Algorithme de Berlekamp

Théorème
Soit $P \in \mathbb{F}_q[X]$ un polynôme sans facteurs carrés. Alors si P n'est pas irréductible il existe un polynôme $V \in \mathbb{F}_q[X]$ non constant modulo P tel que

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

Référence : Beck, *Objectif Agrégation*, pp. 244-246.

Démonstration :
On considère l'application $S_P : \left\{ \begin{array}{ccc} \mathbb{F}_q[X]/(P) & \to & \mathbb{F}_q[X]/(P) \\ Q(X) \pmod P & \mapsto & Q(X^q) \pmod P \end{array} \right.$. On va montrer que S_P est bien définie, est une application linéaire et coïncide avec $(Q \pmod P) \mapsto (Q^q \pmod P)$. On montrera ensuite que polynôme V recherché est un élément de $\ker(S_P - \mathrm{Id})$.

$\varphi : \left\{ \begin{array}{ccc} \mathbb{F}_q[X] & \to & \mathbb{F}_q[X] \\ Q(X) & \mapsto & Q(X^q) \end{array} \right.$ est un morphisme d'anneaux et on a $\varphi(Q) = Q(X^q) = Q(X)^q$. Ensuite en composant φ avec la surjection canonique $\pi : \left\{ \begin{array}{ccc} \mathbb{F}_q[X] & \to & \mathbb{F}_q[X]/(P) \\ Q(X) & \mapsto & Q(X) \pmod{(P)} \end{array} \right.$, on obtient un morphisme d'anneaux $\overline{\varphi} = \pi \circ \varphi$ tel que $\overline{\varphi}(P) = \pi(P^q) = \pi(P)^q = 0$. Donc $\overline{\varphi}$ passe au quotient pour donner S_P et de plus

$$S_P(Q \pmod P) = \pi(Q^q) = \pi(Q)^q = (Q \pmod P)^q.$$

Donc S_P est bien définie, est linéaire et coïncide avec la puissance $q^{\text{ième}}$.

On va maintenant montrer que $\ker(S_P - \mathrm{Id})$ est de dimension égale à r, le nombre de facteurs irréductibles de P. Soient $P_1, \ldots, P_r$ est facteurs irréductibles de P. Par le théorème chinois on a $\mathbb{F}_q[X]/(P) \cong \prod_{i=1}^{r} \underbrace{\mathbb{F}_q[X]/(P_i)}_{:=K_i}$, en notant Φ l'isomorphisme $\left\{ \begin{array}{ccc} \mathbb{F}_q[X]/(P) & \to & \prod_{i=1}^{r} K_i \\ Q \pmod P & \mapsto & (Q \pmod{P_i})_{i \in [\![1,r]\!]} \end{array} \right.$ on a une application linéaire

$$\widetilde{S_p} := \Phi \circ S_P \circ \Phi^{-1} : \left\{ \begin{array}{ccc} \prod_{i=1}^{r} K_i & \to & \prod_{i=1}^{r} K_i \\ (Q_i \pmod{P_i})_{i \in [\![1,r]\!]} & \mapsto & (Q_i^q \pmod{P_i})_{i \in [\![1,r]\!]} \end{array} \right. .$$

De plus $(x_1, \ldots, x_r) \in \ker(\widetilde{S_p} - \mathrm{Id})$ si et seulement si $\forall i \in [\![1, r]\!], x_i^q = x_i \in \mathbb{F}_q[X]/(P_i)$. Les K_i sont des extensions de $\mathbb{F}_q$ car les P_i sont irréductibles et de plus $\mathbb{F}_q$ correspond dans K_i à l'ensemble des x tels que $x^q = x$. En effet pour $x \in \mathbb{F}_q$ on a bien $x^q = x$ et le polynôme $X^q - X$ a au plus q racines dans K_i. Donc $\ker(\widetilde{S_P} - \mathrm{Id}) \cong \mathbb{F}_q^r$, d'où $\dim(\ker(S_P - \mathrm{Id})) = \dim(\ker(\widetilde{S_P} - \mathrm{Id})) = r > 0$.

Maintenant, comme P n'est pas irréductible on a $r > 1$. De plus, l'ensemble des polynômes constant modulo P forment une droite vectorielle de $\mathbb{F}_q[X]/(P)$, donc il existe $V \in \mathbb{F}_q[X]$ non constant modulo P tel que $S_P(V \pmod P) = (V \pmod P)$. Montrons que V est bien le polynôme recherché :

On a vu que $V \in \ker(S_P - \mathrm{Id})$ si et seulement si $\forall i \in [\![1, r]\!], \underbrace{(V \pmod P_i)}_{:=\alpha_i} \in \mathbb{F}_q \hookrightarrow K_i$. Calculons pour $\alpha \in \mathbb{F}_q, \mathrm{pgcd}(P, V - \alpha)$:

C'est un diviseur de P donc $\mathrm{pgcd}(P, V - \alpha) = \prod_{i \in I_\alpha} P_i$ avec $I_\alpha \subset [\![1, r]\!]$. De plus comme les P_i sont premiers entre eux on a $I_\alpha = \{i \in [\![1, r]\!], P_i \mid V - \alpha\}$. Or

$$P_i \mid V - \alpha \Leftrightarrow V - \alpha \equiv 0 \pmod P_i \Leftrightarrow \alpha = \alpha_i,$$

donc $I_\alpha = \{i \in [\![1, r]\!], \alpha_i = \alpha\}$. Comme les α_i sont tous dans $\mathbb{F}_q$ on a $[\![1, r]\!] = \bigcup_{\alpha \in \mathbb{F}_q} I_\alpha$. D'où

$$P = \prod_{i=1}^{r} P_i = \prod_{\alpha \in \mathbb{F}_q} \prod_{i \in I_\alpha} P_i = \prod_{\alpha \in \mathbb{F}_q} \mathrm{pgcd}(P, V - \alpha).$$

■

Ce théorème nous donne un algorithme pour calculer les P_i. En effet, comme le polynôme V est non constant modulo P il existe $i, j \in [\![1, r]\!]$ tels que $\alpha_i \neq \alpha_j$. Donc pour tout $\alpha \in \mathbb{F}_q$ on a $I_\alpha \neq [\![1, r]\!]$ et donc tous les termes du produits sont de degré strictement inférieur à celui de P. Ainsi en réappliquant le théorème aux facteurs non constants et non irréductibles du produit on obtient finalement la décomposition en irréductibles de P.