Algorithme de Berlekamp

(122, 123, 125, 141, 142, 148)

BMP p 244 et Berhuy p 662

Soit p un nombre premier, $q = p^s$, $\mathbb{F}_q$ le corps finis à q éléments. On considère $P \in \mathbb{F}_q[X]$ sans facteurs carrés, on l'écrit : $P = \prod_{i=1}^{r} P_i$ où les P_i sont irréductibles entre eux deux à deux.

Lemme : L'application $S_p : \mathbb{F}_q[X]/\langle P\rangle \longrightarrow \mathbb{F}_q[X]/\langle P\rangle$, $Q(X)[P] \longmapsto Q(X^q)[P]$ est bien définie et coïncide avec l'élévation à la puissance q dans $\mathbb{F}_q[X]/\langle P\rangle$

démo : L'application $\mathbb{F}_q[X] \longrightarrow \mathbb{F}_q[X]$, $Q(X) \longmapsto Q(X^q) = Q^q(X)$ est un morphisme de $\mathbb{F}_q$-Algèbres.

On considère $\Pi : \mathbb{F}_q[X] \longrightarrow \mathbb{F}_q[X]/\langle P\rangle$ la projection canonique, c'est aussi un morphisme de $\mathbb{F}_q$-Algèbres

Par composition, $\delta : \mathbb{F}_q[X] \longrightarrow \mathbb{F}_q[X]/\langle P\rangle$, $Q(X) \longmapsto Q(X^q)[P]$ est bien définie et est un morphisme de $\mathbb{F}_q$-Algèbres.

De plus $\delta(P) = \Pi(P^q(X)) = \Pi(P)^q = 0$, donc δ passe au quotient par $\langle P\rangle$ pour donner S_p.

Enfin, $S_p(Q[P]) = S_p(\Pi(Q)) = \Pi(Q(X^q)) = \Pi(Q^q) = \Pi(Q)^q = Q^q[P]$.

thm : Il existe un polynôme $V \in \mathbb{F}_q[X]$ tel que $P = \prod_{\alpha \in \mathbb{F}_q} \operatorname{pgcd}(P, V-\alpha)$ et cette décomposition est non triviale

démo : On pose $K_i = \mathbb{F}_q[X]/\langle P_i\rangle$ comme P_i est irréductible et $\mathbb{F}_q[X]$ principal, on a K_i est un corps

Ainsi par le thm des restes chinois, il existe

$$\varphi : \mathbb{F}_q[X]/\langle P\rangle \longrightarrow K_1 \times \dots \times K_r, \quad (Q[P]) \longmapsto (Q[P_1], \dots, Q[P_r])$$

un isomorphismes d'algèbres

On pose alors $\tilde{S_p} := \varphi \circ S_p \circ \varphi^{-1} : K_1 \times \dots \times K_r \longrightarrow K_1 \times \dots \times K_r$, $(x_1, \dots, x_r) \longmapsto (x_1^q, \dots, x_r^q)$

* Étape 1 : Calcul de la dimension du noyau de $\tilde{S_p} - Id$.

$(x_1, \dots, x_r) \in \ker(\tilde{S_p} - Id)$ ssi $(x_1^q, \dots, x_r^q) = (x_1, \dots, x_r)$

ssi $\forall i \in [\![1, r]\!]$, $x_i^q = x_i$

Or tout élément de $\mathbb{F}_q \subset K_i$ est racine du polynôme $X^q - X$, ainsi

$(x_1, \dots, x_r) \in \ker(\tilde{S_p} - Id)$ ssi $\forall i \in [\![1, r]\!]$, $x_i \in \mathbb{F}_q$

Ainsi $\ker(\tilde{S_p} - Id) = (\mathbb{F}_q)^r$. Or $\ker(\tilde{S_p} - Id) = \varphi(\ker(S_p - Id))$. Comme φ est un isomorphisme de $\mathbb{F}_q$-ev

on conclut que $\dim(\ker(S_p - \mathrm{Id})) = r$.

* Étape 2 : On suppose $r > 1$. Existence de $V \in \mathbb{F}_q[X]$ non congru à un polynôme constant modulo P tel que $V[\bmod P] \in \ker(S_p - \mathrm{Id})$.

L'ensemble des $U \bmod P$ où U est un polynôme congru à un polynôme constant est la droite vectorielle de $\mathbb{F}_q[X]/\langle P\rangle$ engendrée par 1. Comme $r > 1$, il existe $V \in \mathbb{F}_q[X]$ non congru à un polynôme constant tel que $V[\bmod P] \in \ker(S_p - \mathrm{Id})$.

* Étape 3 : $P = \prod_{\alpha \in \mathbb{F}_q} \mathrm{pgcd}(P, V - \alpha)$.

On a $V[\bmod P] \in \ker(S_p - \mathrm{Id})$ ssi $(V[P_1], \_, V[P_r]) \in (\mathbb{F}_q)^r$

Donc $\forall i \in [\![1, r]\!]$, on note $\alpha_i = V \bmod P_i$.

Pour $\alpha \in \mathbb{F}_q$, montrons que $\mathrm{pgcd}(P, V - \alpha) = \prod_{\{i, \alpha_i = \alpha\}} P_i$

Comme $\mathrm{pgcd}(P, V - \alpha)$ est un diviseur de P, il est de la forme $\mathrm{pgcd}(P, V - \alpha) = \prod_{i \in I_\alpha} P_i$ où $I_\alpha \subset [\![1, r]\!]$.

Comme P_i sont premier entre-eux deux à deux, le lemme de Gauss montre que

$$I_\alpha = \{ i \in [\![1, r]\!], P_i \mid V - \alpha \}.$$

Or pour $i \in [\![1, r]\!]$,

$$\alpha_i = \alpha \text{ ssi } V - \alpha = 0 \pmod{P_i} \text{ ssi } P_i \mid V - \alpha$$

Ainsi $I_\alpha = \{ i \in [\![1, r]\!], \alpha_i = \alpha \}$. D'où $\mathrm{pgcd}(P, V - \alpha) = \prod_{\{i, \alpha_i = \alpha\}} P_i$.

On obtient ainsi

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

* Étape 4 : Montrons que r diminue strictement.

Le fait que V soit non congru à un polynôme constant entraîne qu'il existe $i, j \in [\![1, r]\!]$ tel que $\alpha_i \neq \alpha_j$. Ainsi parmi les facteurs qui apparaissent, au moins deux sont non triviaux et donc ont chacun moins de r facteurs irréductibles.

Questions : Algorithme de Berlekamp.

- Pourquoi $Q(X^q) = Q^q$ dans $\mathbb{F}_q[X]$?

Comme $a^q = a \ \forall a \in \mathbb{F}_q$, on a $\sum a_i (X^q)^i = \sum a_i^q (X^i)^q = \sum (a_i X^i)^q = \left(\sum a_i X^i\right)^q$

↑ car morphisme de Frobenius.

- Tout élément de $\mathbb{F}_q \subset K_i$ est racine du polynôme $X^q - X$ donc $x_i \in \mathbb{F}_q$?

$\mathbb{F}_q \subset K_i$ et si $x \in \mathbb{F}_q^\times$ alors par le thm de lagrange $x^{q-1} = 1$ donc $x^q = x$.

Or 0 vérifie aussi cette égalité, donc on a $x^q = x \ \forall x \in \mathbb{F}_q$.

Or $X^q - X$ est de degré q et $\mathbb{F}_q$ est intègre (car corps) donc il admet au plus q racines.

Avec les éléments de $\mathbb{F}_q$, il en a exactement q, donc $x \in \mathbb{F}_q$ et $x \notin K_i$.

- $V \neq d\,[P] \Rightarrow (i,j) \in [\![1, r]\!]^2$ tel que $d_i \neq d_j$?

Sinon $\forall i \in [\![1,r]\!]$ $d_i = d \in \mathbb{F}_q$ et $\forall i \in [\![1,r]\!]$ $P_i \mid V - d$

$\Rightarrow \prod_{i=1}^{r} P_i \mid V - d$ ↑ $\Rightarrow V = d = cst\ [P]$. contradiction.

P_i sont premiers deux à deux

- exemple : factoriser $X^4 - 1$ sur $\mathbb{F}_3$

$q = 3$ $P(X) = X^4 - 1 = X^4 + 2$ donc $X^4 \equiv -2 \equiv 1 \ [\text{mod } 3]$.

- Calcul de $S_p - id$ dans $\mathcal{B} = (1, x, x^2, x^3)$

donc $(S_p - id)(1) = 1 - 1 = 0$ $(S_p - id)(X) = X^3 - X$ $(S_p - id)(X^2) = X^6 - X^2 = \underbrace{X^4}_{\equiv 1 [\text{mod } 3]} X^2 - X^2 = 0$

$(S_p - id)(X^3) = X^9 - X^3 = \underbrace{X^4 X^4}_{\equiv 1 [\text{mod } 3]} X^1 - X^3$

Ainsi $\Pi = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix} \equiv \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 2 \end{pmatrix} [\text{mod } 3]$

- Trouver $B \in \ker \Pi \Rightarrow \begin{cases} 2y + t = 0 \\ y + 2t = 0 \end{cases} \hookrightarrow y = t$ on pose $z = 1$, $x = 2$ et $y = t = 0$.

Ainsi $B = X^2 + 2$.

- Calcul du pgcd $(X^2 + 2 - \lambda, P)$:

Pour $\lambda = 0 \Rightarrow X^2 + 2 = pgcd(X^2 + 2, P)$ car $X^4 + 2 \overset{\text{par div eucl}}{=} (X^2 + 2)(X^2 + 1)$

Pour $\lambda = 1 \Rightarrow X^2 + 1 = pgcd(X^2 + 1, P)$ div eucl de P par $X^2 + 1$ $P = (X^2 + 1)(X^2 + 2)$

Pour $\lambda = 2$, $1 = \text{pgcd}(X^2, P)$ par div euclidienne

Ainsi $P = (X^2+2)(X^2+1)$.

On réitère avec X^2+1 et X^2+2. or X^2+1 est irréductible dans $\mathbb{F}_3$.

mais X^2+2 a 1 et 2 pour racine

D'où $X^4+2 = (X+1)(X+2)(X^2+1)$.