

TP 4 – CORPS FINIS I

► **PRÉREQUIS** : Chapitre 4 du poly, jusqu'aux corps de rupture (§4.2.2 inclus).

1 Inversion modulo n

Le type *entiers modulo n* est créé avec `Integers(n)`. Écrire une fonction renvoyant l'inverse modulo n d'un entier a grâce à l'implémentation de l'arithmétique de $\mathbb{Z}/n\mathbb{Z}$ de Sage. Quel est le type de l'objet renvoyé par votre fonction ? Si nécessaire, modifier la fonction pour qu'elle renvoie un élément de $\mathbb{Z}$.

2 Calculs dans les corps finis

1. Si l'on veut factoriser $X^2 + 1$ dans $\mathbb{F}_2[X]$, est-ce que `factor(x^2+1)` convient ?

Une façon de manipuler des polynômes à coefficients dans un anneau R avec Sage consiste à définir l'anneau $A = \mathbb{Q}[X]$ de la façon suivante :

```
A.<X>=QQ[]
```

ou via

```
A.<X>=PolynomialRing(R)
```

pour définir l'anneau $R[X]$.

2. Factoriser $X^{16} + X$ dans $\mathbb{F}_2[X]$.
3. Définir une fonction qui prenne en argument un nombre premier p et un entier d et renvoie un polynôme irréductible de degré d sur $\mathbb{F}_p[X]$.
Indication : On pourra utiliser une factorisation du polynôme $X^{p^d} - X$ et le fait que tout polynôme irréductible de degré d sur $\mathbb{F}_p$ le divise.
4. Déterminer un polynôme irréductible P de degré 5 sur $\mathbb{F}_2$. Définir le domaine *corps de rupture de P sur $\mathbb{F}_2$* (voir l'aide de GF).
5. Factoriser P sur ce nouveau corps.
6. La méthode utilisée ci-dessus pour déterminer un polynôme irréductible peut-elle raisonnablement fonctionner pour $p = 2$ et $d = 42$?
7. Donner un équivalent (à p fixé et lorsque d tend vers $+\infty$) pour qu'un polynôme unitaire de degré d tiré uniformément au hasard dans $\mathbb{F}_p[X]$ soit irréductible.
8. Proposer une autre implémentation et préciser combien de tentatives seront nécessaires en moyenne.

3 Générateurs de $\mathbb{F}_q^\times$

9. Soit $x \in \mathbb{F}_{32}$. On suppose que $x \notin \{0, 1\}$. Montrer que x engendre le groupe $\mathbb{F}_{32}^\times$.
10. Montrer à la main que le polynôme $X^3 - X + 1$ est irréductible sur $\mathbb{F}_3$. Notons $\mathbb{F}_{27}$ le corps de rupture de ce polynôme et x la racine privilégiée de $X^3 - X + 1$. Vérifier avec l'aide de Sage que x est un générateur du groupe $\mathbb{F}_{27}^\times$.
11. En utilisant une description convenable du corps $\mathbb{F}_{53}$, déterminer un générateur du groupe $\mathbb{F}_{53}^\times$.
12. Même question pour $\mathbb{F}_{510}^\times$. On implémentera une fonction qui prend q en argument et renvoie un générateur du groupe $\mathbb{F}_q^\times$.

4 Comptage

Soit q une puissance d'un nombre premier. Si $\mathbb{F}_q$ est un corps fini à q éléments et N_d est le nombre de polynômes unitaires irréductibles de degré d dans $\mathbb{F}_q[X]$, alors on sait que

$$q^n = \sum_{d|n} dN_d.$$

12. Implémenter à la main une fonction qui prend en argument un entier n et un nombre premier p et qui renvoie la liste des polynômes irréductibles de degré n unitaires de $\mathbb{F}_p[X]$ lorsque $n \leq 4$. Cette méthode se généraliserait-elle pour tout n ?
13. Déterminer une méthode récursive pour calculer N_n .
14. Implémenter cette méthode de façon à renvoyer une expression en q .