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 $\mathbf{Z}/n\mathbf{Z}$ 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 $\mathbf{Z}$.

2 Calculs dans les corps finis

1. Si l'on veut factoriser X^2+1 dans $\mathbf{F}_2[X]$, 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 $A = R[X]$ de la façon suivante :

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

2. Factoriser $X^{16}+X$ dans $\mathbf{F}_2[X]$.
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 $\mathbf{F}_p[X]$.
   Indication : On pourra utiliser une factorisation du polynôme $X^{p^d}-X$ et le fait que tout polynôme irréductible de degré d sur $\mathbf{F}_p$ le divise.
4. Déterminer un polynôme irréductible P de degré 5 sur $\mathbf{F}_2$. Définir le domaine *corps de rupture de P sur* $\mathbf{F}_2$ (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. Proposer une autre implémentation.

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

1. Soit $x \in \mathbf{F}_{32}$. On suppose que $x \notin \{0,1\}$. Montrer que x engendre le groupe $\mathbf{F}_{32}^\times$.
2. Montrer à la main que le polynôme X^3-X+1 est irréductible sur $\mathbf{F}_3$. Notons $\mathbf{F}_{27}$ 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 $\mathbf{F}_{27}^\times$.
3. En utilisant une description convenable du corps $\mathbf{F}_{5^3}$, déterminer un générateur du groupe $\mathbf{F}_{5^3}^\times$.
4. Même question pour $\mathbf{F}_{5^{10}}^\times$.

4 Comptage

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

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

1. 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 unitaire de $\mathbf{F}_p[X]$ lorsque $n \geqslant 4$. Cette méthode se généraliserait-elle pour tout n ?
2. Déterminer une méthode récursive pour calculer N_n et afficher les 20 premières valeurs. Comparer avec la méthode précédente.
3. Implémenter cette méthode de façon à renvoyer une expression en q. Conjecturer un équivalent de N_n lorsque n tend vers $+\infty$ et me démontrer.