# Algorithme de Berlekamp

Léo Gayral

2017-2018

ref : Beck – Objectif Agrégation – p.244

**Proposition 1.** Soient $q = p^n$ une puissance de premier et $P \in \mathbb{F}_q[X]$ un polynôme sans facteurs carrés. Alors on peut calculer le nombre de facteurs premiers de $P$.

*Démonstration.*
On considère $R := \mathbb{F}_q[X]/(P)$ une $\mathbb{F}_q$-algèbre. Dans $\mathbb{F}_q[X]$, par morphisme de Frobenius on a $(U+V)^q = U^q + V^q$ et $U(X^q) = U^q$, donc dans l'algèbre quotient $R$, $F : \overline{U} \mapsto \overline{U}^q = \overline{U(X^q)}$ est bien un endomorphisme de $\mathbb{F}_q$-algèbre. En particulier, $\ker(F - \mathrm{Id})$ l'ensemble de ses points fixes de $F$ est également une $\mathbb{F}_q$-algèbre.

Considérons $P = \prod_{i=1}^{r} P_i$ une décomposition de $P$ en irréductibles. Comme $P$ est sans facteur carré, les $P_i$ sont premiers entre eux, donc par le théorème des restes chinois, il existe $\varphi : R \to \bigoplus_{i=1}^{r} \mathbb{F}_q[X]/(P_i)$ un isomorphisme de $\mathbb{F}_q$-algèbres – $\varphi$ est en fait la somme des projections $\pi : R \to \mathbb{F}_q[X]/(P_i)$.

En conjuguant par $\varphi$, on transporte $F$ en l'élévation à la puissance $q$ coordonnée par coordonnée sur $\bigoplus_{i=1}^{r} \mathbb{F}_q[X]/(P_i)$. Par isomorphisme, l'ensemble des points fixes de $F$ est isomorphe à la somme des points fixes sur chaque $\mathbb{F}_q[X]/(P_i)$.

Comme $P_i$ est irréductible, $K = \mathbb{F}_q[X]/(P_i)$ est une extension du corps $\mathbb{F}_q$, donc pour $x \in K$ on a $x = x^q$ ssi $x \in \mathbb{F}_q$, donc le noyau de ce morphisme linéaire est de dimension 1.

Le nombre de facteurs irréductibles de $P$ est donc égal à la dimension $r = \dim \ker(F - \mathrm{Id})$. □

**Proposition 2.** Sous les hypothèses précédentes, on peut de plus déterminer algorithmiquement $V \in \mathbb{F}_q[X]$ non constant modulo $P$ tel que $P = \prod_{a \in \mathbb{F}_q} \operatorname{pgcd}(P, V - a)$.

*Démonstration.*
On commence par déterminer le nombre de facteurs $r$ comme ci-dessus. Si $r = 1$, on a terminé. Supposons maintenant $r \geq 2$.

Comme $\ker(F - \mathrm{Id})$ est de dimension $r$, cet espace contient $\overline{V} \notin \overline{1} \cdot \mathbb{F}_q$. Par isomorphisme, $\overline{V}$ correspond à un vecteur $(\alpha_i) \in \mathbb{F}_q^r \subset \bigoplus_{i=1}^{r} \mathbb{F}_q[X]/(P_i)$.

En particulier, $V$ n'est pas constant donc $\operatorname{pgcd}(V - \alpha_i, P_i) = P_i$. On a donc $\operatorname{pgcd}(V - \alpha, P) = \prod_{i=1}^{r} \operatorname{pgcd}(V - \alpha, P_i) = \prod_{\alpha_i = \alpha} P_i$. On a donc $P = \prod_{\alpha \in \mathbb{F}_q} \operatorname{pgcd}(V - \alpha, P)$.

Comme $V$ n'est pas constant modulo $P$, aucun des facteurs ci-dessus n'est de degré $\deg(P)$ donc on a une *vraie* factorisation de $P$. □

**Théorème 1** (Algorithme de Berlekamp)**.** On définit Facteurs($P$), qui prends un polynôme $P \in \mathbb{F}_q[X]$ en entrée et retourne l'ensemble de ses facteurs irréductibles en sortie. Cette fonction est calculée par l'algorithme :

```
si d := deg(P) ≤ 0 :
    retourner ∅
sinon si P' = 0 alors :
    calculer Q tel que P = Q^p
    retourner Facteurs(Q)
sinon :
    calculer U = pgcd(P, P') ≠ P
    si U ≠ 1 :
        retourner Facteurs(P/U)
    sinon :
        calculer M = Mat(F − Id) ∈ M_d(F_q) dans la base (1̄, X̄, ··· , X^{d−1}‾)
        calculer une base B de ker(M) par pivot de Gauss
        si |B| = 1 :
            retourner {P}
        sinon :
            choisir V̄ ∈ B tel que V̄ ∉ 1̄ · F_q
            retourner ⋃_{α∈F_q} Facteurs(pgcd[V − a, P])
```