Corps finis

Ce sujet comporte deux pages, avec un exercice sur chaque page.

Exercice 1. Échauffement

1. Soit $P = X^4 + X^3 + 4 \in \mathbb{F}_5[X]$. En utilisant une commande `sage` adaptée, montrer que P est irréductible.
2. Dans `sage`, définir L, un corps à 625 éléments en utilisant P et en appelant u le générateur.
3. Montrer que le polynôme P n'est pas irréductible sur L. Vérifier cette propriété à l'aide de `sage`.
4. Dans `sage`, calculer $(u^2 + 2)^{17}$.
5. Toujours à l'aide de `sage`, justifier par une division euclidienne le résultat précédent.
6. Soit $a = u^2 + 1$. Dans `sage`, calculer $F^k(a)$ pour $k \in \{1, \ldots, 4\}$ où $F : L \to L$ est le morphisme de Frobenius.
7. Dans `sage` et en utilisant le TD, déterminer un polynôme Q dans $\mathbb{F}_5[X]$ de degré 4, ayant a pour racine quand on le considère comme un élément de $L[X]$.
8. Montrer que Q est irréductible sur $\mathbb{F}_5$. On pourra utiliser le TD et raisonner par l'absurde.
9. Vérifier ce résultat avec `sage`.

Le deuxième exercice est en page suivante.

Exercice 2. Un autre test de primalité

On rappelle que $(\frac{p}{q})$ désigne le symbole de Legendre.

On considère la suite (F_n) définie par

$$F_0 = 0,\ F_1 = 1 \quad \text{et} \quad \forall n \geqslant 0,\ F_{n+2} = F_{n+1} + 3F_n\,.$$

On considère, pour tout entier positif n la propriété :

$$\mathcal{S}_n : \quad F_{n-(\frac{n}{13})} \equiv 0\ [n].$$

On admet pour l'instant que tout $n \geqslant 17$ premier vérifie $\mathcal{S}_n$.

A. La propriété $\mathcal{S}$ induit un test de primalité que nous allons implémenter.

1. Avec `sage`, écrire une procédure permettant pour calculer F_n pour $n \geqslant 0$.
2. Avec `sage`, calculer $(\frac{n}{13})$ pour $n \in \{0, ..., 12\}$. On rappelle que le symbole de Legendre est à valeurs dans $\{0, 1, -1\}$.
3. À l'aide de `sage`, vérifier la véracité de $\mathcal{S}$ pour tous les nombres premiers entre 17 et 50.
4. Implémenter un test de primalité sous la forme d'une fonction `test_primalite(n)` qui renvoie `True` si et seulement si le nombre entier n qui lui est donné est supérieur à 17 et vérifie $\mathcal{S}$.
5. Déterminer les trois plus petits nombres pseudopremiers pour le test précédent (i.e. composé et satisfaisant $\mathcal{S}$).

B. Nous allons maintenant revenir sur la preuve de $\mathcal{S}$ pour les nombres premiers. Dorénavant, p désigne un nombre premier supérieur à 14. On admet (voir TP 5) que le polynôme $P = X^2 - X - 3$ est réductible dans $\mathbb{F}_p[X]$ si et seulement s'il existe $a \in \mathbb{F}_p$ tel que $(2a-1)^2 = 13$ et que dans ce cas, ses racines sont a et $1-a$. Dans ce cas, on a également $F_k \equiv \frac{a^k-(1-a)^k}{2a-1}\ [p]$.

1. Montrer que P est réductible dans $\mathbb{F}_p$ si et seulement si $(\frac{13}{p}) = 1$.

Supposons d'abord P réductible dans $\mathbb{F}_p[X]$.

2. Montrer que $F_{p-1} \equiv 0\ [p]$.
3. Avec `sage`,
   (a) Déterminer le plus petit nombre premier $p > 13$ tel que $(\frac{13}{p}) = 1$.
   (b) Pour ce nombre p, déterminer un élément $a \in \mathbb{F}_p$ vérifiant $(2a-1)^2 = 13$.
   (c) Toujours pour ce nombre p, vérifier que $F_k \equiv \frac{a^k-(1-a)^k}{2a-1}\ [p]$ pour tout entier $k \leqslant 100$.

Supposons maintenant que P est irréductible dans $\mathbb{F}_p[X]$.

4. Quelle est la nature de $K = \mathbb{F}_p[X]/(P)$?
5. Soit $p = 19$. Avec `sage`,
   (a) Vérifier que P est irréductible dans $\mathbb{F}_p[X]$ et définir K (dont on notera x le générateur).
   (b) Vérifier que, *vu dans* K, $F_k = \frac{x^k-(1-x)^k}{2x-1}$ pour tout entier $k \leqslant 100$.
6. Plus généralement, soient p un nombre premier tel que $(\frac{13}{p}) = -1$ et x l'image de X dans K. Montrer que pour tout $k \geqslant 0$, $F_k = \frac{x^k-(1-x)^k}{2x-1}$ dans K.
7. En utilisant le morphisme de Frobenius, montrer que $F_{p+1} \equiv 0\ [p]$.

Et finalement :

8. En admettant le cas particulier suivant de la *réciprocité quadratique* : "si p est un nombre premier, alors $(\frac{13}{p}) = (\frac{p}{13})$", conclure la preuve de $\mathcal{S}$.