UFR Sciences
M2 Calcul Formel

Martin WEIMANN

TP 4 : Factorisation des polynômes sur les corps finis

Exercice 1 (Corps finis) Le moyen le plus simple de représenter le corps fini $K = \mathbb{F}_q$ avec Sage et de taper `K=GF(q)`.

1. Explorer les différentes options et procédures associées à cet objet en tapant `K?`, puis `K.` suivi de la touche tabulation. Afficher la table de multiplication de K.
2. Demander à Sage un élément aléatoire de $\mathbb{F}_{27}$. Que représente z_3 ? Comment calculer z_3^8 ? Comment renommer z_3 ?
3. Concrètement, $\mathbb{F}_{27}$ est représenté comme un quotient $\mathbb{F}_3[X]/(P)$ pour un certain polynôme irréductible $P \in \mathbb{F}_3[X]$. Quel polynôme a utilisé Sage ? Représenter $\mathbb{F}_{27}$ avec un autre polynôme.

Exercice 2 (Racines)
1. Ecrire un programme qui retourne la liste des racines dans $\mathbb{F}_q$, (avec leurs multiplicités) d'un polynôme $Q \in \mathbb{F}_q[X]$ en procédant par évaluation naïve. Comment réduire simplement le polynôme d'entrée Q par un polynôme de degré au plus q ?
2. Tester votre programme sur un polynôme unitaire aléatoire de $\mathbb{F}_{64}[X]$ de degré 10. Comparer avec la fonction `Q.roots()` de Sage.
3. Tester votre programme avec le polynôme $P = X^8 - X \in \mathbb{F}_{64}[X]$. Votre résultat est-il en accord avec la théorie ? Dans quel sous-corps vivent les racines de P ?

Exercice 3 (Irréductibilité)
1. Ecrire un programme qui teste l'irréductibilité d'un polynôme $P \in \mathbb{F}_q[X]$ en vous basant sur le Corollaire 1 du cours.
2. Tester votre programme sur un polynôme unitaire aléatoire de $\mathbb{F}_{17}[X]$ de degré 100. Comparer les temps d'exécution avec la procédure Sage. Refaire de même avec le corps $\mathbb{F}_{16}$. Que constatez-vous ? Explications ?
3. Ecrire un programme qui retourne un polynôme unitaire irréductible de degré donné n de $\mathbb{F}_q[X]$. Combien de tirages en moyenne pour obtenir un polynôme irréductible de degré 15 dans $\mathbb{F}_{17}[X]$?
4. Introduire deux compteurs `Ntot` et `Nirr` et écrire une procédure calculant la proportion `Ntot[d]/Nirr[d]` de polynômes irréductibles unitaires de degrés d dans $\mathbb{F}_q[X]$ sur N tirages aléatoires (basé sur le test d'irréductibilité de Sage, plus performant). Quel est l'avantage des compteurs par rapport à un dictionnaire ou une liste ?
5. Tracer le graphique de ces proportions pour $q = 2$ et $d \in \text{range}(4, 100, 3)$, en considérant un nombre suffisant de tirages aléatoires. Vos résultats sont-il en accord avec la théorie (Théorème 2 du CM) ? Quelle échelle faut-il choisir pour y voir plus clair ?

Exercice 4 (Berlekamp) Soit $f \in \mathbb{F}_q[X]$ sans facteurs multiples. On note $R = \mathbb{F}_q[X]/(f)$.

1. Ecrire un programme `Matrice`(F,q) qui calcule la matrice M de l'endomorphisme

$$\phi_q - Id : R \to R, \qquad g \mapsto g^q - g$$

dans la base $(1, X, X^2, \ldots, X^{d-1})$ de R.

2. Ecrire un programme `Berlekamp`(F, p) qui factorise f selon la méthode de Berlekamp déterministe.

3. Ecrire un programme `Berlekamp2`(F, p) qui factorise f selon la méthode de Berlekamp probabiliste.

4. Comparer les temps de vos deux programmes sur un polynôme aléatoire de degré 10 de $\mathbb{F}_p[X]$ avec $p = 17$ puis $p > 10^7$. Comparer avec la procédure de Sage.

Exercice 5 (Cantor-Zassenhauss) 1. Programmer l'algorithme de factorisation de Cantor-Zassenhauss.

2. Comparer avec l'algorithme de Berlekamp probabiliste sur $X^{3^5} - X \in \mathbb{F}_3[X]$.

3. Modifier votre algorithme de manière à calculer les racines de f.

Exercice 6 (Facteurs multiples) Traiter le cas général où f peut avoir des facteurs multiples (on supposera $f \in \mathbb{F}_p[x]$, avec p premier).