Prérequis.

Théorème 0.0.1. *Soient q une puissance d'un nombre premier et $P \in \mathbf{F}_q[X]$ un polynôme de degré n et sans facteur carré. Alors il existe un algorithme donnant la décomposition de P en produit d'irréductibles. Précisément, on trouve un facteur non constant de P en $O(qn^3)$ opérations.*

Démonstration.

Lemme 0.0.2. *Pour $R \in \mathbf{F}_q[X]$, le morphisme :*

$$S_R : \begin{array}{ccc} \mathbf{F}_q[X]/R & \longrightarrow & \mathbf{F}_q[X]/R \\ \overline{Q} & \longmapsto & \overline{Q(X^q)} \end{array}$$

est bien défini et coïncide avec $\overline{Q} \mapsto \overline{Q}^q$.

Démonstration. L'application $S_0 : Q \in \mathbf{F}_q[X] \mapsto Q(X^q) = Q^q$ est un morphisme d'anneaux, on note $S = \pi \circ S : \mathbf{F}_q[X] \to \mathbf{F}_q[X]/R$ avec π la projection modulo R. Comme $S(R) = 0$, le morphisme S passe au quotient et donne S_R. Ensuite :

$$S_R(Q \bmod R) = S_R(\pi(Q)) = \pi(Q(X^q)) = \pi(Q^q) = \pi(Q)^q$$

comme annoncé. □

Voici la description de l'algorithme. On note $\pi : \mathbf{F}_q[X] \to \mathbf{F}_q[X]/P$ la projection et $x = \pi(X)$. On note $\mathcal{B} = (1, x, \ldots, x^{\deg P - 1})$ qui est une base de $\mathbf{F}_q[X]/P$.

— On calcule la matrice de $S_P - \mathrm{id}$ dans $\mathcal{B}$;

— Le nombre de facteurs irréductibles de P est :

$$r = \dim \mathrm{Ker}(S_P - \mathrm{id}) = \deg P - \mathrm{rg}(S_P - \mathrm{id}).$$

Si $r = 1$, on s'arrête car P est irréductible ;

— On calcule un polynôme V non constant modulo P tel que $\pi(V) \in \mathrm{Ker}(S_P - \mathrm{id})$. Avec l'algorithme d'Euclide, on calcule la décomposition :

$$P = \prod_{\alpha \in \mathbf{F}_q} \mathrm{pgcd}(P, V - \alpha),$$

et l'on recommence avec chaque facteur non trivial.

Il faut montrer que cet algorithme termine et est correct. Notons $P = P_1 \cdot \ldots \cdot P_r$ une décomposition de P en produit d'irréductibles, qui sont premiers entre eux parce que P est sans facteur carré. Notons $\kappa_i = \mathbf{F}_q[X]/P_i$. Par théorème chinois, on a alors un isomorphisme :

$$\phi : \mathbf{F}_q[X]/P \to \kappa_1 \times \cdots \times \kappa_r.$$

Notons $\widehat{S_P} = \phi \circ S_P \circ \phi^{-1}$ qui correspond à l'élévation à la puissance q dans $\kappa_1 \times \cdot \times \kappa_r$. Alors :

$$\begin{aligned}(x_1, \ldots, x_r) \in \mathrm{Ker}(\widehat{S_P} - \mathrm{id}) \text{ ssi } (x_1^q, \ldots, x_r^q) &= (x_1, \ldots, x_r) \\ \text{ssi } \forall i,\ x_i^q &= x_i \text{ dans } \kappa_i.\end{aligned}$$

Or, chaque κ_i est une extension de $\mathbf{F}_q$ et l'on y a $\mathbf{F}_q = \{x \in \kappa_i \mid x^q = x\}$. Ainsi, $(x_1, \ldots, x_r) \in \mathrm{Ker}(\widehat{S_P} - \mathrm{id})$ est équivalent à demander que $x_i \in \mathbf{F}_q \subset \kappa_i$ pour tout i. Par conséquent, $\mathrm{Ker}(\widehat{S_P} - \mathrm{id}) = \mathbf{F}_q^r$ et la dimension de ce noyau compte donc bien le nombre de facteurs irréductibles de P.

On suppose alors $r > 1$, ce qui montre que $\mathrm{Ker}(S_P - \mathrm{id})$ n'est pas réduit à une droite, donc qu'il y existe un polynôme V non constant modulo P. Comme $\pi(V) \in \mathrm{Ker}(S_P - \mathrm{id})$, ce qui précède montre que V modulo P_i est constant, égal disons à $\alpha_i \in \mathbf{F}_q \subset \kappa_i$, pour tout i.

Soit $\alpha \in \mathbf{F}_q$. Comme $\mathrm{pgcd}(P, V - \alpha)$ divise P, il est de la forme $\prod_{I_\alpha} P_i$, et comme les P_i sont premiers entre eux, on a $I_\alpha = \{i \mid P_i | V - \alpha\}$. Or, $\alpha_i = \alpha$ si et seulement si P_i divise $V - \alpha$, donc $I_\alpha = \{i \mid \alpha_i = \alpha\}$. Finalement :

$$P = \prod_{\alpha \in \mathbf{F}_q} \prod_{i | \alpha_i = \alpha} P_i = \prod_{\alpha \in \mathbf{F}_q} \mathrm{pgcd}(P, V - \alpha).$$

Comme V modulo P n'est pas constant, au moins deux facteurs de ce produit sont non triviaux donc le degré décroît strictement à chaque exécution de l'algorithme. En particulier, l'algorithme termine. Et d'après tout ce que l'on vient de voir, il est correct.

Calculons la complexité de l'algorithme. La mise sous forme sans facteur carré revient au calcul de $\mathrm{pgcd}(P, P')$ ce qui se fait en $O(n^2)$ opérations.

La matrice est calculée avec n divisions euclidiennes de polynômes de degré $\leqslant nq$ par P, donc ce calcul se fait en complexité $O(n(n(nq - n + 1))) = O(qn^3)$.

Le pivot de Gauss pour calculer le noyau de la matrice se fait en $O(n^3)$ opérations.

Dans le pire cas, on doit calculer n pgcd non triviaux de degré toujours $\leqslant n$ donc un calcul en $O(n^3)$.

On trouve donc un facteur non constant de P en $O(qn^3)$ opérations. □

Remarques.

— Il faut savoir exécuter cet algorithme sur un exemple. C'est pas difficile si on sait rapidement faire des divisions euclidiennes de polynômes. Par exemple avec $q = 5$ et $P = X^3 + X^2 + X + 2$, on trouve comme matrice :

$$S_P - \mathrm{id} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 3 \\ 0 & 4 & 2 \end{pmatrix}$$

qui est de rang 1. On remarque en fait que la première colonne sera toujours nulle et qu'elle correspond à la droite du noyau formée des polynômes constants modulo

P. On trouve alors un autre élément du noyau, comme $(0, 2, 1)$, qui correspond à $V = X^2+2X$. Enfin, il faut calculer les cinq $\text{pgcd}(P, V-\alpha)$. Les deux premiers et le dernier valent 1, le troisième vaut X^2+2X+3 et le quatrième $X+4$. Ces deux polynômes sont les facteurs irréductibles de P. On le sait parce qu'on a trouvé $r = 2$ et deux pgcds non triviaux donc on peut s'arrêter ! On sent vraiment une sorte de magie dans le calcul de V et des pgcds, qui séparent miraculeusement les facteurs irréductibles.

— Ce n'est pas nécessaire de donner la complexité pendant le développement, mais s'il reste du temps c'est de très bon goût. Et c'est bien de la connaître pour répondre facilement à une éventuelle question du jury à ce propos. De même, il faut bien connaître la complexité de la division euclidienne et celle de l'algorithme d'Euclide.

— Quand P a des facteurs carrés, on peut le mettre sous forme sans facteur carré en le divisant par $\text{pgcd}(P, P')$, et exécuter l'algorithme sur ce quotient et sur le pgcd. Attention, P' peut être nul, mais cela n'arrive que lorsque P est de la forme R^p avec p la caractéristique du corps de base. Et dans ce cas, on peut calculer R et exécuter l'algorithme sur ce polynôme.

— L'algorithme est utilisé dans la pratique pour le calcul efficace du logarithme discret, donc c'est utile en cryptographie.

Recasages.

— 122 : On illustre, un peu comme avec la forme normale de Smith, un algorithme de calcul sur des anneaux de polynômes. La démonstration utilise plusieurs fois la principalité de $\mathbf{F}_q[X]$, par exemple pour dire que l'irréductibilité de P_i entraîne que $\kappa_i = \mathbf{F}_q[X]/P_i$ est un corps. On utilise aussi le fait que c'est un anneau euclidien pour calculer effectivement des restes, et que c'est un anneau factoriel pour les pgcd. Attention à bien motiver la présence de cet algorithme dans la leçon quand même.

— 123 : C'est une très bonne leçon pour ce développement qui est réellement utile en pratique lorsque l'on manipule des corps finis.

— 141 : Parfait. On parle de polynômes irréductibles et de corps de rupture, c'est difficile de faire mieux.

— 142 : On utilise à fond les algorithmes de calcul de division euclidienne et de pgcd. C'est donc une application concrète de l'algorithme d'Euclide. En plus, il y a ce côté magique des pgcds qui font apparaître les facteurs, donc on sent que le calcul des pgcd est central.

— 151 : Voir le nombre de facteurs irréductibles d'un polynôme en calculant la dimension d'un espace vectoriel, ça paraît très fort. Il faut donc mettre l'accent sur ce point. On peut aussi le rapprocher à la factorisation des polynômes cyclotomiques sur les corps finis : Φ_n se décompose sur $\mathbf{F}_q$ en un produit de $\phi(n)/r$ polynômes irréductibles distincts et tous de même degré r égal à l'ordre de q dans $(\mathbf{Z}/n\mathbf{Z})^\times$. Ce théorème utilise le théorème de la base télescopique (de manière équivalente, la description des sous-corps de $\mathbf{F}_{q^r}$), donc le lien avec la leçon n'est

pas idiot (cf. Demazure, page 217).