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 $\mathbf{Z}/p\mathbf{Z}$. Le but de cet exercice est d'implanter l'algorithme de Berlekamp.

1. Écrire une procédure renvoyant la partie sans facteur carré de f (i.e. le produit des facteurs irréductibles distincts de f) dans le cas où f n'est pas un polynôme en X^p. En déduire une procédure permettant de renvoyer une séquence de polynômes sans facteur carré dont le produit vaut f. Traiter ensuite le cas où f est un polynôme en X^p.

   [Utiliser par exemple `Fp=FiniteField(p)` puis `x=polygen(Fp,'x')`.]

2. On suppose maintenant f sans facteur carré (on dit aussi *séparable*) et l'on note A_f la $\mathbf{Z}/p\mathbf{Z}$-algèbre $\mathbf{Z}/p\mathbf{Z}[X]/(f)$. 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 $(\overline{1}, \overline{X}, \ldots, \overline{X^{n-1}})$, où $\overline{U}$ désigne la classe dans A_f de l'élément $U \in \mathbf{Z}/p\mathbf{Z}[X]$.

   [Utiliser la commande `MatrixSpace` pour préciser l'anneau des coefficients.]

3. Écrire une procédure renvoyant le nombre des facteurs irréductibles du polynôme f donné en entrée.

   [Utiliser les commandes `M.kernel()` en se méfiant du fait que le noyau au sens de `Sage` est le noyau *à droite*, et `V.dimension()`.]

4. Écrire une procédure renvoyant un facteur non trivial de l'entrée f ou renvoyant f lui-même si f est irréductible.

   [Utiliser `V.basis()`.]

5. Combiner les étapes précédentes pour écrire une procédure renvoyant la liste des facteurs irréductibles du polynôme f sans facteur carré donné en entrée.

Exercice 2

1. Montrer expérimentalement (en s'aidant éventuellement du premier exercice) que le polynôme $f(X) = X^6 + X^3 + 1$ est tel que les conditions

   (a) f est scindé sur $\mathbf{F}_p$,

   (b) $p \equiv 1 \pmod 9$.

   sont équivalentes si $3 < p \leqslant 1000$.

2. En utilisant la factorisation dans $\mathbf{F}_p[X]$ 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 $\mathbf{Z}[X]$ renvoyant `True` si le polynôme donné en entrée est irréductible sur $\mathbf{Q}$ et `False` si l'on n'est pas arrivé à prouver l'irréductiblité par réduction modulo p, pour $3 \leqslant p \leqslant N$.

3. Le polynôme $X^4 + 1$ est-il irréductible sur $\mathbf{Q}$? Le test de la question précédente permet-il de le montrer ?

4. Comment montrer, en ne réduisant que par des premiers inférieurs à 100, que le polynôme $f = X^4 + 8X + 12 \in \mathbf{Z}[X]$ est irréductible sur $\mathbf{Q}$? Cette stratégie fonctionne-t-elle pour le polynôme $X^4 + 1$? (Question subsidiaire : qu'est-ce qui, à votre avis, justifie la différence de comportement entre les réductions modulo p de f et de $X^4 + 1$?)

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 $f \in \mathbf{F}_p[X]$ sans facteur carré.

1. Implanter l'algorithme de factorisation en degrés distincts vu en cours. La procédure prendra comme argument un polynôme non constant sans facteur carré $f \in \mathbf{F}_p[X]$ (et le nombre premier p) et comme sortie la suite $(g_1, \ldots, g_s)$ 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 $g \in \mathbf{F}_p[X]$ produit de polynômes irréductibles 2 à 2 distincts tous de même degré d (donné en entrée). On pourra tester cette procédure sur les polynômes cyclotomiques Φ_n qui, pour peu que $p \nmid n$, se factorisent (dans $\mathbf{F}_p[X]$) en produit d'irréductibles tous de même degré égal à l'ordre de p dans $(\mathbf{Z}/n\mathbf{Z})^\times$ (preuve ?).
3. Le temps permettant, déduire une procédure récursive donnant la factorisation complète d'un polynôme $f \in \mathbf{F}_p[X]$ unitaire non constant et sans facteur carré en produit de ses facteurs irréductibles.