Université de Paris 7 | **TP15 Factorisation des Polynômes** | **agreg 2012**

(F.Han [1])

Exercice I:

1) Essayez le programme suivant (en mode xcas) : `f:=proc(P) P:=P%0;end;` Que fait : `Q:=x+1%5;f(Q);Q`

2) a) On pose `a:=27%101;`. Comment est calculé `a^j` par xcas lorsque j est grand ? Faites afficher les temps de calculs pour $j = 2^{2^i}$ avec $i \in \{3, 4, 5, 6, 7, 8, \ldots, 18\}$. Commentez.

b) Illustrez graphiquement la croissance en $O(\ln j)$. Afficher des gros points et une droite de régression linéaire bleue.

3) On considère le polynôme : `P:=2*(x^4+x^3+x^2+x+1);` et le polynôme `Q:=P % 7`

a) Quel est le reste de x^7 par Q ? (ie en travaillant dans $\mathbb{Z}/7\mathbb{Z}[x]$).

b) Que donne `rem(x^(2^10),Q);` et `rem(x^(2^33),Q)` ?

c) Comment calculer la puissance rapide de x dans $\mathbb{Z}/p\mathbb{Z}[x]/(P)$? Par exemple calculer : $(1+x)^{2^{33}}[P]$ dans $\mathbb{Z}/7\mathbb{Z}[x]$. (A retenir)

Exercice II: Méthode de Berlekamp

1) Créer une fonction `randP` qui donne un polynôme unitaire au hasard de degré n à coefficients inferieurs à 20. (On pourra étudier si `sum` ou `add` est appropriée, ou si l'on préfère utiliser le point de vue d'xcas, ie polynôme donné par la liste de ses coefficients).

2) On considère le polynôme P obtenu par `expand(mul([seq(randP(rand(7)),i=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 `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 $(X^i)_{0,\ldots,\deg P-1}$, et retourne son noyau. (On s'arrangera pour que le calcul des puissances soit rapide). Améliorez cette fonction pour qu'elle ne fasse cela que si P n'a pas de facteurs multiples dans $\mathbb{Z}/p\mathbb{Z}[x]$. Retourner `[[0]]` dans ce cas.

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

6) Comprendre le théorème de Berlekamp [2] :

Soit P un élément de $F_q[x]$ sans facteurs multiples. Alors le nombre de facteurs irréductibles de P est la dimension du noyau de l'application F_q-linéaire :

$$\begin{array}{lll} F_q[x]/(P) & \to & F_q[x]/(P) \\ f & \mapsto & f^q - f \end{array}$$

7) Choisir un nombre premier impair de préférence [3] plus petit que 20 où le nombre de facteurs est assez petit, et tel que P ait peu de facteurs dans $\mathbb{Z}/p\mathbb{Z}$, et soit 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 $\mathbb{Z}[X]$?

8) Prendre un élément Q du noyau de F. Vérifier qu'il convient.

a) Si P_i est un facteur irréductible de P dans $\mathbb{Z}/p\mathbb{Z}[x]$, rappelez quelles sont les valeurs possibles pour $Q^{\frac{p-1}{2}}[P_i]$. Que représente la condition $Q^{\frac{p-1}{2}} = 1[P]$? Pensez vous qu'elle se réalise souvent ?

b) Trouver un facteur non trivial de P.

9) Faire une procédure `unfacteur` qui pour un diviseur d de P trouve un facteur non trivial de d par la méthode précédente. Si au bout de quelques essais [4] ce facteur est toujours d, elle retourne alors d.

1. http ://www.math.jussieu.fr/∼han/agreg
2. Cf par exemple Demazure cours d'algèbre, ou Cohen : a course in computational number theory
3. On le prend petit pour éventuellement illustrer la remontée Henselienne ensuite.
4. Par exemple 3, inutile de faire une boucle

10) Faire une procédure `facteurpseudoirred` qui utilise par récurrence `unfacteur` pour trouver un facteur probablement irréductible de P. Créer un test pour savoir si un polynôme sans facteurs multiples est irréductible. Tester le facteur obtenu.

11) Tentez de factoriser P dans $\mathbb{Z}/p\mathbb{Z}[X]$ par cette méthode. Que peut on faire pour vérifier si tout ces facteurs sont irréductibles ?