Université Paris-Saclay

Université de Versailles Saint-Quentin-en-Yvelines

M1 Mathématiques et interactions
Site UVSQ

Présentation et Syllabus [1]
(2021 - 2022)

1. Les informations contenues dans le présent document sont susceptibles d'évoluer légèrement.

Table des matières

Présentation

Le Master 1 «Mathématiques et Interactions» (MINT) de l'Université de Versailles Saint-Quentin-en-Yvelines est destiné à des étudiants désirant acquérir une formation solide et moderne dans le domaine des mathématiques et de leurs applications. Il fait partie du Master «Mathématiques et Applications» de l'Université Paris-Saclay.

L'objectif principal de ce master est de former des mathématiciens de haut niveau maîtrisant à la fois des techniques pointues d'algèbre et/ou d'analyse, ainsi que les outils de modélisation et de programmation qui leur ouvriront de nombreux débouchés professionnels.

La formation proposée dans le cadre du Master 1 «Mathématiques et Interactions - site UVSQ» s'articule autour d'un tronc commun et de deux spécialisations au choix. Le tronc commun comporte un socle de connaissances fondamentales en mathématiques, en informatique et en modélisation. Les deux spécialisations proposées sont ««Algèbre appliquée»» (AA) et ««Analyse, Modélisation et Simulation»» (AMS).

Après cette première année de Master, les deux spécialisations se poursuivent dans deux parcours : «Analyse, Modélisation et Simulation» et «Analyse, Arithmétique, Géométrie et Algébre Appliquée», faisant tous deux partie de la deuxième année du Master «Mathématiques et Applications» de l'université Paris-Saclay (voir schéma ci-dessous).

Le présent document contient un descriptif des cours du tronc commun et de chacune des deux spécialisations. On y trouve en particulier le poids, le volume horaire, le contenu et les objectifs de chaque cours. Une liste des enseignants qui interviendront dans ces cours est aussi présentée.

Spécialisation M1 «Algèbre appliquée» (AA)

Les étudiants qui se spécialiseront en algèbre appliquée suivront des cours approfondis en algèbre commutative, arithmétique, cryptographie et théorie algébrique des systèmes.

La spécialisation «Algèbre appliquée» ouvre à des débouchés académiques et privés : thèse dans un organisme public (universités, INRIA, etc.) ou en collaboration avec une entreprise privée, recherche en mathématiques fondamentales ou appliquées à la théorie du contrôle, à la cryptographie et à la sécurité informatique dans les milieux académique ou privé (Accenture, Dictao, Gemalto, Oberthur, Orange, etc.). Les étudiants pourront également s'orienter vers l'informatique théorique et les métiers d'ingénieurs dans le domaine des mathématiques appliquées à l'informatique (cryptologie, robotique).

Spécialisation M1 «Analyse, Modélisation et Simulation» (AMS)

Les étudiants qui suivront la spécialisation «Analyse, Modélisation et Simulation» auront des cours approfondis dans les domaines des équations aux dérivées partielles, de l'optimisation, du calcul scientifique et de la modélisation mécanique.

La spécialisation «Analyse, Modélisation et Simulation» prépare les étudiants à de nombreux débouchés académiques et professionnels. Au terme de leurs deux années de Master, ils pourront par exemple candidater à une thèse dans un organisme public (universités, INRIA, CEA, Onera) ou en collaboration avec une entreprise privée. Ils pourront également postuler à des emplois dans le monde professionnel (Airbus, EDF, Renault, PSA, Safran,Thalès, etc.).

Cours M1 de tronc commun

- Probabilités (semestre 1, 3 ECTS)
- Introduction au calcul formel et projet (semestre 1, 6 ECTS)
- Anglais (semestre 1, 3 ECTS)
- Analyse d'Algorithmes, Programmation (semestre 2, 5 ECTS)
- Introduction au calcul scientifique et projet (semestre 2, 6 ECTS)

Cours M1 de la spécialisation «Algèbre appliquée»

- Algèbre générale (semestre 1, 6 ECTS)
- Théorie des nombres et cryptographie (semestre 1, 6 ECTS)
- Cryptographie (semestre 1, 6 ECTS)
- Algèbre commutative (semestre 2, 6 ECTS)
- Introduction aux courbes elliptiques (semestre 2, 6 ECTS)
- Calcul sécurisé (semestre 2, 4 ECTS)
- Théorie de l'information (semestre 2, 3 ECTS)

Cours M1 de la spécialisation «Analyse, Modélisation et Simulation»

- Introduction à l'analyse fonctionnelle et aux équations aux dérivées partielles (6 ECTS)
- Optimisation numérique (semestre 1, 6 ECTS)
- 2 UE optionnelles au semestre 1 parmi :
  - Bases de la mécanique des milieux continus (semestre 1, 3 ECTS) - optionnelle
  - Mécanique analytique (semestre 1, 3 ECTS) - optionnelle
  - Introduction à la géométrie différentielle (semestre 1, 3 ECTS) - optionnelle
  - Méthodes numériques (semestre 1, 3 ECTS) - optionnelle
- Analyse des équations aux dérivées partielles (semestre 2, 6 ECTS)
- Méthodes numériques avancées et programmation (semestre 2, 6 ECTS)
- Méthodes inverses et assimilation de données (semestre 2, 4 ECTS)

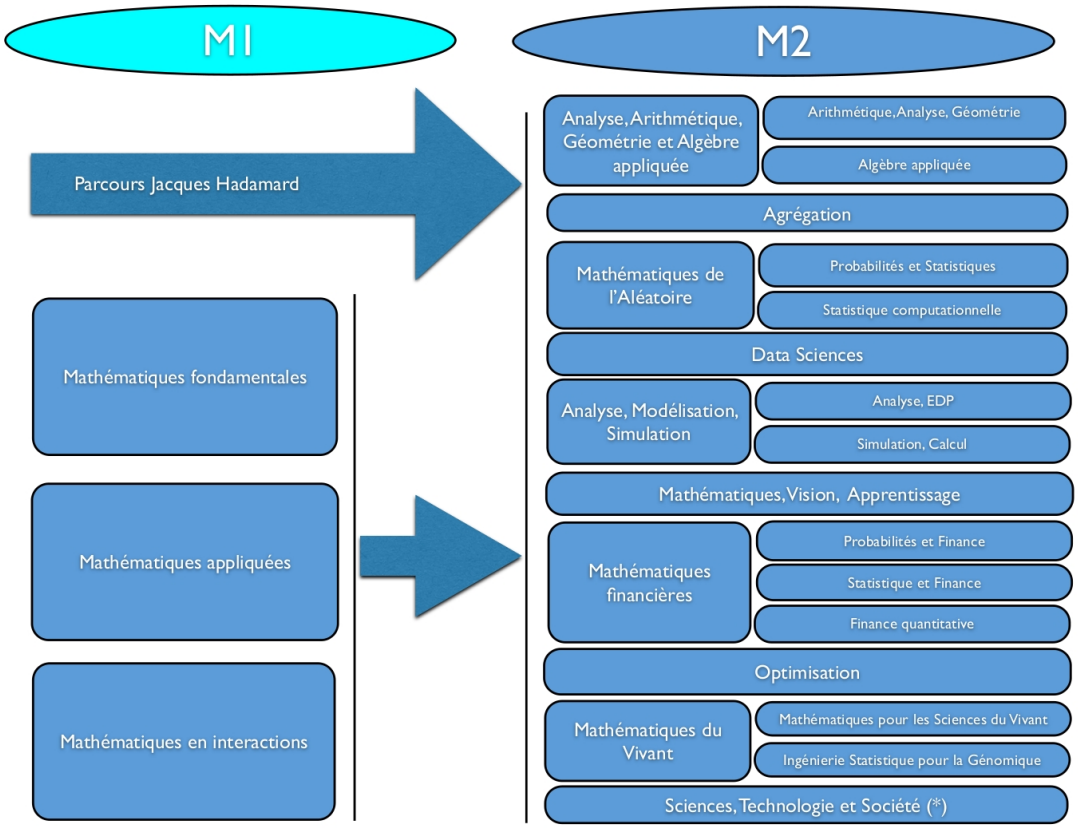
- 1 UE optionnelle au semestre 2 parmi :
  - Théorie de l'information (semestre 2, 3 ECTS) - optionnelle
  - Optimisation et recherche opérationnelle (semestre 2, 3 ECTS) - optionnelle

A l'exception de l'UE "Optimisation et recherche opérationnelle", tous les enseignements auront lieu sur le site de l'UFR Sciences de l'université de Versailles Saint-Quentin-enYvelines, situé au 45 avenue des Etats-Unis, Versailles (78000).

Dans la suite de ce document, on peut trouver d'autres informations telles que
— un schéma global (master 1 et master 2) du Master Mathématiques et Applications de l'université Paris-Saclay
— le calendrier prévisionnel 2020-2021
— les modalités de contrôle de connaissances
— un descriptif de toutes les UE
— les adresses des responsables des masters 1 M1 MINT, MMM et CHPS
— les coordonnées du corps professoral

Schéma du Master **Mathématiques et Applications**

de l'Université Paris-Saclay



Contacts

Enseignants responsables du master 1 MINT

- **Spécialisation "«Algèbre appliquée»" :** Ana-Maria Castravet
  (mél : `ana-maria.castravet@uvsq.fr`)
- **Spécialisation "«Analyse, Modélisation et Simulation»" :** Pierre Gabriel
  (mél : `pierre.gabriel@uvsq.fr`)
- **Responsable global :** Pierre Gabriel
  (mél : `pierre.gabriel@uvsq.fr`)

Secrétariat du département de mathématiques

Mme Estelle Blanc
Bâtiment Fermat, 45 avenue des États-Unis,
78035 Versailles Cedex.
Tél : +33 1 39 25 46 46
Mél : `estelle.blanc@uvsq.fr`

Scolarité

Bureau des Masters
Mme Véronique Delahaye
Bâtiment Fermat, 45 avenue des États-Unis,
78035 Versailles Cedex.
Mél : `veronique.delahaye@uvsq.fr`

Master 1 MMM (Méthodes Mathématiques pour la Mécanique)

Responsable : M. Paolo Vannucci (mél : `paolo.vannucci@uvsq.fr`)

Master 1 CHPS (Calcul Haute Performance et Simulation)

Responsables :
— M. Pablo Oliveira (mél : `pablo.oliveira@uvsq.fr`)
— M. Thomas Dufaud (mél : `thomas.dufaud@uvsq.fr`)

Modalités de contrôle des connaissances 2021 - 2022

Chaque UE (Unité d'Enseignement) est évaluée par une note finale. Cette note est attribuée à chaque étudiant inscrit cette UE en fonction de ses résultats aux contrôles de connaissances. Elle est calculée à partir d'une note de contrôle continu (CC) et/ou d'une note d'évaluation terminale, en fonction de l'UE considérée.

L'évaluation comporte deux sessions. La session de rattrapage (session 2) sera organisée en mai-juin 2021, pour les UE des deux semestres. Son but est de donner une seconde chance aux étudiants n'ayant pas validé certaines UE en session 1. Les notes de contrôle continu sont les mêmes dans les deux sessions.

Pour les UE relevant uniquement du département de mathématiques (voir les "tutelles" dans le descriptif des UE plus bas), la session 1 est évaluée en contrôle continu exclusif. La session 2 est évaluée à partir de la note de contrôle continu de la session 1 et de la note de l'examen de rattrapage selon la formule :
$\max\{(\text{note de rattrapage}) \times 100\%, (\text{note de CC}) \times 40\% + (\text{note de rattrapage}) \times 60\% \}$,
sauf pour les UE "Introduction au calcul formel et projet" et "Introduction au calcul scientifique et projet" pour lesquelles la formule est :
$(\text{note de CC}) \times 50\% + (\text{note de rattrapage}) \times 50\%$.
En particulier il n'y a pas de "max" dans le calcul de la note de session 2 pour ces deux UE qui contiennent une partie "projet".

Pour les UE relevant d'autres départements d'enseignement (à savoir "Anglais", "Cryptographie", "Calcul sécurisé", "Bases de la mécanique des milieux continus", "Mécanique analytique", "Introduction à la géométrie différentielle", "Méthodes numériques" et "Optimisation et recherche opérationnelle"), les étudiants sont invités à se rapprocher des enseignants pour connaître les modalités de contrôle des connaissances.

Emploi du temps

L'emploi du temps est disponible en ligne. Voici le lien https://edt.uvsq.fr/
(dans "Groupes", choisissez "M1 Mathématiques et Interactions").
Cet emploi du temps est susceptible d'être modifié. Il est donc important de le consulter régulièrement et de suivre les informations communiquées par les enseignants.

Calendrier provisoire 2021 - 2022

Le calendrier ci-dessous est susceptible d'être modifié. Il concerne tous les cours du master M1 MINT à l'exception des cours suivants :

- Cryptographie (S1)
- Bases de la mécanique des milieux continus (S1)
- Introduction àla géométrie différentielle (S1)
- Mécanique analytique (S1)
- Méthodes numériques (S1)
- Calcul sécurisé (S2)
- Optimisation et recherche opérationnelle (S2)

Ces cours relèvent du calendrier du master Méthodes Mathématiques pour la Mécanique (MMM), du master Calcul Haute Performance et Simulation (CHPS) ou du département d'informatique.

Calendrier 2021-2022 du master 1 «Mathématiques et Interactions»

Début des cours : lundi 20 septembre 2021.

Date limite d'inscription en ligne : jeudi 30 septembre 2021.

Date limite d'arrivée : lundi 11 octobre 2021.

Vacances de la Toussaint : du 30 octobre au 7 novembre 2021.

Vacances de la Noël : du 18 décembre 2021 au 2 janvier 2022.

Début des cours du semestre 2 : lundi 31 janvier 2022.

Vacances d'hiver : du 26 février au 6 mars 2022.

Vacances de printemps : du 30 avril au 8 mai 2022.

Examens de rattrapage (session 2) : entre le 23 mai et le 30 juin 2022.

Programme des cours

du Master 1

«Mathématiques et Interactions»

Tronc commun

Probabilités

Code UE: MYMAI101
Tutelle: Département de Mathématiques, UVSQ
Volume horaire: CM: 18h TD: 12h
ECTS: 3
Semestre: 1
Caractère: obligatoire
Intervenants: Emmanuel Rio
Lieu: UVSQ
Parcours: «Analyse, Modélisation et Simulation», «Algèbre appliquée»
Evaluation: voir «Modalités de contrôle des connaissances».

Pré-requis: Calcul intégral et Théorie de la mesure ; Probabilités

Description

Le module est consacré principalement à l'étude des chaînes de Markov à espace d'états discret, avec des applications aux marches aléatoires et à des processus à valeurs dans un espace d'états discret. Dans le cadre de cette étude, nous approfondirons les notions d'espérance conditionnelle et de loi conditionnelle. Le cours se terminera par des théorèmes limites incluant des rappels sur les différents modes de convergence possibles dans le domaine des probabilités.

Contenu

- Espaces de probabilités, variables aléatoires, indépendance
- Conditionnement, Espérance conditionnelle.
- Chaînes de Markov discètes, marches aléatoires discrètes
- Convergences des variables aléatoires
- Théorèmes limites pour les chaînes de Markov discètes,

Bibliographie

- J.F. Le Gall. Cours Fimfa. Intégration, probabilités et processus aléatoires. https://www.math.u-psud.fr/ jflegall/IPPA2.pdf
- P. Barbe et M. Ledoux, *Probabilité*, Belin, 1998.
- B. Bercu et D. Chafai, *Modélisation stochastique et simulation. Cours et applications*, Dunod, 2007.
- R. Durrett, *Probability : Theory and Examples*, Duxbury, 2005.
- D. Foata et A. Fuchs : *Calcul des Probabilités : Cours, exercices et problémes corrigés*, Dunod, 2003.
- Olivier Garet, Aline Kurtzmann, *De l'intégration aux probabilités*, Ellipses, 2011.
- P. Baldi, L. Mazliak et P. Priouret *Martingales et Chaînes de Markov*. Hermann, collection Méthodes, 1998.

Introduction au calcul formel et projet

Code UE: MYMAI106
Tutelle: Département de Mathématiques, UVSQ
Volume horaire: CM: 20h TP: 20h
ECTS: 6
Semestre: 1
Intervenants: Pierre-Guy Plamondon
Lieu: UVSQ
Caractère: obligatoire
Parcours: «Analyse, Modélisation et Simulation», «Algèbre appliquée»
Evaluation: voir «Modalités de contrôle des connaissances».

Pré-requis: algèbre et analyse de licence

Description

Ce cours est une initiation au Calcul formel (Computer Algebra en anglais). Celui-ci s'intéresse aux méthodes qui permettent de trouver des résultats de façon :

- Exacte (par opposition au Calcul numérique).
- Effective (par opposition aux théorèmes purement existentiels).
- Efficace (par opposition aux calculs dont la faisabilité est purement théorique).

L'outil de base est donc l'algorithme, dont on verra divers types. La question de l'efficacité donnera lieu à des analyses de complexité. Une partie non négligeable du cours se passera devant des ordinateurs, et sera consacrée à implémenter des algorithmes vus en cours en s'appuyant sur des logiciels de calcul formel tels que Sage. L'UE comporte aussi la réalisation d'au moins un projet dont la thématique et le contenu sont en lien avec les objectifs du cours.

Contenu

- Objets de base : Les grands entiers, les polynômes à 1 variable.
- Représentation. Addition et soustraction. Multiplication. Division euclidienne.
- Algorithme d'Euclide : pgcd, identité de Bézout. Applications.
- Arithmétique modulaire. Théorème chinois des restes.
- Evaluation et interpolation (polynômes de Legendre). Changement de représentation.
- Multiplication rapide : Karatsuba ; transformée de Fourier discrète.
- Division euclidienne rapide grâce à Newton.
- Evaluation et interpolation rapides. Théorème chinois des restes rapide.
- Algorithme d'Euclide rapide.
- Algèbre linéaire rapide : multiplication de matrices selon Strassen.
- Factorisation de polynômes sur un corps fini (Gauss).

Bibliographie

— J. Von zur Gathen & J. Gerhard, *Modern Computer Algebra*, 3rd Edition, Cambridge University Press (2013).

— V. Shoup, *A Computational Introduction to Number Theory and Algebra*, 2nd Edition, Cambridge University Press (2008).

Anglais

Code UE: MSANGS1
Tutelle: Institut d'Etudes Culturelles et Internationales
Volume horaire: CM: 0h TD: 27h
ECTS: 3
Semestre: 1
Caractère: obligatoire
Intervenants: Lionel Thevenard
Lieu: UVSQ
Parcours: «Analyse, Modélisation et Simulation», «Algèbre appliquée»
Evaluation: voir «Modalités de contrôle des connaissances».

Pré-requis:

- Etre capable de comprendre à l'oral comme à l'écrit des supports d'anglais général et scientifique.
- Etre capable de faire des présentations orales et écrites sur des sujets d'actualité divers.
- Avoir d'importantes notions en grammaire anglaise.

Description

Dans un contexte à caractère professionnel, les cours en anglais Master visent à aider les étudiants à faire face aux exigences du monde du travail.

Contenu

- Job Interview
- Debating
- CV - Cover letter - Essay writing
- Listening Comprehension
- TOEIC training

Introduction au calcul scientifique et projet

Code UE: MYMAI209
Tutelle: Département de Mathématiques, UVSQ
Volume horaire: CM: 20h TP: 20h
ECTS: 6
Semestre: 2
Intervenants: Tahar Boulmezaoud
Lieu: UVSQ
Caractère: obligatoire
Parcours: «Analyse, Modélisation et Simulation», «Algèbre appliquée»
Evaluation: voir «Modalités de contrôle des connaissances».

Pré-requis: analyse et algèbre linéaire et matriciel de licence

Description

Le but de cette UE est de préparer les étudiants aux bases de la programmation et du calcul scientifique. Elle comporte essentiellement trois parties.
La première partie du cours sera dédiée à la maitrise des éléments fondamentaux d'un langage de programmation de type C ou Python. L'apprentissage du langage sera accompagné d'une mise en oeuvre de quelques algorithmes numériques.
La deuxième partie sera consacrée aux méthodes numériques modernes et leur implémentation. Il s'agira essentiellement de la résolution de systèmes linéaires, des équations différentielles et des équations aux dérivées partielles. On y abordera aussi l'étude de problèmes issus de la modélisation mathématique de phénomènes rencontrés dans d'autres disciplines (physique, biologie, sciences de l'ingénieur, science de données, etc.).
La troisième partie consistera en la réalisation d'un projet.

Contenu

- Eléments et bases de la programmation en Langage C (ou en Python).
- Rappels sur les méthodes directes pour la résolution de systèmes linéaires
- Méthodes itératives classiques (Jacobi, Gauss-Seidel, relaxation).
- Méthodes itératives modernes. Méthodes des sous-espaces de Krylov.
- Calcul de valeurs propres.
- Schémas de résolution d'équations différentielles.
- Méthode des différences finis.
- Introduction à la méthode des éléments finis (problèmes aux limites 1D et 2D)

Bibliographie

— J. Stoer et R. Bulirsh, Introduction to numerical analysis, Springer (2nd edition).
— Introduction à l'analyse numérique matricielle et Optimisation : Ph. G. Ciarlet, Masson, 1988.
— Introduction au calcul scientifique. Aspects algorithmiques, P. Ciarlet, en ligne.
— Analyse numérique des équations aux dérivées partielles, R. Herbin, HAL, en ligne.

— A. Ern et J.-L. Guermond, éléments finis : théorie, applications, mise en oeuvre, Springer.

Analyse d'algorithmes, Programmation

Code UE: MYMAI201
Tutelle: Département de Mathématiques, UVSQ
Volume horaire: CM: 16h TD: 20h
ECTS: 5
Semestre: 2
Intervenants: Christina Boura et Yann Rotella
Lieu: UVSQ
Caractère: obligatoire
Parcours: «Analyse, Modélisation et Simulation», «Algèbre appliquée», Informatique
Evaluation: voir «Modalités de contrôle des connaissances».

Pré-requis: non suggérés

Description

Introduction aux techniques de conceptions d'algorithmes et d'analyse de performances. TPs sur machine avec environnement Python/Sage.

Contenu

- Analyse d'algorithmes, modèles de complexité, complexité asymptotique, classes de complexité.
- Structures de données et algorithmes : ordonnancement, piles, files, tables de hachage, arbres, graphes.
- Programmation dynamique, programmation linéaire entière.
- Algorithmes arithmétiques : multiplication, pgcd, multiplication de matrices.
- Algorithmes géométriques : programmation linéaire, diagrammes de Vornoï

Bibliographie

- Thomas H. Cormen. Charles E. Leiserson. Ronald L. Rivest. Clifford Stein. Introduction to Algorithms. Third Edition. The MIT Press. Cambridge, Massachusetts.
- Christos H. Papadimitriou. Computational complexity. Addison-Wesley, 1994. 523 pages.

Spécialisation «Algèbre appliquée»

Algèbre générale

Code UE: MYMAI102
Tutelle: Département de Mathématiques, UVSQ
Volume horaire: CM: 24h TD: 24h
ECTS: 6
Semestre: 1
Intervenants: Maria Chlouveraki
Lieu: UVSQ
Caractère: obligatoire
Parcours: «Algèbre appliquée»
Evaluation: voir «Modalités de contrôle des connaissances».

Pré-requis: Algèbre de licence (anneaux, idéaux, groupes)

Description

La théorie de Galois, développée par le mathématicien français Evariste Galois (1811-1832), établit le lien entre deux familles d'objets algébriques : les groupes et les corps. Dans ce cours nous allons étudier des différents types d'extensions de corps (finies, algébriques, séparables, normales, galoisiennes) et leurs groupes d'automorphismes afin d'arriver à démontrer le théorème fondamental de la théorie de Galois qui établit le lien mentionné ci-dessus.

Contenu

- extensions de corps : finies, algébriques, séparables, normales, galoisiennes
- morphismes d'extensions
- groupes de Galois
- théorème fondamental de la théorie de Galois

Bibliographie

- Calais J., Extensions de corps, théorie de Galois, Ellipses, 2006.
- Chambert-Loir A., Algèbre corporelle, disponible à l'adresse : `http://www.math.polytechnique.fr/ chambert/`
- Escofier J.-P., Théorie de Galois, Dunod, 2000.
- Gozard I., Théorie de Galois, Ellipses, 1997.
- Morandi P., Field and Galois theory, GTM 167, Springer, 1996.
- Tauvel P., Corps commutatifs et théorie de Galois, Calvage et Mounet, 2008.

Théorie des nombres et cryptographie

Code UE: MYMAI103
Tutelle: Département de Mathématiques, UVSQ
Volume horaire: CM: 24h TD: 24h
ECTS: 6
Semestre: 1
Intervenants: Ana-Maria Castravet
Lieu: UVSQ
Caractère: obligatoire
Parcours: «Algèbre appliquée»
Evaluation: voir «Modalités de contrôle des connaissances».

Pré-requis: Algèbre de Licence (groupes, anneaux, corps, polynômes et congruences)

Description

L'objectif de ce cours est de mettre en évidence la façon dont des propriétés algébriques (notamment les structures de groupe et d'anneau) peuvent servir à prouver des résultats arithmétiques, avec des applications à la cryptographie. Au début du cours, on rappelle brièvement les notions de théorie des groupes et des anneaux qui seront nécessaires dans la suite. On étudie notamment l'anneau des entiers relatifs et les anneaux de polynômes en une indéterminée à coefficients dans un corps, en insistant sur leurs propriétés algébriques communes. On étudie ensuite les propriétés arithmétiques des anneaux de congruence $\mathbb{Z}/n\mathbb{Z}$ et des corps finis, y compris la loi de réciprocité quadratique de Gauss, et on en déduit plusieurs tests de primalité. On introduit ensuite diverses propriétés de structure (anneaux euclidiens, principaux, factoriels, intégralement clos, etc.) et leurs conséquences en arithmétique (notamment le théorème des deux carrés). On introduit enfin la notion d'entier quadratique et on démontre le théorème des unités, qui permet de résoudre l'équation de Pell $x^2+dy^2=1$.

Contenu

- Groupes et anneaux
- Entiers et polynômes en une indéterminée
- Congruences modulo un entier
- Corps finis
- Les entiers de Gauss et le théorème des deux carrés
- Anneaux euclidiens, principaux, factoriels
- Le théorème des unités et l'équation de Pell

Bibliographie

- M. Demazure, *Cours d'algèbre*, Cassini, 1997.
- M. Hindry, *Arithmétique*, Calvage et Mounet, 2008.
- K. Ireland et M. Rosen, *A classical introduction to modern number theory*, Graduate texts in mathematics **84**, Springer, 1990.

— D. Perrin, *Cours d'algèbre*, Ellipses, 1996.

Cryptographie

Code UE: MIN15123
Tutelle: Département d'Informatique et Département de Mathématiques, UVSQ
Volume horaire: CM: 15h TD: 30h
ECTS: 6
Semestre: 1
Intervenants: Louis Goubin
Lieu: UVSQ
Caractère: obligatoire
Parcours: «Algèbre appliquée»
Evaluation: voir «Modalités de contrôle des connaissances».

Pré-requis: Algèbre et algébre linéaire de licence : arithmétique modulaire, calculs dans les corps finis. Rudiments de théorie des probabilités et de statistiques. Connaissances de base en algorithmique.

Description

Le but est de présenter un panorama des principaux algorithmes utilisés en chiffrement, authentification et signature électronique, ainsi que leur utilisation pour sécuriser les communications numériques.
A l'issue de ce cours, les étudiants devront pouvoir :

- utiliser l'arithmétique modulaire et les opérations de base sur les corps finis liées aux techniques cryptographiques
- décrire les concepts et algorithmes cryptographiques de base, incluant le chiffrement/déchiffrement, les fonctions de hachage et la cryptographie à clé publique
- évaluer la sécurité de primitives cryptographiques
- concevoir et analyser des protocoles pour des objectifs de sécurité variés

Contenu

- Cryptographie à clé secrète, Cryptographie à clé publique
- Attaques brutales, attaques par rejeu
- Attaques à chiffré seul, attaques à clair choisi, attaques à clair et chiffré choisis
- Attaques interactives et non interactives
- Chiffrement par flot, chiffrement par blocs
- Transposition et substitution, schémas de Feistel
- DES, AES
- Fonctions à sens unique, fonctions de hachage
- Algorithmes d'échange de clés
- RSA, Algorithmes zero-knowledge
- Applications

Bibliographie

— N. Koblitz, *A Course in Number Theory and Cryptography*, GTM 114, Springer, 1994.

— A.J. Menezes, P.C. van Oorschot, S.A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1997.

— D. Stinson, *Cryptography : Theory and Practice*, Third Edition (Discrete Mathematics and Its Applications), CRC Press, 2005.

— S. Vaudenay, *A Classical Introduction to Cryptography : Applications for Communications Security*, Springer, 2005.

Algèbre commutative

Code UE: MYMAI203
Tutelle: Département de Mathématiques, UVSQ
Volume horaire: CM: 24h TD: 24h
ECTS: 6
Semestre: 2
Intervenants: Maria Chlouveraki
Lieu: UVSQ
Caractère: obligatoire
Parcours: «Algèbre appliquée»
Evaluation: voir «Modalités de contrôle des connaissances».

Pré-requis: Algèbre de Licence (groupes, anneaux, corps, polynômes et congruences), cours de théorie des nombres et cryptographie

Description

L'objectif de ce cours est de permettre aux étudiants d'aborder sereinement la géométrie algébrique et l'algèbre effective. Le cours est tourné vers l'étude des anneaux de polynômes. On cherche constamment à interpréter géométriquement les théorèmes d'algèbre abstraite : lemme de normalisation vs. projection sur un espace vectoriel, Nullstellensatz vs. recherche de l'idéal d'un fermé algébrique. Interprétation géométrique de la dimension de Krull.

Contenu

- Anneaux noethériens, théorème de la base de Hilbert.
- Topologie de Zariski de k^n.
- Correspondance entre idéaux et fermés algébriques.
- Anneaux de fractions, localisation.
- Extensions entières : going up et going down.
- Lemme de normalisation, degré de transcendance, dimension.
- Nullstellensatz.

Bibliographie

- Atiyah et Mac Donald, *An introduction to commutative algebra*, Addison-Wesley, 1969.
- Chambert-Loir *Algèbre commutative et introduction) la géométrie algébrique* http://www.math.u-psud.fr/ chambert/enseignement/2013-14/aceiga/Dea.pdf
- Cox, Little et O'Shea, *Ideal, varieties and algorithms*, Springer, 1991.
- Matsumura, Hideyuki *Commutative ring theory*. Cambridge University Press, 1986.
- C. Peskine *An algebraic introduction to complex projective geometry, I. Commutative algebra*, Cambridge University Press, 1996.
- D. Perrin, *Cours d'algèbre*, Ellipses, 1996.
- Samuel et Zariski, *Commutative algebra*, 2 volumes, Springer.

Introduction aux courbes elliptiques

Code UE: MYMAI205
Tutelle: Département de Mathématiques UVSQ
Volume horaire: CM: 24h TD: 24h
ECTS: 6
Semestre: 2
Intervenants: Vincent Sécherre et Mohamed Krir
Lieu: UVSQ
Caractère: obligatoire
Parcours: «Algèbre appliquée»
Evaluation: voir «Modalités de contrôle des connaissances».

Pré-requis: Cours de Théorie des nombres et cryptographie, semestre 1 M1

Description

On donne les notions élémentaires introductives à la théorie des courbes elliptiques. L'accent sera mis sur l'aspect concret avec des exemples de calcul explicite. On introduit d'abord le plan projectif sur un corps, on définit ensuite les courbes elliptiques, la loi de groupe, les fonctions rationnelles et les diviseurs. La dernière partie sera consacrée aux notions de morphismes, isogénies, points de torsion et au théorème de Hasse.

Contenu

- Fonctions sur la droite projective
- Courbes elliptiques
- Fonctions rationnelles sur une courbe elliptique
- Diviseurs sur une courbe elliptique
- Morphismes entre courbes elliptiques
- Isogénies
- Points de torsion
- Couplage de Weil
- Théorème de Hasse

Bibliographie

- J. H. Silvermann, *The arithmetic of elliptic curves*, Springer 1986.
- *Tout autre livre introductif sur les courbes elliptiques*

Calcul sécurisé

Code UE: MIN17218
Tutelle: Département d'Informatique et département de Mathématiques, UVSQ
Volume horaire: CM: 12h TD: 24h
ECTS: 4
Semestre: 2
Intervenants: Louis Goubin
Lieu: UVSQ
Caractère: obligatoire
Parcours: «Algèbre appliquée»
Evaluation: voir «Modalités de contrôle des connaissances».

Pré-requis: Cours de cryptographie (M1 MINT, 1er semestre)

Description

Traditionnellement, en cryptographie, on cherche à garantir la confidentialité, l'intégrité et l'authenticité de «messages», qui sont des objets «statiques» (stockés, ou transmis tels quels sur des canaux de communication non sécurisés). En revanche on ne considère pas la sécurité des algorithmes et protocoles cryptographiques eux-mêmes (qui sont en général des programmes, qui s'exécutent, et sont donc des objets «dynamiques»). Par exemple on ne s'intéresse pas :

- à la confidentialité des programmes (le principe de Kerckhoffs suppose qu'ils sont connus de tout le monde),
- ni à leur intégrité (on suppose qu'Alice et Bob exécutent ces algorithmes / protocoles / programmes correctement, sans aucune modification / erreur / bug),
- ni à leur authenticité (on suppose que les algorithmes / protocoles / programmes exécutés par Alice et Bob ont été installés par une autorité de confiance).

Dans l'UE «Calcul sécurisé», on verra qu'en réalité il est très important de sécuriser également les calculs (au sens d'algorithmes / protocoles / programmes).

Contenu

- Le cours couvrira des aspects pratiques de ces problèmes de sécurité (débordement de tampon, rétro-analyse de code, attaques par canaux auxiliaires, injection de fautes, ...)
- Ce sera aussi l'occasion d'approfondir des questions plus théoriques (modélisation de la notion de calcul, machines de Turing, garbled circuits, programmes auto-modifiants, obfuscation de code, ...), en montrant comment ces notions peuvent être utilisées pour prévenir les vulnérabilités du logiciel.
- Le cours et les TDs seront illustrés par de nombreux exemples, notamment issus de la sécurité des cartes à puce, de la virologie informatique, et des applications émergentes dans le «calcul en nuage» (cloud computing).

Théorie de l'information

Code UE: MYMAI213
Tutelle: Département de Mathématiques, UVSQ
Volume horaire: CM: 12h TD: 12h
ECTS: 3
Semestre: 2
Intervenants: Edouard Rousseau
Lieu: UVSQ
Caractère: obligatoire en «Algèbre appliquée», optionnelle en «Analyse, Modélisation et Simulation»
Parcours: «Algèbre appliquée», «Analyse, Modélisation et Simulation»
Evaluation: voir «Modalités de contrôle des connaissances».

Pré-requis: Algèbre linéaire. Quelques éléments d'algèbre. Théorie él"mentaire des probabilités.

Description

Le but d'un système de communication est le transport d'information d'une source à un destinataire via un canal de communication. Ce canal possède en général des imperfections ce qui peut engendrer des erreurs de transmission. Aussi, le canal peut être sujet à des écoutes ce qui peut poser des problèmes de confidentialité. Finalement, l'utilisation d'un canal a un coût, il est donc important d'optimiser son usage.

Pour répondre à ces différentes exigences, on effectue un prétraitement de l'information ; il s'agit de la chaîne de codage. Celle-ci se divise en trois étapes : compression, chiffrement et ajout de redondance. Ces techniques font appel à la théorie des probabilités et à l'algèbre discrète. Ce cours présente les bases de la première et la troisième étape de la chaîne de codage, la seconde étant abondamment étudiée dans des cours de cryptographie.

Contenu

- Notions de base en théorie de l'information (entropie, information mutuelle).
- Algorithmes de compression sans perte (étape 1 de la chaîne de codage).
- Théorie des codes correcteurs d'erreurs (étape 3 de la chaîne de codage).
  - Canal sans mémoire à temps discret. Notion de capacité. Théorème de codage pour un canal bruyant. Principe de décodage par maximum de vraisemblance. Borne sur la probabilité d'erreur de décodage.
  - Théorie des codes correcteurs en blocs. Distance minimale et problématique des bornes sur la taille d'un code. Notion de code parfait.
  - Codes linéaires. Matrice génératrice et matrice de parité. Décodage par syndrome. Codes duaux. Polynôme énumérateur des poids. Identité de Mac-Williams.
  - Etude de certaines familles de codes linéaires (en bloc) et algorithmes de décodage.

— Codes convolutionnels et algorithme de Viterbi.

Bibliographie

— The Theory of Error-Correcting Codes. F. J. MacWilliams, N. J. A. Sloane North Holland Publishing Co. 1977.
— Théorie des codes (Compression, cryptage, correction). J.-G. Dumas, J.-L. Roch, E. Tannier et S. Varrette, Dunod 2007.

Spécialisation «Analyse, Modélisation et Simulation»

Introduction à l'analyse fonctionnelle et aux équations aux dérivées partielles

Code UE: MYMAI104
Tutelle: Département de Mathématiques, UVSQ
Volume horaire: CM: 24h TD: 24h
ECTS: 6
Semestre: 1
Caractère: obligatoire
Intervenants: Pierre Gabriel
Lieu: UVSQ
Parcours: «Analyse, Modélisation et Simulation»
Evaluation: voir «Modalités de contrôle des connaissances».

Pré-requis: Fonctions de plusieurs variables, Calcul différentiel, Calcul intégral, Espaces vectoriels normés

Description

Ce cours commencera par l'introduction à des outils d'analyse hilbertienne et au calcul des distributions. Ces outils seront ensuite employés pour analyser quelques équations aux dérivées partielles elliptiques issues de la physique et de la mécanique.

Contenu

- Rappels et compléments sur les espaces vectoriels normés.
- Espaces de Hilbert, projection orthogonale, base hilbertienne,
- Théorème de Riesz-Fréchet, Théorème de Lax-Milgram
- Eléments sur les distributions. Transformation de Fourier.
- Espace L^2. Espaces de Sobolev H^m.
- Traces et formules de Green.
- Inégalités de Poincaré et de Poincaré-Wirtinger.
- Exemples d'équations aux dérivées partielles. Equation de Poisson. Solution fondamentale.

Bibliographie

- Pierre-Arnaud Raviart & Jean-Marie Thomas : Introduction à l'analyse numérique des équations aux dérivées partielles, Dunod, 1998.
- Haïm Brézis, Analyse fonctionnelle, Dunod, 1983.
- Lawrence C. Evans, Partial differential equations, Graduate Studies in Mathematics, Vol. 19, AMS.
- Laurent Schwartz, Méthodes mathématiques pour les sciences physiques, Hermann, 1961.

Optimisation numérique

Code UE: MYMAI105
Tutelle: Département de Mathématiques, UVSQ
Volume horaire: CM: 24h TD: 24h
ECTS: 6
Semestre: 1
Caractère: obligatoire
Intervenants: Laurent Dumas
Lieu: UVSQ
Parcours: «Analyse, Modélisation et Simulation»
Evaluation: voir «Modalités de contrôle des connaissances».

Pré-requis: Fonctions à plusieurs variables, notions de calcul différentiel.

Description

De très nombreux problèmes en industrie, en physique et en économie consistent en la minimisation (ou la maximisation) d'une fonction objective. Ce cours vise à présenter un grand nombre de méthodes numériques qui ont été développées pour résoudre de tels problèmes. Ces méthodes peuvent être locales ou globales, déterministes ou stochastiques. De nombreux exemples seront implémentés sur machine afin d'illustrer l'emploi en pratique de ces méthodes.

Contenu

1. Introduction et rappels d'analyse
   - exemple de problème d'optimisation de formes en mécanique
   - formules de Taylor
   - rappel des conditions d'optimalité avec et sans contraintes
2. Méthodes de descente sans contrainte (descente avec recherche linéaire, Newton et quasi Newton)
3. Méthodes de descente avec contraintes (gradient projeté, pénalisation externe, algorithme d'Uzawa)
4. Méthodes de nature stochastique : recu

— Introduction. Exemples.
— Convexité : ensembles convexes, fonctions convexes, propriétés.
— Optimisation sans contraintes : conditions d'optimalité d'ordres 1 et 2.
— Optimisation avec contraintes : Théorème de Karush-Kuhn-Tucker, multiplicateurs de Lagrange. Cas d'un programme convexe.
— Programmation linéaire. Méthode du simplexe.
— Calcul de variations
  — Exemples
  — Conditions d'optimalité avec extrémités fixes. Equations d'Euler-Lagrange.
  — Cas d'extrémités libres. Conditions de transversalité.

— Méthodes numériques : méthodes de descente (de gradient, de quasi-newton, etc.), méthodes stochastiques (récuit simulé, algorithmes génétiques, etc.).

Bibliographie

— Ph. G. Ciarlet, Introduction à l'analyse numérique matricielle et Optimisation, Masson, 1988.
— J. F. Bonnans, Optimisation continue : cours et exercices, Dunod, 2006.
— H. B. Hiriart-Urruty and C. Lemaréchal, Convex analysis and minimization algorithms, Vol. I, II, Springer-Verlag, 1993.

Méthodes numériques

Code UE: MYMMM104
Tutelle: Département de physique, UVSQ
Volume horaire: CM: 13.5h TD: 13.5h
ECTS: 3
Semestre: 1
Lieu: Université de Versailles Saint-Quentin-en-Yvelines
Caractère: optionnel (en MINT)
Intervenants: Stéphanie Basseville
Parcours: «Analyse, Modélisation et Simulation»
Evaluation: voir «Modalités de contrôle des connaissances».

Pré-requis: Cours d'analyse numérique de licence de mécanique ou UE équivalente.

Description

La simulation numérique a pris une place essentielle dans la majorité des domaines scientifiques, et en particulier dans celui de la mécanique, et sa maîtrise est devenue incontournable dans une formation axée autour des sciences de l'ingénieur et de la recherche. Plus précisément, ce cours apportera aux étudiants les connaissances de base, nécessaires au traitement numérique des équations aux dérivées partielles issues de la mécanique des milieux continus et introduira les principales méthodes permettant de résoudre ces équations, principalement les méthodes de différences et éléments finis.
Le cours sera accompagné de travaux dirigés.

Contenu

- Présentation d'équations aux dérivées partielles, issues de la physique et/ou de la mécanique des milieux continus.
- Méthode des différences finies (principe, discrétisation, les schémas, conditions de Dirichlet, Neumann, mixtes...)
- Méthode des éléments finis (principe, discrétisation, interpolation, matrices élémetaires, assemblage,...)

Bibliographie

- R. Théodor, Initiation à l'analyse numérique, CNAM cours A, Masson, 1994.
- D. Euvard, Résolution numérique des équations aux dérivées partielles de la physique, de la mécanique et des sciences de l'ingénieur. Masson
- N. Recho, J. Bares, R. Benjamin, Méthode de calcul par éléments finis, Technosup, 2015.
- J-L. Batoz, Modélisation des structures par éléments finis -Tome 1, Hermes.

Introduction à la géométrie différentielle

Code UE: MYMMM***
Tutelle: Département de Physique, UVSQ
Volume horaire: CM: 15h TD: 9h
ECTS: 3
Semestre: 1
Caractère: optionelle
Intervenants: Paolo Vannucci
Lieu: UVSQ
Parcours: «Analyse, Modélisation et Simulation»
Evaluation: voir «Modalités de contrôle des connaissances».

Pré-requis: Calcul différentiel dans $\mathbb{R}^n$.

Contenu

- Géométrie différentielle des courbes et des surfaces : repère de Frénet, courbure, torsion, espace tangent à une surface, formes fondamentales sur une surface, courbure.
- Notion de sous variété de $\mathbb{R}^n$, calcul différentiel du premier ordre sur les sous variétés : espace tangent et cotangent, submersions, immersions plongements, champs de vecteurs, flot, dérivation de Lie des champs, formes différentielles
- Introduction à la notion de variété différentielle et variété riemannienne.

Bibliographie

- Do Carmo : *Differential Geometry of Curves and Surfaces*. Prentice-Hall, 1976.
- Lelong-Ferrand : *Géométrie différentielle : tenseurs, formes différentielles*.

Mécanique analytique

Code UE: MYMMM***
Tutelle: Département de Physique, UVSQ
Volume horaire: CM: 15h TD: 9h
ECTS: 3
Semestre: 1
Caractère: optionelle
Intervenants: Paolo Vannucci
Lieu: UVSQ
Parcours: «Analyse, Modélisation et Simulation»
Evaluation: voir «Modalités de contrôle des connaissances».

Pré-requis: Algèbre linéaire, analyse mathématique, mécanique générale.

Contenu

- Principe des travaux virtuels ; liens holonomes et non, déplacements virtuels, coordonnées lagrangiennes.
- Équations de Lagrange : principe de Hamilton, rappels de calcul des variations ; coordonnées cycliques, intégrales premières, Théorème de Noether. Forces dissipatives, systèmes anholonomes.
- Champs de force centrale ; problèmes de deux corps, orbites dégénerées et générales, stabilité des orbites circulaires, problème de Kepler.
- Propriétés d'inertie de systèmes ; barycentre, tenseur d'inertie, Théorème de Huygens-Steiner.
- Dynamique lagrangienne des corps rigides ; moment linéaire et angulaire, conservation, énergie cinétique, equations du mouvement, Théorème de Koenig. Equations d'Euler, mouvements à la Poinsot, gyroscopes.
- Équilibre : définition et conditions d'équilibre ; stabilité à la Lyapounov, espace des phases, Théorème de Lagrange-Dirichlet ; bifurcation de l'équilibre, claquage.
- Petits mouvements : lemme de diagonalisation simultanée, lagrangienne carrée, équations linéarisées, modes normaux.
- Mécanique Hamiltonienne : équations de Hamilton, dérivation d'un principe variationnel, mise en oeuvre du formalisme hamiltonien.

Bibliographie

- H. Goldstein : *Mécanique Classique*. PUF
- L. Landau, E. Lifshitz : *Physique Théorique : Mécanique*. Ellipses

Bases de la mécanique des milieux continus

Code UE: MYMMM105
Tutelle: Département de physique, UVSQ
Volume horaire: CM: 15h TD: 09h
ECTS: 3
Semestre: 1
Lieu: Université de Versailles Saint-Quentin-en-Yvelines
Caractère: optionnelle
Intervenants: Paolo Vannucci
Parcours: «Analyse, Modélisation et Simulation»
Evaluation: voir «Modalités de contrôle des connaissances».

Pré-requis: Mécanique générale, algèbre matricielle

Description

Ce cours est un module d'introduction aux notions fondamentales de la mécanique des corps déformables. Les questions concernant la deformation des milieux continus, les actions internes, les lois de comportement y sont abordées. Ce module est une étape préliminaire pour les développements qui seront abordés dans d'autres modules concernant la modélisation des solides et des structures.

Contenu

- Rappels de mécanique générale : principes fondamentaux, énergie, travail, contraintes au mouvement, équations de Lagrange.
- Milieux déformables : Gradient et mesures de la déformation ; linéarisation : le tenseur des déformations infinitésimales.
- Lois de bilan : conservation de la masse, de la quantité de mouvement, de son moment et de l'énergie ; actions internes, notion de contrainte mécanique, tenseur de la contrainte de Cauchy, équations locales de mouvement et d'équilibre.
- Elasticité : loi de Hooke, équations de Lamé, matériaux anisotropes, théorèmes fondamentaux de la théorie de l'élasticité. Problème thermo-élastique : loi de Hooke-Duhamel. Résolution des problèmes d'élastostatique : approche semi-inverse, cas notables.

Bibliographie

- H. Goldberg : Classical mechanics. 1950.
- S. Timoshenko, J. N. Goodier : *Theory of elasticity*. Second edition. McGraw-Hill, 1951.
- P. Vannucci : Mécanique générale. Téléchargeable, 2003.
- P. Germain, P. Muller : Introduction à la mécanique des milieux continus. Masson, 1980.

Analyse des équations aux dérivées partielles

Code UE: MYMAI207
Tutelle: Département de Mathématiques, UVSQ
Volume horaire: CM: 24h TD: 24h
ECTS: 6
Semestre: 2
Caractère: obligatoire
Intervenants: Tahar Boulmezaoud
Lieu: UVSQ
Parcours: «Analyse, Modélisation et Simulation»
Evaluation: voir «Modalités de contrôle des connaissances».

Pré-requis: Calcul intégral, calcul différentiel, notions de distributions, éléments de topologie

Description

Ce cours a comme ambition d'introduire quelques outils d'analyse des équations aux dérivées partielles. Il commencera par quelques notions et résultats de base en analyse fonctionnelle et concernant les espaces de Sobolev. On abordera ensuite létude de quelques équations fondamentales telles que l'équation des ondes et l'équation de Schrödinger.

Contenu

- Rappels de topologie générale (espaces topologiques, espaces métriques, espaces vectoriels topologiques, espaces vectoriels normés, etc).
- Eléments d'Analyse fonctionnelle :
  - Compléments sur les espaces de Hilbert et de Banach.
  - Dualité.
  - Théorèmes de Hahn-Banach et Banach-Steinhaus. Théorème de l'application ouverte, théorème du graphe fermé.
  - Convergences faible et faible étoile.
- Espaces L^p et espaces de Sobolev. Théorèmes de densité. Théorèmes de trace. Formules de Green.
- Formulation variationnelle.
- Équation de Poisson dans des domaines bornés.
- Équations d'évolution. Équation de la chaleur. Équation des ondes. Équation de Schrödinger

Bibliographie

- Haïm Brézis, Analyse fonctionnelle, Dunod, 1983.
- Claude Zuily, Distributions et équations aux dérivées partielles, Hermann, 2001.
- Lawrence C. Evans, Partial differential equations, Graduate Studies in Mathematics, Vol. 19, AMS.

Méthodes numériques avancées et programmation

Code UE: MYMAI206
Tutelle: Département de Mathématiques, UVSQ
Volume horaire: CM: 24h TD: 24h
ECTS: 6
Semestre: 2
Caractère: obligatoire
Intervenants: Christophe Chalons
Lieu: UVSQ
Parcours: «Analyse, Modélisation et Simulation»
Evaluation: voir «Modalités de contrôle des connaissances».

Pré-requis: notions sur les distributions et les espaces de Sobolev (suggérés mais non obligatoires)

Description

L'objectif de ce cours est de proposer une introduction à l'analyse mathématique et à l'approximation numérique des solutions de certaines équations aux dérivées partielles (EDP). Ces équations interviennent de manière récurrente dans de nombreuses applications, qu'il s'agisse d'ingénierie mécanique et physique (aéronautique, nucléaire, ingénierie pétrolière, automobile...) ou de finance, d'économie, de chimie...etc.
Nous présenterons des résultats importants d'analyse théorique des EDP ainsi que les trois grandes classes de méthodes numériques associées (méthode des éléments finis, méthode des volumes finis et méthode des différences finies).
L'objectif de ce cours est également d'apporter aux élèves une première expertise numérique pour la résolution des équations aux dérivées partielles en leur proposant de programmer, de tester et de comparer différentes méthodes sur des problèmes concrets.

Contenu

- EDP elliptiques
  - Rappels sur les distributions et les espaces de Sobolev
  - Formulation variationnelle
  - Théorème de Lax-Milgram
  - Etude de la méthode des éléments finis en 1D et en 2D
- EDP hyperboliques
  - Equation de transport et équation des ondes
  - Introduction à la méthode des volumes finis
- EDP paraboliques
  - Equation de la chaleur
  - Introduction à la méthode des différences finies

Bibliographie

1 Pierre-Arnaud Raviart, Jean-Marie Thomas : Introduction à l'analyse numérique des équations aux dérivées partielles, éditions Dunod 1998.
2 Brigitte Lucquin : Equations aux dérivées partielles et leurs approximations, Ellipses, 2004.
3 E. Godlewski et P.-A. Raviart : Hyperbolic systems of conservation laws, Ellipses 1991.
4 Lawrence C. Evans : Partial differential equations, Graduate Studies in Mathematics, Vol. 19, AMS.
5 C. Strikwerda : Finite Difference Schemes and Partial Differential Equations, SIAM 2004.
6 L. Hörmander : Lectures on Nonlinear Hyperbolic Differential Equations, Springer 1997.
7 F. Lagoutière : Polycopié de cours sur les Equations aux dérivées partielles et leurs approximations, Université Paris-Sud.

Méthodes Inverses et assimilation de données

Code UE: MYMAI210
Tutelle: Département de Mathématiques, UVSQ
Volume horaire: CM: 12h TD: 18h
ECTS: 6
Semestre: 2
Caractère: obligatoire
Intervenants: Maëlle Nodet
Lieu: UVSQ
Parcours: «Analyse, Modélisation et Simulation»
Evaluation: voir «Modalités de contrôle des connaissances».

Pré-requis: Algèbre et analyse (dont optimisation) de licence

Description

Ce cours propose une introduction aux méthodes inverses, telles qu'elles sont utilisées dans les applications environnementales et industrielles. Deux grandes classes de méthodes seront étudiées, celles basées sur le filtre de Kalman et celles basées sur la théorie du contrôle optimal, et leur base commune, l'estimation statistique optimale, sera aussi introduite.

Contenu

- Outils nécessaires, rappels
  - Calcul différentiel
  - Optimisation
  - Algèbre linéaire
  - Statistiques
- Estimation statistique optimale. La méthode BLUE
- Filtre de Kalman
- Assimilation variationnelle
- Méthode adjointe
- Compléments (sous réserve du temps restant)

Bibliographie

- Asch, M., Bocquet, M., Nodet, M. (2016). Data assimilation : methods, algorithms, and applications (Vol. 11). SIAM.

Théorie de l'information

Code UE: MYMAI213
Tutelle: Département de Mathématiques, UVSQ
Volume horaire: CM: 12h TD: 12h
ECTS: 3
Semestre: 2
Intervenants: Edouard Rousseau
Lieu: UVSQ
Caractère: obligatoire en «Algèbre appliquée», optionnelle en «Analyse, Modélisation et Simulation»
Parcours: «Algèbre appliquée», «Analyse, Modélisation et Simulation»
Evaluation: voir «Modalités de contrôle des connaissances».

Pré-requis: Algèbre linéaire. Quelques éléments d'algèbre. Théorie él"mentaire des probabilités.

Description

Le but d'un système de communication est le transport d'information d'une source à un destinataire via un canal de communication. Ce canal possède en général des imperfections ce qui peut engendrer des erreurs de transmission. Aussi, le canal peut être sujet à des écoutes ce qui peut poser des problèmes de confidentialité. Finalement, l'utilisation d'un canal a un coût, il est donc important d'optimiser son usage.

Pour répondre à ces différentes exigences, on effectue un prétraitement de l'information ; il s'agit de la chaîne de codage. Celle-ci se divise en trois étapes : compression, chiffrement et ajout de redondance. Ces techniques font appel à la théorie des probabilités et à l'algèbre discrète. Ce cours présente les bases de la première et la troisième étape de la chaîne de codage, la seconde étant abondamment étudiée dans des cours de cryptographie.

Contenu

- Notions de base en théorie de l'information (entropie, information mutuelle).
- Algorithmes de compression sans perte (étape 1 de la chaîne de codage).
- Théorie des codes correcteurs d'erreurs (étape 3 de la chaîne de codage).
  - Canal sans mémoire à temps discret. Notion de capacité. Théorème de codage pour un canal bruyant. Principe de décodage par maximum de vraisemblance. Borne sur la probabilité d'erreur de décodage.
  - Théorie des codes correcteurs en blocs. Distance minimale et problématique des bornes sur la taille d'un code. Notion de code parfait.
  - Codes linéaires. Matrice génératrice et matrice de parité. Décodage par syndrome. Codes duaux. Polynôme énumérateur des poids. Identité de Mac-Williams.
  - Etude de certaines familles de codes linéaires (en bloc) et algorithmes de décodage.

— Codes convolutionnels et algorithme de Viterbi.

Bibliographie

— The Theory of Error-Correcting Codes. F. J. MacWilliams, N. J. A. Sloane North Holland Publishing Co. 1977.
— Théorie des codes (Compression, cryptage, correction). J.-G. Dumas, J.-L. Roch, E. Tannier et S. Varrette, Dunod 2007.

Optimisation et Recherche Opérationnelle

Code UE: MYCHP200
Tutelle: ISTY, UVSQ
Volume horaire: CM: 12h TD: 18h
ECTS: 3
Semestre: 2
Caractère: Optionnelle
Intervenants: Devan Sohier
Lieu: Bâtiment Rabelais, Guyancourt
Parcours: «Analyse, Modélisation et Simulation»
Evaluation: voir «Modalités de contrôle des connaissances».

Description

L'objectif de ce cours est l'acquisition de méthodes fondamentales en optimisation et notamment en recherche opérationnelle.

Contenu

- Graphes et optimisation
- Programmation linéaire (simplexe, dual)
- Programmation linéaire en nombre entiers (modélisation, approximation heuristiques, branch and bound)
- Processus de décision de Markov : modélisation et algorithmes de résolution
- Recherche opérationnelle en-ligne : modélisation et algorithmes de résolution
- Introduction aux méthodes méta-heuristiques

Corps professoral

Stephanie Basseville
Adresse : Département des sciences physiques
Université de Versailles Saint-Quentin-en-Yvelines
45, Avenue des Etats-Unis
78035 Versailles Cedex.
Tél. : +33 (0) 1 39 25 30 26
Mél : stephanie.basseville@uvsq.fr
Web :
Cours en master 1 :
- Méthodes numériques

Tahar Z. Boulmezaoud
Adresse : Laboratoire de Mathématiques de Versailles
Université de Versailles Saint-Quentin-en-Yvelines
45, Avenue des Etats-Unis
78035 Versailles Cedex.
Tél. : +33 (0)1 39 25 36 23
Mél : tahar.boulmezaoud@uvsq.fr
Web : https://boulmezaoud.perso.math.cnrs.fr/
Cours en master 1 :
- Introduction au calcul scientifique et projet
- Analyse des EDP

Christina Boura
Adresse : Laboratoire de Mathématiques de Versailles
Université de Versailles Saint-Quentin-en-Yvelines
45, Avenue des Etats-Unis
78035 Versailles Cedex.
Tél. : +33 (0)1 39 25 43 23
Mél : christina.boura@uvsq.fr
Web : https://christinaboura.wordpress.com/
Cours en master 1 :
- Analyse d'algorithmes, programmation

Ana-Maria Castravet
Adresse : Laboratoire de Mathématiques de Versailles
Université de Versailles Saint-Quentin-en-Yvelines
45, Avenue des Etats-Unis
78035 Versailles Cedex.
Tél. : +33 (0)1 39 25 46 41
Mél : ana-maria.castravet@uvsq.fr
Web : https://sites.google.com/view/castravet/home
Cours en master 1 :
- Théorie des nombres et cryptographie

Christophe Chalons
Adresse : Laboratoire de Mathématiques de Versailles
Université de Versailles Saint-Quentin-en-Yvelines
45, Avenue des Etats-Unis
78035 Versailles Cedex.
Tél. : +33 (0)1 39 25 30 68
Mél : christophe.chalons@uvsq.fr
Web : http://chalons.perso.math.cnrs.fr/
Cours en master 1 :
— Méthodes numériques avancées et programmation

Maria Chlouveraki
Adresse : Laboratoire de Mathématiques de Versailles
Université de Versailles Saint-Quentin-en-Yvelines
45, Avenue des Etats-Unis
78035 Versailles Cedex.
Tél. : +33 (0)1 39 25 46 38
Mél : maria.chlouveraki@uvsq.fr
Web : http://chlouveraki.perso.math.cnrs.fr/
Cours en master 1 :
— Algèbre générale
— Algèbre commutative

Laurent Dumas
Adresse : Laboratoire de Mathématiques de Versailles
Université de Versailles Saint-Quentin-en-Yvelines
45, Avenue des Etats-Unis
78035 Versailles Cedex.
Tél. : +33 (0)1 39 25 30 66
Mél : laurent.dumas@uvsq.fr
Web : http://dumas.perso.math.cnrs.fr/
Cours en master 1 :
— Optimisation

Pierre Gabriel
Adresse : Laboratoire de Mathématiques de Versailles
Université de Versailles Saint-Quentin-en-Yvelines
45, Avenue des Etats-Unis
78035 Versailles Cedex.
Tél. : +33 (0)1 39 25 30 64
Mél : pierre.gabriel@uvsq.fr
Web : http://pgabriel.perso.math.cnrs.fr/
Cours en master 1 :
— Introduction à l'analyse fonctionnelle et aux équations aux dérivées partielles

Louis Goubin
Adresse : UVSQ - Laboratoire PRISM
Batiment Descartes
45 Avenue des Etats Unis
78035 Versailles Cedex.
Tél. : ++ 33 (0)1 39 25 43 29
Mél : louis.goubin@uvsq.fr
Web : http://www.goubin.fr/
Cours en master 1 :
- Crypthographie
- Calcul sécurisé

Mohamed Krir
Adresse : Laboratoire de Mathématiques de Versailles
Université de Versailles Saint-Quentin-en-Yvelines
45, Avenue des Etats-Unis
78035 Versailles Cedex.
Tél. : +33 (0)1 39 25 46 23
Mél : mohamed.krir@uvsq.fr
Web : http://www.departement.math.uvsq.fr/node/712
Cours en master 1 :
- Théorie des nombres et cryptographie
- Introduction aux courbes elliptiques

Pierre-Guy Plamondon
Adresse : Laboratoire de Mathématiques de Versailles
Université de Versailles Saint-Quentin-en-Yvelines
45, Avenue des Etats-Unis
78035 Versailles Cedex.
Tél. : +33 (0)1 39 25 36 17
Mél : pierre-guy.plamondon@uvsq.fr
Web : https://www.imo.universite-paris-saclay.fr/ plamondon/
Cours en master 1 :
- Introduction au calcul formel et projet

Emmanuel Rio
Adresse : Laboratoire de Mathématiques de Versailles
Université de Versailles Saint-Quentin-en-Yvelines
45, Avenue des Etats-Unis
78035 Versailles Cedex.
Tél. : +33 (0)1 39 25 36 26
Mél : emmanuel.rio@uvsq.fr
Web : https://lmv.math.cnrs.fr/en/laboratory/directory/emmanuel-rio/
Cours en master 1 :
— Probabilités

Yann Rotella
Adresse : Laboratoire de Mathématiques de Versailles
Université de Versailles Saint-Quentin-en-Yvelines
45, Avenue des Etats-Unis
78035 Versailles Cedex.
Tél. : +33 (0)1 39 25 40 35
Mél : yann.rotella@uvsq.fr
Web : https://rotella.fr/
Cours en master 1 :
— Analyse d'algorithmes, programmation

Édouard Rousseau
Adresse : Laboratoire de Mathématiques de Versailles
Université de Versailles Saint-Quentin-en-Yvelines
45, Avenue des Etats-Unis
78035 Versailles Cedex.
Tél. : +33 (0)1 39 25 ** **
Mél : edouard.rousseau@uvsq.fr
Web : https://erou.github.io/
Cours en master 1 :
— Théorie de l'information

Vincent Sécherre
Adresse : Laboratoire de Mathématiques de Versailles
Université de Versailles Saint-Quentin-en-Yvelines
45, Avenue des Etats-Unis
78035 Versailles Cedex.
Tél. : +33 (0)1 39 25 36 20
Mél : vincent.secherre@uvsq.fr
Web :
https://lmv.math.cnrs.fr/laboratoire/annuaire/membres-du-laboratoire/vincent-secherre/
Cours en master 1 :
— Théorie des nombres et Cryptographie

Devan Sohier
Adresse : UVSQ - ISTY - Laboratoire Li-PaRAD EA-7432
9 boulevard d'Alembert, bâtiment François Rabelais
78280 GUYANCOURT
Tél. : ++ 33 (0) 1 39 25 43 38
Mél : devan.sohier@uvsq.fr
Web : http://www.liparad.uvsq.fr/
Cours en master 1 :
- Optimisation et recherche opérationnelle

Lionel Thevenard
Adresse :
Tél. :
Mél :
Web :
Cours en master 1 :
- Anglais

Paolo Vannucci
Adresse : Laboratoire de Mathématiques de Versailles
45 Avenue des Etats Unis
78000 Versailles.
Tél. : +33 (0)1 39 25 42 18
Mél : paolo.vannucci@uvsq.fr
Web : https://sites.google.com/site/paolovannucciwebsite/home
Cours en master 1 :
- Bases de la mécanique des milieux continus
- Introduction à la géométrie différentielle
- Mécanique analytique