Faculté des Sciences & Techniques
Département de Mathématiques

Année 2017-2018

Master 1- Cryptis
Projet d'Initiation à la Recherche

Calcul de la période d'une suite récurrente linéaire modulo un entier naturel

Le contexte

Très utilisés en informatique, cryptologie ou en simulation stochastique, les nombres pseudo-aléatoires sont aussi présents sur les machines de loteries réelles ou virtuelles. L'un des procédés utilisés pour les générer est basé sur l'étude des suites récurrentes linéaires modulo un entier naturel. De telles suites, pouvant être obtenues rapidement grâce à un LFSR (Linear Feedback Shift Register), sont périodiques et possèdent des propriétés statistiques intéressantes. Elles satisfont en particulier aux critères de Golomb (voir par exemple [4]). L'objet de ce mémoire est la détermination de la période de telles suites.

Travail à faire

Soit $m \in \mathbb{N}^*$ et A l'anneau $\mathbb{Z}/m\mathbb{Z}$ muni des lois usuelles. Soit $u = (u_n)_{n\geq 0}$ une suite d'éléments de A. On dit que u est une suite récurrente linéaire à coefficients dans A s'il existe $h \in \mathbb{N}^*$ et des éléments $c_0, \ldots, c_{h-1}$ dans A tels que :

$$\forall n \in \mathbb{N}, \quad u_{n+h} - c_{h-1}(n)u_{n+h-1} - \cdots - c_0(n)u_n = 0.$$

Le polynôme associé $\mathrm{Car}_u(X) = X^h - c_{h-1}X^{h-1} - \cdots - c_0 \in A[X]$ est appelé polynôme caractéristique de la suite u.
On désigne par $\mathcal{R}(A)$ l'ensemble de telles suites.
Il s'agit d'abord de se familiariser avec les propriétés algébriques de base de l'ensemble $\mathcal{R}(A_m)$ muni de l'addition usuelles et des produits de Hadamard et de Cauchy (voir par exemple la partie 1 de l'article [1]). Ensuite, pour $u \in \mathcal{R}(A)$, en utilisant les propriétés de l'algèbre quotient $A[X]/ < \mathrm{Car}_u(X) >$ et en particulier la décomposition et l'exposant de $\mathrm{Car}_u(X)$ dans cette algèbre, déterminer les propriétés et le calcul de la période de u (cf. l'article [2]).
Enfin, il conviendra de mettre en œuvre les algorithmes de calcul décrits dans [2].

Références

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

[2] J. Larry Lehman, C. Triola, *Recursive sequences and polynomial congruences*, Involve, a journal of mathematics, Math. Sciences Pulishers, **3** n°2 (2010). pp 130–135

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

[4] G. Castagos, *Cours de Cryptanalyse*,
`https://www.math.u-bordeaux.fr/~gcastagn/Cryptanalyse/cours-17-18.pdf`

Contact : anec@unilim.fr