

FEUILLE D'EXERCICES n° 11

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 $D = \text{pgcd}(A, Q)$. Si $D \neq 1$, sortir D .
 - 3: Calculer $B = A^{(q^d-1)/2} - 1 \pmod{Q}$
 - 4: Calculer $D = \text{pgcd}(B, Q)$. 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 $m \geq 1$, 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 \mathbb{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, \dots, 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 $\varphi_i(P \pmod{Q}) = P \pmod{P_i}$.

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 – [BERLEKAMP ET IRRÉDUCTIBILITÉ]

Soient p un nombre premier et $P = x^p - x - 1 \in \mathbb{F}_p[x]$. En utilisant l'endomorphisme de $\mathbb{F}_p[x]/(P)$ qui à a associe a^p , montrer que P est irréductible.