

# TP 7 – CORPS FINIS III

► PRÉREQUIS : Chapitre 6 du poly.

## Exercice I

Pour l'algorithme de Berlekamp (chapitre 6 du poly), nous aurons besoin de considérer des quotients  $k[X]/(P)$  pour  $k$  un corps fini et  $P \in k[X]$  un polynôme qui ne sera pas forcément irréductible (l'anneau  $k[X]/(P)$  ne sera peut-être pas un corps, et donc pas un corps de rupture puisque cette notion suppose que  $P$  soit irréductible).

1. Définir l'anneau des polynômes  $A := \mathbf{F}_5[X]$ .
2. Étudier l'aide associée à `A.quotient` et définir l'anneau quotient  $B := A/(P)$  où  $P := X^{10} + X + 2 \in A$ . Notons  $x$  la classe de  $X$  dans  $B$ .
3. Déterminer une base de  $B$  comme  $\mathbf{F}_5$ -espace vectoriel.
4. Calculer la classe de  $X^{1000000}$  dans  $B$ .
5. Déterminer le plus petit entier  $n \geq 1$  tel que  $x^{5^n} = x$  dans  $B$ . En déduire que  $P$  n'est pas un polynôme irréductible.
6. Déterminer un représentant  $Q \in A$  de degré  $< 10$  de  $x^{5^3} - x \in B$ .
7. Calculer le pgcd de  $P$  et  $Q$ .

## Exercice II

Dans cet énoncé,  $p$  est un nombre premier et on considère des polynômes en une variable  $X$  à coefficients dans  $\mathbf{F}_p$ . On stockera la valeur de  $p$  dans une variable globale. On s'intéresse à la factorisation d'un tel polynôme  $P \in \mathbf{F}_p[X]$  : on voudrait ultimement écrire une fonction qui renvoie la factorisation complète de  $P$  sous la forme d'un tableau de polynômes irréductibles.

Jusqu'à la question 3. incluse, on suppose que le polynôme  $P$  est non constant et séparable et on va lui appliquer l'algorithme de Berlekamp pour en déterminer un facteur irréductible.

1. Écrire une fonction prenant en argument  $P$  et renvoyant la matrice dans la base canonique de l'endomorphisme  $\mathbf{F}_p$ -linéaire de  $\mathbf{F}_p[X]/(P)$  qui à  $y$  associe  $y^p - y$ .
2. Écrire une fonction appelant la fonction précédente et renvoyant  $P$  si  $P$  est irréductible et un diviseur non trivial sinon.
3. Écrire une fonction `factorise` renvoyant la liste des facteurs irréductibles de  $P$  (toujours sous l'hypothèse que  $P$  est séparable).
4. On pose  $P = X^6 + X^3 + 1$ . En utilisant votre fonction de factorisation, montrer expérimentalement que si  $3 < p < 1000$  est un nombre premier, alors  $P$  est séparable et les conditions suivantes sont équivalentes :
  - (i)  $p$  est congru à 1 modulo 9;
  - (ii)  $P$  est scindé sur  $\mathbf{F}_p$ .
5. Généraliser la portée de votre fonction `factorise` pour qu'elle fonctionne même si  $P$  n'est pas séparable.
6. Examiner la factorisation de  $X^4 + 1$  dans  $\mathbf{F}_p[X]$  pour les premiers nombres premiers  $p$  impairs. Semble-t-il exister un lien entre la forme de cette factorisation et la classe de congruence de  $p$  modulo 8? Vérifier expérimentalement ceci pour tout  $p$  impair inférieur à 1000.
7. En utilisant la factorisation dans  $\mathbf{F}_p[X]$  pour  $p$  variant parmi les nombres premiers compris entre 2 et  $N$  (où  $N$  est un entier à préciser en entrée), écrire un test d'irréductibilité pour les polynômes de  $\mathbf{Z}[X]$  renvoyant `True` si le polynôme donné en entrée est irréductible sur  $\mathbf{Q}[X]$  et `False` si l'on n'est pas parvenu à prouver l'irréductibilité par réduction modulo  $p$  pour  $3 \leq p \leq N$ . Quel est le lien entre irréductibilité sur  $\mathbf{Q}[X]$  et sur  $\mathbf{Z}[X]$ ?  
Le polynôme de la question précédente est-il irréductible sur  $\mathbf{Q}$ ?  $\mathbf{Z}$ ? Ce test permet-il de l'établir?
8. Comment montrer en ne réduisant que modulo des nombres premiers inférieurs à 100 que le polynôme  $X^4 + 8X + 12 \in \mathbf{Z}[X]$  est irréductible sur  $\mathbf{Q}$ ? Cette stratégie fonctionne-t-elle pour  $X^4 + 1$ ? Qu'est-ce qui, à votre avis, justifie la différence de comportement modulo  $p$  de ces deux polynômes?
9. Adapter votre fonction `factorise` pour qu'elle puisse fonctionner avec des polynômes dont l'indéterminée ne serait pas forcément notée  $X$ .
10. Quelle est la complexité de l'algorithme de Berlekamp?

## Exercice III

Soit  $P \in \mathbf{F}_p[X]$  sans facteur carré. On s'intéresse dans cet exercice à la factorisation de  $P$  en degrés distincts. On rappelle que pour tout  $d \geq 1$ ,  $X^{p^d} - X$  est le produit de tous les polynômes unitaires irréductibles de  $\mathbf{F}_p[X]$  de degré divisant  $d$ . On appelle alors *factorisation de  $P$  en degrés distincts* la suite  $(g_1, \dots, g_s)$  de polynômes  $g_i \in \mathbf{F}_p[X]$  où  $g_i$  est le produit de tous les polynômes irréductibles unitaires de degré  $i$  divisant  $P$ , avec  $g_s \neq 1$ .

On propose l'algorithme suivant tant que  $P_i \neq 1$  avec  $P_0 = P$  :

- (i) On calcule  $h_i = X^{p^i} - X$ ;
- (ii) On calcule  $g_i = \text{pgcd}(h_i, P_{i-1})$ ;
- (iii) On pose  $P_i = \frac{P_{i-1}}{g_i}$ .

1. Justifier que l'algorithme ci-dessus termine et fournit bien la factorisation en degrés distincts de  $P$ .
2. Implémenter cet algorithme. On fera notamment au préalable un test pour vérifier que  $P$  est séparable et on renverra un message d'erreur le cas échéant.
3. Tester votre algorithme sur le polynôme  $X^6 + 2X^5 + 4X^4 + 4X^3 + 3X^2 + 2X$  et sur les polynômes cyclotomiques  $\Phi_n$  qui, pour peu que  $p \nmid n$ , se factorisent sur  $\mathbf{F}_p[X]$  en produit d'irréductibles tous de même degré égal à l'ordre de  $p$  dans  $(\mathbf{Z}/n\mathbf{Z})^\times$ .
4. Quelle est la complexité de cet algorithme? La comparer à un algorithme qui ferait appel à Berlekamp.

On suppose à présent que  $p$  est un nombre premier impair et on présente un algorithme probabiliste, dit de **Cantor-Zassenhaus** pour factoriser  $P$ . On rappelle que dans  $\mathbf{F}_q$ , si l'on tire  $a$  au hasard,  $a^{\frac{q-1}{2}}$  vaut 1 ou  $-1$  avec probabilité  $\frac{1}{2}$ . L'idée de l'algorithme est la suivante. Imaginons que  $P$  se décompose en produit de facteurs irréductibles **tous de même degré**, disons  $d$ . On a alors que  $P = P_1 \cdots P_r$  avec  $dr = n$  et les  $P_i$  irréductibles deux à deux non associés. On rappelle qu'on a alors l'isomorphisme

$$\mathbf{F}_p[X]/(P) \cong \prod_{i=1}^r \mathbf{F}_p[X]/(P_i)$$

où chaque  $\mathbf{F}_p[X]/(P_i)$  est isomorphe à  $\mathbf{F}_{p^d}$ . On propose alors l'algorithme probabiliste suivant. Soit  $k$  un nombre d'étape fixé en entrée, jusqu'à atteindre  $k$  étapes ou trouver un facteur irréductible non trivial, on tire  $a \in \mathbf{F}_p[X]$  de degré strictement inférieur à celui de  $P$  uniformément au hasard. On calcule alors  $g_1 := \text{pgcd}(a, P)$ . Si  $g_1 \neq 1$ , on renvoie  $g_1$  qui est un facteur non trivial de  $P$ . Sinon, on calcule  $b = a^{\frac{p^d-1}{2}}$  modulo  $p$  et on calcule  $g_2 := \text{pgcd}(b-1, P)$ . Si  $g_2 \neq 1, P$ , on renvoie  $g_2$  et sinon on recommence.

5. Justifier que cet algorithme échoue à renvoyer un facteur irréductible non trivial de  $P$  avec probabilité  $2^{(1-r)k} \leq 2^{-k}$ . En déduire un algorithme pour factoriser tout polynôme  $P$  avec probabilité d'échec inférieure à 0,99%
6. Implémenter l'algorithme en question.
7. Pourquoi a-t-on imposé  $p$  impair? Étudier la complexité de l'algorithme ci-dessus et le comparer à Berlekamp.