UE Algèbre effective et applications

Niveau d'étude
Bac +4

ECTS
6 crédits

Composante
UFR IM2AG (informatique, mathématiques et mathématiques appliquées)

Période de l'année
Printemps (janv. à avril/mai)

- **Langue(s) d'enseignement:** Français
- **Ouvert aux étudiants en échange:** Non
- **Code d'export Apogée:** GBMG8U12

Présentation

Description

L'algèbre effective est le domaine des mathématiques où on s'intéresse au calcul exact des objets intervenant en algèbre au sens large (arithmétique des entiers, arithmétique des polynômes et algèbre linéaire sur un corps fini et sur les rationnels), avec l'objectif de les rendre efficaces par rapport à la taille des données, en estimant leur complexité. Les applications sont nombreuses : calcul formel, cryptographie, codes correcteurs (par exemple QR codes)... On montrera plusieurs exemples où des calculs modulo un nombre premier permet d'accélérer les calculs sur les rationnels.
Une partie des exercices nécessite l'utilisation d'un logiciel de calcul formel tel que Xcas sur PC, mobile ou calculatrice CAS.

Descriptif

1. Arithmétique des polynômes à 1 variable (dont interpolation et FFT), arithmétique des entiers et liens entre eux. Puissance modulaire rapide, application: test de primalité, RSA.
2. PGCD dans Z/pZ[X]. Application à la simplification dans Q[X]. Irréductibilité dans Z/pZ[X], application à la représentation des corps finis, application à la factorisation dans Q[X]. Calcul efficace dans GF(2,n).
3. Théorème fondemental de l'algèbre : localisation de racines de polynômes dans C[X] (Newton, Aberth ; Sturm, Descartes). Résultant, algorithmes de calcul, application au calcul de primitives de fractions rationnelles, à la résolution de certains systèmes polynomiaux. Générateurs effectifs d'extensions de Q.

4. Matrice à coefficients dans un corps fini et sur les rationnels: réduction de Gauss, déterminant, polynôme caractéristique. Applications : codes correcteurs.

Pré-requis recommandés

arithmétique sur Z et Q[X]: PGCD, identité de Bézout, restes chinois, factorisation, algèbre linéaire dans R^n.

Période : Semestre 8

Bibliographie

- A Computational Introduction to Number Theory and Algebra par Victor Shoup: http://shoup.net/ntb/
- Modern Computer Arithmetic, Richard Brent and Paul Zimmermann, http://www.loria.fr/~zimmerma/mca/pub226.html
- Algorithmes efficaces en calcul formel par A. Bostan, F. Chyzak, M. Giusti, R. Lebreton, G. Lecerf, B. Salvy, E. Schost https://hal.archives-ouvertes.fr/AECF
- Algorithmes de calcul, B. Parisse, https://www-fourier.univ-grenoble-alpes.fr/~parisse/doc/fr/algo.pdf
- A Course in Computational Algebraic Number Theory, de Henri Cohen
- Modern Computer Algebra, par J. Von zur Gathen et J. Gerhard
- Cours de calcul formel (2 tomes), Saux Picart et Rannou.

Infos pratiques

Contacts

Responsable pédagogique

Bernard Parisse

Bernard.Parisse@ujf-grenoble.fr,Bernard.Parisse@univ-grenoble-alpes.fr

Campus

Grenoble - Domaine universitaire