# Algorithme de Berlekamp

Soient $p$ un nombre premier, $n \in \mathbb{N}^*$, et $q = p^n$. Le but de l'algorithme de Berlekamp est de trouver un facteur non trivial d'un polynôme $P \in \mathbb{F}_q[X]$ réductible sans facteur carré.

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

<u>Démonstration :</u> On pose $\delta_1 : \begin{array}{ccc} \mathbb{F}_q[X] & \longrightarrow & \mathbb{F}_q[X] \\ Q(X) & \longmapsto & Q(X^q) \end{array}$, qui est un morphisme d'anneaux et correspond à l'élévation à la puissance $q$. On note $\pi : \mathbb{F}_q[X] \longrightarrow \mathbb{F}_q[X]/(R)$ la projection canonique, et on pose $\delta = \pi \circ \delta_1 : \mathbb{F}_q[X] \longrightarrow \mathbb{F}_q[X]/(R)$.
Le morphisme d'anneaux $\delta$ passe au quotient par $(R)$ et donne $S_R$, qui est donc bien défini. Soit $Q \in \mathbb{F}_q[X]$. On a
$$S_R(Q \bmod R) = S_R(\pi(Q)) = \pi(Q(X^q)) = \pi(Q^q) = \pi(Q)^q.$$

<u>Algorithme de Berlekamp :</u> Soit $P \in \mathbb{F}_q[X]$ un polynôme sans facteurs carrés.
On note $\pi : \mathbb{F}_q[X] \longrightarrow \mathbb{F}_q[X]/(P)$ la projection canonique et $x = \pi(X)$. On considère la base $\mathcal{B} = \{1, x, \dots, x^{\deg P - 1}\}$ de $\mathbb{F}_q[X]/(P)$. Le processus suivant s'arrête après un nombre fini d'étapes et donne la décomposition en facteurs irréductibles de $P$ :

① On calcule la matrice de $S_P - \mathrm{id}$ dans la base $\mathcal{B}$ ;

② Le nombre de facteurs irréductibles de $P$ est $r = \dim(\ker(S_P - \mathrm{id})) = \deg P - \mathrm{rg}(S_P - \mathrm{id})$.
Si $r = 1$, on arrête l'algorithme. Sinon, on passe à l'étape suivante.

③ On calcule un polynôme $V$ non congru modulo $P$ à un polynôme constant de $\mathbb{F}_q[X]$ et tel que $V \bmod P \in \ker(S_P - \mathrm{id})$. On a alors $P = \prod_{\alpha \in \mathbb{F}_q} \mathrm{pgcd}(P, V - \alpha)$, et on retourne à l'étape ① avec chaque facteur non trivial.

Démonstration : Soit $P = P_1 \dots P_r$ la décomposition en produit d'irréductibles (deux à deux distincts) de $P$. On va montrer que $r = \dim(\ker(S_P - id))$.

On pose, pour tout $i \in [\![1,r]\!]$, $K_i = \mathbb{F}_q[X]/(P_i)$. Le théorème chinois fournit l'isomorphisme de $\mathbb{F}_q$-algèbres $\varphi : \mathbb{F}_q[X]/(P) \longrightarrow K_1 \times \dots \times K_r$

$$A \bmod P \longmapsto (A \bmod P_1, \dots, A \bmod P_r)$$

On pose alors $\tilde{S}_P = \varphi \circ S_P \circ \varphi^{-1}$, qui correspond à l'élévation à la puissance $q$ (composante par composante) dans l'anneau $K_1 \times \dots \times K_r$.

Alors $(x_1, \dots, x_r) \in \ker(\tilde{S}_P - id) \Leftrightarrow (x_1^q, \dots, x_r^q) = (x_1, \dots, x_r)$

$\Leftrightarrow \forall i \in [\![1,r]\!],\ x_i^q = x_i$ dans $K_i$.

Soit $K$ une extension de corps de $\mathbb{F}_q$. Alors l'image de $\mathbb{F}_q$ dans $K$ est l'ensemble des éléments de $K$ tels que $x^q = x$.

Donc $(x_1, \dots, x_r) \in \ker(\tilde{S}_P - id) \Leftrightarrow \forall i \in [\![1,r]\!],\ x_i \in \mathbb{F}_q$,

ce qui donne $\ker(\tilde{S}_P - id) \simeq \mathbb{F}_q^r$, donc $r = \dim(\ker(\tilde{S}_P - id))$.

On suppose à présent $r > 1$.

On commence par remarquer que l'ensemble des $(U \bmod P)$, où $U$ est congru modulo $P$ à un polynôme constant, est la droite vectorielle de $\mathbb{F}_q[X]/(P)$ engendrée par $1$. Comme $\dim(\ker(S_P - id)) = r > 1$, il existe $V \in \mathbb{F}_q[X]$ non congru modulo $P$ à un polynôme constant tel que $(V \bmod P) \in \ker(S_P - id)$.

On a $(V \bmod P_1, \dots, V \bmod P_r) \in \mathbb{F}_q^r$, et on pose, pour tout $i \in [\![1,r]\!]$, $\alpha_i = V \bmod P_i$. Soit $\alpha \in \mathbb{F}_q$. On va montrer l'égalité $\operatorname{pgcd}(P, V-\alpha) = \prod_{\{i,\ \alpha_i = \alpha\}} P_i$.

Comme $\operatorname{pgcd}(P, V-\alpha)$ divise $P$, on a $\operatorname{pgcd}(P, V-\alpha) = \prod_{i \in I_\alpha} P_i$, avec $I_\alpha \subset [\![1,r]\!]$.

Les $P_i$ étant deux à deux premiers entre eux, on a, par lemme de Gauss,

$I_\alpha = \{ i \in [\![1,r]\!] \ / \ P_i \mid V - \alpha \}$.

Cependant, pour $i \in [\![1, r]\!]$, on a :

$$\alpha_i = \alpha \Leftrightarrow V - \alpha = 0 \mod P_i \Leftrightarrow P_i \mid V - \alpha$$

donc $I_\alpha = \{i \in [\![1, r]\!] \,/\, \alpha_i = \alpha\}$, ce qui donne $\text{pgcd}(P, V - \alpha) = \prod_{\{i,\, \alpha_i = \alpha\}} P_i$.

On a alors $P = \prod_{i=1}^{r} P_i = \prod_{\alpha \in \mathbb{F}_q} \left( \prod_{\{i,\alpha_i = \alpha\}} P_i \right)$

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

ce qui achève la preuve.

<u>Algorithme de factorisation:</u> Soit $P \in \mathbb{F}_q[X]$.

① Si $P$ est constant, on sort de l'algorithme.

② On calcule $U = \text{pgcd}(P, P')$. Plusieurs cas se présentent :

- Si $U = 1$, on applique l'algorithme de Berlekamp à $P$;
- Si $U = P$, on calcule $R$ tel que $R^p = P$ et on retourne à l'étape 1 avec $R$;
- Sinon, on pose $V = \dfrac{P}{U}$. Alors $U$ et $V$ sont des facteurs non triviaux

de $P$, et on retourne à l'étape 1 avec $U$ et $V$.