Ref: Saux-Picard, Rannou, Cours de calcul formel, corps finis (...) p. 55

Développement : algorithme de Berlekamp

Leçons : 123, 141, 148

Théorème : Soit $q = p^\alpha$ avec p 1er, $\alpha \in \mathbb{N}^*$, $P \in \mathbb{F}_q[X]$ produit de facteurs irréductibles $P_1, \dots, P_r$ 2 à 2 $\neq$.

$\psi : \mathbb{F}_q[X]/(P) \longrightarrow \mathbb{F}_q[X]/(P)$, $\bar{Q} \longmapsto \bar{Q}^q$ est un morphisme d'anneau $\mathbb{F}_q$-linéaire

tel que si $Q \in \mathbb{F}_q[X]$ avec $\begin{cases} \bar{Q} \in \mathrm{Ker}(\psi - id) \\ 1 \leq \deg Q \leq \deg P - 1 \end{cases}$, alors

$P = \prod_{\alpha \in \mathbb{F}_q} \mathrm{pgcd}(P, Q - \alpha)$ et cette décomposition de P n'est pas triviale (si P n'est pas irréd.)

Preuve :

L'anneau est de caract. p donc ψ est un morphisme (Frobenius itéré) et si $\lambda \in \mathbb{F}_q$, $\lambda^q = \lambda$ donc ψ est $\mathbb{F}_q$-linéaire.

Soit $Q \in \mathbb{F}_q[X]$

Les P_i sont 1ers entre eux donc par le théorème chinois, on a un isom. d'anneaux

$$\mathbb{F}_q[X]/(P) \xrightarrow{\sim} \prod_{i=1}^{r} \underbrace{\mathbb{F}_q[X]/(P_i)}_{}$$

corps de caractéristique p, extension de $\mathbb{F}_q$ de degré $d°P_i$.

$R \bmod P \longmapsto (R[P_1], \dots, R[P_r])$

$\bar{Q} \in \mathrm{Ker}(\psi - id) \Leftrightarrow Q^q = Q \bmod P$

$\Leftrightarrow Q^q = Q \bmod P_i \ \forall i$

$\Leftrightarrow \forall i, Q \bmod P_i \in \mathbb{F}_q \Leftrightarrow \exists (\alpha_1, \dots, \alpha_r) \in \mathbb{F}_q^r$ t.q. $Q = \alpha_i [P_i] \ \forall i$

si $\gamma \mid \beta$,
($\exists$ un unique ssc de $\mathbb{F}_{p^\beta}$ de cardinal p^γ , c'est $\{x \in \mathbb{F}_{p^\beta} \mid x^{p^\gamma} - x = 0\}$)

En particulier, $\dim(\ker(\Psi - id)) = r$ le nombre de facteurs irréductibles de P. (si $r=1$, P est irréd)

Si $Q \in \mathbb{F}_q[X]$ et $\begin{cases} 1 \le \deg Q \le \deg P - 1 \\ Q \bmod P \in \ker(\Psi - id) \end{cases}$, $P \mid Q^q - Q$ donc et $Q^q - Q \neq 0$ (un cst)

$$P = \operatorname{pgcd}(P, Q^q - Q) = \operatorname{pgcd}\left(P, \prod_{\alpha \in \mathbb{F}_q} (Q - \alpha)\right)$$ car $X^q - X = \prod_{\alpha \in \mathbb{F}_q} (X - \alpha)$ puis évaluation en Q.

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

car les $(Q-\alpha)_\alpha$ sont 1 ers entre eux : on a la relat de Bezout (si $\alpha \neq \beta$)
$$\frac{Q-\alpha}{\beta - \alpha} - \frac{Q-\beta}{\beta-\alpha} = 1$$

Les $\operatorname{pgcd}(P, Q-\alpha)$ ont $d^\circ \le d^\circ(Q-\alpha) \le d^\circ P - 1$ donc non associés à P et non tous constant car leur produit est de degré $d^\circ P$.

On en déduit l'algorithme de factorisation :
1) Calcul de la matrice de Ψ dans la base $(1, X, \dots, X^{d-1})$ $(d = d^\circ P)$
   Le calcul de $X^q [P]$ $O(\log(q)\, d^2)$ op. ds $\mathbb{F}_q$ (exp rapide)
   Le calcul de $(X^q)^i [P]$ pour $i = 1, \dots, d-1$ donc $O(\sum_{i=1}^{d} d \cdot d^2)$ $(d$ mult ds $\mathbb{F}_q$ mod $P)$
2) Calcul de $\dim(\ker(\Psi - id))$ $O(d^3)$ par pivot de Gauss
   si $= 1$ P est irréd. on s'arrête.

3) Choix d'un élément α du noyau non constant, calcul des $\gcd(P, Q-\alpha)$ jusqu'à trouver un facteur non trivial $O(d^2)$, au plus fait q fois donc un tout $O(q d^2)$

On répète sur les quotients $r \leq d$ donc on répète au plus d fois

En tout $O(qd^3)$ dans $\mathbb{F}_q$

Rq: ne marche que pour q petit!

Exemple: $q=5$, $P = X^5 + 2X^3 + 4X + 1$. On peut vérifier que $P' = 4X^3 + 6X^2 + 4$, $P \wedge P' = 1$ P est sans fact. carré

$X^5 = 4X^3 + X^2 + 2X + 2 \ [P]$
$X^{10} = X^3 + 3X^2 + 2X + 4 \ [P]$
$X^{15} = 4X^3 \ [P]$

Mat $\Psi = \begin{pmatrix} 1 & 2 & 4 & 0 \\ 0 & 2 & 2 & 0 \\ 0 & 1 & 3 & 0 \\ 0 & 4 & 1 & 4 \end{pmatrix}$

$\dim \ker(\Psi - id) = 2$ P est produit de 2 fact. irréd. de $d^\circ 2$.

on a une base $\left(\begin{pmatrix} 0 \\ 2 \\ 4 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \right)$ $\quad v_1 \quad v_2$

$v_1 + v_2$ correspond à $W = 1 + 2X + 4X^2 + X^3$

$P \wedge W = X^2 + 2X + 3$ donc $P = (X^2 + 2X + 3)(X^2 - 3)$