UFR Sciences
M2 Calcul Formel

M. WEIMANN

Factorisation dans $\mathbb{F}_q[x]$

Références :

— Bostan, Chyzak, Giusti, Lebreton, Lecerf, Salvy, Schost, *Algorithmes efficaces en Calcul Formel* (2017).
— Cohen, *A Course in Computational Algebraic Number Theory*, Springer Verlag (1996).
— Lang, *Algèbre*, Dunod, Paris (2004).
— Mignotte, *Mathématiques pour le calcul formel*, PUF (1989).

Les algorithmes de factorisation présentés ici sont détaillés dans [Cohen] et [Mignotte].

1 Rappels sur les corps finis

Soit K un corps fini de cardinal q. Puisque le groupe additif K est fini, il existe un plus petit entier $p \geq 2$ tel que $p \cdot 1_K = 0_K$. Cet entier est nécessairement premier (exo). On l'appelle la *caractéristique de* K. La caractéristique divise le cardinal q du groupe K par le théorème de Lagrange. En particulier, $q \geq p$.

1.1 Unicité et représentation du corps $\mathbb{F}_p$

Si $q = p$, alors K ne contient pas de sous-corps strict d'après ce qui précède. On dit que K est un corps premier. L'application $\mathbb{Z} \to K$ définie par $n \mapsto n \cdot 1_K$ est surjective de noyau $p\mathbb{Z}$, donc induit un isomorphisme de corps

$$K \simeq \mathbb{Z}/p\mathbb{Z}.$$

Ainsi il existe un unique corps (à isomorphisme près) de cardinal premier p. On le note $\mathbb{F}_p$. Pour représenter les éléments de $\mathbb{F}_p$, il suffit donc d'utiliser les entiers entre 0 et $p-1$ et les opérations sur les entiers modulo p (c'est par exemple ce que fait Sage par défaut).

1.2 Existence et unicité du corps $\mathbb{F}_q$

Lemme 1 Soit K un corps fini de caractéristique p et cardinal q. Alors K est une extension algébrique de $\mathbb{F}_p$. En particulier, il existe $e \geq 1$ tel que $q = p^e$.

Preuve. On vérifie que le morphisme

$$\begin{array}{rcl} \mathbb{Z}/p\mathbb{Z} & \to & K \\ n \bmod p & \mapsto & n \cdot 1_K \end{array}$$

est bien défini et injectif. Son image est donc un sous-corps de K isomorphe à $\mathbb{Z}/p\mathbb{Z}$, que l'on note encore $\mathbb{F}_p$. C'est le plus petit corps inclus dans K. Ainsi, K est une extension du corps $\mathbb{F}_p$, qui est

nécessairement finie puisque K est fini, donc algébrique. A ce titre, K est un $\mathbb{F}_p$-espace vectoriel de dimension finie $e \geq 1$ et il suit que $q = p^e$. □

On fixe désormais $\overline{\mathbb{F}}_p$ une clôture algébrique de $\mathbb{F}_p$. Une telle clôture existe et est unique à isomorphisme près en vertu de théorèmes généraux de la théorie des corps.

Lemme 2 Pour tout entier $e \geq 1$, il existe un unique sous-corps de $\overline{\mathbb{F}}_p$ de cardinal $q = p^e$. Ce sous-corps est

$$\mathbb{F}_q := \left\{ x \in \overline{\mathbb{F}}_p \mid x^q - x = 0 \right\}.$$

Preuve. *Existence.* Puisque $\overline{\mathbb{F}}_p$ est de caractéristique p, on a $(x+y)^p = x^p + y^p$ du fait que si p est premier, les coefficients binomiaux $\binom{p}{j}$ pour $1 \leq j \leq p-1$ sont divisibles par p (exo). En élevant e fois à la puissance p, on en déduit $(x+y)^q = x^q + y^q$. On vérifie alors aisément que le sous-ensemble $\mathbb{F}_q$ ainsi défini est un corps. Puisque le polynôme $X^q - X$ n'a pas de racines multiples (sinon il aurait une racine en commun avec sa dérivée qui est -1), on déduit que $\mathbb{F}_q$ est de cardinal q.

Unicité. Soit $K \subset \overline{\mathbb{F}}_p$ un corps fini de cardinal q. Si $x \in K \setminus \{0\}$, alors x est inversible dans K (K est un corps), i.e. x appartient au groupe multiplicatif $K^\times$ qui a cardinal $q-1$. Il suit du théorème de Lagrange que $x^{q-1} = 1$. Ainsi, $x^q = x$ pour tout $x \in K$ et $K \subset \mathbb{F}_q$. Ces corps ayant même cardinal, ils sont égaux. □

Il existe donc un et un seul corps fini de cardinal q *à isomorphisme près*, et ce corps $\mathbb{F}_q$ est le corps de décomposition du polynôme $X^q - X = \prod_{z \in \mathbb{F}_q} (X - z)$.

1.3 Représentation modulaire des éléments de $\mathbb{F}_q$

Soit $q = p^e$. D'après le Lemme 1, $\mathbb{F}_q$ est une extension algébrique de degré e de $\mathbb{F}_p$. Il existe donc $P \in \mathbb{F}_p[X]$ irréductible de degré e (on verra plus loin comment construire des polynômes irréductibles) tel que

$$\mathbb{F}_q \simeq \mathbb{F}_p[X]/(P)$$

Ainsi, les éléments de $\mathbb{F}_q$ peuvent se représenter comme des polynômes de $\mathbb{F}_p[X]$ de degré au plus $e-1$, modulo la relation $P(X) = 0$. L'inversion dans $\mathbb{F}_q$ peut alors se calculer grâce à l'algorithme d'Euclide étendu.

Notons que si $Q \in \mathbb{F}_p[X]$ est un autre polynôme irréductible de degré e, le Lemme 2 induit un isomorphisme

$$\mathbb{F}_p[X]/(P) \simeq \mathbb{F}_p[X]/(Q)$$

puisque le terme de droite est lui aussi un corps de cardinal q. C'est une différence majeure avec les corps de nombres : deux extensions de $\mathbb{Q}$ de même degrés ne sont en général pas isomorphes en tant que corps (elles le sont seulement en tant que $\mathbb{Q}$-espaces vectoriels).

Exercice 1 Montrer que les polynômes $P = X^2 + X + 2$ et $Q = X^2 + 2X + 2$ sont irréductibles dans $\mathbb{F}_3[X]$ puis construire un isomorphisme explicite entre les corps $\mathbb{F}_3[X]/(P)$ et $\mathbb{F}_3[X]/(Q)$.

Exercice 2 Montrer que les corps $\mathbb{Q}[\sqrt{2}]$ et $\mathbb{Q}[\sqrt{3}]$ ne sont pas isomorphes.

1.4 Sous-corps d'un corps fini

Proposition 1 Soit p premier et $e, d \geq 1$. On a les équivalences

$$\mathbb{F}_{p^d} \subset \mathbb{F}_{p^e} \iff d \text{ divise } e \iff X^{p^d} - X \text{ divise } X^{p^e} - X$$

Preuve.

(1) $\Rightarrow$ (2). Si $\mathbb{F}_{p^d}$ est un sous-corps de $\mathbb{F}_{p^e}$, alors $\mathbb{F}_{p^e}$ est un $\mathbb{F}_{p^d}$-espace vectoriel de dimension finie $n \geq 1$. Ainsi, $p^e = (p^d)^n$ (pour une raison de cardinal) et d divise e.

(2) $\Rightarrow$ (3). Suppose $e = nd$ avec $n \geq 1$. On a

$$X^{p^e} = (X^{p^d})^{p^{(n-1)d}} \equiv X^{p^{(n-1)d}} \mod X^{p^d} - X \equiv \cdots \equiv X \mod X^{p^d} - X$$

d'où il suit $X^{p^e} - X \equiv 0 \mod X^{p^d} - X$, c'est à dire $X^{p^d} - X$ divise $X^{p^e} - X$.

(3) $\Rightarrow$ (1). Si $X^{p^d} - X$ divise $X^{p^e} - X$, alors toute racine de $X^{p^d} - X$ est racine de $X^{p^e} - X$, c'est à dire $\mathbb{F}_{p^d} \subset \mathbb{F}_{p^e}$ d'après le Lemme 2. □

2 Polynômes irréductibles de $\mathbb{F}_q[X]$

Proposition 2 Soit $f \in \mathbb{F}_q[X]$ irréductible de degré d. Alors f divise $X^{q^d} - X$ et $\mathbb{F}_{q^d}$ est la plus petite extension de $\mathbb{F}_q$ contenant les racines de f (i.e. $\mathbb{F}_{q^d}$ est le corps de décomposition de f).

Preuve. Un polynôme f irréductible de degré d définit une extension $\mathbb{F}_q[X]/(f)$ de degré d de $\mathbb{F}_q$, donc de cardinal q^d. Ainsi $\mathbb{F}_q[X]/(f) \simeq \mathbb{F}_{q^d}$ d'après le Lemme 2. Notons $x = X \mod f$. Alors $x \in \mathbb{F}_{q^d}$ est une racine de f. Puisque $x^{q^d} - x = 0$ (Lemme 2) et f est irréductible, il s'ensuit que f divise $X^{q^d} - X$ dans $\mathbb{F}_q[X]$. Ainsi, toutes les racines de f sont racines de $X^{q^d} - X$, i.e. appartiennent à $\mathbb{F}_{q^d}$. Donc $\mathbb{F}_{q^d}$ contient le corps de décomposition de f. Comme ce dernier est une extension de degré au moins $\deg(f) = d$ sur $\mathbb{F}_q$ (corps de rupture d'un polynôme irréductible), c'est nécessairement $\mathbb{F}_{q^d}$. □

Le théorème suivant donne une description des polynômes irréductibles de $\mathbb{F}_q[X]$. C'est un résultat clé pour la factorisation dans $\mathbb{F}_q[X]$.

Théorème 1 Pour tout $d \geq 1$, le polynôme $X^{q^d} - X \in \mathbb{F}_q[X]$ est le produit de tous les polynômes unitaires irréductibles de $\mathbb{F}_q[X]$ dont le degré divise d.

Preuve. On a vu que $X^{q^d} - X$ est sans facteurs multiples, car de dérivée -1. Il suffit donc de montrer que si $f \in \mathbb{F}_q[X]$ est unitaire irréductible de degré n, alors f divise $X^{q^d} - X$ ssi n divise d. On sait que f divise $X^{q^n} - X$ d'après la proposition 2. Donc si n divise d, alors f divise $X^{q^d} - X$ d'après la Proposition 1. Réciproquement, si f divise $X^{q^d} - X$, alors le corps de décomposition $\mathbb{F}_{q^n}$ de f est inclus dans le corps de décomposition de $X^{q^d} - X$, qui est $\mathbb{F}_{q^d}$ d'après le Lemme 2. Ainsi, $\mathbb{F}_{q^n} \subset \mathbb{F}_{q^d}$ et n divise d d'après la Proposition 1. □

2.1 Tester l'irréductibilité d'un polynôme

Corollaire 1 Un polynôme $f \in \mathbb{F}_q[X]$ de degré $d \geq 1$ est irréductible si et seulement si

1. f divise $X^{q^d} - X$ et
2. $\text{pgcd}(X^{q^{d/e}} - X, f) = 1$ pour tout diviseur premier e de d.

Preuve. Si f est irréductible de degré d, alors f divise $X^{q^d} - X$ mais est premier à $X^{q^e} - X$ pour $e < d$ en vertu du théorème 1. Réciproquement, supposons f réductible et soit g un facteur irréductible de f de degré $n < d$. Si f vérifie le point 1, alors n divise d d'après le théorème 1. Comme $n < d$, il existe donc e diviseur premier de d tel que n divise d/e, auquel cas g divise $X^{q^{d/e}} - X$ d'après la proposition 2, contredisant 2. □.

On déduit immédiatement du Corollaire 1 un test d'irréductibilité dans $\mathbb{F}_q[X]$. On peut montrer qu'il peut être implémenté de manière à coûter au plus $\tilde{O}(d^{1.5} + d \log q)$ opérations dans $\mathbb{F}_q$.

Mise en garde : il est essentiel d'utiliser un algorithme d'exponentiation rapide dans $\mathbb{F}_q[X]/(f)$ pour calculer les différentes puissances mises en jeux.

2.2 Fabriquer un polynôme irréductible

L'idée toute simple est de choisir un polynôme aléatoire unitaire de degré d dans $\mathbb{F}_p[X]$ puis de tester son irréductibilité, et ce jusqu'à obtenir un polynôme irréductible (algorithme de Ben-Or). La probabilité de tomber sur un polynôme irréductible peut s'estimer à l'aide du résultat suivant (admis) :

Théorème 2 La probabilité $P(d, q)$ qu'un polynôme unitaire de degré d dans $\mathbb{F}_q[X]$ soit irréductible satisfait les estimations

$$\frac{1}{2d} \leq P(d, q) \leq \frac{1}{d}$$

dès lors que $q^d \geq 16$. □

Remarque : On remarque que les polynômes irréductibles se raréfient quand d augmente, tout comme les nombres premiers se raréfient dans la suite des nombres entiers.

La complexité des algorithmes sous-jacents est de $\mathcal{O}(d^2 \log(q))$ opérations dans $\mathbb{F}_q$. Cette estimation est basée sur le fait que les facteurs de $X^{q^d} - X$ sont en moyenne de degré $\mathcal{O}(\log(d))$.

3 Factorisation dans $\mathbb{F}_q[X]$

Comme l'anneau $\mathbb{F}_q[X]$ est factoriel, tout polynôme univarié $f \in \mathbb{F}_q[X]$ se factorise de manière unique sous la forme

$$f = c f_1^{m_1} \cdots f_s^{m_s},$$

où $c \in \mathbb{F}_q^*$, $m_i \in \mathbb{N}^*$, et les $f_i \in \mathbb{F}_q[X]$ sont des polynômes irréductibles unitaires non constants et distincts deux à deux.

L'objectif de ce paragraphe est de développer un algorithme qui, étant donné $f \in \mathbb{F}_q[X]$, retourne la liste $[c, (f_1, m_1), \ldots, (f_s, m_s)]$. On étudiera dans un premier temps le cas réduit, ou sans facteurs multiples ($m_i = 1$), pour lequel on détaillera deux algorithmes : Berlekamp et Cantor-Zassenhaus. On traitera dans un second temps le cas général.

3.1 Complexité actuelle de la factorisation

Bien que nous ne prouverons pas ce théorème (essentiellement par faute de temps), énonçons un résultat de complexité pour la factorisation :

Théorème 3 Un polynôme de degré d dans $\mathbb{F}_q[X]$ peut être factorisé avec un nombre moyen d'opérations dans $\mathbb{F}_q$ de $\tilde{O}(d^2 + d \log q)$ si p est impair, ou $\tilde{O}(d^2 \log q)$ si $p = 2$.

L'algorithme est probabiliste, ce qui explique que l'on compte le nombre "moyen" d'opérations. Cette borne théorique correspond aussi à la complexité expérimentale de la plupart des algorithmes implémentés. Cela reste un problème ouvert actif de développer des algorithmes de factorisation déterministe de complexité polynomiale en $d, \log(q)$.

A noter qu'il existe depuis peu des algorithmes (probabilistes) de meilleures complexités asymptotiques que celle énoncée ci-dessus, mais qui ne semblent pas plus efficaces que les algorithmes usuels pour les tailles de problèmes que l'on peut traiter avec les ordinateurs actuels.

3.2 La méthode de Berlekamp

On suppose dans cette section que f est sans facteurs multiples ($m_i = 1$ pour tout i). La méthode de Berlekamp permet de ramener à un problème d'algèbre linéaire le calcul du nombre de facteurs irréductibles d'un polynôme $f \in \mathbb{F}_q[X]$ sans facteurs carrés.

3.2.1 Trouver le nombre de facteurs

L'objet central de l'algorithme de Berlekamp est l'algèbre quotient

$$R = \mathbb{F}_q[X]/(f).$$

C'est une $\mathbb{F}_q$-algèbre de rang $d := deg(f)$. Comme les f_i sont irréductibles, les algèbres quotients

$$R_i = \mathbb{F}_q[X]/(f_i)$$

sont des corps, extensions finies de $\mathbb{F}_q$ de degrés $\deg(f_i)$. Les f_i étant premiers deux à deux, le lemme des restes chinois nous assure que l'application

$$\begin{array}{rccc} r: & R & \longrightarrow & R_1 \times \cdots \times R_s \\ & g \bmod f & \longmapsto & (g \bmod f_1, \ldots, g \bmod f_s) \end{array} \tag{1}$$

est un isomorphisme d'algèbres. Nous noterons r_i les applications coordonnées, $r = (r_1, \ldots, r_s)$.

Lemme 3 L'application de Frobenius ϕ_q, définie par

$$\begin{array}{rccc} \phi_q: & R & \to & R \\ & g & \mapsto & g^q \end{array} \tag{2}$$

est $\mathbb{F}_q$-linéaire.

Preuve. Soient $c \in \mathbb{F}_q$ et $g, h \in R$. D'après le Lemme 2, on a $c^q = c$, donc $\phi_q(cg) = c\phi_q(g)$. De plus, l'algèbre R étant de caractéristique p, on a

$$(g+h)^p = g^p + h^p,$$

puisque, si p est un nombre premier, les coefficients binomiaux $\binom{p}{j}$ pour $1 \leq j \leq p-1$ sont divisibles par p (exo). Comme $q = p^e$, il s'ensuit par induction que $(g+h)^q = g^q + h^q$. □

Lemme 4 L'*algèbre de Berlekamp* $\mathcal{B} := \ker(\phi_q - Id) \subset R$ est un $\mathbb{F}_q$-espace vectoriel de dimension égale au nombre s de facteurs irréductibles de f dans $\mathbb{F}_q[X]$.

Preuve. Le morphisme $r = (r_1, \ldots, r_s)$ étant un isomorphisme d'algèbres *compatible* avec les actions des Frobenius, on a les équivalences

$$g \in \mathcal{B} \iff g^q = g \iff r(g)^q = r(g) \iff r_i(g)^q = r_i(g)\ \forall i.$$

D'après le Lemme 2, il suit que $g \in \mathcal{B}$ si et seulement si $r_i(g)$ appartient au sous-corps $\mathbb{F}_q \subset R_i$ pour tout $i = 1, \ldots, s$. En particulier, r induit un isomorphisme de $\mathbb{F}_q$-espace vectoriels $r : \mathcal{B} \simeq \mathbb{F}_q^s$. □

Nous avons donc un moyen de déterminer s en calculant la dimension du noyau de la matrice de l'endomorphisme $\phi_p - Id$. En pratique, on utilisera la base $(1, X, \ldots, X^{d-1})$ de R.

Remarque 1 La méthode de Berlekamp offre en particulier un autre test d'irréductibilité que celui déjà présenté : il suffit de calculer s et de vérifier si $s = 1$. Son coût est cependant un peu plus élevé, du fait du calcul du noyau de la matrice sous-jacente.

3.2.2 Déterminer les facteurs : approche déterministe

Voyons maintenant comment déterminer effectivement ces facteurs, si $s > 1$. D'aprés le Lemme 2, on a dans $\mathbb{F}_q[X]$ l'égalité :

$$X^q - X = \prod_{\omega \in \mathbb{F}_q} (X - \omega) \tag{3}$$

de sorte que pour tout $g \in \mathbb{F}_q[X]$ avec $\deg(g) \geq 1$ on a par composition :

$$g^q - g = \prod_{\omega \in \mathbb{F}_q} (g - \omega).$$

Les facteurs $g - \omega$ étant premiers deux à deux, on a :

$$\operatorname{pgcd}(f, g^q - g) = \prod_{\omega \in \mathbb{F}_q} \operatorname{pgcd}(f, g - \omega). \tag{4}$$

En particulier, si $\bar{g} := g \mod (f)$ appartient à $\mathcal{B}$, on a $\operatorname{pgcd}(f, g^q - g) = f$ et (4) donne une factorisation de f :

$$f = \prod_{\omega \in \mathbb{F}_q} \operatorname{pgcd}(f, g - \omega). \tag{5}$$

Le lemme suivant nous assure que cette factorisation n'est pas triviale dès lors que $\bar{g} \in R \setminus \mathbb{F}_q$ (g non constant mod f).

Lemme 5 Pour tout $\bar{g} \in \mathcal{B}$ non constant, il existe $\omega \in \mathbb{F}_q$ tel que $\mathrm{pgcd}(f, g-\omega)$ soit un facteur non trivial de f (différent de 1 et f).

Preuve. D'après (5), il existe ω tel que $\mathrm{pgcd}(f, g-\omega)$ soit un diviseur de f non constant. Comme g est non constant modulo (f), on a forcément $\mathrm{pgcd}(f, g-\omega) \neq f$, donc $\mathrm{pgcd}(f, g-\omega)$ est un facteur non trivial de f. □

Ainsi, si $s > 1$, les facteurs de f sont à rechercher parmis la liste des polynômes $\mathrm{pgcd}(f, g-\omega)$, où g parcourt une base de $\mathcal{B}$ et $\omega \in \mathbb{F}_q$. Si q est grand, on cherche en pratique une factorisation non triviale $f = f_1 f_2$ et on rappelle récursivement l'algorithme sur f_1 et f_2.

3.2.3 Déterminer les facteurs : approche probabiliste

L'approche précédente requiert de calculer $\mathrm{pgcd}(f, g-\omega)$ pour g parcourant une base de $\mathcal{B}$ et ω parcourant $\mathbb{F}_q$. La complexité est au moins linéaire en q et l'algorithme s'avère vite impraticable lorsque q est grand. Dans ce cas, il existe une autre approche probabiliste plus performante. On suppose désormais $p \neq 2$ (la caractéristique $p = 2$ se traite différemment, nous n'aborderons pas ce point ici).

Plutôt que de chercher les facteurs de f parmi les facteurs $g - \omega$ de $g^q - g$, nous allons utiliser la factorisation

$$g^q - g = g(g^{\frac{q-1}{2}} - 1)(g^{\frac{q-1}{2}} + 1),$$

valable dès lors que $p \neq 2$. On a alors $\bar{g} \in \mathcal{B}$ si et seulement si f divise $g^q - g$, si et seulement si

$$f = \mathrm{pgcd}(f, g^q - g) = \mathrm{pgcd}(f, g)\,\mathrm{pgcd}(f, g^{\frac{q-1}{2}} - 1)\,\mathrm{pgcd}(f, g^{\frac{q-1}{2}} + 1). \tag{6}$$

La proposition 3 suivante montre que cette factorisation est non triviale avec une grande probabilité dès lors que $s \geq 2$. On a d'abord besoin d'un résultat auxiliaire.

Lemme 6 Soit $p \neq 2$ un nombre premier. Les deux sous-ensembles

$$S_+ := \{z \in \mathbb{F}_q^\times, \quad z^{\frac{q-1}{2}} - 1 = 0\} \quad \text{et} \quad S_- := \{z \in \mathbb{F}_q^\times, \quad z^{\frac{q-1}{2}} + 1 = 0\}$$

sont de même cardinal $(q-1)/2$ et réalisent une partition de $\mathbb{F}_q^\times$.

Preuve. D'après le Lemme 2, et puisque q est impair, on a

$$0 = z^{q-1} - 1 = (z^{\frac{q-1}{2}} - 1)(z^{\frac{q-1}{2}} + 1) \quad \forall\, z \in \mathbb{F}_q^\times,$$

d'où il découle une partition $\mathbb{F}_q^\times = S_+ \cup S_-$. Comme S_+ et S_- sont chacun de cardinal au plus $(q-1)/2$ et $\mathbb{F}_q^\times$ est de cardinal $q-1$, on obtient le résultat. □

Proposition 3 Soit $(g_1, \ldots, g_s)$ une base de $\mathcal{B}$ (les g_i vus comme des polynômes de $\mathbb{F}_q[X]$ de degrés $< n$) et soit g une combinaison linéaire des g_i à coefficients aléatoires dans $\mathbb{F}_q$. Alors, la probabilité que la factorisation (6) soit triviale est $\leq 1/2^{(s-1)}$.

Preuve. On a $g \in \mathcal{B}$ si et seulement si $g \mod (f_i) \in \mathbb{F}_q \subset \mathbb{F}_q[X]/(f_i)$ pour tout i. Ainsi, si g est combinaison $\mathbb{F}_q$-linéaire aléatoire des g_i, alors $z_i := g \mod (f_i) \in \mathbb{F}_q$ prend chaque valeur de $\mathbb{F}_q$ avec équiprobabilité $1/q$, et ce pour $i = 1, \ldots, s$.

• S'il existe i tel que $z_i = 0$, alors f_i divise g et $\text{pgcd}(f, g) \neq 1$. Comme $\deg(g) < \deg(f)$, on a aussi $\text{pgcd}(f, g) \neq f$. La factorisation (6) est alors non triviale, c'est gagné.

• Si $z_i \neq 0$ pour tout i, alors aucun f_i ne divise g et $\text{pgcd}(f, g) = 1$. Dans ce cas, la factorisation (6) est triviale si et seulement si f divise $g^{(p-1)/2} - 1$ ou f divise $g^{(p+1)/2} - 1$, i.e. si et seulement si $z_i^{(p-1)/2} - 1 = 0$ pour tout i ou bien $z_i^{(p+1)/2} + 1 = 0$ pour tout i. Chacun de ces deux évènements apparaît avec probabilité $1/2^s$ d'après le Lemme 6. Donc la probabilité que la factorisation (6) soit triviale est $\leq 1/2^{(s-1)}$. □

Si (6) donne une factorisation non triviale, on rappelle récursivement l'algorithme sur les facteurs trouvés. Sinon, on recommence avec un autre choix de g. La probabilité de n'obtenir que des facteurs triviaux après k itérations vaut

$$1/2^{k(s-1)} \leq 1/2^k,$$

et la probabilité de trouver une factorisation non triviale de f tend vers 1 lorsque k tend vers l'infini. En pratique, 1 ou 2 itérations suffisent, et l'approche probabiliste aura une meilleure complexité en moyenne que l'approche déterministe (cf TP).

3.2.4 Application à la recherche de racines

L'algorithme précédent admet comme application immédiate la recherche des racines rationnelles (c'est à dire dans $\mathbb{F}_q$) d'un polynôme $f \in \mathbb{F}_q[X]$ sans facteurs multiples. En effet, ces racines sont en bijection avec les facteurs irréductibles de degrés 1 de f. Il suffit donc de factoriser f sur $\mathbb{F}_q[X]$ et de chercher les facteurs de degrés 1. Cependant, il n'est pas satisfaisant d'un point de vue complexité de factoriser complètement un polynôme si l'on ne recherche que les facteurs d'un degré donné. Le Lemme 2 permet de résoudre simplement ce problème. En effet, on sait que le polynôme $X^q - X$ est le produit de tous les polynômes (unitaires) de degrés 1 de $\mathbb{F}_q[X]$:

$$X^q - X = \prod_{\omega \in \mathbb{F}_q} (X - \omega). \tag{7}$$

Ainsi,

$$h := \text{pgcd}(X^q - X, f)$$

est égal au produit de tous les facteurs de degré 1 de f, et il suffit d'appliquer l'algorithme de Berlekamp sur h pour trouver les facteurs de degrés 1 (donc les racines) de f.

3.3 La méthode de Cantor-Zassenhaus

Nous avons vu la méthode de Berlekamp, essentiellement basée sur l'algèbre linéaire. On va maintenant voir une autre méthode connue et fréquemment utilisée, la méthode de Cantor-Zassenhaus. C'est une généralisation de la recherche de racines : elle consiste dans un premier temps à regrouper les facteurs de même degrés (*distinct degree factorization*) puis à casser ces groupes de facteurs selon une méthode probabiliste similaire à celle développée ci-dessus.

3.3.1 Factorisation en degrés distincts

Soit $f \in \mathbb{F}_q[X]$ unitaire de degré d. On définit une suite de polynômes $h_1, \ldots, h_d$ de la manière suivante.

- On définit $h_1 := \text{pgcd}(X^q - X, f)$.
- On définit $h_{i+1} := \text{pgcd}(X^{q^{i+1}} - X, f/h_1 \cdots h_i)$.

On obtient ainsi une factorisation $f = h_1 \cdots h_d$ (avec possiblement $h_i = 1$). Il découle du Théorème 1 que chaque h_i est le produit de tous les facteurs irréductibles de f degrés i. On appelle cette factorisation *la factorisation de f en degrés distincts*.

Attention, penser une fois de plus à l'exponentiation rapide modulo f pour calculer les pgcd successifs.

3.3.2 Cantor-Zassenhaus

Puisque l'on peut facilement écrire un polynôme sans facteurs carrés comme produit de facteurs irréductibles de même degré, il nous suffit maintenant de savoir factoriser de tels polynômes. L'approche est similaire à celle développée pour Berlekamp probabiliste.

Soit donc un polynôme $f \in \mathbb{F}_q[X]$ sans facteur carré, produit de facteurs irréductibles de degré exactement r. D'après le Théorème 1, on sait que f divise $X^{q^r} - X$. D'autre part, on a le lemme suivant

Lemme 7 Pour tout $g \in \mathbb{F}_q[X]$, $X^{q^r} - X$ divise $g^{q^r} - g$.

Preuve. Soit $g = \sum a_i X^i \in \mathbb{F}_q[X]$. On déduit en itérant r fois le Lemme 3 que $g(X)^{q^r} = g(X^{q^r})$ d'où il suit que

$$g(X)^{q^r} - g(X) = g(X^{q^r}) - g(X) = \sum a_i (X^{iq^r} - X^i).$$

Or $X^{iq^r} = (X^{q^r})^i \equiv X^i \mod X^{q^r} - X$. Il suit que $X^{q^r} - X$ divise chaque terme $X^{iq^r} - X^i$ et le résultat souhaité en découle. □

On écrit maintenant

$$g^{q^r} - g = g(g^{(q^r-1)/2} - 1)(g^{(q^r-1)/2} + 1)$$

Ces trois facteurs étant premiers entre eux, et comme f divise $g^{q^r} - g$, on obtient la d écomposition de f suivante :

$$f = \text{pgcd}(f, g)\,\text{pgcd}(f, g^{(q^r-1)/2} - 1)\,\text{pgcd}(f, g^{(q^r-1)/2} + 1) \tag{8}$$

L'algorithme de Cantor-Zassenhaus consiste à tirer au sort un polynôme g de degré $2r$ et de vérifier si la décomposition précédente est non triviale. On a lemme suivant

Lemme 8 Soit $f \in \mathbb{F}_q[X]$ sans facteurs carrés produit d'au moins 2 facteurs irréductibles de même degrés r. Alors la probabilité que la factorisation (8) induite par $g \in \mathbb{F}_q[X]$ de degré $2r$ soit non triviale est d'au moins $1/2$.

Preuve. La preuve est dans le même esprit que la situation décrite pour Berlekamp probabiliste.

Le principe de l'algorithme est donc simple : choisir g aléatoire jusqu'à ce que (8) donne une factorisation non trivial de f. Attention, penser à utiliser un algorithme d'exponentiation rapide dans $\mathbb{F}_q[X]/(f)$ pour calculer $g^{p^r-1} \mod f$ lors des calculs de pgcd.

4 Le cas avec facteurs multiples

On suppose ici $f \in \mathbb{F}_p[X]$ pour simplifier, où p est un nombre premier. Si un polynôme $f \in \mathbb{F}_p[X]$ a des facteurs multiples, alors le résultant de f et de sa dérivée s'annule :

$$Res(f, f') = 0.$$

En effet, si g^2 divise f, alors g divise f' : les facteurs multiples sont des facteurs communs à f et f' et sont donc à rechercher parmis les facteurs de $\text{pgcd}(f, f')$. La dérivée de f va donc jouer un rôle central ici. Contrairement aux corps de caractéristique nulle, une difficulté s'ajoute : un polynôme peut être de dérivée nulle sans être constant (par exemple $f(X) = X^2$ dans $\mathbb{F}_2[X]$). Ces polynômes sont caractérisés par le lemme suivant.

Lemme 9 Soit $f \in \mathbb{F}_p[X]$ un polynôme unitaire non constant. On a $f' = 0$ si et seulement s'il existe $q \in \{p, p^2, p^3, \ldots\}$ et $g \in \mathbb{F}_p[X]$ tels que $f = g^q$ et $g' \neq 0$.

Preuve. Si $f = g^q$, alors il est clair que $f' = qg'g^{q-1} = 0$ puisque p divise q. Supposons maintenant $f' = 0$. Ecrivons $f = \sum_{i=0}^{n} c_i X^i$. Alors $f' = \sum_{i=0}^{n} ic_i X^i$ et $f' = 0$ implique $ic_i = 0$ pour $i = 0, \ldots, n$. Ainsi $c_i = 0$ pour tout i non nul modulo p et

$$f(X) = c_0 + c_p X^p + \cdots + c_{kp} X^{kp} = (c_0 + c_p X + \cdots + c_{kp} X^k)^p.$$

La deuxième égalité est basée sur la linéarité du Frobenius : $(cg + dh)^p = cg^p + dh^p$ pour tout h, g dans $\mathbb{F}_p[X]$ et tout c, d dans $\mathbb{F}_p$. Ainsi $f = g_0^p$ pour un certain $g_0 \in \mathbb{F}_p[X]$ non constant. Si $g_0' = 0$, on a par le même raisonnement $g_0 = g_1^p$ et $f = g_1^{p^2}$. Si $g_1' = 0$, on continue...Ce processus s'arrête et $f = g^q$ pour un $q \in \{p, p^2, p^3, \ldots\}$ inférieur ou égal à $\deg(f)$. On a $g' \neq 0$ car q est maximal et g est non constant. □

Corollaire 2 Soit $f \in \mathbb{F}_p[X]$ un polynôme unitaire non constant. Alors f a un facteur multiple si et seulement si $Res(f, f') = 0$.

Preuve. On a vu que si g^2 divise f alors $Res(f, f') = 0$. Supposons maintenant que $Res(f, f') = 0$. Il existe donc un facteur commun irrédutible non constant $g \in \mathbb{F}_p[X]$ à f et f'. Supposons que g aie multiplicité 1 dans f. On a alors $f = gh$ avec $\text{pgcd}(h, g) = 1$. On a $f' = g'h + h'g$. Comme par hypothèse g divise f et f', il suit que g divise $g'h$. Comme g et h sont supposés premiers entre eux, il suit que g divise g'. Comme $\deg(g') < \deg(g)$, on a forcément $g' = 0$, contredisant l'hypothèse g non constant irréductible par le lemme précédent. Donc g est un facteur multiple de f. □

Remarque Le lemme et son corollaire ne sont pas vrais sur n'importe quel corps de caractéristique p : on a toujours $f' = 0$ implique $f(X) = g(X^q)$, mais l'égalité $g(X^q) = g(X)^q$ n'est pas toujours

satisfaite. Considérer par exemple $f(X) := X^p - t \in \mathbb{F}_p(t)[X]$. Ce polynôme non constant satisfait $f' = 0$ (et $\mathrm{pgcd}(f, f') = 0$), mais on peut montrer que f est malgré cela irréductible sur le corps $\mathbb{F}_p(t)$. La différence réside dans le fait que le corps des coefficients $\mathbb{F}_p(t)$ n'est pas fixé par le Frobenius $f \to f^p$.

Les facteurs irréductibles de f apparaissant avec une multiplicité divisible par p sont donc à isoler des autres facteurs de f. On s'intéresse donc à factoriser f sous la forme

$$f = a \times b$$

avec $a = g^q$ pour q une puissance de p, b sans facteur irréductible de multiplicité divisible de p, et a et b premiers entre eux. Comment obtenir une telle factorisation ?

Etape 1. *On cherche b.* Ecrivons

$$b = b_1^{n_1} \times \cdots \times b_k^{n_k}$$

la décomposition irréductible de b. On a

$$b' = h \prod_{i=1}^{k} b_i^{n_i - 1}, \quad \text{avec} \quad h = \sum_{i=1}^{k} n_i b_i' \prod_{j \neq i} b_j.$$

Par hypothèse, b_i est premier avec b_j pour $j \neq i$. De plus, b_i étant irréductible il est premier avec b_i' (sinon, on aurait $b_i' = 0$ contredisant l'irréductibilité de b_i par le lemme précédant). Comme n_i est inversible modulo p par hypothèse, il en découle que

$$\mathrm{pgcd}(b_i, h) = \mathrm{pgcd}(b_i, n_i b_i' \prod_{j \neq i} b_j) = 1.$$

Il s'ensuit que $\mathrm{pgcd}(b, b') = \prod_{i=1}^{r} b_i^{n_i - 1}$ et

$$bb := \frac{b}{\mathrm{pgcd}(b, b')} = b_1 \times \cdots \times b_k$$

représente la partie sans facteurs carrés de b, que l'on peut factoriser par exemple avec l'algorithme de Berlekamp. Pour trouver bb à partir de f, il suffit de remarquer que $a' = 0$ entraine $f' = ab'$ et

$$\mathrm{pgcd}(f, f') = \mathrm{pgcd}(ab, ab') = a \,\mathrm{pgcd}(b, b').$$

Ainsi, bb s'obtient à partir de f comme

$$bb = \frac{b}{\mathrm{pgcd}(b, b')} = \frac{f}{\mathrm{pgcd}(f, f')}.$$

Finalement, la multiplicité n_i de b_i se calcule aisément, par exemple comme le plus petit entier m tel que b_i^m divise f. Ceci nous donne le facteur b de f et sa factorisation irréductible.

Etape 2. *On traite a.* Une fois b connu, le facteur a s'obtient simplement comme le quotient de f par b. Si a est constant, c'est fini et on retourne la factorisation de b. Sinon, il existe d'après le Lemme 3 un unique $g \in \mathbb{F}_p[X]$ et un unique $q \in \{p, p^2, p^3, \ldots\}$ tels que $a = g^q$ et $g' \neq 0$. Il est facile de déterminer g et q (exercices). On appelle alors récursivement l'algorithme de factorisation sur g. On en déduit la factorisation irréductible de g, dont on déduit la factorisation irréductible de a (il suffit de multiplier les multiplicités des facteurs de g par q). Finalement, on déduit des factorisations de a et de b la factorisation de f.

5 L'algorithme complet de factorisation dans $\mathbb{F}_p[X]$

En combinant toutes les procédures décrites précédamment, on obtient finalement un algorithme complet de factorisation sur $\mathbb{F}_p[X]$. On suppose donnée une procédure **Facto(f,p)** (type Berlekamp ou Cantor-Zassenhaus) qui prend en entrée un premier p et un polynôme $F \in \mathbb{Z}[X]$ sans facteurs carrés et qui retourne la liste $[f_1, \ldots, f_r]$ des facteurs irréductibles de F modulo (p).

FactoModp(F,p) :

Entrée : $F \in \mathbb{Z}[X]$ et $p \in \mathbb{N}$ premier.

Sortie : $L = [c, (f_1, m_1), \ldots, (f_s, m_s)]$, avec c coefficient dominant de $f \mod (p)$, les $f_i \in \mathbb{F}_p[X]$ facteurs moniques irréductibles non constants de $f := F \mod (p)$ et m_i leurs multiplicités.

$f := F \mod (p)$.

Si f est constant :

retourner $L := [f]$.

Sinon :

$c :=$ coefficient dominant de f

$f := f/c$.

Si $Res(f, f') \neq 0$:

Calculer $[f_1, \ldots, f_r] =$ **Facto(f,p)**

Retourner $L := [c, (f_1, 1), \ldots, (f_r, 1)]$

Sinon :

Calculer $bb := f/\operatorname{pgcd}(f, f')$.

Si $\deg(bb) = 0$:

Poser $L_b := \{\emptyset\}$

Sinon :

Calculer $[b_1, b_2, \ldots] :=$ **Facto (bb,p)**

Calculer les multiplicités b_i des facteurs b_i de f.

En déduire b et $L_b := [c, (b_1, n_1), (b_2, n_2), \ldots]$

Calculer $a :=$quotient(f, b).

Si $\deg(a) = 0$:

Retourner $L := L_b$

Sinon :

Calculer (g, q) tel que $a = g^q$, avec $g' \neq 0$

Calculer $[(g_1, e_1), (g_2, e_2), \ldots] =$ **FactoModp(g,p)** (algorithme récursif)

Calculer $L_a := [(g_1, qe_1), (g_2, qe_2), \ldots]$

Retourner $L := L_a + L_b$ où $+$ désigne la concaténation.

Théorème 4 L'algorithme **Factorisation** termine et retourne la factorisation irréductible de f.

Preuve. A chaque appel récursif de la fonction **Factorisation**, le degré du polynôme g décroît strictement. Donc l'algorithme termine. Il retourne la factorisation irréductible de f d'après les résultats préalablement prouvés. □