Algorithme de Cantor-Zassenhaus

Perrine Jouteur

Ce développement se place dans les leçons 123, 141 et 142. Deux bonnes références sont *A Course in Computational Algebraic Number Theory* de Cohen, et le *Cours d'algèbre algorithmique* de Demazure.

1 Contexte et prérequis

On se place sur un corps fini de caractéristique p impaire, $\mathbb{F}_q$.

On énonce d'abord un lemme qui servira dans la suite.

Lemme 1.1 Soit $k \in \mathbb{N}^*$. Le polynôme $X^{q^k} - X$ est le produit de tous les polynômes irréductibles de degré divisant k de $\mathbb{F}_q[X]$.

On aura également besoin du théorème chinois dans les anneaux de polynômes.

Le but de l'algorithme est de factoriser un polynôme dont les facteurs irréductibles sont distincts deux à deux et d'un même degré. Regardons comment se ramener à de tels polynômes si on part d'un cas général.

Étape 1 : Éliminer les facteurs carré

On peut extraire la partie sans facteur carré d'un polynôme quelconque, en regardant d'abord les facteurs dont la multiplicité n'est pas divisible par p, puis en prenant la racine $p$ième (grâce à Frobenius), et en recommençant.

Mais en fait, on peut faire beaucoup plus simple : soit P un polynôme dans $\mathbb{F}_q[X]$. On regarde

$$\Pi = \text{pgcd}(P, P')$$

Si $\Pi = 1$, alors P est sans facteur carré donc on peut appliquer l'algo de Cantor-Zassenhaus.
Si $\Pi = P$ alors $P' = 0$ donc P est une puissance $p$ième : il existe $Q \in \mathbb{F}_q[X]$ tel que $P = Q^p$. Donc on peut regarder Q et refaire la même chose.
Si Π n'est ni 1 ni P, on a trouvé un facteur non trivial de P donc on est très content, on divise P par Π et on recommence.

Étape 2 : Regrouper les facteurs irréductibles de même degré

Cette étape est très simple, il suffit, d'après le lemme 1.1, de faire successivement le pgcd de P et de $X^{q^d} - X$, pour $d = 1, \cdots, \deg(P)$.

2 Le développement

Théorème 2.1
Soit P un polynôme dont tous les facteurs irréductibles sont distincts et de degré d fixé.
Soit T un polynôme unitaire de degré strictement inférieur à $2d$. Alors

$$P = \text{pgcd}(P, T)\,\text{pgcd}(P, T^{(q^d-1)/2} - 1)\,\text{pgcd}(P, T^{(q^d-1)/2} + 1) \qquad (*)$$

Et de plus, si P n'est pas irréductible, la probabilité que $T^{(q^d-1)/2} - 1$ soit un facteur non trivial de P est supérieure à $\frac{1}{2} - \frac{1}{2q^{2d}}$, si on tire T uniformément parmi les polynômes de $\mathbb{F}_q[X]$ de degré strictement inférieur à $2d$.

Démonstration
• Montrons d'abord l'égalité $(*)$. On a, par identité remarquable et grâce au fait que q est impair, que

$$T^{q^d} - T = T(T^{\frac{q^d-1}{2}} - 1)(T^{\frac{q^d-1}{2}} + 1)$$

Comme les trois facteurs de cette décomposition sont premiers entre eux deux à deux, on a donc $\operatorname{pgcd}(P, T^{q^d} - T) = \operatorname{pgcd}(P, T)\operatorname{pgcd}(P, T^{(q^d-1)/2} - 1)\operatorname{pgcd}(P, T^{(q^d-1)/2} + 1)$. Il reste à montrer que P divise $T^{q^d} - T$ pour avoir $(*)$.
Écrivons $P = P_1 \cdots P_r$, la décomposition en facteurs irréductibles de P. Comme chaque facteur est irréductible de degré d, les quotients $\mathbb{F}_q[X]/(P_i)$ sont isomorphes à $\mathbb{F}_{q^d}$. Notons ϕ_i un isomorphisme entre $\mathbb{F}_q[X]/(P_i)$ et $\mathbb{F}_{q^d}$. Par théorème de Lagrange, on a $\phi_i([T]_{P_i})^{q^d} = \phi([T]_{P_i})$. Ainsi $\phi_i([T^{q^d} - T]_{P_i}) = 0$, puis par injectivité, $[T^{q^d} - T]_{P_i} = 0$. Par théorème chinois, $T^{q^d} - T$ est donc nul dans $\mathbb{F}_q[X]/(P)$, et ainsi P divise $T^{q^d} - T$. L'égalité recherchée en découle.

• Minorons à présent la probabilité $\mathbb{P}$ de trouver un facteur non trivial de P par cette méthode.
Supposons que P ne soit pas irréductible. Soient π_0 et π_1 deux facteurs irréductibles de P, distincts. Considérons l'application suivante

$$\begin{array}{ccc} \mathbb{F}_q[X]_{<2d} & \longrightarrow & \mathbb{F}_q[X]/(\pi_0) \times \mathbb{F}_q[X]/(\pi_1) \\ T & \longmapsto & ([T]_{\pi_0}, [T]_{\pi_1}) \end{array}$$

Cette application est bijective. En effet, elle est injective car si T_1 et T_2 sont envoyés sur la même image, alors π_0 et π_1 divise $T_1 - T_2$, donc $\pi_0\pi_1$ divise $T_1 - T_2$ et pour des raisons de degré, nécessairement $T_1 = T_2$. La surjectivité vient du fait que les ensembles de départ et d'arrivée sont de même cardinal.
De plus, pour $i = 0, 1$, comme π_i est irréductible de degré d, le quotient $\mathbb{F}_q[X]/(\pi_i)$ est un corps isomorphe à $\mathbb{F}_{q^d}$.
Soit $T \in \mathbb{F}_q[X]$, de degré strictement inférieur à $2d$. Notons $(t_0, t_1) \in (\mathbb{F}_{q^d})^2$ l'image de T par l'application ci-dessus, et supposons que la décomposition $(*)$ soit triviale. On peut distinguer plusieurs cas.

Cas 1 : $\operatorname{pgcd}(P, T) = P$. Alors $P|T$, mais le degré de P est au moins égal à $2d$ puisque π_0 et π_1 sont des facteurs de P, donc $T = 0$ puis $(t_0, t_1) = (0, 0)$.

Cas 2 : $\operatorname{pgcd}(P, T^{(q^d-1)/2} - 1) = P$.
Alors P divise $T^{(q^d-1)/2} - 1$, et a fortiori π_0 et π_1 divisent $T^{(q^d-1)/2} - 1$, d'où, dans $\mathbb{F}_{q^d}$,

$$t_0^{(q^d-1)/2} = 1 \text{ et } t_1^{(q^d-1)/2} = 1$$

Ceci signifie que t_0 et t_1 sont des carrés dans $\mathbb{F}_{q^d}$.

Cas 3 : $\operatorname{pgcd}(P, T^{(q^d-1)/2} + 1) = P$.
Alors de même, on obtient, dans $\mathbb{F}_{q^d}$,

$$t_0^{(q^d-1)/2} = -1 \text{ et } t_1^{(q^d-1)/2} = -1$$

Ceci signifie que ni t_0 ni t_1 ne sont des carrés dans $\mathbb{F}_{q^d}$.

Conclusion : on a montré que si la décomposition $(*)$ est triviale, alors ou bien t_0 et t_1 sont tous les deux des carrés, ou bien aucun ne l'est.
En prenant la contraposée, on a que si t_0 est un carré et t_1 un non carré, ou si t_0 est un non carré et t_1 un carré, alors $(*)$ est non triviale. Il suffit donc de compter le nombre de couples (t_0, t_1) dans $\mathbb{F}_{q^d}$ tels que t_0 soit un carré et pas t_1 ou vice-versa. Comme il y a $\frac{q^d+1}{2}$ carrés dans $\mathbb{F}_{q^d}$, il y a $2 \times \frac{q^d+1}{2}\frac{q^d-1}{2}$ tels couples. Finalement,

$$\mathbb{P} \geqslant \frac{2 \times \frac{q^d+1}{2}\frac{q^d-1}{2}}{q^{2d}} = \frac{1}{2} - \frac{1}{2q^{2d}}$$

Dans le pire cas, $q = 3$ et $d = 1$, et on a quand même $\mathbb{P} \geq \frac{1}{2} - \frac{1}{18} = \frac{4}{9}$. ■

Remarque 2.1 On a travaillé ici avec q impair. Si on est en caractéristique 2, on peut faire la même chose en posant $U = X + X^2 + X^4 + \cdots X^{2^{d-1}}$, et en remarquant que pour tout polynôme T,

$$P = \operatorname{pgcd}(P, U \circ T)\operatorname{pgcd}(P, U \circ T + 1)$$