Sujet de Projet 3A pour les élèves de l'École polytechnique

Titre : *Factorisation des polynômes sur les corps finis.*

Thématiques : calcul formel, corps finis.

Lieu

Laboratoire d'informatique de l'École polytechnique, LIX, UMR 7161 CNRS
Campus de l'École polytechnique
1 rue Honoré d'Estienne d'Orves
Bâtiment Alan Turing, CS35003
91120 Palaiseau, France

Directeur de laboratoire : Mme Mireille Régnier (regnier@lix.polytechnique.fr)

Équipe : MAX, Modélisation Algébrique

Directeur de projet

M. Grégoire Lecerf
Fonction : chargé de recherche CNRS 1re classe, habilité à diriger des recherches
Bureau : 1009
Téléphone : +33(0)1 77 57 80 81
Courriel : gregoire.lecerf@lix.polytechnique.fr
URL : http://lecerf.perso.math.cnrs.fr/index.en.html

Description

Ce projet est une initiation aux algorithmes de factorisation des polynômes à une variable sur les corps finis. On abordera les méthodes déterministes par algèbre linéaire et les méthodes probabilistes plus rapides par composition modulaire. Des implantations prototypes seront réalisées en utilisant les bibliothèques de calcul de MATHEMAGIX (http://www.mathemagix.org).

Si le temps le permet le cas des polynômes de petits degrés sur des grands corps finis pourra être abordé.

Pour les algorithmes de base on utilisera le chapitre 19 de [1] et le chapitre 14 du livre [2].

Bibliographie

[1] A. Bostan, F. Chyzak, M. Giusti, R. Lebreton, G. Lecerf, B. Salvy, et É. Schost. *Algorithmes efficaces en calcul formel*. Preprint version, https://hal.archives-ouvertes.fr/AECF, 2017.

[2] J. von zur Gathen, et J. Gerhard. *Modern computer algebra*. 2e édition, Cambridge University Press, 2003.

Compétences souhaitées

Algorithmique ; Théorie des corps.