UE Algèbre et arithmétique effectives

Niveau d'étude
Bac +3

ECTS
6 crédits

Crédits ECTS Echange
6.0

Composante
UFR Informatique, mathématiques et mathématiques appliquées (IM2AG)

Période de l'année
Automne (sept. à dec./janv.)

Diplômes intégrant cet élément

- Licence Informatique

Langue(s) d'enseignement: Français
Méthodes d'enseignement: En présence
Forme d'enseignement : Travaux pratiques
Ouvert aux étudiants en échange: Oui
Crédits ECTS Echange: 6.0
Code d'export Apogée: GBMI5U20

Présentation

Description

Bref descriptif du cours
Ce cours propose une introduction à la théorie élémentaire des nombres et à l'algèbre. On mettra l'accent sur les algorithmes et l'analyse de leur complexité, et sur les applications, notamment en cryptographie et en théorie des codes correcteurs. Les séances de travaux pratiques offrent une introduction à SageMath, un logiciel open-source qui regroupe une vaste gamme d'outils pour plusieurs domaines des mathématiques. Il sera utilisé pour implémenter les algorithmes étudiés, expérimenter sur des exemples concrets, "visualiser" et mieux comprendre certaines notions abstraites.

Contenu pédagogique

1) Arithmétique élémentaire
• Division euclidienne, divisibilité, PGCD, identité de Bézout, théorème fondamental de l'arithmétique
• Algorithme d'Euclide (classique et étendu), analyse de complexité
2) Entiers modulo n
• Relation de congruence modulo n et structure de Z/nZ
• Inversibilité, résolution de congruences linéaires
• Théorème des restes chinois, résolution d'un système de congruences
3) Structures algébriques
• Groupes, sous-groupes, théorème de Lagrange, groupes quotients
• Anneaux, corps, idéaux, anneaux quotients
• homomorphismes de groupes et d'anneaux, théorèmes d'isomorphisme
4) Algèbre linéaire effective
• Systèmes d'équations linéaires (à coefficients dans Q ou Z/pZ), opérations élémentaires, formes échelonnée et échelonnée réduite
• Algorithme de Gauss-Jordan, complexité
• Factorisation PLE et applications
5) Applications
• Cryptographie : RSA, tests de primalité, échange de clés à la Diffie-Hellman, problème du logarithme discret
• Théorie des codes correcteurs (extra)

Heures d'enseignement

CMTD	Cours magistral - Travaux dirigés	36h
TP	TP	18h

Pré-requis recommandés

Notions de base en arithmétique et algèbre linéaire.

Période : Semestre 5

Infos pratiques

Lieu(x) ville

Grenoble

Campus

Grenoble - Domaine universitaire