Faculté des Sciences & Techniques
Département de Mathématiques

Année 2016-2017

Master 1- Cryptis
Projet d'Initiation à la Recherche

Corps de décomposition et calcul de la période d'une suite récurrente linéaire

Travail à faire

Soit A un anneau commutatif et $\mathcal{R}(A)$ l'ensemble des suites récurrentes linéaires sur A. L'objet de ce mémoire est d'abord de se familiariser avec les propriétés algébriques de base de l'ensemble $\mathcal{R}(A)$ muni de l'addition usuelles et des produits de Hadamard et de Cauchy (voir par exemple la partie 1 de l'article [1]). Ensuite, dans le cas où $A = \mathbb{Z}$, après une *lecture critique* de l'article [2], il s'agira de mettre en œuvre, via Maple, des programmes de calcul de la période de certaines éléments de $\mathcal{R}(A)$ modulo un nombre premier.

Références

[1] L. Cerlienco, M. Mignotte, F. Piras, *Suites récurrentes linéaires, propriétés arithmétiques et algébriques*, L'enseignement mathématique **33** (1987). pp 67–108

[2] S. Gupta, P. Rockstroh, F. Edouard Su, *Splitting fields and Periods of Fibonacci Sequences Modulo Primes*, Math. mag **85** (2012). pp 130–135

[3] R. Lidl, H. Niederreiter, *Introduction to finite Fields and their applications,* Cambridge University Press, 1994 pp 175–188.

Contact : anec@unilim.fr