
Factorisation de polynômes modulo p

Exercice 1. Soient p un nombre premier impair et f un polynôme non constant de degré n à coefficients dans $\mathbb{F}_p$. On suppose que f est sans facteur carré. Le but de cet exercice est d'implanter l'algorithme de Berlekamp.

1. On note A_f l'algèbre $\mathbb{F}_p[X]/(f)$. Écrire une procédure prenant f en entrée et renvoyant la matrice de l'endomorphisme $x \mapsto x^p - x$ de A_f dans la base $(\bar{1}, \bar{X}, \dots, \bar{X}^{n-1})$, où $\bar{U}$ désigne la classe de l'élément $U \in \mathbb{F}_p[X]$ dans A_f . On pourra utiliser les commandes `PolynomialQuotientRing` pour définir un anneau quotient et `MatrixSpace` pour définir un espace de matrices.
2. Écrire une procédure renvoyant le nombre des facteurs irréductibles du polynôme f donné en entrée. On pourra utiliser les commandes `Q.right_kernel()` (où Q est une matrice) et `V.dimension()` (où V est un espace vectoriel).
3. Écrire une procédure renvoyant un facteur non trivial de l'entrée f ou renvoyant f lui-même si f est irréductible. On pourra utiliser la commande `V.basis()`.
4. Écrire une procédure renvoyant la liste des facteurs irréductibles d'un polynôme f sans facteur carré.

Exercice 2.

1. On considère le polynôme $f(X) = X^6 + X^3 + 1$. Vérifier expérimentalement que les conditions
 - (a) f est scindé sur $\mathbb{F}_p$,
 - (b) $p \equiv 1 \pmod{9}$.
 sont équivalentes si $3 < p \leq 1000$.
2. En utilisant la factorisation dans $\mathbb{F}_p[X]$ pour p variant parmi les nombres premiers compris entre 3 et N (où N est un entier à préciser dans les entrées), écrire un test d'irréductibilité pour les polynômes de $\mathbb{Z}[X]$ renvoyant `True` si le polynôme donné en entrée est irréductible sur $\mathbb{Q}$ et `False` si l'on n'est pas arrivé à prouver l'irréductibilité par réduction modulo p , pour $3 \leq p \leq N$.
3. Le polynôme $X^4 + 1$ est-il irréductible sur $\mathbb{Q}$? Le test de la question précédente permet-il de le montrer?

Exercice 3. Soit p un nombre premier impair. Le but de cet exercice est l'implantation d'un algorithme de factorisation en degrés distincts puis de l'algorithme de Cantor-Zassenhaus de factorisation en degré égal prenant tous deux comme argument un polynôme $f \in \mathbb{F}_p[X]$ sans facteur carré.

1. Implanter l'algorithme de factorisation en degrés distincts. La procédure prendra comme argument un polynôme non constant sans facteur carré $f \in \mathbb{F}_p[X]$ (et le nombre premier p) et comme sortie la suite $(g_1, \dots, g_s)$ telle que $\prod_i g_i = f$, et chaque g_i est produit d'irréductibles distincts de degré i .
2. Écrire une procédure permettant de trouver un facteur non trivial d'un polynôme $g \in \mathbb{F}_p[X]$ produit de polynômes irréductibles deux à deux distincts tous de même degré d (donné en entrée).
3. Dédire une procédure récursive donnant la factorisation complète d'un polynôme $f \in \mathbb{F}_p[X]$ unitaire non constant et sans facteur carré en produit de ses facteurs irréductibles.
4. Traiter le cas d'un polynôme unitaire non constant mais qui pourrait avoir des facteurs carrés.