UNIVERSITÉ MONTPELLIER 2
SCIENCES ET TECHNIQUES

FLMA607 – Calcul formel – 2010-2011

TP 4 : Factorisation de polynômes (trois séances)

Exercice 1

1) Écrire une procédure `borneML` qui, étant donné un polynôme $P \in \mathbb{Z}[X]$ calcule la borne de Mignotte-Landau pour les coefficients de g_1 et g_2 dans une factorisation $P = g_1 g_2$.
2) En utilisant cette borne, implémenter l'algorithme naïf de factorisation des polynômes dans $\mathbb{Z}[X]$ (on fait tous les essais possibles en respectant cette borne...). Tester votre procédure sur quelques exemples de petit degré. À partir de quel degré le temps de calcul devient-il prohibitif ?
3) Implémenter l'algorithme de Kronecker. Comparer le temps de calcul sur les mêmes exemples que ceux choisis ci-dessus. Cet algorithme est-il satisfaisant ?

Exercice 2

Implémenter une procédure testant la séparabilité des éléments de $\mathbb{F}_p[X]$ (p est donné par l'utilisateur de la procédure).

Exercice 3

Implémenter une procédure qui calcule le nombre de facteurs irréductibles d'un polynôme séparable $P \in \mathbb{F}_p[X]$. On pourra utiliser une procédure intermédiaire qui calcule la matrice de l'application linéaire

$$\begin{array}{ccc} \mathbb{F}_p[X]/(P) & \longrightarrow & \mathbb{F}_p[X]/(P) \\ Q & \longmapsto & Q^p - Q. \end{array}$$

Exercice 4

Écrire une procédure qui prend en entrée un polynôme f et un entier p premier et impair, et qui retourne une décomposition de f en facteurs irréductibles. Le calcul sera fait par l'algorithme de Berlekamp. On supposera que f est séparable sur $\mathbb{F}_p[x]$.

Exercice 5

On désire factoriser un polynôme séparable de $\mathbb{Z}[X]$ par la méthode suivante : on le factorise dans $\mathbb{F}_p[X]$ pour un entier p bien choisi, puis on en déduit le résultat grâce à la borne de Mignotte-Landau.
1) Écrire une procédure `choix_p` qui choisit (bien) un nombre premier p.
2) En utilisant les procédures ci-dessus et la procédure `borneML` de l'exercice 1, écrire une procédure qui factorise les polynômes de $\mathbb{Z}[X]$ par l'algorithme de Berlekamp. Comparer les résultats (et les temps de calcul) avec les algorithmes de l'exercice 1, et avec la commande `factor` de Maple.

Exercice 6

Écrire une procédure `sfc` qui calcule la factorisation « sans facteur carré » d'un polynôme $P \in \mathbb{Z}[X]$. (On pourra supposer P primitif.)