AGRÉGATION
TP CORPS FINIS

CHRISTOPHE RITZENTHALER

1. Manipulations de base

Les corps finis se définissent par la fonction `FiniteField(q)` ou `GF(q)`. Lorsque q n'est pas premier, il faut définir un générateur de $\mathbb{F}_q$ comme $\mathbb{F}_p$-algèbre. Par exemple pour $\mathbb{F}_{3^5}$, on écrira `F.<a>=GF(q)`. Pour trouver le polynôme minimal utilisé par Sage pour définir l'extension, on demande `F.polynomial()`.

Pour définir un anneau de polynômes en les variables $x_1, \dots, x_n$ sur un anneau A, cela se fait grâce à `R.<x1,...,xn>=PolynomialRing(A)`.

(1) Définir l'anneau $R = \mathbb{F}_5[x]$ puis le polynôme $P = x^3 + 3x + 2$. Est ce que P est irréductible ?
(2) Réduire le polynôme cyclotomique ϕ_{25} dans R. On le note Q. Le factoriser.
(3) Définir le corps de rupture de P grâce à
```
F53.<a>=GF(5^3, name='a', modulus=P)
```
(4) Soit la courbe affine $y^2 = x^3 + 5x + 3$ sur $\mathbb{F}_{5^3}$. Trouver tous les points sur cette courbe.

On considère le polynôme $P = x^3 + 3x + 1$ sur $\mathbb{F}_{17}$.

(5) Évaluer $x^2 + 3$ en toutes les racines sde P sur $\bar{\mathbb{F}}_{17}$.

2. Pohlig-Hellman

Utiliser Pohlig-Hellman avec l'exemple suivant: $5^x \equiv 3 \pmod{2017}$.

3. Calcul du logarithme discret dans $\mathbb{F}_p^*$

Implémenter la méthode rho de Pollard classique. L'essayer sur $2^x \equiv 22 \pmod{101}$.