Algorithme de Berlekamp

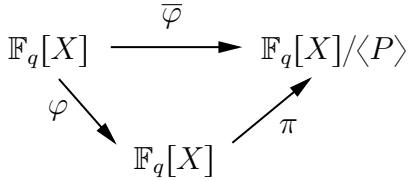
- Isenmann, Pecatte, *L'oral à l'agrégation de mathématiques.* (19-24)
- Beck, Malick, Peyré, *Objectif agrégation.* (244-247)

Soit $q = p^n$ avec p premier. Soit $P \in \mathbb{F}_q[X]$ sans facteur carré. On peut calculer le nombre de facteurs irréductibles de P et si P n'est pas irréductible alors il existe $V \in \mathbb{F}_q[X]$ non constant mod P tel que $P = \prod_{a \in \mathbb{F}_q} \operatorname{pgcd}(P, V - a)$.

Démonstration. Posons

$$\begin{array}{rccc} S_P : & \mathbb{F}_q[X]/\langle P\rangle & \to & \mathbb{F}_q[X]/\langle P\rangle \\ & Q(X) \bmod P & \mapsto & Q(X^q) \bmod P \end{array}$$

• Montrons que S_P est bien définie et coïncide avec l'élévation à la puissance q dans $\mathbb{F}_q[X]/\langle P\rangle$. Posons $\varphi : \begin{array}{ccc} \mathbb{F}_q[X] & \to & \mathbb{F}_q[X] \\ Q(X) & \mapsto & Q(X^q) \end{array}$ un morphisme d'anneaux tel que $\forall a \in \mathbb{F}_q$, $\varphi(a) = a$. Ainsi, on a $\forall Q \in \mathbb{F}_q[X],\ \varphi(Q) = Q(X^q) = Q^q$.
En composant avec $\pi : \mathbb{F}_q[X] \to \mathbb{F}_q[X]/\langle P\rangle$ la surjection canonique, on obtient $\bar\varphi = \pi \circ \varphi$ un morphisme d'anneaux tel que $\bar\varphi(P) = \pi(P^q) = \pi(P)^q = 0$ (car π est un morphisme d'anneaux). Donc, $\bar\varphi$ passe au quotient par $\langle P\rangle$ pour donner S_P et de plus :



$$S_P(Q \bmod P) = S_P(\pi(Q)) = \pi(Q(X^q)) = \pi(Q(X)^q) = \pi(Q(X))^q = (Q \bmod P)^q$$

Ainsi, S_P est coïncide avec l'élévation à la puissance q.

• Soit $P = P_1 \cdots P_r$ la décomposition en irréductibles sur $\mathbb{F}_q[X]$.
Montrons que $\dim \operatorname{Ker}(S_P - \mathrm{Id}) = r$. Posons $\forall i \in [\![1, r]\!]$, $K_i = \mathbb{F}_q[X]/\langle P_i\rangle$ un corps car P_i est irréductible (corps de rupture de P_i).
Le théorème chinois (voir IP 2.4.) donne l'isomorphisme de $\mathbb{F}_q$-algèbres (car les P_i sont premiers 2 à 2) : $\begin{array}{rccc} \Psi : & \mathbb{F}_q[X]/\langle P\rangle & \to & K_1 \times \cdots \times K_r \\ & Q \bmod P & \mapsto & (Q \bmod P_1, \ldots, Q \bmod P_r) \end{array}$
Posons $\tilde S_P = \Psi \circ S_P \circ \Psi^{-1} : K_1 \times \cdots \times K_r \to K_1 \times \cdots \times K_r$ l'élévation à la puissance q dans l'anneau produit $K_1 \times \cdots \times K_r$ (composante par composante).
En effet, $\Psi \circ S_P \circ \Psi^{-1}(x) = \Psi(\Psi^{-1}(x)^q) = \Psi(\Psi^{-1}(x))^q = x^q$.
Ainsi,

$$\begin{aligned} (Q_1, \ldots, Q_r) \in \operatorname{Ker}(\tilde S_P - \mathrm{Id}) &\Leftrightarrow (Q_1^q, \ldots, Q_r^q) = (Q_1, \ldots, Q_r) \\ &\Leftrightarrow \forall i \in [\![1, r]\!],\ Q_i^q = Q_i \text{ dans } K_i \end{aligned}$$

Or $\forall i \in [\![1, r]\!],\ K_i$ est une extension de $\mathbb{F}_q$ donc par le lemme $Q_i^q = Q_i \Leftrightarrow Q_i \in \mathbb{F}_q$.
Par conséquent, $\operatorname{Ker}(\tilde S_P - \mathrm{Id}) = (\mathbb{F}_q)^r$ et on a $\operatorname{Ker}(\tilde S_P - \mathrm{Id}) = \Psi(\operatorname{Ker}(S_P - \mathrm{Id}))$ et Ψ est un isomorphisme. D'où $\dim \operatorname{Ker}(\tilde S_P - \mathrm{Id}) = \dim \operatorname{Ker}(S_P - \mathrm{Id}) = r$.

• Si $r \geqslant 2$. Les polynômes constants mod P forment un s.e.v. de $\mathbb{F}_q[X]/\langle P\rangle$ de dimension 1 engendré par 1.
Comme $\dim \operatorname{Ker}(S_P - \mathrm{Id})) \geqslant 2$ alors il existe $V \in \mathbb{F}_q[X]$ non congru mod P à un polynôme constant tel que $(V \bmod P) \in \operatorname{Ker}(S_P - \mathrm{Id})$ i.e. $(V \bmod P_1, \ldots, V \bmod P_r) \in (\mathbb{F}_q)^r$.
On pose $\forall i \in [\![1, r]\!]$, $\alpha_i = (V \bmod P_i) \in \mathbb{F}_q$.
Pour $\alpha \in \mathbb{F}_q$, montrons que $\operatorname{pgcd}(P, V - \alpha) = \prod_{\{i,\ \alpha_i = \alpha\}} P_i$.
Comme $\operatorname{pgcd}(P, V - \alpha) \mid P$ alors $\operatorname{pgcd}(P, V - \alpha) = \prod_{i \in I_\alpha} P_i$ avec $I_\alpha \subset [\![1, r]\!]$.
Comme les P_i sont premiers 2 à 2 alors par le lemme de Gauss ($a \mid bc$ et $\operatorname{pgcd}(b, c) = 1$

alors $a \mid c$), on a $I_\alpha = \{i \in [\![1, r]\!],\ P_i \mid V - \alpha\}$.
Or $P_i \mid V - \alpha \Leftrightarrow V - \alpha = 0 \bmod P_i \Leftrightarrow \alpha_i = \alpha$. Donc $I_\alpha = \{i \in [\![1, r]\!],\ \alpha_i = \alpha\}$.

$$P = \prod_{i=1}^{r} P_i = \prod_{\alpha \in \mathbb{F}_q} \left(\prod_{\{i,\ \alpha_i = \alpha\}} P_i \right) = \prod_{\alpha \in \mathbb{F}_q} \operatorname{pgcd}(P, V - \alpha)$$

□

Remarque.

- L'algorithme s'arrête bien car à chaque itération r diminue.
- $\mathbb{F}_q[X]/(P)$ est un corps si P est irréductible, sinon c'est seulement une $\mathbb{F}_q$-algèbre.
- C'était l'algorithme le plus performant jusqu'en 1981 où celui de Cantor-Zassenhaus est devenu plus rapide.
- Cet algorithme nécessite le calcul de pgcd par le biais de l'algorithme d'Euclide et le calcul du rang de matrices par pivot de Gauss.
- Cet algorithme donne une méthode de factorisation des polynômes dans $\mathbb{F}_q$.
- C'est un outil important dans la cryptographie, dans la factorisation des polynômes à coefficients entiers...

Application : On itère ce processus pour extraire successivement les facteurs irréductibles de P. Si on se donne un polynôme dans $\mathbb{F}_q$:

- on le rend unitaire en multipliant par l'inverse du coefficient dominant
- on le rend sans facteur carré en considérant le PGCD de P et P' (jusqu'à ce qu'il n'y en ait plus)
- on calcule la matrice de $X \mapsto X^q - X$ dans la base $(1, X, \ldots, X^{q-1})$ modulo P (il faut calculer les puissances de X modulo P)
- on exhibe un élément V non constant (modulo P) dans le noyau
- et on écrit $P = \prod_{\alpha \in \mathbb{F}_q} \operatorname{pgcd}(P, V - \alpha)$

Complexité : En pratique, l'algorithme de Berlekamp nécessite le calcul de pgcd (via l'algorithme d'Euclide) et de rang de matrice (via le pivot de Gauss). On a alors, la complexité du pivot de Gauss en $\operatorname{ord}(\deg(P)^3)$ puisque la taille de la matrice de $S_P - \mathrm{Id}$ dans la base $\mathcal{B}$ est de $\deg(P)$. De plus, on effectue q calcul de pgcd dans l'algorithme de d'Euclide car on a $\deg(P)$ étapes de calcul de l'algorithme d'Euclide et une division par x en deg(P). On en déduit que la factorisation de P se fait en $\operatorname{ord}(q \deg(P)^2)$. Donc un appel de l'algorithme de Berlekamp se fait en $\operatorname{ord}\big(\deg(P)^3 + q \deg(P)^2\big)$.

Lemme : Soit L une extension de $\mathbb{F}_q$. Alors $x \in L$ vérifie $x^q = x$ ssi $x \in \mathbb{F}_q$.

Démonstration.
($\Rightarrow$) D'après le théorème de Lagrange, $\forall x \in \mathbb{F}_q^*$, $x^{q-1} = 1$.
Donc $x^q = x$ (vrai aussi pour $x = 0$).
($\Leftarrow$) On a trouvé q racines au polynôme $X^q - X$ sur L. Comme L est un corps et que $\deg P = q$ alors P possède au plus q racines. □