Université Bordeaux 1 | **Algèbre et calcul formel – Master**
Mathématiques | Année 2018–2019

FEUILLE D'EXERCICES n^{o} 10

Travail sur machine

Ce travail porte sur les algorithmes de factorisation sur un corps fini vus en cours.

Exercice 1 – [Calculs sur les corps finis]

1) $\mathbb{F}_p$: soit p un nombre premier. On rappelle que pour définir $\mathbb{F}_p$ sur sage, on peut écrire `k=GF(p)` (où p est bien sûr préalablement défini).

2) $\mathbb{F}_q$: soit $q = p^k$ une puissance de p.

a) Pour définir $\mathbb{F}_q$, on peut utiliser un polynôme irréductible P de degré k de $\mathbb{F}_3[x]$ de la manière suivante.

```
k.<a>=GF(q,P)
```

Alors, $\mathbb{F}_q$ est défini par $\mathbb{F}_p[x]/(P)$ et a est la classe de x dans ce quotient.

b) On peut aussi laisser sage choisir le polynôme P en tapant `k.<a>=GF(q)`. Alors a est la classe de x dans un certain quotient $\mathbb{F}_p[x]/(P)$. Pour connaître P, il suffit d'utiliser la commande `k.modulus()`.

c) On peut même taper simplement `k=GF(q)`. Pour retrouver le P et le a, on utilise alors les commandes `k.modulus()` et `k.gen()`.

3) Anneau de polynôme. Si k est un corps codé `k`, on définit l'anneau $k[x]$ par `kx.<x>=PolynomialRing(k)`. Pour tirer au hasard un polynôme de degré entre 0 et n :

```
kx.random_element((0,n))
```

4) Exponentiation rapide. Soient f et g deux polynômes de $k[x]$ et n un entier. Pour calculer $f^n \mod g$ rapidement, on dispose de la commande `pow(f,n,g)`.

5) Anneaux quotients. On peut s'en passer pour la suite de ce travail. La commande suivante permet de définir l'anneau quotient $k[x]/(f)$.

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

Alors z est la classe de x dans le quotient $k[x]/(f)$.

Exercice 2 – [Algorithme de Cantor-Zassenhaus]

Dans cet exercice et ceux qui suivent, q est une puissance d'un nombre premier impair.

1) Programmer l'algorithme de Cantor-Zassenhaus.

2) Tester votre fonction 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.

3) Le n-ème polynôme cyclotomique est donné par `cyclotomic_polynomial(n)`. Tester votre fonction sur le polynôme cyclotomique Φ_{16} vu comme un polynôme de $\mathbb{F}_3[x]$ avec $d = 4$, puis de $\mathbb{F}_9[x]$ avec $d = 2$.

4) On peut montrer que dans $\mathbb{F}_q[x]$, le polynôme Φ_n est produit de polynômes irréductibles de degré d, où d est l'ordre de q dans $(\mathbb{Z}/n\mathbb{Z})^*$. Pour calculer cet ordre, on peut faire les opérations suivantes.

```
A=Integers(n)
Aq=A(q)
Aq.multiplicative_order()
```

Ici, `A` est l'anneau $\mathbb{Z}/n\mathbb{Z}$ et `Aq` est la classe de q dans cet anneau.

Sachant cela, tester l'algorithme de Cantor-Zassenhaus sur $\Phi_{25} \in \mathbb{F}_9[x]$.

Exercice 3 – [Calcul de tous les facteurs]
Écrire une fonction `DegresEgaux` qui, étant donné un polynôme Q 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 pour trouver un facteur D et s'appellera elle-même récursivement sur D et Q/D.

Exercice 4 – [Racines dans $\mathbb{F}_q$ d'un polynôme f de $\mathbb{F}_q[x]$]
Pour calculer ces racines, il suffit de calculer $D = \mathrm{pgcd}(x^q - x, f)$ et d'appliquer à D la fonction `DegresEgaux` de l'exercice précédent. Programmer cette fonction de calcul des racines de f.

Exercice 5 – [Factorisation complète]
Les polynômes sont dans $\mathbb{F}_q[x]$.

1) Soit $P = x^{11} + 3x^{10} + 2x^9 + 3x^8 + x^7 + x^5 + 3x^4 + 2x^2 + 4x \in \mathbb{F}_5[x]$.

a) Calculer le produit D_1 des éléments de $\mathrm{Irr}(5,1)$ qui divisent P (en calculant $\mathrm{pgcd}(x^5 - x, P)$).

b) En utilisant `DegresEgaux`, calculer la factorisation de D_1.

c) Pour tout irréductible $P_{1,i}$ divisant D_1, calculer la plus grande puissance $\alpha_{1,i}$ de $P_{1,i}$ qui divise P, et remplacer P par $P/P_{1,i}^{\alpha_{1,i}}$.

d) calculer le produit D_2 des éléments de $\mathrm{Irr}(5,2)$ qui divisent le nouveau P (en calculant $\mathrm{pgcd}(x^{5^2} - x, P)$).

e) En utilisant `DegresEgaux`, calculer la factorisation de D_2.

f) Pour tout irréductible $P_{2,i}$ divisant D_2, calculer la plus grande puissance $\alpha_{2,i}$ de $P_{2,i}$ qui divise P, et remplacer P par $P/P_{2,i}^{\alpha_{2,i}}$.

g) En déduire la factorisation complète de P.

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

Exercice 6 – [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 7 – [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 $\mathrm{pgcd}(f, f')$.

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

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 $F - \mathrm{Id}$ 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 $\mathrm{pgcd}(a, f)$ et $\mathrm{pgcd}(a^2-1, f)$. Recommencer jusqu'à obtenir un facteur non trivial de f.

Exercice 8 – [Algorithme de Berlekamp]
Le programmer.