TP 4 : Corps finis

1 Manipulations modulo p

Exercice 1.1. [Opérations de base modulo p et P]
Pour rappel, un entier est considéré comme classe modulo n grâce à `%` ou `mod`.

1. Définir deux entiers modulo 2021 et calculer leur produit et leurs cubes.
2. De même, définir grâce à `%` ou `mod` deux polynômes modulo 257 et calculer leur somme et produit. Bien s'assurer qu'ils sont donnés sous forme réduite.

Exercice 1.2. [Calculs polynomiaux]
On fixe un polynôme unitaire $P \in (\mathbb{Z}/p\mathbb{Z})[X]$ de degré d à définir comme plus haut (ou avec `randpoly`).

1. Utiliser les fonctions `divide` ou `rem` pour calculer le représentant de $Q \in (\mathbb{Z}/p\mathbb{Z})[X]$ dans $A = (\mathbb{Z}/p\mathbb{Z})[X]/(P)$ de degré $< d$.
2. En déduire comment calculer somme et produit de deux éléments dans A en pratique, et le faire sur un exemple.
3. Implémenter l'exponentiation rapide dans A (et comparer avec `powmod`).

Exercice 1.3. [Test d'irréductibilité dans $(\mathbb{Z}/p\mathbb{Z})[X]$]
On continue avec un même polynôme $P \in (\mathbb{Z}/p\mathbb{Z})[X]$.

1. Rappeler pourquoi P est irréductible si et seulement si $\mathrm{pgcd}(P, X^{p^k} - X) = 1$ pour tout $k \leq \deg P/2$.
2. Tester naïvement cette méthode pour $p = 7$ et un polynôme de degré 8.
3. Montrer que le pgcd plus haut est aussi celui de P et $Q_k - X$ avec Q_k le reste de la division euclidienne de X^{p^k} par P.
4. En déduire une manière rapide de calculer ce pgcd, et écrire une fonction `estirreductible` pour tester l'irréductibilité de P. Évaluer sa complexité.
5. En utiliser `randpoly` et la fonction précédente, construire une fonction pour trouver un polynôme irréductible sur $(\mathbb{Z}/p\mathbb{Z})$ de degré fixé.

2 Les corps finis à proprement parler

Exercice 2.1. [Construction générale]
Pour un corps fini non premier, on utilise plusieurs constructions possibles, à tester une par une.

1. `GF(p, n)` construit un corps fini de cardinal p^n, avec un générateur noté par défaut `g`.
2. `GF(p,n,alpha)` le construit avec un générateur appelé α.
3. `GF(p,P)` le construit si P est irréductible de degré n, et alors la variable du polynôme devient le générateur edu corps.

Ensuite, quelle que soit l'implémentation choisie, tester la somme et les puissances d'un élément.

— Construire un polynôme sur un corps fini puis le factoriser.

Exercice 2.2. [Polynôme minimal d'un élément]
On se fixe dans un corps fini, par exemple $\mathbb{F}_{5^3}$.

1. Pour $\alpha \in \mathbb{F}_{5^3}$, rappeler comment trouver les autres racines du polynôme minimal de α sur $\mathbb{F}_5$.
2. Écrire une fonction `polymin` permettant de calculer ce polynôme minimal.

Exercice 2.3. [Matrices sur un corps fini]
Construire une matrice carrée de taille 3 à coefficients dans un corps de cardinal 25.

1. Calculer son polynôme caractéristique et son rang.
2. Déterminer son polynôme minimal et son ordre.