Corps finis : algorithme de factorisation de Berlekamp

Soit q une puissance d'un nombre premier, et $P \in \mathbb{F}_q[X]$ un polynôme de degré $n \geq 2$, sans facteur carré. On note $P = P_1 \dots P_r$ la décomposition en facteurs irréductibles de P (qui n'est pas connue), et pour tout $i \in [\![1, r]\!]$, on note d_i le degré de P_i.
Dans la suite, on note E le quotient $\mathbb{F}_q[X]/(P)$.

1. Justifier que E est une $\mathbb{F}_q$-algèbre de dimension n, et en donner une base $\mathcal{B}$.
2. Montrer que l'application $\Phi_q : a \mapsto a^q - a$ est un endomorphisme de E. Comment peut-on obtenir sa matrice dans la base $\mathcal{B}$?
   Écrire un programme qui prend en entrée le polynôme P et renvoie la matrice de Φ_q.
3. Démontrer l'existence d'un isomorphisme de $\mathbb{F}_q$-algèbre
   $$\psi : E \simeq \mathbb{F}_{q^{d_1}} \times \cdots \times \mathbb{F}_{q^{d_r}}$$
   et déterminer l'expression de $\psi \circ \Phi_q \circ \psi^{-1}$.
4. Montrer que $\psi(\ker \Phi_q) = \mathbb{F}_q \times \cdots \times \mathbb{F}_q$, et en déduire que $\dim \ker(\Phi_q) = r$.
5. Écrire un programme qui renvoie le nombre de facteurs irréductibles de P et le tester.
   Quelle est sa complexité ?
6. Comment peut-on adapter ce programme en test d'irréducibilité ? La complexité du test obtenu est-elle meilleure que celle de l'algorithme de Ben-Or ?

Dans la suite, on suppose $r > 1$, c'est-à-dire que P n'est pas irréductible, et on va expliquer comment le factoriser.

7. Expliquer comment construire effectivement une base de $\ker \Phi_q$, et avec quelle complexité.
   En pratique, on pourra utiliser la commande `kernel` ou `right_kernel`.
8. Soit $Q \in \mathbb{F}_q[X]$ avec $\deg(Q) < n$, et $\overline{Q}$ sa classe dans E. Montrer que :
   $$\deg Q = 0 \iff \exists\, a \in \mathbb{F}_q,\ \psi(\overline{Q}) = (a, a, \dots, a)$$
9. En déduire que si $\overline{Q} \in \ker(\Phi_q) \setminus \mathrm{Vect}(\overline{1})$, alors il existe $a_1, \dots, a_r \in \mathbb{F}_q$ non tous égaux tels que $\psi(\overline{Q}) = (a_1, \dots, a_r)$.
10. On garde les notations de la question précédente. Soit $i \in [\![1, r]\!]$; il existe alors $j \in [\![1, r]\!]$ tel que $a_i \neq a_j$. Montrer que $P_i \mid Q - a_i$ et que $P_j \nmid Q - a_i$ et en déduire que le pgcd de $Q - a_i$ et de P donne une factorisation non triviale de P.
11. L'algorithme de Berlekamp consiste à prendre un élément $\overline{Q}$ non trivial dans $\ker \Phi_q$, puis à calculer, pour tout $a \in \mathbb{F}_q$, le pgcd de $Q - a$ avec P jusqu'à obtenir une factorisation non triviale. On relance ensuite l'algorithme sur les deux facteurs trouvés.

    Implémenter cet algorithme et donner une estimation de sa complexité. Quel est son inconvénient principal ?