Université de Paris 7 (F.Han[1])

TP13 Factorisation de Polynômes

agreg 2017

Exercice I: Méthode de Berlekamp (cf. Pb de rang, corps finis, polynômes)

1) Créer une fonction `randP(n)` qui donne un polynôme unitaire au hasard de degré n à coefficients inferieurs à 20. (On pourra étudier si `sum` ou `add` est appropriée dans le cas où n est une valeur symbolique plutot qu'un entier explicite.

2) On considère le polynôme P obtenu par `normal(mul([seq(randP(rand(7)),j=1..5)]));`

3) Vérifier que P n'a que des racines simples, sinon recommencer.

4) On considère un nombre premier p.

a) Créer une procédure `berl(p,P)` qui calcule la matrice (de Berlekamp) `F` de l'application $\mathbb{Z}/p\mathbb{Z}[x]/(P) \to \mathbb{Z}/p\mathbb{Z}[x]/(P)$ $f \mapsto f^p - f$ dans la base $(x^i)_{0,\ldots,\deg P-1}$. On utilisera une fonction xcas pour les puissances rapides.

b) Tester pour différentes valeurs de p le rang de F. Illustrer/Conjecturer un lien entre la dimension du noyau de F, et la factorisation de P sans $\mathbb{Z}/p\mathbb{Z}$.

5) Choisir un nombre premier impair de préférence[2] plus petit que 20 où le nombre de facteurs de P dans $\mathbb{Z}[x]$ est assez petit, et tel que P ait peu de facteurs dans $\mathbb{Z}/p\mathbb{Z}[x]$, et soit encore sans facteurs multiples dans $\mathbb{Z}/p\mathbb{Z}[x]$ pour cette valeur de p. Le nombre de facteurs est il forcément le nombre de facteurs dans $\mathbb{Z}[x]$? (illustrez)

6) Choisissez au hasard un élément Q du noyau de F pour la valeur de p choisie. Vérifier qu'il convient, et trouver un facteur non trivial de P en remaquant que l'un des 3 pgcd suivant est non trivial dans $\mathbb{Z}/p\mathbb{Z}[x]$: $Q \wedge P$, $Q^{\frac{p-1}{2}} - 1 \wedge P$, $Q^{\frac{p-1}{2}} + 1 \wedge P$.

7) En déduire une méthode pour factoriser un polynôme réduit sur un corps fini.

Exercice II: Remontée Henselienne

On peut prendre le polynôme P précédent ou un autre.

1) Prendre un diviseur A de P dans $\mathbb{Z}/p\mathbb{Z}[X]$. On note $B = P/A$ dans $\mathbb{Z}/p\mathbb{Z}[X]$. Trouver U, V tels que $A.U + B.V = 1[p]$

2) Obtenir un diviseur de P dans $\mathbb{Z}/p^2\mathbb{Z}[X]$ congru à A modulo p. Puis illustrer une remontée aboutissant à un facteur de P dans $\mathbb{Z}[x]$.

3) Illuster que certaines remontées ne donnent pas un facteur dans $\mathbb{Z}[x]$

4) Quel est $max_i C_m^i$? Faire une procédure de m, P : `borne` qui calcule une valeur flottante de ce nombre multiplié par la norme de $P = \sum_i a_i.x^i$: $||P|| = \sqrt{\sum_i |a_i|^2}$.

5) Avec les notations précédentes, on a le Théorème (cf Knuth T2 p 457 ou BPR p147) :

$$Q, P \in \mathbb{Z}[x],\ \deg Q = m, Q = \sum_j b_j x^j, \text{ alors}$$

$$|b_j| \leq ||P||.C_m^j$$

(pour le démontrer on pourra utiliser le lemme :

$$||(z-\alpha).P(z)|| = ||(\bar{\alpha}.z - 1).P(z)||$$

et remarquer que le produit des modules des racines complexes de P de module > 1 est inférieur à $||P||/a_n$.

1. http ://www.math.jussieu.fr/∼han/agreg
2. On le prend petit pour éventuellement illustrer la remontée Henselienne ensuite.