Factorisation de polynômes

Salim Rostam
Complément d'algèbre pour l'agrégation, ENS Rennes

Avant-propos : la factorisation de polynômes n'est pas au programme, mais est dans la frontière immédiate.

Références classiques :
— BMP, *Objectif Agrégation* [BMP] ;
— Demazure, *Cours d'algèbre* [Dem].
Références plus spécifiques :
— Cohen, *A course in Computational algebraic number theory* [Coh] ;
— von zur Gathen–Gerhard, *Modern Computer Algebra* [GaGe].

Soit K un corps. L'anneau $K[X]$ est euclidien donc factoriel, en particulier tout polynôme $P \in K[X]$ non nul s'écrit de façon unique

$$P = uP_1^{\alpha_1} \cdots P_r^{\alpha_r},$$

avec $P_i \in K[X]$ non constant unitaire, $\alpha_i \geq 1$ et $u \in K^*$. L'objectif est de déterminer cette décomposition.

On peut déterminer si un polynôme est irréductible par exemple pour déterminer le degré d'une extension de corps, et par exemple chercher des factorisations est utile dans certains algorithmes de logarithme discret (important pour les cryptosystèmes asymétriques, par exemple RSA, ou les codes correcteurs).

1 Recherche de racines

Sur $\mathbb{F}_q$, une méthode naïve de recherche de racines est simplement d'essayer tous les éléments... ! Une méthode beaucoup moins naïve pour trouver les racines de $P \in \mathbb{F}_q[X]$ est de factoriser $\operatorname{pgcd}(P, X^q - X)$ (cf. Proposition 3.5). On est par exemple dans le cas d'application de l'algorithme de Cantor–Zassenhaus (cf. Section 6), et on aura une complexité moyenne en $O(n \log q)$ (en omettant les facteurs en $\log n$, cf. [GaGe, Corollary 14.16]), donc plus petite que le $O(nq)$ de la méthode naïve (avec $n = \deg P$). On peut appliquer cette méthode pour la recherche de racines entières de polynômes de $\mathbb{Z}[X]$ en regardant modulo un bon nombre premier, cf. [GaGe, Theorem 14.18]. On dispose également de la méthode plus élémentaire suivante.

Proposition 1.1. *Soit $P = \sum_{i=0}^n p_i X^i \in \mathbb{Z}[X]$. Si $\frac{a}{b} \in \mathbb{Q}$ (écriture irréductible) est racine de P alors $b \mid p_n$ et $a \mid p_0$. En particulier, si P est unitaire alors toute racine rationnelle de P est entière.*

Démonstration. On a $\sum_{i=0}^n p_i \frac{a^i}{b^i} = 0$ donc $\sum_{i=0}^n p_i a^i b^{n-i} = 0$ donc $p_0 b^n + \sum_{i=1}^{n-1} p_i a^i b^{n-i} + p_n a^n = 0$. Ainsi $a \mid p_0 b^n$ donc $a \mid p_0$ et $b \mid p_n a^n$ donc $b \mid p_n$. □

Le résultat précédent peut être judicieusement appliqué à la recherche de valeurs propres « évidentes ».

2 Critères d'irréductibilité

Pour cette section, on se réfère au Perrin.

Proposition 2.1 (Critère d'Eisenstein)**.** *Soit A un anneau factoriel. Soit $P = a_nX^n + \cdots + a_0 \in A[X]$. On suppose qu'il existe $p \in A$ irréductible tel que :*

(i) $p \nmid a_n$ *;*

(ii) $p \mid a_i$ *pour tout* $i \in \{0, \ldots, n-1\}$ *;*

(iii) $p^2 \nmid a_0$.

Alors P est irréductible dans $\mathrm{Frac}(A)[X]$*. (De plus, le polynôme P est irréductible dans $A[X]$ si et seulement si on a également* $\mathrm{pgcd}(a_i)_i = 1$*.)*

Démonstration. Cf. Perrin ; on utilise le fait que $\mathrm{Frac}(A/(p))[X]$ est factoriel □

Applications 2.2. 1. Le polynôme $X^{p-1} + \cdots + X + 1$ est irréductible sur $\mathbb{Z}$ si p est premier.

2. Le polynôme $X^n - a$ est irréductible sur $\mathbb{Z}$ si a possède un facteur premier de multiplicité 1.

Proposition 2.3. *Soit A un anneau factoriel et soit I un idéal premier de A. Soit $P = a_nX^n + \cdots + a_0 \in A[X]$ tel que sa réduction modulo I :*

(i) soit de degré n (i.e. $a_n \notin I$) ;

(ii) soit irréductible sur $\mathrm{Frac}(A/I)$.

Alors P est irréductible sur $\mathrm{Frac}(A)$ *(et de plus irréductible sur A si ...(comme avant)).*

Applications 2.4. 1. Le polynôme $X^3 + 2022X^2 - 293X + 2021$ est irréductible sur $\mathbb{Z}$, puisque modulo 2 il donne $X^3 + X + 1 \in \mathbb{F}_2[X]$ qui est irréductible (car de degré $\in \{2, 3\}$ sans racine).

2. Le polynôme $X^2 + Y^2 + 1 \in \mathbb{R}[X, Y]$ est irréductible, puisque dans $\mathbb{R}[X, Y]/(Y) \simeq \mathbb{R}[X]$ il donne $X^2 + 1$ qui est irréductible (même raison).

Remarque 2.5. Attention, cette méthode de réduction ne fonctionne pas toujours (*i.e.* elle n'est pas une condition nécessaire). Par exemple, le polynôme $\Phi_8 = X^4 + 1$ est irréductible sur $\mathbb{Z}$ mais réductible sur $\mathbb{F}_p$ pour tout p premier (cf. Perrin, Proposition 3.11).

3 Tests d'irréductibilité

Proposition 3.1. *Soit k un corps et soit $P \in k[X]$ de degré 2 ou 3. Alors P est irréductible sur k si et seulement si P n'admet pas de racine sur k.*

Remarque 3.2. L'énoncé devient faux dès le degré 4, comme le montre le polynôme $X^4 + 1 = X^4 + 2X^2 + 1 - 2X^2 = (X^2 + 1)^2 - (\sqrt{2}X)^2 = (X^2 + \sqrt{2}X + 1)(X^2 - \sqrt{2}X + 1) \in \mathbb{R}[X]$.

Le critère précédent se généralise de la façon suivante.

Proposition 3.3. *Soit k un corps et soit $P \in k[X]$ de degré $d \geq 2$. Le polynôme P est irréductible si et seulement pour toute extension de corps K/k de degré $\leq \frac{d}{2}$, le polynôme P n'admet pas de racine dans K.*

Démonstration. (Perrin.) Si P est irréductible et si $x \in K$ est une racine où K est une extension de k alors $K = k(x) \simeq k[X]/(P)$ est un corps de rupture, de degré $d > \frac{d}{2}$.

Réciproquement, si P est réductible alors on peut écrire $P = QR$ avec $Q, R \in k[X]$ vérifiant $\deg Q, \deg R > 0$ et $\deg Q + \deg R = d$. Ainsi, on peut supposer $\deg Q \leq \frac{d}{2}$ et donc P possède une racine dans $k[X]/(Q)$ qui est de degré $\deg Q \leq \frac{d}{2}$ sur k. □

Applications 3.4.
— Le polynôme $X^4 + X + 1$ est irréductible sur $\mathbb{F}_2$. Il suffit de vérifier qu'il n'admet pas de racine dans $\mathbb{F}_4$. Sur $\mathbb{F}_2$ c'est clair puisque $x^4 = x$, et sur $\mathbb{F}_4 \simeq \mathbb{F}_2(j)$ avec $j^2 + j + 1 = 0$ alors $x \in \mathbb{F}_4 \setminus \mathbb{F}_2$ vérifie $x \in \{j, j + 1 = -j^2\}$ donc $x^3 = 1$ donc $x^4 = j$ donc $x^4 + x + 1 = 2j + 1 = 1 \neq 0$.
— En utilisant un critère précédent, on en déduit que $3X^4 + 2022X^2 + 21X + 17$ est irréductible sur $\mathbb{Z}$ (réduire modulo 2).

On se place maintenant sur un corps fini $\mathbb{F}_q$. On rappelle le résultat classique suivant (cf. tout cours sur les corps finis).

Proposition 3.5. *On a $X^{q^n} - X = \prod_{d|n} \prod_{P \in I(q,d)} P$ où $I(q, d)$ est l'ensemble des polynômes irréductibles unitaires de degré d de $\mathbb{F}_q[X]$.*

Démonstration. Le polynôme $X^{q^n} - X$ est sans facteur carré. Si P est un facteur irréductible de degré d alors les racines de P dans un corps de rupture de P vérifient $x^{q^n} - x = 0$ donc sont dans $\mathbb{F}_{q^n}$, qui est donc une extension de $\mathbb{F}_{q^d}$ donc $d \mid n$. Réciproquement, si $d \mid n$ et si $P \in I(q, d)$ alors $\mathbb{F}_p[X]/(P) \simeq \mathbb{F}_{q^d}$ est un sous-corps de $\mathbb{F}_{q^n}$ donc l'image x de X vérifie $x^{q^n} - x = 0$ donc $X^{q^n} - X \in \mathbb{F}_q[X]$ est nul modulo P donc P le divise. □

Corollaire 3.6. *Soit $P \in \mathbb{F}_q[X]$ de degré $d \geq 2$. Le polynôme P est irréductible si et seulement si :*

i) $P \mid X^{q^d} - X$;

ii) $\operatorname{pgcd}(P, X^{q^{d/\ell}} - X) = 1$ *pour tout diviseur premier strict ℓ de d.*

4 Suppression des facteurs carrés

([GaGe, Exercise 14.27].) Soit k un corps et $P \in k[X]$ que l'on désire décomposer en produits d'irréductibles. Si $P = \prod_i P_i^{\alpha_i}$, il suffit de décomposer $\tilde{P} = \prod_i P_i$ en produit d'irréductibles (pour trouver les multiplicités on fera des divisions euclidiennes). Si k est de caractéristique 0 alors :

$$\tilde{P} = \frac{P}{\operatorname{pgcd}(P, P')}$$

En effet, $\operatorname{pgcd}(P, P')$ est de la forme $\prod_i P_i^{\beta_i}$ avec $\beta_i \leq \alpha_i$, et en dérivant on trouve que $P_i^{\alpha_i - 1} \mid P'$ et $P_i^{\alpha_i} \nmid P'$.

Si k est de caractéristique p positive, la situation est différente si p divise α_i (en particulier, cette situation n'arrive pas si $p > \deg P$) puisqu'alors $P_i^{\alpha_i}$ divise P' si $p \mid \alpha_i$. Plus précisément, on a dans ce cas :

$$\operatorname{pgcd}(P, P') = \prod_{p|\alpha_i} P_i^{\alpha_i} \prod_{p \nmid \alpha_i} P_i^{\alpha_i - 1},$$

et

$$\Pi := \frac{P}{\operatorname{pgcd}(P, P')} = \prod_{p \nmid \alpha_i} P_i.$$

Si $n := \deg P$, on a alors

$$\operatorname{pgcd}(P, \Pi^n) = \prod_{p \nmid \alpha_i} P_i^{\alpha_i},$$

et

$$Q \coloneqq \frac{P}{\operatorname{pgcd}(P, \Pi^n)} = \prod_{p|\alpha_i} P_i^{\alpha_i}.$$

Ainsi, il existe $R \in \mathbb{F}_q[X]$ tel que $Q = R^p$ (que l'on trouve via les coefficients de Q), on a $R = \prod_{p|\alpha_i} P_i^{\alpha_i/p}$ et on récure. (Voir aussi [Coh, 3.4.2] pour un autre algorithme.)

En réalité, on verra dans la suite que, bien que les deux algorithmes que l'on présente nécessitent des polynômes sans facteur carré, il ne sera pas nécessaire de déterminer le polynôme $\tilde{P}$.

5 Factorisation déterministe sur $\mathbb{F}_q$: algorithme de Berlekamp

([BMP, §5.3.2].) On va dans cette section et la suivante présenter deux algorithmes de factorisation sur $\mathbb{F}_q[X]$ avec $q = p^s$ et p premier :

— l'algorithme de Berlekamp, qui s'applique à des polynômes sans facteurs carrés ;
— l'algorithme, probabiliste, de Cantor–Zassenhaus, qui s'applique également à des polynômes sans facteurs carrés mais dont les facteurs irréductibles sont cette fois tous de même degrés.

Donnons un résultat préliminaire.

Lemme 5.1. *Soit $P \in \mathbb{F}_q[X]$. On a $P' = 0$ si et seulement s'il existe $Q \in \mathbb{F}_q[X]$ tel que $P = Q^p$. Dans ce cas, on peut déterminer Q de façon simple à partir de P.*

Démonstration. Si $P = Q^p$ alors $P' = pQ'Q^{p-1} = 0 \in \mathbb{F}_q[X]$. Réciproquement, si $P' = 0$ alors nécessairement $P = \sum_n a_n X^{pn}$ donc $P = Q^p$ avec $Q \coloneqq \sum_n b_n X^n \in \mathbb{F}_q[X]$ avec $b_n^p = a_n$ (donné par $b_n = a_n^{q/p}$). □

Dorénavant, le polynôme $P \in \mathbb{F}_q[X]$ sera toujours supposé non constant.

5.1 Algorithme de Berlekamp

Je cite l'article sur l'algorithme de Berlekamp de Wikipedia (https://fr.wikipedia.org/wiki/Algorithme_de_Berlekamp).

> [L'algorithme de Berlekamp] a été découvert par Elwyn Berlekamp [(1940–2019, américain)] en 1967, et est resté l'algorithme le plus performant concernant ce problème jusqu'en 1981, et la découverte de l'algorithme de Cantor–Zassenhaus.

Pour $R \in \mathbb{F}_q[X]$, on considère l'automorphisme F_R de la $\mathbb{F}_q$-algèbre $\mathbb{F}_q[X]/(R)$ donné par l'élévation à la puissance q. (On peut remarquer qu'étant donné $Q \in \mathbb{F}_q[X]$ on a $F_R(Q(X) \bmod R) = Q(X^q) \bmod R$, voir [BMP, Lemme 5.35].) Si $\deg R \geq 1$, l'endomorphisme F_R possède toujours 1 comme valeur propre (pour le vecteur propre 1). Le résultat suivant donne la dimension du sous-espace propre associé.

Proposition 5.2. *Soit $P \in \mathbb{F}_q[X]$ un polynôme sans facteur carré. Le nombre de facteurs irréductibles de P est donné par :*

$$\dim \ker(F_P - \mathrm{id}) = \deg(P) - \operatorname{rg}(F_P - \mathrm{id}).$$

Démonstration. Soit $P = \prod_{i=1}^r P_i$ la décomposition en irréductibles dans $\mathbb{F}_q[X]$. Soit $K_i \coloneqq \mathbb{F}_q[X]/(P_i)$. Par le théorème chinois, l'application :

$$\gamma : \left| \begin{array}{ccc} \mathbb{F}_q[X]/(P) & \longrightarrow & K_1 \times \cdots \times K_r \\ Q \mod P & \longmapsto & (Q \mod P_1, \ldots, Q \mod P_r) \end{array} \right. ,$$

est un isomorphisme de $\mathbb{F}_q$-algèbres puisque les P_i sont distincts par hypothèse (et donc premiers deux à deux car irréductibles). On considère maintenant l'application :

$$\tilde{F}_P \coloneqq \gamma \circ F_P \circ \gamma^{-1} : \prod_i K_i \to \prod_i K_i, \tag{$\dagger$}$$

qui est donnée par l'élévation à la puissance q puisque $\tilde{F}_P(x) = \gamma \circ F_p(\gamma^{-1}(x)) = \gamma(\gamma^{-1}(x)^q) = \gamma(\gamma^{-1}(x))^q = x^q$. Ainsi, $(x_1, \dots, x_r) \in \ker(\tilde{F}_P - \mathrm{id})$ si et seulement si $x_i^q = x_i$ pour tout i. Chaque K_i étant une extension de $\mathbb{F}_q$, on en déduit que $x_i^q = x_i$ si et seulement si x_i est dans la copie de $\mathbb{F}_q$ dans K_i. On en déduit que :

$$\ker(\tilde{F}_P - \mathrm{id}) \simeq \mathbb{F}_q^r,$$

et on conclut puisque $\ker(\tilde{F}_P - \mathrm{id}) = \gamma(\ker(F_P - \mathrm{id}))$ et que γ est un isomorphisme. L'égalité de l'énoncé découle du théorème du rang, puisque $\dim \mathbb{F}_q[X]/(P) = \deg P$. □

Remarque 5.3. Ce résultat donne en particulier une CNS d'irréductibilité. On peut par exemple l'appliquer pour montrer que $X^p - X - 1 \in \mathbb{F}_p[X]$ est irréductible (cf. [BMP, Exercice 5.3]).

Remarque 5.4. On peut voir ce que donne la Proposition 5.2 dans les deux cas extrêmes P irréductible et P scindé sur $\mathbb{F}_q$. Soit n le degré de P.

- Si P est irréductible alors $\mathbb{F}_q[X]/(P) \simeq \mathbb{F}_{q^n}$ donc les éléments fixes par la puissance q-ième sont les éléments de $\mathbb{F}_q$ donc on a bien $\dim \ker(F_P - \mathrm{id}) = 1$.
- Si P est scindé sur $\mathbb{F}_q$ alors $\mathbb{F}_q[X]/(P) \simeq (\mathbb{F}_q)^n$ par le théorème chinois donc tous les éléments sont fixes par la puissance q-ième donc $F_P = \mathrm{id}$ donc $\dim \ker(F_P - \mathrm{id}) = n$.

Proposition 5.5. *Soit $P \in \mathbb{F}_q[X]$ un polynôme sans facteur carré. Soit $V \in \mathbb{F}_p[X]$ tel que $V \bmod P \in \ker(F_P - \mathrm{id})$.*

(i) On a $P = \prod_{\alpha \in \mathbb{F}_q} \mathrm{pgcd}(P, V - \alpha)$.

(ii) Si de plus P est réductible et $V \bmod P \notin \mathbb{F}_q$ alors il existe $\alpha \in \mathbb{F}_q$ tels que $1 \leq \mathrm{pgcd}(P, V - \alpha) < \deg P$.

Démonstration. Soit r le nombre de facteurs irréductibles (distincts) de P.

(*i*) Pour tout $i \in \{1, \dots, r\}$ on note $\alpha_i \coloneqq V \bmod P_i \in \mathbb{F}_q \subseteq K_i$ (on a bien $V \bmod P_i \in \mathbb{F}_q$ par ($\dagger$)). Soit $\alpha \in \mathbb{F}_q$. Puisque les P_i sont irréductibles distincts, on a :

$$\mathrm{pgcd}(P, V - \alpha) = \prod_{i \in I_\alpha} P_i,$$

avec $I_\alpha \coloneqq \{i \in \{1, \dots, r\} : P_i \text{ divise } V - \alpha\}$. Or, on a :

$$P_i \mid V - \alpha \iff V = \alpha \mod P_i \iff \alpha = \alpha_i,$$

ainsi $I_\alpha = \{i \in \{1, \dots, r\} : \alpha_i = \alpha\}$. On en déduit le résultat annoncé :

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

(*ii*) Remarquons que $r \geq 2$ et qu'un tel V existe bien par la Proposition 5.2. Il suffit de montrer que pour tout $\alpha \in \mathbb{F}_q$ on a $\mathrm{pgcd}(P, V - \alpha) \neq P$. Mais c'est clair puisque si $\mathrm{pgcd}(P, V - \alpha) = P$ alors $P \mid V - \alpha$ donc $V = \alpha \bmod P$ donc $V \bmod P = \alpha \in \mathbb{F}_q$.

□

Remarque 5.6. Si P est scindé sur $\mathbb{F}_q$, alors comme on l'a vu dans la Remarque 5.4 on a $F_P = \mathrm{id}$ donc la condition sur V se traduit en $V \in \mathbb{F}_p[X]$ non constant. Si $\lambda \in \mathbb{F}_q$ est une racine de P alors λ est également racine de $V - \alpha$ avec $\alpha \coloneqq V(\lambda)$ donc $X - \lambda \mid \mathrm{pgcd}(P, V - \alpha)$. Ainsi, de façon générale la stratégie de factorisation de la Proposition 5.5 revient un peu à la stratégie naïve de recherche de racine sur $\mathbb{F}_q$ par énumération de tous les éléments du corps.

Algorithme 5.7 (Berlekamp 1967)**.** L'algorithme de Berlekamp consiste à appliquer récursivement la Proposition 5.5, en testant à chaque étape si les facteurs non constants $\mathrm{pgcd}(P, V - \alpha)$ pour $\alpha \in \mathbb{F}_q$ sont irréductibles via la Proposition 5.2.

En partant d'un polynôme $P \in \mathbb{F}_q[X]$ de degré ≥ 2 quelconque (avec potentiellement des facteurs carrés), pour factoriser P on calcule d'abord $\Pi \coloneqq \mathrm{pgcd}(P, P')$.

— Si $\Pi = 1$ alors P est sans facteur carré donc on peut lui appliquer directement l'algorithme de Berlekamp.
— Si $\Pi = P$ alors $P \mid P'$ donc $P' = 0$ donc $P = Q^p$ d'après le Lemme 5.1 et on factorise Q.
— Sinon, on a $1 \leq \deg \Pi, \deg \frac{P}{\Pi} < \deg P$ et on factorise Π et $\frac{P}{\Pi}$.

En particulier, on remarque qu'on n'a pas besoin de déterminer le « sans facteur carréisé » de P comme en Section 4.

Remarque 5.8. Au niveau de la complexité (d'une étape) : la Proposition 5.2 est en $O(\deg(P)^3)$, et la Proposition 5.5 est en $O(q \deg(P)^2)$ (pour le calcul des pgcd). La complexité d'une étape est donc $O(\deg(P)^3 + q \deg(P)^2)$.

5.2 Version probabiliste

([Dem, §9.6.3].) L'algorithme de Berlekamp est très efficace si q est petit, car α parcourt $\mathbb{F}_q$ (en revanche, pour q grand c'est moins efficace, pour la même raison) ; en particulier, si $q = 2$ alors à chaque étape le polynôme est soit irréductible soit un produit de deux polynômes irréductibles. De façon générale, les éléments $\alpha_i = V \mod P_i \in \mathbb{F}_q \subseteq K_i$ vérifient $\alpha_i = 0$ ou $\alpha_i^{\frac{q-1}{2}} = \pm 1$ donc $P_i \mid V, V^{\frac{q-1}{2}} - 1$ ou $V^{\frac{q-1}{2}} + 1$. Par le théorème de Gauss on obtient $P \mid V(V^{\frac{q-1}{2}} - 1)(V^{\frac{q-1}{2}} + 1)$, donc (en supposant q impair, les polynômes en V étant alors premiers entre eux car sans racine commune dans une extension) :

$$P = \mathrm{pgcd}(P, V)\, \mathrm{pgcd}(P, V^{\frac{q-1}{2}} - 1)\, \mathrm{pgcd}(P, V^{\frac{q-1}{2}} + 1). \qquad (\ddagger)$$

Cette décomposition est triviale seulement si les α_i sont soit tous nuls, soit tous résidus quadratiques (*i.e.* $\alpha_i^{\frac{q-1}{2}} = 1$, cf. complément sur la cyclotomie) soit tous non résidus quadratiques. Le premier cas se produit exactement une fois, le deuxième et le troisième chacun $(\frac{q-1}{2})^r$ fois, ou r est le nombre de facteurs irréductibles de P. Ainsi, si V est tiré uniformément dans $\ker(F_P - \mathrm{id})$, la probabilité que la décomposition soit triviale est :

$$q^{-r}\left(1 + 2\left(\frac{q-1}{2}\right)^r\right) \leq 2q^{-r}\left(\frac{q}{2}\right)^r = 2^{1-r} \leq \frac{1}{2},$$

si on est parti d'un polynôme réductible. En tirant N fois un polynôme au hasard, la probabilité de ne pas de trouver de facteur non trivial pour un polynôme réductible est donc $\leq 2^{-N}$. On obtient ainsi un algorithme probabiliste (d'irréductibilité et) de factorisation, le $O(q \deg(P)^2)$ étant remplacé par $O(\log(q) \deg(P)^2)$ (le $\log(q)$ provenant de l'exponentiation rapide dans $\mathbb{F}_q[X]/(P)$).

6 Factorisation probabiliste sur $\mathbb{F}_q$: algorithme de Cantor–Zassenhaus

([Dem, §9.6.4].) On peut développer l'idée de §5.2 pour obtenir un algorithme probabiliste encore plus simple. Encore une fois, l'algorithme part d'un polynôme P sans facteur carré, mais cette fois supposé tel que tous ses facteurs irréductibles sont de même degré d, en particulier $P \mid X^{p^d} - X$ par la Proposition 3.5. On suppose pour l'instant q impair.

L'idée est la suivante. Soit $V \in \mathbb{F}_q[X]$. On va montrer qu'une égalité du même type que (‡) est vérifiée. On a $V(V^{\frac{q^d-1}{2}} - 1)(V^{\frac{q^d-1}{2}} + 1) = V^{q^d} - V$, et ce polynôme est un multiple de $X^{q^d} - X$. En effet, modulo $X^{q^d} - X$ on a :

$$V(X)^{p^d} \equiv V(X^{p^d}) \equiv V(X).$$

On déduit donc que $P \mid V^{q^d} - V$, donc par ce qui précède (comme pour (‡) les facteurs sont premiers entre eux) :

$$P = \operatorname{pgcd}(P, V) \operatorname{pgcd}(P, V^{\frac{q^d-1}{2}} - 1) \operatorname{pgcd}(P, V^{\frac{q^d-1}{2}} + 1).$$

Remarque 6.1. En pratique, on calcule $V^{\frac{q^d-1}{2}}$ modulo P !

Proposition 6.2. *On suppose P réductible. Si V est tiré uniformément parmi les polynômes de degré $< 2d$, la probabilité que $\operatorname{pgcd}(P, V^{\frac{q^d-1}{2}} - 1)$ soit un facteur non trivial (i.e. ni 1 ni P) est au moins $\frac{4}{9} \approx 0.44$.*

Démonstration. Soient P_1 et P_2 deux facteurs irréductibles distincts de P. On pose $W \coloneqq V^{\frac{q^d-1}{2}} - 1$. Si $P_1 \mid W$ et $P_2 \nmid W$ ou l'inverse alors $\operatorname{pgcd}(P, W)$ est un facteur non trivial, ainsi la probabilité $\wp$ recherchée vérifie :

$$\wp \geq \mathbb{P}(P_1 \mid W \text{ et } P_2 \nmid W) + \mathbb{P}(P_1 \nmid W \text{ et } P_2 \mid W).$$

Par hypothèse, les polynômes P_i sont de degré d. On obtient ainsi (le premier $\simeq$ étant une bijection ensembliste, les autres des isomorphismes de $\mathbb{F}_q$-algèbres) :

$$\begin{aligned} \{V \in \mathbb{F}_q[X] : \deg V < 2d\} &\simeq \mathbb{F}_q[X]/(P_1 P_2) \\ &\simeq \mathbb{F}_q[X]/(P_1) \times \mathbb{F}_q[X]/(P_2) \\ &\simeq (\mathbb{F}_{q^d})^2. \end{aligned}$$

D'après l'isomorphisme explicite du théorème chinois, un élément de $\tilde{V}$ de $\mathbb{F}_q[X]/(P_1P_2)$, qui a pour image $(\tilde{V}_1, \tilde{V}_2)$ dans $\mathbb{F}_q[X]/(P_1) \times \mathbb{F}_q[X]/(P_2)$, vérifie $P_i \mid \tilde{V}$ ssi $\tilde{V}_i = 0$. Ainsi, on aura $P_i \mid W$ ssi l'image de W via l'isomphisme explicite du théorème chinois dans $\mathbb{F}_q[X]/(P_i) \simeq \mathbb{F}_{q^d}$ est nulle. Or $W = V^{\frac{q^d-1}{2}} - 1$ donc l'image de W est de la forme $x^{\frac{q^d-1}{2}} - 1$ avec $x = V \mod P_i$, qui est nulle pour exactement x un carré de $\mathbb{F}_{q^d}^\times$, qui sont au nombre de $\frac{q^d-1}{2}$. Puisque V prend chaque élément de $\mathbb{F}_q[X]/(P_1P_2)$ le même nombre (1) de fois, on en déduit que chaque élément de $\mathbb{F}_q[X]/(P_1) \times \mathbb{F}_q[X]/(P_2)$ est également pris le même nombre de fois. On en déduit que x suit

une loi uniforme dans $\mathbb{F}_q[X]/(P_i)$ et on obtient, en rappelant que $q \geq 3$ et $d \geq 1$,

$$\begin{aligned}\mathbb{P}(P_1 \mid W \text{ et } P_2 \nmid W) &= q^{-d}\frac{q^d-1}{2} \times q^{-d}\frac{q^d+1}{2} \\ &= \frac{q^{2d}-1}{4q^{2d}} \\ &= \frac{1}{4} - \frac{1}{4q^{2d}} \\ &\geq \frac{1}{4} - \frac{1}{4\cdot 3^2} \\ &= \frac{8}{36} \\ &= \frac{2}{9}.\end{aligned}$$

Ainsi, on trouve $\wp \geq 2 \times \frac{2}{9} = \frac{4}{9}$. □

Algorithme 6.3 (Cantor [1]–Zassenhaus [2] 1981)**.** On tire V au hasard parmi les polynômes de $\mathbb{F}_q[X]$ de degré $< 2d$ jusqu'à ce que $Q := \operatorname{pgcd}(P, V^{\frac{q^d-1}{2}} - 1)$ soit un facteur non trivial de P. Lorsque c'est le cas on itère avec Q et $\frac{P}{Q}$.

Remarque 6.4. À chaque étape on a une probabilité d'au plus $\frac{5}{9}$ de trouver un facteur trivial. La probabilité de ne trouver que des facteurs triviaux après 10 essais est d'au plus $\left(\frac{5}{9}\right)^{10} \leq 0.3\%$. Ainsi, on peut par exemple décider que si on n'a trouvé que des facteurs triviaux après 10 tirages alors le polynôme est irréductible.

Remarque 6.5. L'exponentiation rapide dans $\mathbb{F}_q[X]/(P)$ est en $O(\log(q^d)) = O(d \log q)$ étapes. Chaque étape est une division euclidienne par P, de degré rd, qui commence avec un polynôme de degré $2d$ donc chaque division euclidienne est en $O(\deg(P)^2)$. On calcule finalement le pgcd, qui possède également cette complexité. Finalement, la complexité pour trouver un facteur non trivial est en $O(\deg(P)^2 d \log q)$. C'est donc plus petit que les $O(\deg(P)^3 + \deg(P)^2 q)$ de Berlekamp (cf. Remarque 5.8), mais comparable avec les $O(\deg(P)^3 + \deg(P)^2 \log q)$ de la version probabiliste du §5.2.

Remarque 6.6. On peut alors se demander ce qui se passe si on tire V au hasard de degré $2d$ et on regarde simplement si $\operatorname{pgcd}(P, V)$ est un facteur non trivial de P. Cette fois, on a $P_i \mid V$ si et seulement si l'image de V dans le théorème chinois est nulle, donc 1 choix. On a donc :

$$\begin{aligned}\mathbb{P}(P_1 \mid V \text{ et } P_2 \nmid V) &= q^{-d}1 \times q^{-d}(q^d - 1) \\ &= \frac{q^d-1}{q^{2d}}.\end{aligned}$$

Ainsi, la probabilité que $\operatorname{pgcd}(P, V)$ soit un facteur non trivial de P est minorée à quelque chose près par q^{-d} donc on ne peut rien conclure (il faudrait tirer disons q^d polynômes mais du coup ça n'est pas efficace du tout).

Il reste encore à voir comment appliquer cet algorithme à partir d'un polynôme où les facteurs irréductibles ne sont pas forcément tous de même degrés. Rappelons que l'on a vu dans la Section 5 comment se ramener au cas d'un polynôme sans facteur carré. Si P est sans facteur

1. David Geoffrey Cantor (1939–2012, américain), à ne pas confondre avec Georg Cantor (1845–1918, allemand), fondateur de la théorie des ensembles !
2. Hans Julius Zassenhaus (1912–1991, allemand).

carré de degré n, d'après la Proposition 3.5 le polynôme $P^{(1)} \coloneqq \mathrm{pgcd}(P, X^q - X)$ ne possède que les facteurs irréductibles de P de degré 1, puis $P^{(2)} \coloneqq \mathrm{pgcd}(\frac{P}{P^{(1)}}, X^{q^2} - X)$ ne possède que les facteurs irréductibles de P de degré 2, puis :

$$P^{(d)} \coloneqq \mathrm{pgcd}\left(\frac{P}{\prod_{d'<d} P^{(d')}}, X^{q^d} - X\right),$$

ne possède que les facteurs irréductibles de P de degré d.

Remarque 6.7. ([Coh, §3.4.4].) Lorsque q est pair (donc une puissance de 2), la fraction $\frac{q^d-1}{2}$ n'est plus entière. On remplace alors la factorisation $X^{q^d} - X = X(X^{\frac{q^d-1}{2}} - 1)(X^{\frac{q^d-1}{2}} + 1)$ par :

$$X^{q^d} - X = U(X)(U(X) + 1),$$

où $U(X) \coloneqq \sum_{i=0}^{d-1} X^{2^i}$. On a en effet $U(X)^2 = \sum_{i=1}^{d} X^{2^i}$ donc $U(X)^2 + U(X) = X^{2^d} + X$ comme voulu. Dans l'algorithme, on remplace alors $\mathrm{pgcd}(P, V^{\frac{q^d-1}{2}} - 1)$ par $\mathrm{pgcd}(P, U \circ V)$.

7 Factorisation sur $\mathbb{Z}$

([Dem, §9.6.5], [Coh, §3.5].) On rappelle que, par le théorème de Gauss, factoriser sur $\mathbb{Z}$ ou $\mathbb{Q}$ revient essentiellement au même (un polynôme à coefficients entiers est irréductible sur $\mathbb{Z}$ ss'il est primitif, *i.e.* ses coefficients sont premiers entre eux dans leur ensemble, et irréductible sur $\mathbb{Q}$, voir par exemple le Perrin).

Le principe est le suivant. On dispose de bornes sur les coefficient des facteurs d'un polynôme (bornes de Landau et de Mignotte). Pour un premier p assez grand, on peut donc factoriser dans $\mathbb{Z}/p\mathbb{Z}[X]$ puis voir ce que donnent les facteurs quand ils sont vus dans $\mathbb{Z}$ (avec la représentation $-(p-1)/2 \dots (p-1)/2$).

Exemple 7.1. (Cf. [Coh, §3.5.2].) En réduisant $P \coloneqq X^6 - 6X^4 - 2X^3 - 7X^2 + 6X + 1$ modulo 47, on trouve $\overline{P} = (X - 22)(X - 13)(X - 12)(X + 12)(X^2 - 12X - 4)$ (les coefficients sont dans $\{-23, \dots, 23\}$). Puisque le coefficient constant de P est 1 et que $P(\pm 1) \neq 0$, on en déduit que P ne possède pas de facteur de degré 1. La factorisation ne peut se relever sur $\mathbb{Z}$ en un facteur de degré 2 pour la même raison donc nécessairement P est un produit de deux polynômes de degré 3, dont l'un est divisible par $X^2 - 12X - 4$. Les polynômes de degré 1 dont le produit avec celui-là ont un coefficient constant ± 1 sont $X - 12$ et $X + 12$, mais avec le $X - 12$ on a $X^3 + 23X^2 - X + 1$ et le 23 est trop grand pour la borne de P. On a $(X + 12)(X^2 - 12X - 4) = X^3 - 7X - 1$ dans $\mathbb{Z}/47\mathbb{Z}[X]$ et on vérifie qu'il divise bien P puisque $P = (X^3 - 7X - 1)(X^3 + X + 1)$ (si ça n'avait pas été le cas on aurait conclut que P est irréductible).

Le problème est que le premier p devient potentiellement assez grand. On remplace alors $\mathbb{Z}/p\mathbb{Z}$ par $\mathbb{Z}/q^n\mathbb{Z}$ où q est premier (plus petit) et n assez grand. Pour cela, on passe de $\mathbb{Z}/q\mathbb{Z}$ à $\mathbb{Z}/q^2\mathbb{Z}$, …, à $\mathbb{Z}/q^n\mathbb{Z}$ par le *lemme de Hensel* ($\approx$ méthode de Newton algébrique).

Références

[BMP] V. Beck, J Malick et G. Peyré, *Objectif Agrégation.*

[Coh] H. Cohen, *A Course in Computational Algebraic Number Theory.*

[Dem] M. Demazure, *Cours d'algèbre.*

[GaGe] J. von zur Gathen, J. Gerhard, *Modern Computer Algebra.*