Université Bordeaux 1 **Algèbre et calcul formel – Master**
Mathématiques Année 2014–2015

FEUILLE D'EXERCICES n° 10

Exercice 1 – [Cantor-Zassenhaus en caractéristique 2]
On rappelle l'algorithme de Cantor-Zassenhaus en caractéristique impaire.

Algorithme 1. Factorisation dans $\mathbb{F}_q[x]$.

Entrées: $q = p^k$, où p est un nombre premier impair, $Q \in \mathbb{F}_q[x]$ de degré n, produit de polynômes irréductibles deux à deux distincts de degré d.
Sorties: Un diviseur non trivial de Q, ou bien "échec".
1: Tirer au hasard $A \in \mathbb{F}_q[x]$ de degré inférieur à n.
2: Calculer $D = \mathrm{pgcd}(A, Q)$. Si $D \neq 1$, sortir D.
3: Calculer $B = A^{(q^d-1)/2} - 1 \bmod Q$
4: Calculer $D = \mathrm{pgcd}(B, Q)$. Si $D \neq 1$ et $D \neq Q$, sortir D. Sinon, sortir "échec".

---

1) En appliquant cet algorithme, factoriser le polynôme $x^4 + x^3 + x - 1$ de $\mathbb{F}_3[x]$, en prenant $d = 2$ et $A = x - 1$.

2) Soit $m \geqslant 1$, et soit

$$T_m = x^{2^{m-1}} + x^{2^{m-2}} + \cdots + x^4 + x^2 + x \in \mathbb{F}_2[x].$$

a) Montrer que $T_m(T_m + 1) = x^{2^m} + x$.

b) En déduire que si $\alpha \in \mathbb{F}_{2^m}$, alors $T_m(\alpha) \in \mathbb{F}_2$.

c) Montrer que l'application $\alpha \mapsto T_m(\alpha)$ de $\mathbb{F}_{2^m}$ dans $\mathbb{F}_2$ est une application linéaire de F_2-espaces vectoriels. En déduire que les ensembles $\{\alpha \in \mathbb{F}_{2^m} \ : \ T_m(\alpha) = 0\}$ et $\{\alpha \in \mathbb{F}_{2^m} \ : \ T_m(\alpha) = 1\}$ ont même cardinal, soit 2^{m-1}.

Soient maintenant $q = 2^k$ et $Q \in \mathbb{F}_q[x]$ de degré n. On suppose que Q est produit de r polynômes irréductibles sur $\mathbb{F}_q$ qu'on note $P_1, \ldots, P_r$, deux à deux distincts et tous de même degré d. On note $R = \mathbb{F}_q[x]/(Q)$, $R_i = \mathbb{F}_q[x]/(P_i)$ et φ_i l'application canonique de R dans R_i définie par $\varphi_i(P \mod Q) = P \mod P_i$.

3) Soit $A \in R$. Montrer que $\varphi_i(T_{kd}(A)) = T_{kd}(\varphi_i(A)$. En déduire que $\varphi_i(T_{kd}(A)) \in \mathbb{F}_2$ et que si A est choisi au hasard dans R avec probabilité uniforme, $T_{kd}(A)$ appartient à $\mathbb{F}_2$ avec probabilité 2^{1-r}.

4) En déduire un algorithme pour factoriser Q et montrer que sa probabilité d'échec est inférieure à $1/2$.

Exercice 2 – [Algorithme de Berlekamp : un exemple simple]
Soit $f = x^4 + x^3 + x - 1 \in \mathbb{F}_3[x]$. On suppose qu'on a déjà calculé $\mathrm{pgcd}(f, f') = 1$.

1) Le polynôme f a-t-il des racines dans $\mathbb{F}_3$? En déduire sans calculs $\mathrm{pgcd}(f, x^3 - x)$.

2) Sachant cela, quelles sont les structures possibles de l'anneau $A = \mathbb{F}_3[x]/(f)$?

3) Soit F l'aplication de A dans lui-même qui à x associe x^3. Écrire la matrice de $F - \mathrm{Id}$ dans la base $1, x, x^2, x^3$ de A, et calculer son noyau N.

4) Prendre un élément a de ce noyau et calculer pgcd (a, f), puis $\mathrm{pgcd}(a-1, f)$. Recommencer jusqu'à obtenir un facteur non trivial de f.

5) Vérifier que pour tout élément a de N et tout facteur irréductible g de f, il existe bien un entier k tel que

$$a \equiv k \mod g.$$

Exercice 3 – [Algorithme de Berlekamp : un autre exemple simple]
Soit $f = x^6 + 2x^5 + x^4 + 2x^3 + x - 1 \in \mathbb{F}_5[x]$. On suppose qu'on a déjà calculé que $\mathrm{pgcd}(f, f') = 1$.

1) Le polynôme f a-t-il des racines dans $\mathbb{F}_5$? En déduire sans calculs $\mathrm{pgcd}(f, x^5 - x)$.

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

3) 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. On pourra utiliser sans démonstration les résultats suivants.

$$\begin{aligned}
x^{10} &\equiv -2x^5 + 2x^4 - x^3 - x^2 + x - 2 \mod f \\
x^{15} &\equiv -x^5 + 2x^4 - 2x^3 + 2x + 2 \mod f \\
x^{20} &\equiv -2x^5 + 2x^4 + x^3 + 1 \mod f \\
x^{25} &\equiv x \mod f.
\end{aligned}$$

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

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