Berlekamp

Thm : Soit $P \in \mathbb{F}_q[X]$ sans facteurs carrés.
On définit $x = X \bmod P$ dans $\mathbb{F}_q[X]/(P)$ et $\mathcal{B} = \{1, x, \dots, x^{\deg P - 1}\}$ base de $\mathbb{F}_q[X]/(P)$.

Le processus suivant s'arrête au bout d'un nbe fini d'étapes :

1) On calcule la matrice $S_p - id$ dans $\mathcal{B}$ avec $S_p : Q(x) \bmod P \to Q(x^q) \bmod P$.
2) Le nbe de facteurs irreds de P est $r = \dim(\ker(S_p - id))$.

Si $r = 1$, P irred. et on s'arrête.
Sinon :

3) On calcule V pol. non congrue mod P à une constante de $\mathbb{F}_q[X]$ et tq $V \bmod P \in \ker(S_p - id)$.

On a ainsi, $P = \prod_{\alpha \in \mathbb{F}_q} PGCD(P, V - \alpha)$ (avec euclide)

On retourne au ② pour les facteurs non triviaux.

Preuve :

Soit $P = P_1 \cdots P_r$ dec. en irred.

① • Mq $r = \dim(\ker(S_p - id))$: On pose $K_i = \mathbb{F}_q[X]/(P_i)$.

On pose $\phi : \mathbb{F}_q[X]/(P) \to K_1 \times \cdots \times K_r$ iso de $\mathbb{F}_q$-algèbres
$Q \bmod P \to (Q \bmod P_1, \dots, Q \bmod P_r)$

par le thm chinois.

Posons $\hat{S_p} = \phi \circ S_p \circ \phi^{-1} : K_1 \times \cdots \times K_r \to K_1 \times \cdots \times K_r$,
l'élévation à la puissance q dans l'anneau $K_1 \times \cdots \times K_r$.

Ainsi, $(x_1, \dots, x_r) \in \ker(\hat{S_p} - id) \iff (x_1^q, \dots, x_r^q) = (x_1, \dots, x_r)$
$\iff \forall i \in [\![1, r]\!],\ x_i^q = x_i$ dans K_i.

Or $\mathbb{F}_q \hookrightarrow K_i$ et tous les éléments de $\mathbb{F}_q$ satisfont $x_i^q = x_i$.
Comme K_i est un corps commutatif, on a au plus q solutions à l'équation $x^q = x$; ce sont les éléments de $\mathbb{F}_q$.

Donc $\ker(\hat{S_p} - id) \simeq (\mathbb{F}_q)^r$.
Mais $\ker(\hat{S_p} - id) = \phi^{\text{res}}(\ker(S_p - id))$
$\Rightarrow \dim(\ker(S_p - id)) = \dim(\mathbb{F}_q)^r = r$.

② Expression des P_i

Soit $r>1$, $\{V \bmod P \mid V \equiv \text{cste} \bmod P\}$ est la droite vectorielle de $\mathbb{F}_q[X]/(P)$ engendrée par 1.
Comme $\dim(\ker(S_p - id)) = r > 1$, $\exists V \in \mathbb{F}_q[X]$ non congru modulo P à un pol. cst tq $(V \bmod P) \in \ker(S_p - id)$.

Soit $\alpha_i = V \bmod P_i$ et $\alpha \in \mathbb{F}_q$.
Alors $PGCD(V-\alpha, P) \mid P$
$\Rightarrow PGCD(V-\alpha, P) = \prod_{i \in I_\alpha} P_i$ où $I_\alpha \subset [\![1, r]\!]$
(lemme de Gauss)
mais $P_i \mid V-\alpha \Leftrightarrow \alpha_i = \alpha$.
Donc $I_\alpha = \{i \mid \alpha_i = \alpha\}$.

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

③ r diminue
Le choix d'un $V \not\equiv \text{cste} \bmod P \Rightarrow \exists i, j \in [\![1, r]\!]^2 / \alpha_i \neq \alpha_j$ (sinon $V-\alpha \mid P_i, \forall i \Rightarrow V \equiv \alpha \bmod P$)
Donc on a un facteur non trivial (sinon $PGCD(V-\alpha, P) = P$
$\Rightarrow I_\alpha = [\![1, r]\!]$
et $\alpha_i = \alpha, \forall 1 \leq i \leq r$).

Donc r diminue.

Obtenir S_p :
Par la prop universelle des polynômes, $S_1 : \mathbb{F}_q[X] \to \mathbb{F}_q[X]$, $Q(X) \to Q(X^q)$ est l'unique morphisme d'anneau vérifiant $S_1(a) = a$, $\forall a \in \mathbb{F}_q$ et $S_1(X) = X^q$.
Comme $a^q = a$, $\forall a \in \mathbb{F}_q$, $S_1(Q) = Q(X^q) = Q^q$, $\forall Q \in \mathbb{F}_q[X]$.
Soit $\pi : \mathbb{F}_q[X] \to \mathbb{F}_q[X]/(P)$ surj. canonique et $S = \pi \circ S_1$.
π est un morphisme d'anneaux donc $S(P) = \pi(P)^q = 0$.

Donc S passe au quotient par (P) donnant Sp.
On a enfin, $Sp(Q \bmod P) = Sp(\pi(Q)) = \pi(Q(X^q))$
$= \pi(Q^q) = \pi(Q)^q$, (↑ l'énoncé)