Algèbre effective et applications

Samuel.Le-Fourn@univ-grenoble-alpes.fr
Bernard.Parisse@univ-grenoble-alpes.fr

Présentation

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 permettent d'accélérer les calculs sur les rationnels.
Prérequis : arithmétique sur $\mathbb{Z}$ et $\mathbb{Q}[X]$: PGCD, identité de Bézout, restes chinois, factorisation, algèbre linéaire dans $\mathbb{R}^n$.

Contenu

- 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.
- PGCD dans $\mathbb{Z}/p\mathbb{Z}[X]$. Application à la simplification dans $\mathbb{Q}[X]$. Irréductibilité dans $\mathbb{Z}/p\mathbb{Z}[X]$, application à la représentation des corps finis, application à la factorisation dans $\mathbb{Q}[X]$. Calcul efficace dans F_{2^n}.
- Théorème fondemental de l'algèbre : localisation de racines de polynômes dans $\mathbb{C}[X]$ (Newton, Aberth ; Sturm, Descartes). Résultant, algorithmes de calcul, applications. Générateurs effectifs d'extensions de $\mathbb{Q}$.
- Matrice à coefficients dans un corps fini et sur les rationnels : réduction de Gauss, déterminant, polynôme caractéristique. Applications : codes correcteurs.