Université de Bordeaux
Mathématiques

Algèbre et calcul formel – Master
Année 2015–2016

FEUILLE D'EXERCICES n° 10

Travail sur machine

Ce travail porte sur les algorithmes de factorisation sur un corps fini vus en cours. Pour simplifier, on va travailler sur $\mathbb{F}_p$, où p est un nombre premier impair.

On rappelle que pour définir $\mathbb{F}_p$ sur sage, on peut écrire

```
k=GF(p)
```

(où p est bien sûr préalablement défini). Ensuite, on définit l'anneau $k[x]$ par

```
pr.<x>=PolynomialRing(k)
```

Dans ces algorithmes, on doit faire des calculs modulo f (où f est le polynôme à factoriser). Pour cela, on définit l'anneau quotient $k[x]/(f)$:

```
AnneauQuotient.<z>=pr.quotient(f)
```

Alors z est l'image de x dans le quotient $k[x]/(f)$. Par exemple, si on veut calculer $h = x^p$ modulo f, on peut faire :

```
h=z**p
```

Si ensuite on veut considérer h comme un polynôme en x, on écrit

```
h.lift()
```

Plus généralement, si g est un polynôme en x et si on veut calculer g^i modulo f, on peut faire

```
(g(z)**i).lift()
```

Exercice 1 – [Algorithme de Cantor-Zassenhaus]
Le programmer sur $\mathbb{F}_p$, où p est un nombre premier impair. et l'essayer sur des polynômes produits de polynômes irréductibles de même degré. Par exemple, l'essayer sur $x^8 + 8x^6 + 9x^4 + 6x^2 + 4 \in \mathbb{F}_{11}[x]$. Ici, le degré des polynômes irréductibles est égal à 2.

Exercice 2 – [Factorisation complète dans $\mathbb{F}_p[x]$]
Ici, p désigne toujours un nombre premier impair. Les polynômes sont dans $\mathbb{F}_p[x]$.

1) Écrire une fonction qui, étant donné un polynôme sans facteur carré dont tous les facteurs irréductibles sont de degré d, rend ces facteurs irréductibles. Cette fonction utilisera l'algorithme de Cantor-Zassenhaus de la question précédente, et s'appellera elle-même récursivement.

2) Écrire une fonction qui, étant donné un polynôme quelconque, donne sa décomposition complète, en utilisant la stratégie donnée en cours.

Exercice 3 – [Racines dans $\mathbb{F}_p$ d'un polynôme de $\mathbb{F}_p[x]$]
Pour calculer ces racines, il suffit d'appliquer la méthode de "factorisation en degrés distincts" pour "$d = 1$", puis d'appliquer l'algorithme de la question 1 de l'exercice précédent. Programmer cette fonction.

Exercice 4 – [Matrices]
Il existe différentes façons de définir une matrice. Nous allons ici définir d'abord l'espace des matrices qui nous intéresse. Par exemple, on définit $\mathcal{M}_3(\mathbb{F}_3)$ par la commande

```
MF3=MatrixSpace(GF(3),3,3)
```

Alors, la commande

```
M=MF3([1,2,0,1,0,1,2,2,1])
```

définit une matrice.

Il peut aussi être commode de définir une matrice par une formule donnant ses coefficients. Par exemple, la matrice $A = (a_{ij})$ de $\mathcal{M}_6(\mathbb{Q})$ telle que $a_{ij} = i + j$ peut être définie comme suit.

```
A=matrix(QQ,6,6,lambda i,j:i+j)
```

Revenons à la matrice M. Pour obtenir son noyau à droite, on utilise la commande

```
KerM=M.right_kernel()
```

Pour une base du noyau

```
KerM.basis()
```

Comme d'habitude, pour un élément au hasard dans ce noyau, on peut utiliser la commande

```
KerM.random_element()
```

Enfin, la commande

```
MF3(1)
```

donne la matrice identité dans $\mathcal{M}_3(\mathbb{F}_3)$.

Exercice 5 – [Algorithme de Berlekamp : un exemple simple]
Soit $f = x^6 + 2x^5 + x^4 + 2x^3 + x - 1 \in \mathbb{F}_5[x]$.

1) Calculer $\text{pgcd}(f, f')$.

2) Calculer $\text{pgcd}(f, x^5 - x)$.

3) Sachant cela, quelles sont les structures possibles de l'anneau $A = \mathbb{F}_5[x]/(f)$?

4) Soit F l'aplication de A dans lui-même qui à x associe x^5. Écrire la matrice de $F - \text{Id}$ dans la base $1, x, \ldots, x^5$ de A, et calculer son noyau N.

5) Combien f possède-t-il de facteurs irréductibles ? Quel est leur degré ?

6) Prendre un élément a au hasard dans N et calculer $\text{pgcd}(a, f)$ et $\text{pgcd}(a^2-1, f)$. Recommencer jusqu'à obtenir un facteur non trivial de f.