an interactive manner with a strong emphasis on student participation.

Commutative Algebra

Teacher(s)
Gabor WIESE, Ann KIEFER, Bryan ADVOCAAT

Language
English

Description
The successful students possesses deepened and extended knowledge of the topics treated in Commutative Algebra.

In number theory one is naturally led to study more general numbers than just the classical integers and, thus, to introduce the concept of integral elements in number fields. The rings of integers in number fields have certain very beautiful properties (such as the unique factorisation of ideals) which characterise them as Dedekind rings. Parallelly, in geometry one studies affine varieties through their coordinate rings. It turns out that the coordinate ring of a curve is a Dedekind ring if and only if the curve is non-singular (e.g. has no self-intersection).
With this in mind, we shall work towards the concept and the characterisation of Dedekind rings. Along the way, we shall introduce and demonstrate through examples basic concepts of algebraic geometry and algebraic number theory. Moreover, we shall be naturally led to treat many concepts from commutative algebra.

Depending on the previous knowledge of the audience, the lecture will cover all or parts of the following topics:
(1) General concepts in the theory of commutative rings
- rings, ideals and modules
- Noetherian rings
- tensor products
- localization
- completion
- dimension

(2) Number rings
- integral extensions

- ideals and discriminants
- Noether's normalisation theorem
- Dedekind rings
- unique ideal factorisation

(3) Plane Curves

- affine space
- coordinate rings and Zariski topology
- Hilbert's Nullstellensatz
- resultant and intersection of curves
- morphisms of curves
- singular points

Data Science

Teacher(s)
Christoph SCHOMMER

Language
English

Description

On successful completion of the course the student should be able to:

- Explain and apply basic theoretical concepts on selected aspects of data processing.
- Develop appropriate solutions for data-centered problems.
- Consolidation of the acquired competences in the subject area through a Master's thesis.

In this course, the term data' is seen centric and we will look at data from different perspectives. We will discuss selected aspects of Data Preparation and Preprocessing, Data Statistics, Data Security, Data Privacy, Data Management, Big and Small Data, Data Retrieval, Data Visualization, and Data Analytics.

Algorithmic Number Theory

Teacher(s)
Franck LEPREVOST

Language
English

Description

On successful completion of the course, the student should be able to:

- Explain the main algorithms for primality testing, factorizing large integers, solving the discrete logarithm problem, both in the multiplicative group of finite fields, as well as in the context of elliptic curves defined over finite fields
- Read and understand some scientific articles published in the domain, and ask relevant questions
- Give a talk for peers on related topics

- Organize his approach to general problems in an algorithmic way

The lecture will introduce some of the most important algorithms used for computing with integers modulo m, including the Chinese Remainder Theorem, will introduce a series of theorems (Fermat's small theorem, theorem of Lagrange, exponentiation method, etc) that allow to accelerate computations in these rings. Fields, especially finite fields, will be introduced from an algorithmic angle. Usual probable primality tests will be described. They will provide the context for the introduction of Legendre symbols, the quadratic reciprocity law, etc. Usual integer factorization methods will be introduced as well, including the method of Fermat up to the quadratic field sieve. A series of cryptographic primitives will be given both for a finite group in general, and for specific groups in particular, arising from finite fields, or from elliptic curves defined over finite fields. If time allows, some methods for the computation of the number of points of an elliptic curve over a finite field will be given. This series of lectures will be completed by some broader conferences presenting the material in a more general setting.

Erasmus Mundus Joint Master in Cybersecurity (CYBERUS)

Cybersecurity and AI

Teacher(s)
Maxime CORDY, Salijona DYRMISHI, Salah GHAMIZI

Language
English

Description
///

EU Digital sovereignty : Cyberthreats to the EU and Cyberactors

Teacher(s)
Roger TAFOTIE

Language
English

Description
///

Security of databases

Teacher(s)
///

Language
English

Description
///

Security of Software defined networking

Teacher(s)
Tegawendé François d Assise BISSYANDE

Language
English

Description
///

Static and dynamic software security analysis

Teacher(s)
Jacques KLEIN, Marco ALECCI

Language
English

Description
The student should be able to critically read publications related to static and dynamic analysis (research paper, etc.) * The student should be able to select an adapted approach to solve a specific static analysis problem * The student should be able to implement static analysis techniques * The student should be able to run a fuzzer
Static analyses are used in various situations, from compiler code optimization to security analysis of Android applications. This course provides the concepts and techniques underlying static program analysis. Topics include forward/backward data-flow analysis, inter-procedural analysis, pointer analysis and call graph construction. A particular focus will be given to recent and advanced techniques such as Android bytecode static analysis for security. The course will mix theory and practice. Students will implement simple analyses and complete a course project. In the second part of the course, the student will learn the foundations of dynamic analysis techniques and, in particular, the foundations of fuzzing techniques that are widely used to detect vulnerabilities.

Digital Wallets

Teacher(s)
Gilbert FRIDGEN, Johannes SEDLMEIR, Muriel-Larissa FRANK

Language
English

Description

Students can identify application areas of digital wallets and the corresponding decentralized information systems, design appropriate solutions based on the cryptographic building blocks they learned, consider security threats and countermeasures, and are aware of common pitfalls from a user perspective.

1. **Cryptographic building blocks**
    1. Hashing, Merkle trees & Merkle proofs
    2. Merkle-Patricia Trees
    3. Symmetric and asymmetric encryption
    4. Digital signatures, digital certificates, and the Internet PKI
    5. Elliptic curves, pairings, and BLS signatures

2. **Foundations of zero-knowledge proofs**
    1. From graph three coloring to “everything is provable in zero knowledge)
    2. Polynomial commitment schemes (PCS) à Examples: KZG, FRI
    3. Interactive oracle proofs (IOPs) à Examples: R1CS and PlonKish arithmetization
    4. zk-SNARKs from PCS and IOPs
    5. The Cambrian explosion of SNARKs
    6. Custom gates
    7. Recursion and proof composition
    8. Coding-Session (with Circom)

3. **Foundations of blockchain**
    1. Why blockchain?
    2. From replicated state machines to cryptocurrencies
    3. Consensus mechanisms
    4. Smart contracts
    5. Energy consumption
    6. Attacks on proof of work (PoW) and proof of stake (PoS)
    7. (De-) Centralization layers and PoW vs PoS security
    8. Scaling issues: Concepts (payment channels, optimistic and zk-rollups, bridges, stateless clients and Verkle trees, data availability sampling) and solutions (Ethereum roadmap)
    9. Privacy issues: Concepts (zero-knowledge proofs, multi-party computation) and solutions ((Zcash/TornadoCash, (VERI-)ZEXE)

4. **Decentralized finance**
    1. Coding-Session with Solidity/Remix
    2. Token standards
    3. Liquidity pools
    4. Survey of DeFi applications
    5. Miner extractable value, fair ordering and proposer builder separation
    6. Flashloans, Oracles & DeFi attacks

5. **Digital wallets**
    1. Custodial vs. non-custodial wallets

2. Metamask
3. Cold vs. hot wallets
4. Trusted hardware and secure elements
5. Secret sharing and secure key management
6. Ethereum account abstraction

6. **Digital identity wallets**
    1. Challenges of fragmented and federated identity management
    2. Issuer, holder, and verifier
    3. Revocation and trust registries
    4. Data minimization with zero-knowledge proofs
    5. Demo: Lissi
    6. Man-in-the-middle attacks and mitigations
    7. Secure key management and recovery
    8. Can we trust our phones?
    9. User experience

7. **Paper discussion: Privacy and compliance in central bank digital currencies**
    1. CBDCs
    2. A history of digital cash: From e-Cash to Zcash
    3. Software vs. hardware based solutions
    4. Money Mules and the role of digital identities

Security of Mobile computing

Teacher(s)
Tegawendé François d Assise BISSYANDE

Language
English

Description

At the end of this course, learners will be familiar with most recent security issues in mobile computing. They will be knowledgeable in the research trends as well as with the practice

This course is designed to offer to the students some insights about the state of the art literature on the security in the mobile computing realm.
After an introduction, the course will develop through presentations of recent attacks, research findings as well as perspective of new security enhancement models.

EurIdentity Certificate

Teacher(s)
Sonja KMEC, Philippe POIRIER etc.

Language
English

Description

After successfully completing this module, the students will

- have a fundamental knowledge about European values (i.e., human dignity, freedom, democracy, equality, the rule of law and respect for human rights) and are able to reflect about them.
- have fundamental knowledge about the institutions, economy, politics, history, culture, law of the European states, Council of Europe and European Union.
- be able to work together productively in international & intercultural teams.
- be able to self-structure their learning in a fully online course setting.
- be able to synthesize diverse topics about Europe and European values, each topic being delivered by a different lecturer coming from different academic fields with their respective academic and teaching culture.

The module consists of two parts, Seminar 1 and Seminar 2. Seminar 1 contains 7 topic units and Seminar 2 comprises 5 topic units; all 12 being mandatory.
Contents of Seminar 1 “European values and identities”:

- Identity politics and representations: Group formation in the 20th and 21st centuries
- Sociology of religious and philosophical pluralisms
- Rule of law and fundamental rights in Europe
- European Economic and Social History 1870-2020
- History of Public Power in Europe 1870-2020
- Art trends in Europe
- European Labour Market

Contents of Seminar 2 “European challenges and actors”:

- Actors and decision-making processes in Europe
- The Economic Dimension of the EU
- European geopolitical actors and issues
- Rights and duties of European Individuals
- European scientific and environmental challenges and issues

Important:
This course includes a willingness to deal with learning platforms with other universities and acertain skill in dealing with computers / laptops. The course takes place ONLINE.