ÉNS de Lyon — Option C
M2 FEADéP — 2020–2021

TD/TP Corps finis

Exercice 1 — Calculs dans les corps finis —

1. Créer le corps $k = \mathbb{F}_{121}$ à l'aide de la commande GF.

2. Comment spécifier le polynôme définissant un corps fini ?

3. Afficher le polynôme définissant k. Énumérer les éléments de k.

4. Soit a le générateur de k. Quel est l'inverse de a ? Quel est l'ordre de a dans $k^\times$?

5. Factoriser le polynôme $ax^7 - 3x + 2$ dans $k[x]$.

6. Construire le corps $\mathbb{F}_{16}$ en utilisant le polynôme $x^4 + x^3 + x^2 + x + 1$ sur $\mathbb{F}_2$. Quel est, dans ce cas, l'ordre multiplicatif du générateur de $\mathbb{F}_{16}$?

Exercice 2 — Construction de polynômes irréductibles —

Soit q une puissance d'un nombre premier, et $n \geq 1$ un entier. On considère l'algorithme probabiliste suivant :

Choisir au hasard $P \in \mathbb{F}_q[X]$ de degré n ;
Si P est irréductible, renvoyer P, sinon recommencer.

1. Implémenter l'algorithme ci-dessus.

2. Étudier expérimentalement le nombre d'essais nécessaires pour trouver un polynôme irréductible, pour différentes valeurs de q et n.

Exercice 3 — Algorithme de Cipolla —

L'algorithme de Cipolla (1907) est un algorithme d'extraction de racine carrée dans $\mathbb{F}_p$, où $p \geq 3$ est un nombre premier. Soit n un carré dans $\mathbb{F}_p^\times$.

1. Montrer que le nombre de couples $(a, b) \in \mathbb{F}_p \times \mathbb{F}_p$ tels que $a^2 - n = b^2$ est égal à $p - 1$.

2. En déduire que le nombre de $a \in \mathbb{F}_p$ tels que $a^2 - n$ est un carré dans $\mathbb{F}_p$ est égal à $(p + 1)/2$.

D'après la question précédente, il existe $a \in \mathbb{F}_p$ tel que $a^2 - n$ n'est pas un carré. Soit $K = \mathbb{F}_p[X]/(X^2 - (a^2 - n))$. On note $\sqrt{a^2 - n}$ la classe de X dans K.

3. Déterminer un polynôme $Q \in \mathbb{F}_p[X]$ de degré 2 dont les racines sont $a \pm \sqrt{a^2 - n}$.

4. Montrer que $(a + \sqrt{a^2 - n})^{(p+1)/2}$ est une racine carrée de n dans $\mathbb{F}_p$.

5. Comment calculer $(a + \sqrt{a^2 - n})^{(p+1)/2}$?

6. Comment tester si un élément x de $\mathbb{F}_p$ est un carré ?

7. Si l'on choisit a au hasard dans $\mathbb{F}_p$, quelle est la probabilité que $a^2 - n$ ne soit pas un carré dans $\mathbb{F}_p$?

8. Écrire une fonction qui prend en entrée un nombre premier p et un entier n, qui teste si n est un carré dans $\mathbb{F}_p$ et si oui, qui renvoie une racine carrée de n dans $\mathbb{F}_p$.

Exercice 4 — Table de Zech —

Soit $n \in \mathbb{N}^*$ et a un générateur de $\mathbb{F}_{2^n}^\times$. Pour $i \in \mathbb{Z}/(2^n-1)\mathbb{Z}$, $i \neq 0$, on définit $z(i)$ par $1 + a^i = a^{z(i)}$.

1. Montrer que z est une involution sans point fixe de l'ensemble $(\mathbb{Z}/(2^n-1)\mathbb{Z})\backslash\{0\}$.

2. Montrer les formules $z(2i) = 2z(i)$ et $z(-i) = z(i) - i$ pour tout i.

3. On représente les éléments de $\mathbb{F}_{2^n}^\times$ en associant à chaque $x \in \mathbb{F}_{2^n}^\times$ l'unique entier $i \in \mathbb{Z}/(2^n-1)\mathbb{Z}$ tel que $x = a^i$. Expliquer comment z permet de calculer la somme de deux éléments de $\mathbb{F}_{2^n}$.

4. Écrire un algorithme qui prend en entrée un entier n et qui renvoie la table des valeurs de z (pour trouver un générateur a, on utilisera l'argument `modulus = "primitive"` lors de la création du corps fini).