Algorithme de Berlekamp

Théorème : Soit p premier, $n \in \mathbb{N}*$ et $q = p^n$. On se donne $P \in \mathbb{F}_q[X]$ sans facteur carré. Si P n'est pas irréductible, il existe $V \in \mathbb{F}_q[X]$ tel que

$$P = \prod_{\alpha \in \mathbb{F}_q} \text{pgcd}(V - \alpha, P).$$

Lemme : Soit $R \in \mathbb{F}_q[X]$. On pose $S_R : \begin{array}{ccc} \mathbb{F}_q[X]/(R) & \longrightarrow & \mathbb{F}_q[X]/(R) \\ \overline{(Q(X))} & \longmapsto & \overline{Q(X^q)} \end{array}$. L'application S_R est linéaire, bien définie et correspond à l'élévation à la puissance q dans $\mathbb{F}_q[X]/(R)$.

Preuve du lemme : Soit $\delta : \begin{array}{ccc} \mathbb{F}_q[X] & \longrightarrow & \mathbb{F}_q[X] \\ Q(X) & \longmapsto & Q(X^q) \end{array}$, c'est un morphisme d'anneau sans trop de soucis. Comme nous somme en caractéristique p, il vient aussi que $\delta(Q(X)) = Q(X)^q$.
On pose alors $\pi : \mathbb{F}_q[X] \to \mathbb{F}_q[X]/(R)$ la projection canonique et $\Delta : \pi \circ \delta$. Comme π est un morphisme d'anneau, Δ aussi et on trouve alors $\Delta(R(X)) : \pi(R(x))^q = 0$. On peut ainsi passer au quotient l'application Δ pour avoir S_R comme voulue et qui est donc bien définie.
De plus on voit que $S_R(\overline{Q(X)}) = S_R(\pi(Q(X))) = \pi(Q(X)^q) = \overline{Q(X)}^q$, d'où la complétion de la preuve. □

Voici maintenant l'algorithme en question :
En notant $x = \pi(X)$ et $\mathcal{B} = (1, x, ..., x^{\deg(P)-1})$ qui est une base de $\mathbb{F}_q[X]/(P)$ on considère l'algorithme suivant :
1) On calcule la matrice de $S_R - \text{Id}$ dans la base $\mathcal{B}$
2) On montre que P possède $r = \dim(\ker(S_R - \text{Id}))$ facteurs irréductibles.
3) On montre qu'il existe V non-constant modulo P dans le noyau de $S_R - Id$ tel que

$$P = \prod_{\alpha \in \mathbb{F}_q} \text{pgcd}(V - \alpha, P).$$

.
Preuve du théorème :
1,2) Comme $\mathbb{F}_q[X]$ est factoriel on peut se donner $P = \prod_{1 \leq i \leq r} P_i$ la décomposition en facteurs irréductibles de P. On pose alors $K_i = \mathbb{F}_q[X]/(P_i)$ pour tout i.
Soit

$$\varphi : \begin{array}{ccc} \mathbb{F}_q[X]/(P) & \longrightarrow & K_1 \times ... \times K_r \\ Q\text{mod}(P) & \longmapsto & (Q\text{mod}(P_1), ..., Q\text{mod}(P_i)) \end{array}.$$

Le lemme chinois nous donne directement le fait que φ est une isomorphisme. On pose $\tilde{S_P} = \varphi \circ S_P \circ \varphi^{-1}$. On remarque alors que cette application correspond à l'élévation à la puissance q composante par composante grâce au lemme.
Ainsi, $(x_1, ..., x_r) \in \ker(\tilde{S_P} - \text{Id}) \iff x_i^q = x_i$ pour tout i. Or $x_i^q = x_i \iff x_i \in \mathbb{F}_q$. En effet, P_i est

irréductible donc $\mathbb{F}_q[X]/(P_i)$ est une extension de corps de F_q. Donc le polynôme $X^q - X$ admet au maximum q racines. Or l'image de l'injection de F_q dans $\mathbb{F}_q[X]/(P_i)$ est de cardinal q et incluse dans les racines de $X^q - X$ par Lagrange, d'où l'équivalence.
Finalement on en déduit que $\ker(\tilde{S}_P - \text{Id}) = (\mathbb{F}_q)^r$. Mais $\tilde{S}_P - Id$ et $S_p - \text{Id}$ sont semblables donc la dimension de leur noyau est la même et vaut $\dim((F_q)^r) = r$.

3) Si $r = 1$, P est irréductible et on a finit. Sinon, $r \geq 2$. Dans ce cas, $\{\text{Constantes modulo P}\} = \text{Vect}(\overline{1})$ est un sous espace-vectoriel de dimension 1. Grâce à l'étape 2 on peut alors se donner un élément V non constant modulo P dans le noyau de $S_P - \text{Id}$. Notons alors $\alpha_i = V \text{mod} P_i$. On a déjà vu que $\alpha_i \in \mathbb{F}_q$ pour tout i.

Montrons maintenant $\text{pgcd}(V - \alpha, P) = \prod_{\{i:\alpha_i = \alpha\}} P_i$.
Comme $\text{pgcd}(V - \alpha, P) | P$, par factorialité il existe $I_\alpha \subset \{1, ..., n\}$ tel que $\text{pgcd}(V - \alpha, P) = \prod_{I_\alpha} P_i$. On a alors $I_\alpha = \{i : P_i | V - \alpha\}$:
- L'inclusion direct est triviale par définition.
- L'inclusion réciproque est plus subtile. Soit $j \in \{i : P_i | V - \alpha\}$. Comme $P_j | \text{pgcd}(V - \alpha, P)$ et que les P_i sont tous premiers entre eux, le lemme de Gauss affirme qu'il existe i dans I_α tel que $P_j | P_i$ ie $P_i = P_j$ car P_i est irréductible, d'où l'inclusion réciproque.

On conclut en écrivant que $P = \prod_{1 \leq i \leq r} P_i = \prod_{\alpha \in \mathbb{F}_q} \prod_{\{i:\alpha_i = \alpha\}} P_i = \prod_{\alpha \in \mathbb{F}_q} \text{pgcd}(V - \alpha, P)$. □

Pré-requis importants : Il faut être à l'aise sur

- Le théorème chinois
- La factorialité des anneaux de polynômes
- L'injection de $\mathbb{F}_q$ dans ses sur-corps