

## Corps finis II

### Exercice 1. ÉCHAUFFEMENT.

1. Définir un corps  $\mathbb{F}_{25}$  à 25 éléments en appelant  $a$  l'image de l'indéterminée le quotient.
2. Déterminer le polynôme  $P$  choisi par `sage` pour cette définition.
3. Calculer  $a^6$ , en utilisant `sage`. Justifier le résultat par un calcul de division euclidienne.
4. En utilisant `sage`, infirmer ou confirmer l'irréductibilité de  $P$  dans  $\mathbb{F}_{25}[Y]$ .

### Exercice 2. SOUS-CORPS D'UN CORPS FINI.

1. Montrer que l'ensemble des points fixes d'un morphisme de corps est un sous-corps.
2. Soit  $p$  premier. Montrer que si  $K$  est un sous-corps de  $\mathbb{F}_{p^n}$  alors son cardinal est de la forme  $p^k$  où  $k$  divise  $n$  et
 
$$K = \{a \in \mathbb{F}_{p^n} \mid a^{p^k} = a\}.$$
3. Expliciter avec `sage` le morphisme de Frobenius  $F$  de  $\mathbb{F}_8$ , puis calculer les ensembles de points fixes de  $F \circ F$  puis  $F \circ F \circ F$ . Commenter les résultats obtenus.
4. Déterminer à l'aide de `sage` tous les sous-corps de  $\mathbb{F}_{16}$ .

### Exercice 3. MORPHISME DE FROBENIUS ET RACINES.

Soit  $P = X^3 + X^2 + 2X + 1$ .

1. Factoriser  $P$  sur  $\mathbb{F}_{17}$  avec `sage`.
2. Factoriser  $P$  sur  $\mathbb{F}_{289}$  avec `sage`.
3. Déterminer avec `sage` l'effet du morphisme de Frobenius sur les racines de  $P$  dans  $\mathbb{F}_{289}$ .
4. Montrer que le morphisme de Frobenius permute les racines de  $P$ .
5. On écrit  $\mathbb{F}_{289} = \mathbb{F}_{17}[X]/(Q)$  où  $Q = X^2 - X + 3$ . On note  $a$  la classe du polynôme  $X$  dans ce quotient. Déterminer un polynôme unitaire  $R$  de degré 3 de  $\mathbb{F}_{17}[X]$  tel que  $2$  et  $a + 1$  soient des racines de  $R$  dans  $\mathbb{F}_{289}$ . Ce polynôme est-il unique ?

### Exercice 4. ALGORITHME DE CIPOLLA.

Dans cet exercice, on étudie l'algorithme de Cipolla d'extraction de racines carrées modulo  $p$ . Soit  $p$  un nombre premier *impair* et  $D$  un élément de  $\mathbb{F}_p$  qui est un carré non nul.

1. Soit  $u \in \mathbb{F}_p$ . À quelle condition sur  $u$  et  $D$  le polynôme  $P = X^2 - uX + D$  est-il irréductible sur  $\mathbb{F}_p$  ?

2. Écrire une fonction `trouve_u(D, p)` qui une fois donné un couple  $(D, p)$  choisit au hasard des éléments  $u$  de  $\mathbb{F}_p$  et renvoie le premier pour lequel le polynôme associé  $P$  est irréductible. Pour tester si un élément est un carré dans  $\mathbb{F}_p$ , on utilisera la commande `legendre_symbol(a, p)` qui calcule le symbole de Legendre  $\left(\frac{a}{p}\right)$  et pour choisir un élément aléatoire, on utilisera `random_element()`.
3. Soit  $u$  un élément de  $\mathbb{F}_p$  tel que  $P = X^2 - uX + D$  est irréductible dans  $\mathbb{F}_p[X]$ . Combien le corps  $K = \mathbb{F}_p[X]/(P)$  contient-il d'éléments ?
4. On note  $x$  l'image du polynôme  $X$  dans  $K$ . Soit  $Q = Y^2 - uY + D \in K[Y]$ . Montrer que  $Q = (Y - x)(Y - x^p)$  est la factorisation de  $Q$  sur  $K$ . Montrer que  $x^{\frac{p+1}{2}}$  est une racine de  $D$  dans  $\mathbb{F}_p$ .
5. Implémenter une fonction `cipolla(D, p)` qui vérifie si  $D$  est un carré modulo  $p$ , et qui dans ce cas renvoie une racine de  $D$  modulo  $p$  (la fonction `cipolla` peut sinon retourner un message d'erreur).
6. Écrire une fonction `proba_cipolla(p)` prenant en entrée un nombre premier  $p$  et renvoyant la moyenne sur les carrés non nuls  $D$  de  $\mathbb{F}_p$  de la probabilité qu'un élément  $u \in \mathbb{F}_p$ , choisi uniformément au hasard, donne lieu à un polynôme  $P$  irréductible. On pourra par exemple :
  - (a) établir la liste  $L$  de tous les carrés non nuls de  $\mathbb{F}_p$  (de sorte que chacun d'entre eux n'apparaisse qu'une seule fois dans la liste),
  - (b) pour chaque élément  $D$  de  $L$ , compter le nombre d'éléments  $u$  de  $\mathbb{F}_p$  pour lesquels le polynôme  $P$  associé est irréductible,
  - (c) en déduire la probabilité désirée.
7. Illustrer avec `sage` le fait que la probabilité précédente est  $\frac{1}{2}(1 - \frac{1}{p})$ .
8. Écrire une fonction `proba_cipolla_2(D, p, n)` qui prend en entrée un nombre premier  $p$ , un carré non nul  $D$  de  $\mathbb{F}_p$  et un entier  $n$ , qui tire  $n$  éléments  $u$  de  $\mathbb{F}_p$  au hasard et teste si  $P = X^2 - uX + D$  est irréductible et qui renvoie le nombre de résultats positifs.
9. Utiliser la fonction précédente pour illustrer la probabilité de réussite de `trouve_u`.
10. (Bonus) Démontrer que la probabilité qu'une paire  $(u, D)$  choisie uniformément au hasard donne lieu à un polynôme  $P$  irréductible est  $\frac{1}{2}(1 - \frac{1}{p})$ .