Berlekamp [OA p 244]

Algo Soit $p \in \mathbb{P}$ et $q = p^\alpha$. Soit $P \in \mathbb{F}_q[X]$ sans facteur carré.

On note $x = X \bmod P$ dans l'anneau $\mathbb{F}_q[X]/(P)$ dont 1 base est alors $(1, x, \dots x^{\deg(P)-1}) = B$

l'algo suivant (Berlekamp) permet d'obtenir la décomposition en facteurs irréd de P:

(1) $S_p : \left\{ \begin{array}{ccc} \mathbb{F}_q[X]/(P) & \longrightarrow & \mathbb{F}_q[X]/(P) \\ Q \bmod P & \mapsto & Q^q \bmod P \end{array} \right.$ est linéaire. On K la matrice de $S_p - Id$ ds base B

(2) Le nb r de facteurs irréd de P est égal à la dimension de $\ker(S_p - Id)$

On K donc r avec pivot de Gauss. Si $r = 1$, P est irréd et on a fini. Sinon:

(3) On choisit V non constant $\in \mathbb{F}_q[X]/(P)$ et tq $V \in \ker(S_p - Id)$

On K avec Euclide les $\gcd(P, V - a)$ $\forall a \in \mathbb{F}_q$. Alors $P = \prod_{a \in \mathbb{F}_q} \gcd(P, V - a)$

On réapplique l'algo aux facteurs non triviaux (γ en a) de ce produit.

démo L'algo termine et est correct.

- S_p est $\mathbb{F}_q$ linéaire (m démo que pour "le morphisme de Frobenius en est 1"

- $\exists! p$, $P = \prod_{i=1}^{r} P_i$ où les P_i sont irréd et 2à2 $\neq$ (P est sans facteur carré)

et r = nb de pol irréd ds la décomposition de P

Les P_i sont 2à2 1er entre eux donc $\exists!$ (R chinois) $\exists$ 1 isomorphisme de $\mathbb{F}_q$-alg

$$\varphi : \left\{ \begin{array}{ccc} \mathbb{F}_q[X]/(P) & \longrightarrow & \mathbb{F}_q[X]/(P_1) \times \dots \times \mathbb{F}_q[X]/(P_r) \\ Q \bmod P & \mapsto & (Q \bmod P_1, \dots, Q \bmod P_r) \end{array} \right.$$

$\forall i \in [\![1, r]\!]$, $K_i = \mathbb{F}_q[X]/(P_i)$ est un corps (carac $= p$, cardinal $= p^{\deg(P_i)}$) car P_i irréd ds $\mathbb{F}_q$

Soit $Q \in \mathbb{F}_q[X]/(P)$ et notons $\varphi(Q) = (Q_1, \dots, Q_r)$

$$\begin{aligned} Q \in \ker(S_p - Id) &\iff Q^q - Q = 0 \bmod P \\ &\iff \forall i \in [\![1, r]\!],\ Q_i^q - Q_i = 0 \bmod P_i \quad \text{(isom)} \\ &\iff \forall i \in [\![1, r]\!],\ Q_i^q = Q_i \text{ dans } K_i \\ &\overset{(*)}{\iff} \forall i \in [\![1, r]\!],\ Q_i \in \mathbb{F}_q \iff (Q_1, \dots, Q_r) \in \mathbb{F}_q^r \end{aligned}$$

$(*)$ est vrai car $\forall i \in [\![1, r]\!]$, $\{x \in K_i \mid x^q = x\} = \mathbb{F}_q$ car $\forall x \in \mathbb{F}_q \subset K_i$, $x^q = x$ (puissance de $\mathbb{F}_q^\times$)

et le polynôme $X^q - X$ a moins de q racines dans K_i ; on en a déjà q. D'où =

On en déduit que $\ker(S_P - Id) = \varphi^{-1}(\mathbb{F}_q^2)$ et comme φ = isom, $\dim_{\mathbb{F}_q}(\ker(S_P - Id)) = \dim_{\mathbb{F}_q}(\mathbb{F}_q^2) = 2$

- On suppose $r > 1$. Cela assure $\exists V \in \mathbb{F}_q[X]$ tq $V \not\equiv$ cst mod P et $(V \bmod P) \in \ker(S_P - Id)$

Comme $(V \bmod P) \in \ker(S_P - Id)$, $\forall i \in [\![1, r]\!]$ $(V \bmod P_i) = a_i \in \mathbb{F}_q$ (on vient de 3 manières)

Soit $a \in \mathbb{F}_q$. On note $D = \text{pgcd}(P, V-a)$: c'est un produit d'été de $\{P_i \mid 1 \le i \le r\}$ car $D \mid P$

Comme les P_i et 1^{ers} entre eux, / Gauss D = produit des (P_i qui $\mid V-a$)

On a, $\forall i$, $V - a \equiv a_i - a \bmod P_i$ donc $P_i \mid V-a \iff a_i = a$.

Donc $\text{pgcd}(P, V-a) = \prod_{i, a_i = a} P_i$.

En multiplionnant $[\![1, r]\!]$, on a $P = \prod_{i=1}^{r} P_i = \prod_{a \in \mathbb{F}_q} \prod_{\substack{i \in [\![1,r]\!] \\ a_i = a}} P_i = \prod_{a \in \mathbb{F}_q} \text{pgcd}(P, V-a)$

Tous les facteurs de ce produit $\mid P$ donc sont aussi facteurs carrés donc on peut leur appliquer Berlekamp

- Reste à mq l'algo termine : on mq le nb r de facteurs irred de l'entrée décroit strict

C'est le cas car au moins 1 des $\text{pgcd}(P, V-a)$ est un diviseur strict de P :

En effet $(V \bmod P) \neq$ cste donc $\exists i \neq j$ tq $a_i \neq a_j$ (sinon $\forall i$ $a_i = a \in \mathbb{F}_q$ et $\forall i$, $P_i \mid V-a$

donc $\prod P_i = P \mid V-a$ car les P_i et 1^{ers} entre eux car $V \equiv a \equiv$ cste mod $P \Rightarrow \not\downarrow$)

Or $P_i \mid \text{pgcd}(P, V-a_i) \Rightarrow \deg(\text{pgcd}(V-a_i, P)) > 0$

et $P_j \nmid \text{pgcd}(P, V-a_i) \Rightarrow \deg(\text{pgcd}(V-a_i, P)) < \deg(P)$ et $\text{pgcd}(P, V-a_i)$: facteur strict

(rq) Algo de factorisation de $P \in \mathbb{F}_q[X]$

→ Si $P' = 0$, $\exists R \in \mathbb{F}_q[X]$ tq $P = R^p$. Appliquer l'algo à R

→ Si $P' \neq 0$ et $D = \text{pgcd}(P, P') \neq 1$, D = diviseur strict de P Appliquer l'algo à D et $\frac{P}{D}$

→ Si $P' \neq 0$ et $D = 1$, P est aussi facteur carré. Appliquer l'algo à P

(rq) Complexité $O(\deg(P)^3)$ pour pivot de Gauss sur taille de $S_P - Id = \deg(P)$

+ q calculs de pgcd / algo d'Euclide ($\deg(P)$ étapes d'Euclide + 1 division en $\deg(P)$)

donc $O(q \deg(P)^2)$ pour la factorisation de P

$\Rightarrow$ 1 passe dans Berlekamp en $O(\deg(P)^3 + q\deg(P)^2)$