Algorithme de Berlekamp

Cf Object. Agregation p245.
Demazure, cours d'algèbre p232.

Le but de cet algorithme est de fournir la décomposition en produit de facteurs irréductibles d'un polynôme sur un corps fini. On se restreint à des polynômes sans facteurs multiples, sachant s'y ramener d'après 96.

Soit p un nombre premier. Soit $n \in \mathbb{N}^*$. On pose $q = p^n$
Soit $P \in \mathbb{F}_q[X]$, un polynôme sans facteur multiple.
La décomposition en facteurs irréductibles (DFI) s'écrit alors $P = \prod_{i=1}^{s} P_i$. Notons $d = \deg(P)$.

Notons que P est irréductible ssi $s = 1$.

98.1 Berlekamp (P) :

- Pour j allant de 0 à $d-1$ calculer $(X^j)^q$ modulo (P).
- En déduire $M = Mat_{\mathcal{B}}(S)$ où $\mathcal{B} = (1, X, \dots X^{d-1})$ base de $\mathbb{F}_q[X]/(P)$
  $S = \left(\begin{array}{ccc} \mathbb{F}_q[X] & \to & \mathbb{F}_q[X] \\ x & \mapsto & x^q \end{array} \right)$
- Par le pivot de Gauss calculer $\ker(M - Id) = K$
- Si $\dim K = 1$
  alors renvoyer P
  sinon choisir $V \in K$ non constant
  pour chaque $\alpha \in \mathbb{F}_q$, calculer $d_\alpha = PGCD(P, V - \alpha)$
  et appliquer Berlekamp à d_α (si $d_\alpha \neq 1$)

98.2 **Pté** Cet algorithme termine nécessairement et fournit bien une DFI de P.

Preuve : 1) LEMME CHINOIS ET ISOMORPHISME

(On note $A \wedge B$ pour $PGCD(A, B)$)

On a $\forall (i,j) \in [\![1..s]\!]^2 \quad i \neq j \Rightarrow (P_i, P_j) = (P_i \wedge P_j) = (1) = \mathbb{F}_q[X]$
De plus $\bigwedge_{i=1}^{s} (P_i) = \left(\prod_{i=1}^{s} P_i \right) = (P)$.

On peut donc appliquer le lemme chinois qui assure que

$\gamma = \left(\begin{array}{ccc} A := \mathbb{F}_q[X]/(P) & \longrightarrow & \prod_{i=1}^{s} A_i := \mathbb{F}_q[X]/(P_i) \\ \overline{Q}^{(P)} & \longrightarrow & \left(\overline{Q}^{(P_i)}\right)_{i \in [\![1..s]\!]} \end{array} \right)$ est un isomorphisme d'anneaux.

(où $\overline{Q}^{(P)}$ désigne la classe de Q modulo P ie $\{Q + RP \mid R \in \mathbb{F}_q[X]\}$
$\overline{Q}^{(P_i)}$ ——— P_i ie $\{Q + RP_i \mid$ ——— $\}$)

En fait γ est même un isomorphisme de $\mathbb{F}_q$-EV.

En effet si $\lambda \in \mathbb{F}_q[X]$ et $\overline{Q} \in A$

$$\begin{aligned} \lambda . \gamma(\overline{Q}^{(P)}) &= \lambda . \left(\overline{Q}^{(P_i)}\right)_{i \in [\![1..s]\!]} \\ &= \left(\lambda . \overline{Q}^{(P_i)}\right)_{i \in [\![1..s]\!]} && \text{) déf d'EV produit.} \\ &= \left(\overline{\lambda \times_{\mathbb{F}_q[X]} Q}^{(P_i)}\right) && \text{) déf de la structure de } \mathbb{F}_q\text{-EV de } A_i \text{ vu comme quotient d'EV} \\ &= \gamma\left(\overline{\lambda \times_{\mathbb{F}_q[X]} Q}^{(P)}\right) \\ &= \gamma(\lambda . \overline{Q}^{(P)}) && \text{) déf de la structure de } \mathbb{F}_q\text{-EV de } A \text{ vu comme quotient d'EV.} \end{aligned}$$

2) CALCUL DE s.

On introduit $S = \left(\begin{array}{ccc} A & \to & A \\ \overline{Q}^{(P)} & \mapsto & \overline{Q^q}^{(P)} \end{array} \right)$ et pour $i \in [\![1..s]\!]$ $S_i = \left(\begin{array}{ccc} A_i & \to & A_i \\ \overline{Q}^{(P_i)} & \mapsto & \overline{Q^q}^{(P_i)} \end{array} \right)$

Ce sont les puissances n-ièmes resp. des morphismes de Frobenius.

On note $A^S = \{x \in A \mid S(x) = x\} = \ker(S - id_A)$ les points fixes de S.

Soit $\overline{Q}^{(P)} \in A$.

$$\begin{aligned} \overline{Q}^{(P)} \in A^S &\Leftrightarrow S(\overline{Q}^{(P)}) = \overline{Q}^{(P)} \\ &\Leftrightarrow \gamma\left(\overline{Q^q}^{(P)}\right) = \gamma(\overline{Q}^{(P)}) && \text{) car } \gamma \text{ bijective} \\ &\Leftrightarrow \forall i \in [\![1..s]\!] \quad \overline{Q^q}^{(P_i)} = \overline{Q}^{(P_i)} \\ &\Leftrightarrow \forall i \in [\![1..s]\!] \quad \overline{Q}^{(P_i)^q} = \overline{Q}^{(P_i)} && \text{) lemme : Si } \mathbb{K} \text{ est une ext de } \mathbb{F}_q \text{ alors } \forall x \in \mathbb{K},\ x \in \mathbb{F}_q \text{ ssi } x^q = x \\ &\Leftrightarrow \forall i \in [\![1..s]\!] \quad \overline{Q}^{(P_i)} \in \underbrace{\mathbb{F}_q . 1_{A_i}}_{\text{droite vectorielle de } A_i} \\ &\Leftrightarrow \gamma(\overline{Q}^{(P)}) \in \bigoplus_{i=1}^{s} \mathbb{F}_q . 1_{A_i} \end{aligned}$$

Donc $\dim_{\mathbb{F}_q}(A^S) = \dim\left(\bigoplus_{i=1}^{s} \mathbb{F}_q . 1_{A_i}\right) = s$ soit $\underline{\underline{s = \dim_{\mathbb{F}_q}(A^S)}}$

(car γ iso de $\mathbb{K}$-EV)

Alors que ce qui se passe du côté des $\mathbb{F}_i$ se fait "en boîte noire", on a accès aux points fixes de S du côté de A : c'est le $\ker_{\mathbb{K}}(M - I_d)$ qu'on a calculé d'où $\underline{\underline{s = \dim_{\mathbb{K}}(K)}}$

3) COMPRENDRE LES PGCD $(P, Q-\alpha)$

Dans le cas où s valait 1 on s'est arrêté car cela signifiait P irréductible.
Supposons maintenant $s>1$. A^S étant de dimension >1 il ne peut être réduit à $\mathbb{F}_q.1_A$ qui est la droite vectorielle des classes de polynômes constants modulo (P). Il existe donc $\overline{Q}^{(P)} \in A^S \setminus \mathbb{F}_q.1_A$.
$\forall i \in [1..s]$ $\overline{Q}^{(P_i)} \in \mathbb{F}_q.1_{A_i}$ d'après l'équivalence précédente.

Rq Dans les A_i les points fixes de S_i sont les classes de polynômes constants justement parce que les P_i sont irréductibles.

Choisissons de meilleurs représentants : $\exists \alpha_i \in \mathbb{F}_q$ tel que $\overline{Q}^{(P_i)} = \overline{\alpha_i X^0}^{(P_i)}$

MQ $\forall \alpha \in \mathbb{F}_q$, $\mathrm{PGCD}(P, Q-\alpha) = \prod_{\substack{i=1 \\ \alpha_i = \alpha}}^{S} P_i$

Soit $i \in [1..s]$ $\overline{Q}^{(P_i)} = \overline{\alpha_i X^0}^{(P_i)}$ soit $Q - \alpha_i \equiv 0 [P_i]$ soit $P_i \mid Q-\alpha_i$
↳ si $\alpha = \alpha_i$ $P_i \mid Q-\alpha$
↳ si $\alpha \neq \alpha_i$ $Q-\alpha \equiv Q-\alpha_i+\alpha_i-\alpha \equiv \alpha_i-\alpha \ [P_i]$ or α_i et α étant des constantes leur différence n'est pas résidue modulo (P_i), autrement dit $\alpha_i-\alpha \not\equiv 0 [P_i]$ donc $P_i \nmid Q-\alpha_i$

Comme $\mathrm{PGCD}(P, Q-\alpha)$ s'écrit, en tant que diviseur de P, nécessairement comme produit de certains P_i on en déduit $\mathrm{PGCD}(P, Q-\alpha) = \prod_{\substack{i=1 \\ \alpha_i = \alpha}}^{S} P_i$.

On en déduit que $P = \prod_{i=1}^{S} P_i = \prod_{\alpha \in \mathbb{F}_q} \prod_{\substack{i=1 \\ \alpha_i = \alpha}}^{S} P_i = \prod_{\alpha \in \mathbb{F}_q} \mathrm{PGCD}(P, Q-\alpha)$

Et cette décomposition est meilleure car calculable. Il reste cependant à montrer qu'elle n'est pas triviale, c-à-d qu'il n'existe aucun terme valant P.
$\mathrm{PGCD}(P, Q-\alpha) = P$ ssi $\forall i \in [1..s]$ $\alpha_i = \alpha$ ssi $(\overline{Q}^{(P_i)})_{i \in [1..s]} = (\overline{\alpha X^0}^{(P_i)})_{i \in [1..s]}$
ssi $\gamma(\overline{Q}^{(P)}) = \gamma(\overline{\alpha X^0}^{(P)}) = \gamma(\alpha.1_A)$ ssi $\overline{Q}^{(P)} = \alpha.1_A$
IMPOSSIBLE car on a pris $\overline{Q}^{(P)}$ "non constant" c-à-d n'appartenant pas à $\mathbb{F}_q.1_A$.
Ceci assure que cette décomposition fournit au moins deux facteurs stricts de P, de degré st. moindre. Ainsi l'algorithme termine nécessairement.