Algorithme de Cantor-Zassenhaus.

Cf Demazure Cours d'Algèbre p 234.

Comme l'algorithme de Berlekamp, Cantor-Zassenhaus a pour but parmis la décomposition en facteur irréductible (DFI) d'un polynôme sur un corps fini. Attention on se restreint ici aux polynômes sans facteurs multiple et dont tous les facteurs sont de même degré, sachant qu'on peut s'y ramener algorithmiquement d'après 96 et 97.

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 facteurs multiple et dont tous les facteurs irréductibles sont de degré r, supposé connu (Cf 97).
La DFI de P s'écrit alors $P = \prod_{i=1}^{s} P_i$ où $\forall i \in [\![1..s]\!]$ $\deg(P_i) = r$.

Ptié $\forall Q \in \mathbb{F}_q[X]$ $P = \mathrm{PGCD}(P, Q^{q^r} - Q) \times \mathrm{PGCD}(P, Q^{\frac{q^r-1}{2}} - 1) \times \mathrm{PGCD}(P, Q^{\frac{q^r-1}{2}} + 1)$

Preuve 1) MONTRER QUE $P \mid Q^{q^r} - Q$

- Puisque $X^{q^r} - X$ est le produit de tous les irréductibles de $\mathbb{F}_q$ de degré divisant r (Cf 97.1) il est en particulier divisible par P. Donc $P \mid X^{q^r} - X$
- Montrons que $X^{q^r} - X \mid Q^{q^r} - Q$. Si $Q = \sum_{i=1}^{d} a_i X^i$

$$Q^{q^r} = \Big(\sum_{i=1}^{d} a_i X^i\Big)^{q^r} \underset{\text{Frobenius } r \text{ fois prolongé aux polynômes}}{=} \sum_{i=1}^{d} (a_i X^i)^{q^r} = \sum_{i=1}^{d} \underbrace{(a_i)^{q^r}}_{= a_i \text{ car } a_i \in \mathbb{F}_q} X^{i \times q^r} = \sum_{i=1}^{d} a_i X^{i \times q^r}$$

Donc $Q^{q^r} - Q = \sum_{i=1}^{d} a_i \left((X^{q^r})^i - X^i\right)$ or $\forall i \in [\![1..d]\!]$ $X^{q^r} - X \mid (X^{q^r})^i - X^i$
donc $X^{q^r} - X \mid Q^{q^r} - Q$. (utiliser la formule $(a^n - b^n) = (a-b)\left(\sum_{i=0}^{n-1} a^i b^{n-1-i}\right)$)

- Par transitivité $P \mid Q^{q^r} - Q$

2) CONCLURE

$$\cdot\ Q^{q^r} - Q = Q(Q^{q^r-1} - 1) = Q\left((Q^{\frac{q^r-1}{2}})^2 - 1^2\right) = Q\underbrace{\left(Q^{\frac{q^r-1}{2}} + 1\right)}_{:= Q_1}\underbrace{\left(Q^{\frac{q^r-1}{2}} - 1\right)}_{:= Q_2}.$$

- $\frac{1}{2} Q_1 - \frac{1}{2} Q_2 = 1$ donc $\mathrm{PGCD}(Q_1, Q_2) = 1$.
- $-Q^{\frac{q^r-1}{2}-1} \times Q + 1 \times Q_1 = 1$ donc $\mathrm{PGCD}(Q, Q_1) = 1$
- $Q^{\frac{q^r-1}{2}-1} \times Q - 1 \times Q_2 = 1$ donc $\mathrm{PGCD}(Q, Q_2) = 1$

$\Big\}$ $\mathrm{PGCD}(P, Q \times Q_1 \times Q_2) = \mathrm{PGCD}(P, Q) \times \mathrm{PGCD}(P, Q_1) \times \mathrm{PGCD}(P, Q_2)$

Or $\mathrm{PGCD}(P, Q \times Q_2 \times Q_1) = \mathrm{PGCD}(P, Q^{q^r} - Q)$
$= P$ car $P \mid Q^{q^r} - Q$.

□

Pté Si P est non irréductible et si Q est choisi aléatoirement parmi les polynômes de $\mathbb{F}_q[X]$ de degré $\leq 2r$, la probabilité que la décomposition $P = PGCD(P,Q) \times PGCD(P,Q_1) \times PGCD(P,Q_2)$ soit triviale est inférieure à $\frac{2}{2^s}$ où $s = \frac{\deg(P)}{r}$.

Preuve Puisque P non irréductible $s \geq 2$.

Pour $(i,j) \in [\![1..q]\!]^2$ tel que $i \neq j$ on considère $\begin{cases} \mathbb{K}_i = \mathbb{F}_q(X)/(P_i) \\ \mathbb{K}_j = \mathbb{F}_q(X)/(P_j) \end{cases}$

Puisque $\deg(P_i) = \deg(P_j) = r$ on a $\#\mathbb{K}_i = \#\mathbb{K}_j = q^r$.

On pose $\varphi_{i,j} = \left(\begin{array}{ccc} \mathbb{F}_q[X]_{<2r} & \longrightarrow & \mathbb{K}_1 \times \mathbb{K}_2 \\ Q & \longmapsto & \left(\overline{Q}^{(P_1)}, \overline{Q}^{(P_2)}\right) \end{array} \right)$ où $\overline{Q}^{(P_1)}$ = classe de Q modulo (P_1), $\overline{Q}^{(P_2)}$ = ——— (P_2).

$\varphi_{i,j}$ est un morphisme d'anneau.

MQ $\varphi_{i,j}$ INJECTIVE

$\forall Q \in \mathbb{F}_q[X]_{<2r}$ $Q \in \ker \varphi_{i,j} \Leftrightarrow \varphi(Q) = (0,0) \Leftrightarrow P_1 \mid Q$ et $P_2 \mid Q$

$\Rightarrow P_1 P_2 \mid Q$ (car $P_1 \wedge P_2 = 1$)

$\Rightarrow Q = 0$ ou $\deg(Q) \geq \deg(P_1 P_2) = 2r$

$\Rightarrow Q = 0$ car $\deg(Q) < 2r$

Donc φ est injective (Et par suite bijective car $\#\mathbb{F}[X]_{<2r} = \#[\![0..q^{2r}-1]\!] = q^{2r} = q^{\hat{}2} = \#\mathbb{K}_i \times \#\mathbb{K}_j$)

Soit $Q \in \mathbb{F}_q[X]_{<2r}$ unitaire. → MQ LE PRODUIT EST TRIVIAL $\Rightarrow \overline{Q}^{(P_i)}$ et $\overline{Q}^{(P_j)}$ SONT DE Ã NATURE QUADRATIQUE

Le produit est dit trivial si l'un des termes vaut P (et alors les autres 1).

- $PGCD(Q,P) = P \Leftrightarrow P \mid Q \Rightarrow \begin{matrix} P_i \mid Q \\ P_j \mid Q \end{matrix} \Rightarrow \begin{matrix} \overline{Q}^{(P_i)} = 0 \\ \overline{Q}^{(P_j)} = 0 \end{matrix} \Rightarrow \varphi_{i,j}(Q) = 0 \Rightarrow Q = 0$ (car Q unitaire).

- $PGCD(Q_1,P) = P \Leftrightarrow P \mid Q_1 \Rightarrow \begin{matrix} P_i \mid Q_1 \\ P_j \mid Q_1 \end{matrix} \Rightarrow \begin{cases} \overline{Q^{\frac{\wedge-1}{2}}}^{(P_i)} = \overline{1}^{(P_i)} = 1_{\mathbb{K}_i} \\ \overline{Q^{\frac{\wedge-1}{2}}}^{(P_j)} = \overline{1}^{(P_j)} = 1_{\mathbb{K}_j} \end{cases}$

$\Rightarrow \begin{cases} q_i^{\frac{\wedge-1}{2}} = 1 \\ q_j^{\frac{\wedge-1}{2}} = 1 \end{cases}$ où $q_i = \overline{Q}^{(P_i)}$ et $q_j = \overline{Q}^{(P_j)}$.

$\Rightarrow q_i$ et q_j sont résidus quadratiques.

- De $\hat{m}$ $PGCD(Q_2,P) = P \Rightarrow \begin{cases} q_i^{\frac{\wedge-1}{2}} = -1 \\ q_j^{\frac{\wedge-1}{2}} = -1 \end{cases}$ $\Rightarrow q_i$ et q_j ne sont pas résidus quadratiques

RÉSUMER

On note $(q_i)_{i \in [\![1..s]\!]}$ les $\left(\overline{Q}^{(P_i)}\right)_{i \in [\![1..s]\!]}$.

Si le produit est trivial soit tous les q_i sont des résidus quadratiques, soit tous les q_i ne sont pas résidus quadratiques.

MAJORER LA PROBABILITÉ

On admet que si on choisit Q uniformément parmi les polynômes unitaires de $\mathbb{F}_q[X]$ de degré $< 2r$, les $(g_i)_{i \in [\![1..s]\!]}$ suivent chacun une loi uniforme sur $\mathbb{F}_q[X]/(P_i)^\times = \mathbb{K}_i^\times$. Or puisque $\mathbb{K}_i^{\times\square}$ est un sous groupe d'indice 2 de $\mathbb{K}_i^\times$, cela implique l'on a une chance sur deux que g_i soit dans $\mathbb{K}_i^{\times\square}$, une chance sur deux qu'il ne soit pas résidu quadratique. On en déduit (indépendance des g_i) que la probabilité que tous les g_i soient des carrés est $\frac{1}{2^s}$ et celle qu'ils soient tous non résidus quadratique est aussi $\frac{1}{2^s}$. La probabilité que le produit soit trivial est donc majorée par $\frac{1}{2^s} + \frac{1}{2^s} = \frac{2}{2^s}$.

Notant que les facteurs $\mathrm{PGCD}(P, Q)$, $\mathrm{PGCD}(P, Q_1)$ et $\mathrm{PGCD}(P, Q_2)$ sont **encore sans** facteur multiples et produit d'irréductibles de même degré r (tout ça parce qu'ils divisent P) on a l'algorithme probabiliste suivant.

Cantor-Zassenhaus (P, r, ε) où P = produit d'irréductibles 2à2 $\neq$ de même degré r, ε un paramètre fixant la précision de l'algo.

$n = \deg(P)$
s tel que $r^s = n$
k le plus petit tel que $(2^{1-s})^k \leq \varepsilon$

On choisit Q aléatoirement parmi les polynômes unitaires de $\mathbb{F}_q[X]$ de degré $< 2r$.
On calcule
$$Q_1 = Q^{q^{\frac{n}{2}}-1} - 1 \mod P$$
$$Q_2 = Q^{q^{\frac{n}{2}}-1} + 1 \mod P$$
$$A_0 = \mathrm{PGCD}(P, Q)$$
$$A_1 = \mathrm{PGCD}(P, Q_1)$$
$$A_2 = \mathrm{PGCD}(P, Q_2)$$
Si $A_1 \neq P$ et $A_2 \neq P$ on appelle récursivement l'algo sur A_0, A_1, A_2, sachant que la factorisation de P sera le produit de celles de A_0, A_1 et A_2,
Sinon on choisit un nouveau Q aléatoirement et on recommence.
Toutefois si après k étapes on n'a eu que des produits triviaux, on renvoie P considérant qu'il est irréductible, sachant que le risque que ce soit à tort est $\leq \varepsilon$.