ÉNS de Lyon Option C
2018-2019

Corps finis

Exercice 1 — **1.** Créer le corps $k = \mathbb{F}_{11^3}$ à l'aide de la commande GF. Poser $a = k.\text{gen}()$. Énumérer les éléments de k. Quel est l'inverse de $a^3 - 1$? Quel est l'ordre multiplicatif de a (on pourra utiliser multiplicative.order) ? Obtenir le polynôme définissant k à l'aide de k.polynomial().

2. Factoriser le polynôme $a * x^7 - 3x + 2$.

3. Construire $\mathbb{F}_{16}$ en utilisant le polynôme $X^4 + X^3 + X^2 + X + 1$.

Exercice 2 — Écrire une procédure prenant en entrée un entier q qui est une puissance d'un nombre premier et un entier n, et qui renvoie un polynôme aléatoire irréductible de degré n de $\mathbb{F}_q[X]$.

Exercice 3 —Algorithme de Cipolla

L'algorithme de Cipolla, qui date de 1907 est un algorithme d'extraction de racine carré dans $\mathbb{F}_p$, où $p \in \mathbb{P} \setminus \{2\}$. Soit $n \in \mathbb{F}_p$ qui est un carré. Soit $a \in \mathbb{F}_p$ tel que $a^2 - n$ n'est pas un carré. Soit $\sqrt{a^2 - n} = \overline{X} \in \mathbb{F}_p[X]/(X^2 - (a^2 - n)) = \mathbb{F}_{p^2}$. Alors $(a + \sqrt{a^2 - n})^{(p+1)/2} \in \mathbb{F}_p$ est une racine carrée de n.

1. Soit $x \in \mathbb{F}_p$. Comment tester si a est un carré ? Si on choisit n au hasard dans $\mathbb{F}_p$, quelle est la probabilité que $a^2 - n$ ne soit pas un carré modulo p ?

2. Écrire une procédure qui prend en entrée un nombre premier p et un entier n, qui teste si $n[p]$ est un carré et si oui, qui renvoie une racine carrée de n modulo p.

Remarque : on peut aussi utiliser la fonction square.

Exercice 4 —Logarithme de Zech Soit $n \in \mathbb{N}^*$ et $a \in \mathbb{F}_{2^n}^*$ d'ordre $2^n - 1$ dans $\mathbb{F}_{2^n}^*$. Pour $i \in \mathbb{Z}/(2^n - 1)\mathbb{Z}$, on définit $z(i)$ par $a^i = 1 + a^{z(i)}$. On rappelle que z est une involution sans point fixe qui vérifie $z(2i) = 2z(i)$ et $z(-i) = z(i) - i$ pour tout $i \in \mathbb{Z}/(2^m - 1)\mathbb{Z}$.

1. Écrire un algorithme qui prend un entier n et qui renvoie la table de z.