

Factorisation de polynômes sur les corps finis

Dans tout ce qui suit, \mathbb{F}_q désignera le corps fini ayant q éléments, où $q = p^\delta$ avec p un nombre premier (la caractéristique du corps) et δ un entier naturel non nul (le degré sur le corps premier). On pourra éventuellement se limiter au cas où $\delta = 1$, i.e. $q = p$ premier.

Introduction

Il existe un certain nombre d'analogies entre l'anneau \mathbb{Z} des entiers relatifs et l'anneau $\mathbb{F}_q[t]$ des polynômes en une indéterminée (notée t) sur un corps fini : par exemple, si les entiers sont écrits en base p et que les polynômes sur \mathbb{F}_p sont représentés par leur écriture comme combinaison de puissances de t , l'addition, et la multiplication « naïve », se font par le même algorithme, à ceci près que dans le cas des entiers il faut tenir compte des retenues (ou « reports ») d'un chiffre sur le suivant qui n'existent pas sur les polynômes ; mais les algorithmes de multiplication rapide, comme celui de Karatsuba ou ceux de (Schönhage et) Strassen s'appliquent aussi bien pour un cas que pour l'autre. De manière plus fondamentale, aussi bien les entiers que les polynômes admettent une *division euclidienne*, qui permet par exemple de faire des calculs dans $\mathbb{Z}/n\mathbb{Z}$ (respectivement $\mathbb{F}_q[t]/(f)$) ou d'appliquer l'*algorithme d'Euclide* pour trouver le p.g.c.d. de deux entiers (respectivement polynômes), et dans les deux cas il existe une décomposition essentiellement unique en facteurs irréductibles (nombres premiers, respectivement polynômes irréductibles (unitaires)).

On peut se demander si l'analogie couvre également les algorithmes permettant d'effectuer cette décomposition en facteurs irréductibles. Il n'en est rien : la factorisation des grands entiers semble être une tâche beaucoup plus difficile que celle des polynômes de grand degré sur les corps finis. Pour se faire une idée, disons que les records mondiaux de factorisation d'entiers « typiques » se situent en 2006 autour de 200 chiffres décimaux (650 bits), et que les meilleurs algorithmes connus (comme la méthode du crible général du corps de nombres) ont des complexités de la forme $O(\exp(C n^\alpha (\log n)^\beta))$ avec $0 < \alpha < 1$, où n est la taille du nombre à factoriser ; par comparaison,

on va voir que la factorisation de polynômes sur un corps fini peut se faire — mais de façon probabiliste — en temps essentiellement *polynomial* en son degré (ce qui revient à $\alpha = 0$ dans la complexité ci-dessus) : une machine moderne peut factoriser un polynôme de degré plusieurs milliers (sur \mathbb{F}_2 , disons) en seulement quelques secondes.

On se propose, donc, de décrire quelques approches du problème de factoriser algorithmiquement des polynômes sur un corps fini. On se placera souvent implicitement dans la situation où q est de taille très modeste.

On aura fréquemment besoin de la remarque suivante : pour calculer $\text{pgcd}(u, v)$ avec l'algorithme d'Euclide (où $u, v \in \mathbb{F}_q[t]$), il suffit de connaître v modulo u (ou réciproquement), ce qui permet par exemple de calculer $\text{pgcd}(u, v^k)$ (avec k un entier éventuellement très grand) sans avoir à calculer v^k dans $\mathbb{F}_q[t]$, puisqu'il suffit de le calculer dans $\mathbb{F}_q[t]/(u)$ en utilisant une méthode d'exponentiation rapide (typiquement par élévations au carré successives).

1 Réduction au cas sans facteur carré

Un polynôme à coefficients dans \mathbb{F}_q est dit *sans facteur carré* lorsque les exposants des facteurs dans sa décomposition en irréductibles valent tous 1 ; de façon équivalente, f est sans facteur carré lorsque les seuls polynômes g tels que g^e divise f avec $e > 1$ sont les constantes. Dans certains algorithmes de factorisation, il est utile, ou efficace, ou nécessaire, de se ramener au cas où f est sans facteur carré : ceci présente notamment l'intérêt que f est sans facteur carré si et seulement si l'anneau $\mathbb{F}_q[t]/(f)$ est un produit de corps (théorème chinois), une propriété fréquemment utile.

Contrairement à la propriété analogue pour les entiers, il est facile de tester si un polynôme $f \in \mathbb{F}_q[t]$ est sans facteur carré : en effet, on a f sans facteur carré si et seulement si $\text{pgcd}(f, f') = 1$, où f' désigne la dérivée de f . Pour en dire plus, supposons que $f = \prod_{i=1}^r h_i^{e_i}$ (mettons unitaire) où les h_i sont irréductibles (sous-entendu, unitaires) tous distincts et $e_i \geq 1$. Alors si on pose $u = \text{pgcd}(f, f')$, on montre que $u = \prod_{i=1}^r h_i^{e_i - \varepsilon_i}$ où $\varepsilon_i = 1$ sauf si p divise e_i auquel cas $\varepsilon_i = 0$; on en déduit notamment que $f/u = \prod_i h_i$ (sans facteur carré), où cette fois le produit est pris sur les i tels que p ne divise pas e_i . Pour extraire les h_i dont l'exposant est multiple de p , on peut considérer $v = u / \text{pgcd}(u, (f/u)^N)$: pour N suffisamment grand ($N = \deg f$ suffit certainement), on a $v = \prod_i h_i^{e_i}$ où le produit est pris sur les i tels que p divise e_i , autrement dit $v = w^p$ pour un certain w , qu'on peut calculer

(si $v = \sum_j a_j t^{pj}$ alors $w = \sum_j \sqrt[p]{a_j} t^j$). En appliquant, de façon récursive si besoin est, l'algorithme à w , on peut ainsi calculer $\prod_i h_i$ (la « partie sans carré » de f) même en séparant les h_i selon la plus grande puissance de p qui divise l'exposant e_i .

Certainement, factoriser $\prod_i h_i$ suffit à factoriser f (trouver les exposants ne présente pas de difficulté, même s'il existe des méthodes éventuellement plus raffinées que la division successive pour éviter des calculs inutiles). On pourra donc dans toute la suite se ramener au besoin à l'étude de polynômes sans facteur carré.

2 Test d'irréductibilité

Avant d'aborder le problème de la factorisation, on peut considérer celui, plus simple¹, de tester l'irréductibilité. Si $f \in \mathbb{F}_q[t]$ (unitaire, disons) est irréductible, de degré n , alors f divise $t^{q^n} - t$ puisque ce dernier est le produit de tous les polynômes irréductibles de degré divisant n sur \mathbb{F}_q , et est premier avec $t^{q^k} - t$ pour tout diviseur strict k de n ; et réciproquement, si f divise $t^{q^n} - t$ et $\text{pgcd}(f, t^{q^k} - t) = 1$ pour tout k divisant strictement n , alors f est irréductible (la première hypothèse impliquant que tout facteur irréductible de f est de degré divisant n et la seconde qu'il n'est pas de degré divisant $k < n$). Ceci constitue le *test d'irréductibilité de Rabin*. On peut observer qu'il suffit de considérer les k de la forme n/ℓ avec ℓ premier; par ailleurs, il existe différents raffinements permettant d'éviter des calculs inutiles dans l'évaluation des t^{q^k} modulo f (le plus basique consistant à classer les k par ordre croissant et à calculer $t^{q^{k'}}$ comme $(t^{q^k})^{q^{k'-k}}$ si $k' > k$).

S'il s'agit de *générer* des polynômes irréductibles sur \mathbb{F}_q , le mieux est encore de tirer de façon répétée un polynôme au hasard et de tester son irréductibilité jusqu'à en trouver un qui passe le test : la probabilité qu'un polynôme aléatoire de degré n sur \mathbb{F}_q soit irréductible est approximativement $\frac{1}{n}$, ce qui justifie un nombre d'essais raisonnable. Lorsqu'on cherche à tester l'irréductibilité d'un polynôme f choisi aléatoirement, on applique généralement le test de Ben-Or, qui consiste simplement à calculer $\text{pgcd}(f, t^{q^i} - t)$ pour $i = 1, \dots, \lfloor \frac{n}{2} \rfloor$ (où $n = \deg f$) et s'arrêter (f n'est pas irréductible) si jamais un p.g.c.d. n'est pas 1 : la raison est que le plus petit facteur irréductible d'un polynôme aléatoire uniforme de degré n est de degré $O(\log n)$ en moyenne, et le test de Ben-Or est plus efficace pour éliminer rapidement les polynômes ayant un petit facteur. L'intérêt de générer des polynômes irr-

¹Dans le cas des entiers, ce test aussi se fait en temps polynomial.

ductibles sur \mathbb{F}_p est de permettre de faire des calculs dans \mathbb{F}_{p^n} (vu comme $\mathbb{F}_p[t]/(f)$).

3 Décomposition en degrés distincts

Il y a peu à faire pour passer d'un test d'irréductibilité à un algorithme de factorisation en degrés distincts : ce terme signifie qu'on ne cherche pas encore à isoler tous les facteurs irréductibles du polynôme à factoriser, mais seulement à séparer les facteurs selon leur degré. L'idée est de nouveau d'utiliser le fait que $t^{q^d} - t$ est le produit de tous les polynômes irréductibles de degré divisant d . En élevant successivement t à la puissance q (en travaillant modulo f), on calcule successivement les images de $t^{q^i} - t$ dans $\mathbb{F}_q[t]/(f)$: partant de $f_1 = f$, qu'on supposera sans facteur carré, on calcule successivement $f_{i+1} = f_i / \text{pgcd}(f_i, t^{q^i} - t)$ (jusqu'à tomber sur $f_i = 1$) ; alors les $g_i = \text{pgcd}(f_i, t^{q^i} - t)$ calculés successivement sont justement les produits des facteurs irréductibles de degré i de f . Il suffira donc de les factoriser chacun séparément pour obtenir la factorisation recherchée de f . Remarquons que l'algorithme peut être interrompu dès que $\deg f_i < 2i$, car f_i n'a que des facteurs irréductibles de degré au moins i , et, puisqu'il est sans facteur carré, l'inégalité en question garantit son irréductibilité.

Naturellement, si $\deg g_i = i$, on sait d'ores et déjà que g_i est irréductible (et ce cas est le plus fréquent). Ce n'est que lorsque $\deg g_i > i$ qu'il reste encore quelque chose à factoriser.

4 L'algorithme de Cantor-Zassenhaus

D'après l'étude précédente, on est maintenant ramené au problème suivant : donné f un polynôme de degré n , sans facteur carré, dont tous les facteurs irréductibles ont degré d (un diviseur strict de n), on cherche à trouver les facteurs en question — ou au moins une décomposition non triviale de f . Notons f_1, \dots, f_r les facteurs (deux à deux distincts) recherchés, de sorte que $f = f_1 \cdots f_r$ et $n = dr$. Le théorème chinois assure que $\mathbb{F}_q[t]/(f) = \mathbb{F}_q[t]/(f_1) \times \cdots \times \mathbb{F}_q[t]/(f_r)$, où chaque $\mathbb{F}_q[t]/(f_i)$ est isomorphe à \mathbb{F}_{q^d} . Comme les f_i sont inconnus, on ne sait pas projeter un élément $a \in \mathbb{F}_q[t]/(f)$ sur chacune de ses coordonnées (a_1, \dots, a_r) dans la décomposition en question ; on sait cependant détecter si certains des a_i sont nuls : en effet, cela se produit exactement lorsque $\text{pgcd}(f, a) \neq 1$. En particulier, si on trouve un élément a de $\mathbb{F}_q[t]/(f)$, non nul (modulo f), dont au moins

une des coordonnées a_i est nulle, alors $\text{pgcd}(f, a)$ fournira un diviseur non trivial de f , ce qu'on cherche.

Supposons q impair (c'est-à-dire $p \neq 2$). L'astuce de l'algorithme de Cantor-Zassenhaus est la suivante : on va trouver un élément b de $\mathbb{F}_q[t]/(f)$ dont les coordonnées sur chaque $\mathbb{F}_q[t]/(f_i)$ dans la décomposition chinoise valent $+1$ ou -1 , et dès que toutes les composantes ne sont pas égales, l'élément en question donnera une décomposition non triviale de f (quitte à soustraire 1, certaines des coordonnées seront 0 mais pas toutes). Pour cela, on utilise le lemme suivant (dû à Euler et Legendre) :

Lemme. *Soit q une puissance d'un nombre premier impair. Alors $x^{(q-1)/2}$ vaut $+1$ ou -1 pour tout $x \in \mathbb{F}_q^\times$, il vaut $+1$ exactement lorsque x est un carré dans \mathbb{F}_q^\times , et il y a $(q-1)/2$ tels x (et donc aussi $(q-1)/2$ pour lesquels il vaut -1).*

L'algorithme consiste à prendre $a \in \mathbb{F}_q[t]/(f)$ tiré au hasard (c'est-à-dire qu'on prend $a \in \mathbb{F}_q[t]$ de degré $< n$ pour le représenter, dont chaque coefficient est tiré aléatoirement et indépendamment) et non nul (quitte à refaire le tirage). On commence par calculer $\text{pgcd}(f, a)$: s'il est différent de 1, on a trouvé un facteur non trivial de f . Sinon c'est que chaque coordonnée a_i est non nulle. On calcule alors $b = a^{(q^d-1)/2}$: d'après le lemme, chaque coordonnée b_i de b dans la décomposition chinoise vaut $+1$ ou -1 . Si b est autre que $+1$ ou -1 alors $\text{pgcd}(f, b-1)$ fournit un facteur non trivial de f , comme souhaité.

L'algorithme échoue lorsque $b = \pm 1$ (ou lorsque $a = 0$), auquel cas il faut simplement réessayer pour un nouveau tirage. Examinons quelle est cette probabilité d'échec : le lemme assure qu'il y a $\frac{q^d-1}{2}$ éléments de \mathbb{F}_{q^d} dont la puissance $(\frac{q^d-1}{2})$ -ième vaille $+1$, et autant pour -1 ; le nombre de a qui conduisent à un échec est donc $2(\frac{q^d-1}{2})^r + 1$, ce qui, comme $r \geq 2$, est moins de la moitié des q^{dr} éléments de $\mathbb{F}_q[t]/(f)$. La probabilité d'échec est donc au plus $\frac{1}{2}$, et peut être rendue arbitrairement faible en multipliant les tentatives.

Une fois obtenue une factorisation non triviale de f par l'algorithme ainsi décrit, il suffit de l'appliquer de nouveau récursivement sur chacun des facteurs, en s'arrêtant dès qu'on obtient un facteur de degré d (il est irréductible). Ceci achève de fournir un algorithme de factorisation.

Reste à expliquer ce qu'on peut faire en caractéristique $p = 2$: dans ce cas, on applique la variante suivante du lemme :

Lemme. *Soit $q = 2^\Delta$ une puissance de 2. Alors $x + x^2 + \dots + x^{2^{\Delta-1}}$ vaut 0*

ou 1 pour tout $x \in \mathbb{F}_q$, il vaut 0 exactement lorsque x est de la forme $y^2 + y$, et il y a $q/2$ tels x (et donc aussi $q/2$ pour lesquels il vaut 1).

et l'algorithme est tout à fait analogue, si ce n'est que dès le départ l'élément $b = a + a^2 + \dots + a^{2^{d\delta-1}}$ a des composantes valant 0 ou 1.

5 L'algorithme de Berlekamp

On décrit maintenant un algorithme différent, qui utilise cette fois des techniques d'algèbre linéaire.

Soit $f \in \mathbb{F}_q[t]$ un polynôme sans facteur carré de degré n , et de nouveau écrivons $f = f_1 \cdots f_r$ sa décomposition en facteurs irréductibles (mais cette fois on ne suppose plus que les f_i ont tous le même degré). On a toujours $\mathbb{F}_q[t]/(f) = \mathbb{F}_q[t]/(f_1) \times \cdots \times \mathbb{F}_q[t]/(f_r)$ par le théorème chinois, où $\mathbb{F}_q[t]/(f_i) \cong \mathbb{F}_{q^{\deg f_i}}$. On considérera surtout $\mathbb{F}_q[t]/(f)$ comme un \mathbb{F}_q -espace vectoriel, ayant pour base $1, t, \dots, t^{n-1}$. Sur cet espace vectoriel, on considère l'endomorphisme de Frobenius d'élévation à la puissance q , soit $Q: x \mapsto x^q$, et l'endomorphisme identité $I: x \mapsto x$: la différence $Q - I$ a pour noyau le sous-espace $B = \ker(Q - I)$ des x tels que $x^q = x$, et ce sous-espace se voit dans la décomposition chinoise comme l'ensemble des x dont toutes les coordonnées sont dans \mathbb{F}_q ; en particulier, on a $\dim_{\mathbb{F}_q} B = r$. Ceci fournit d'ores et déjà un critère d'irréductibilité de f (c'est-à-dire $r = 1$), le *test de Butler* : en effet, les méthodes d'algèbre linéaire (comme la méthode du pivot) permettent de trouver une base τ_1, \dots, τ_r de B (à partir de la matrice de $Q - I$, qui est calculable) et en particulier de déterminer r .

Plus généralement, une fois connue la base τ_1, \dots, τ_r de B , l'algorithme de Berlekamp consiste à tirer au hasard $c_1, \dots, c_r \in \mathbb{F}_q$ et à poser $a = c_1\tau_1 + \dots + c_r\tau_r \in B$. On procède alors essentiellement comme dans l'algorithme de Cantor-Zassenhaus décrit plus haut : si $\text{pgcd}(f, a)$ est différent de 1 (mais que a n'est pas nul...), on a obtenu une décomposition non triviale de f ; sinon (mettons que $p \neq 2$), on calcule $b = a^{(q-1)/2}$: si b ne vaut ni $+1$ ni -1 alors $\text{pgcd}(f, b - 1)$ fournit une décomposition non triviale de f , et la probabilité d'échec est majorée par $\frac{1}{2}$.

Lorsqu'on applique l'algorithme de Berlekamp, une fois connue la base τ_1, \dots, τ_r de B , elle sert pour toute la factorisation de f , il n'est pas besoin de la recalculer lorsqu'on a partiellement factorisé f . De façon générale, c'est dans ce calcul de base que réside l'essentiel de la complexité de l'algorithme, et toutes sortes d'améliorations et de raffinements existent (notamment pour ne pas avoir à écrire complètement la matrice $n \times n$ de $Q - I$).