Extensions de $\mathbb{F}_p$ et polynômes cyclotomiques

Extensions du corps fini $\mathbb{F}_p$

Un corps fini $\mathbb{F}_q$, où $q = p^r$, est une extension de $\mathbb{F}_p$, qui peut être défini comme quotient de $\mathbb{F}_p[x]$ par un polynôme irréductible :

$$\frac{\mathbb{F}_p[x]}{(g(x))} \cong \mathbb{F}_p[\alpha] = \mathbb{F}_q.$$

On identifie l'image de x avec α , qui est une racine dans $\mathbb{F}_q$ du polynôme $g(x) \in \mathbb{F}_p[x]$. En notant que $\alpha \neq 0$ est un élément du groupe cyclique $\mathbb{F}_q^*$ d'ordre $n = q - 1$, on observe qu'il satisfait $\alpha^n = 1$ (par Lagrange). Par conséquent $g(x)$ est un diviseur irréductible du polynôme $x^n - 1 \in \mathbb{F}_p[x]$. En effet, tout élément de $\mathbb{F}_q^*$ est une racine de $x^n - 1$, et donc :

$$x^n - 1 = \prod_{\alpha \in \mathbb{F}_q^*} (x - \alpha) \in \mathbb{F}_p[x]$$

Alors les facteurs irréductibles de $x^n - 1$ dans $\mathbb{F}_p[x]$ parcourent les polynômes minimaux des éléments non nuls de $\mathbb{F}_q/\mathbb{F}_p$. Cela motive l'étude des polynômes cyclotomiques, et leur rapport avec les corps finis.

Exemple. On considère le corps fini $\mathbb{F}_4$, extension du corps $\mathbb{F}_2$. En écrivant $\mathbb{F}_4 = \mathbb{F}_2[\alpha]$, pour un choix de α dans $\mathbb{F}_4 \setminus \mathbb{F}_2$, on note :

- $\mathbb{F}_4 = \mathbb{F}_2 \oplus \mathbb{F}_2\alpha$ en tant qu'espace vectoriel sur $\mathbb{F}_2$, avec base $\{1, \alpha\}$.
- Le groupe $\mathbb{F}_4^*$ est une groupe cyclique d'ordre 3, engendré par α .
- En regardant $\mathbb{F}_4$ comme ensemble, comme espace vectoriel, et $\mathbb{F}_4^*$ comme groupe, on peut identifier le seul autre élément (à part α) de $\mathbb{F}_4 \setminus \mathbb{F}_2$ est l'élément :

$$\beta = \alpha^2 = \alpha^{-1} = \alpha + 1.$$

On en déduit que α (et également β) est une racine de $x^2 + x + 1 \in \mathbb{F}_2[x]$ qui est un diviseur irréductible de $x^3 - 1 (= x^3 + 1)$ dans $\mathbb{F}_2[x]$. La factorisation

$$x^3 - 1 = (x - 1)(x^2 + x + 1),$$

donne le premier exemple d'une factorisation en polynômes cyclotomiques.

Dans la suite, on va étudier le rôle des polynômes cyclotomiques dans la construction des corps finis et classifications de leurs éléments par ordre dans les groupes d'unités. Les factorisations des polynômes cyclotomiques dans $\mathbb{F}_p[x]$ joue un rôle clé dans la structure des corps finis. On finit par l'étude des algorithmes pour factorisation de polynômes, et les mathématiques sous-jacent. L'analogie entre les anneaux $\mathbb{F}_p[x]$ et $\mathbb{Z}$ permet de comparer et trouver des distinctions entre les problèmes de factorisation des polynômes et des entiers.

Polynômes cyclotomiques

Soit $\Phi_n(x)$ le *polynôme cyclotomique* défini récursivement par

$$x^n - 1 = \prod_{m|n} \Phi_m(x).$$

En particulier, $\Phi_1(x) = x - 1$ et pour p premier, $\Phi_p(x) = x^{p-1} + \dots + x + 1$.

Rappel. La *caractéristique* d'un anneau A (unitaire) est le générateur (non-négatif) du noyau de l'unique homomorphisme $\mathbb{Z} \rightarrow A$. Si n est la caractéristique de A , il existe une injection (unique) $\mathbb{Z}/n\mathbb{Z} \rightarrow A$.

Propriétés des polynômes cyclotomiques en caractéristique 0

1. $\Phi_n(x) \in \mathbb{Z}[x]$
2. $\Phi_n(x)$ est irréductible dans $\mathbb{Q}[x]$.
3. $\deg(\Phi_n(x)) = \varphi(n)$ ($= |(\mathbb{Z}/n\mathbb{Z})^*|$ par définition)
4. Dans $\mathbb{C}[x]$, en posant $\zeta_n = e^{2\pi i/n}$, on a

$$\Phi_n(x) = \prod_{k \in (\mathbb{Z}/n\mathbb{Z})^*} (x - \zeta_n^k).$$

5. $\mathbb{Q}[x]/(\Phi_n(x)) \cong \mathbb{Q}(\zeta_n)$ et $\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*$.

Remarque. Ces propriétés sont très classiques. Concernant la structure du groupe de Galois, on remarque que $\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ est le groupe d'automorphismes de $\mathbb{Q}(\zeta_n)$, et l'isomorphisme

$$(\mathbb{Z}/n\mathbb{Z})^* \longrightarrow \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$$

associe à k l'automorphisme prolongeant $\zeta_n \mapsto \zeta_n^k$.

Les groupes cycliques $\mu_n = \{\zeta_n^k \mid k \in \mathbb{Z}/n\mathbb{Z}\}$ des racines n -ièmes de l'unité sont les seuls sous-groupes finis de $\mathbb{C}^*$, et les polynômes cyclotomiques sont les polynômes minimaux de ces éléments distingués. Or, la définition analytique $\zeta_n = e^{2\pi i/n}$, ne se généralise pas aux corps finis. Par ailleurs, tous les éléments non nuls d'un corps fini ont un ordre fini (et le groupe $\mathbb{F}_q^*$ est un groupe cyclique), alors racines d'un polynôme $x^n - 1$, donc la construction algébrique des n -ième racines d'unité, par voie des polynômes cyclotomiques, joue un rôle important dans la théorie des corps finis.

Propriétés des polynômes cyclotomiques en caractéristique p

1. Si $n = p^r - 1$, alors $\Phi_n(x)$ est un produit de polynômes irréductibles de degré r .
2. Si n et p sont premiers entre eux et $r = \text{ord}(p, n)$ est l'ordre de p dans $(\mathbb{Z}/n\mathbb{Z})^*$, alors $\Phi_n(x)$ est un produit de polynômes irréductibles de degré r .
3. Si n et p sont premiers entre eux, alors $\Phi_{p^i n}(x) = \Phi_n(x)^{\varphi(p^i)}$.

Preuve des propriétés des polynômes cyclotomiques.

1. Toute racine de $\Phi_n(x)$ dans $\mathbb{F}_{p^r}$ est un générateur du groupe $\mathbb{F}_{p^r}^*$, donc aussi de l'extension $\mathbb{F}_{p^r}/\mathbb{F}_p$. Par conséquent, son polynôme minimal est de degré r .
2. Toute racine de $\Phi_n(x)$ dans $\mathbb{F}_{p^r}$ est élément de l'ordre n de $\mathbb{F}_{p^r}^*$. Les conditions suivantes sur un tel élément α sont équivalentes :

- α est dans $\mathbb{F}_{p^s}$.
- n divise $p^s - 1$.
- $\text{ord}(p, n)$ divise s .

Si un élément α n'appartient à aucun sous-corps $\mathbb{F}_{p^s}$ propre (où s est diviseur propre de r), il engendre l'extension $\mathbb{F}_{p^r}/\mathbb{F}_p$, et son polynôme minimal relatif à $\mathbb{F}_p$ est de degré r . Par conséquent, les diviseurs irréductibles de $\Phi_n(x)$ sont tous de degré r .

Remarque. Si $n = p^r - 1$, alors l'ordre de p dans $(\mathbb{Z}/n\mathbb{Z})^*$ est r , donc ce résultat est une généralisation du résultat précédent.

3. Le résultant suit de la factorisation $x^{np^i} - 1 = (x^n - 1)^{p^i}$ dans $\mathbb{F}_p[x]$.

En utilisant le fait que tout corps fini de p^r éléments est le corps de décomposition de $x^{p^r} - x$, on démontre le théorème suivant, duquel on dérive les propriétés ci-dessus.

Théorème. *Pour chaque p premier et $r \geq 1$, il existe un et un seul corps, à isomorphisme près, avec p^r éléments.*

On peut construire "le" corps fini à p^r éléments, comme $\mathbb{F}_{p^r} = \mathbb{F}_p[\zeta_n]$ où le polynôme minimal de ζ_n est un diviseur f_n irréductible de degré r du polynôme cyclotomique $\Phi_n(x)$, pour $n = p^r - 1$. En général, il y a plusieurs choix de diviseur irréductible f_n de $\Phi_n(x)$, et si $m|n$, ($m \neq n$) est tel que l'ordre de p est (toujours) r modulo m (dans le quotient de groupes $\mathbb{Z}/n\mathbb{Z}^* \rightarrow \mathbb{Z}/m\mathbb{Z}^*$), on a $\mathbb{F}_p[\zeta_m] \cong \mathbb{F}_p[\zeta_n]$.

Éléments primitifs de $\mathbb{F}_{p^r}/\mathbb{F}_p$ et de $\mathbb{F}_{p^r}^*$. Dans une extension L/K , on dit que $\alpha \in L$ est un élément *primitif* (relatif à K) si $L = K[\alpha]$. Pour toute extension finie de corps, il existe un élément primitif. Pour un corps fini $L = \mathbb{F}_{p^r}$ un élément α du groupe $\mathbb{F}_{p^r}^*$ est *primitif* si et seulement si l'ordre de α est $p^r - 1$.

On suppose donc fixé $L = \mathbb{F}_{p^r}$ et $K = \mathbb{F}_p$. Dans le premier cas, la définition de primitif concerne la propriété d'être un générateur de L comme K -algèbre et dans le deuxième elle concerne la propriété d'être un générateur du groupe L^* . Il est donc nécessaire de préciser le contexte de l'extension L/K ou du groupe L^* .

Un *polynôme* de $\mathbb{F}_p[x]$ de degré r est dit *primitif* si et seulement s'il est le polynôme minimal d'un élément primitif de $\mathbb{F}_{p^r}^*$. Un polynôme primitif de $\mathbb{F}_p[x]$ est nécessairement irréductible, mais pas inversement.

Exercices

1. Combien d'anneaux commutatifs de cardinal 4 existent-ils ? (Indication : Considérer les éventuels homomorphismes surjectifs $\mathbb{Z} \rightarrow A$ ou $\mathbb{F}_2[x] \rightarrow A$.)
2. Montre que r divise $\varphi(p^r - 1)$. Plus généralement, pour tout entier $a > 1$ et $r \geq 1$, démontrer que r divise $\varphi(a^r - 1)$. (Indication : utiliser le théorème de Lagrange.)
3. Trouver les premiers p et les entiers $r \geq 1$ tel qu'il existe un seul polynôme primitif de degré r dans $\mathbb{F}_p[x]$.
4. Montrer qu'il existe un polynôme primitif de degré r dans $\mathbb{F}_p[x]$ pour tout premier p et entier r .
5. Montrer qu'il existe un polynôme irréductible de degré r dans $\mathbb{F}_p[x]$ pour tout premier p et entier r .
6. Démontrer l'unicité du corps de $q = p^r$ éléments en le décrivant comme corps de décomposition de $x^q - x$.
7. Montrer que $x^p - x - a$ est irréductible dans $\mathbb{F}_p[x]$ pour tout a dans $\mathbb{F}_p^*$.
8. Déterminer la factorisation de $\Phi_7(x)$ dans $\mathbb{F}_2[x]$.
9. Décrire les éléments primitifs de $\mathbb{F}_{2^3}/\mathbb{F}_2$ et de $\mathbb{F}_{2^3}^*$ en termes de racines des polynômes cyclotomiques.
10. Déterminer la factorisation de $\Phi_{15}(x)$ dans $\mathbb{F}_2[x]$.
11. Décrire les éléments primitifs de $\mathbb{F}_{2^4}/\mathbb{F}_2$ et de $\mathbb{F}_{2^4}^*$ en termes des racines des polynômes cyclotomiques.
12. Trouver des isomorphismes :

$$\mathbb{F}_2[\zeta_{15}] = \mathbb{F}_2[x]/(x^4 + x + 1) \longrightarrow \mathbb{F}_2[\zeta_5] = \mathbb{F}_2[x]/(x^4 + x^3 + x^2 + x + 1),$$

et

$$\mathbb{F}_2[\zeta_{15}] = \mathbb{F}_2[x]/(x^4 + x + 1) \longrightarrow \mathbb{F}_2[\zeta_{15}] = \mathbb{F}_2[x]/(x^4 + x^3 + 1).$$

13. Montrer que $\phi(\alpha) = \alpha^p$ est un homomorphisme d'anneaux $A \rightarrow A$ pour tout anneau A de caractéristique p premier. Il s'appelle l'endomorphisme de Frobenius (ou l'automorphisme de Frobenius lorsqu'il est un isomorphisme).
14. Montrer que tout homomorphisme d'un corps K est injectif, et conclure que l'endomorphisme de Frobenius est un automorphisme dans le cas d'un corps fini.
15. Soit $\phi : \mathbb{F}_q \rightarrow \mathbb{F}_q$ l'automorphisme de Frobenius, où $q = p^r$. Déterminer les éléments fixés par ϕ et par ϕ^r .
16. Démontrer que $\text{Gal}(\mathbb{F}_q/\mathbb{F}_p) = \langle \phi \rangle$, un groupe cyclique d'ordre r .

Factorisation des polynômes sur $\mathbb{F}_p$

Factorisation des polynômes sur $\mathbb{F}_p$

L'objectif de cette section est de détailler un algorithme probabiliste pour la factorisation d'un polynôme f sur le corps fini $\mathbb{F}_p$.

Remarque. On rappelle qu'un algorithme probabiliste comporte des choix aléatoires selon lequel la durée du calcul peut changer. Il peut donc s'avérer impossible de borner le temps de calcul, qu'on remplace avec la notion de temps espéré de calcul, une espérance mathématiques. En particulier un algorithme probabiliste avec complexité polynôme est un algorithme dont le temps espéré est borné par une fonction polynôme de la taille d'entrée.

L'idée de l'algorithme est d'utiliser la structure du groupe des unités de l'algèbre quotient

$$(\mathbb{F}_p[x]/(f))^*.$$

En particulier on veut construire des éléments u d'ordre 2 de ce groupe, dit des éléments de 2-torsion. En effet, si u satisfait $u^2 - 1 \equiv 0 \pmod{f}$, et $u \neq \pm 1$, alors en caractéristique $p \neq 2$, on a

$$f = \text{pgcd}(u^2 - 1, f) = \text{pgcd}(u - 1, f)\text{pgcd}(u + 1, f)$$

est une factorisation non triviale.

Définition. Pour un groupe abélien G , on écrit $G[\ell] = \{\gamma \in G \mid \gamma^\ell = e\}$, pour le sous-groupe d'éléments d'ordre divisant ℓ , dit le groupe de ℓ -torsion.

Avant d'enoncer le théorème qui suit, on présente un lemme qui simplifie sa démonstration.

Lemme. *Un groupe abélien G est cyclique si et seulement si $G[\ell]$ est cyclique pour tout premier ℓ divisant $|G|$.*

Démonstration. Exercice. (Conséquence de la classification des groupes finis abéliens.) $\square$

Théorème. *Soit $\mathbb{F}_q$ un corps fini de q éléments. Alors $\mathbb{F}_q^* \cong \mathbb{Z}/(q-1)\mathbb{Z}$.*

On note que l'opération de groupe dans $\mathbb{F}_q^$ est multiplication, tandis que l'opération de groupe de $\mathbb{Z}/(q-1)\mathbb{Z}$ est addition.*

Démonstration. Il est clair que les deux groupes sont abéliens d'ordre $q-1$ et il suffit de montrer que $G = \mathbb{F}_q^*$ est cyclique. Il suffit donc d'établir l'identité :

$$\prod_{\gamma \in G[\ell]} (x - \gamma) = x^\ell - 1 \in \mathbb{F}_p[x],$$

car, si vrai, on obtient que $|G[\ell]| = \ell$, donc $G[\ell]$ est cyclique. Il est clair que le produit divise le côté droit, parce que tout $\gamma \in G[\ell]$ est une racine de $x^\ell - 1$, et alors $x - \gamma$ divise $x^\ell - 1$. Comme le degré du produit est $|G[\ell]| = \ell^t \geq \ell$, on conclut qu'on a égalité $|G[\ell]| = \ell$ et $\prod_{\gamma \in G[\ell]} (x - \gamma) = x^\ell - 1$. $\square$

Problème de factorisation

On fait une comparaison des factorisation des polynômes et entiers, pour comprendre pourquoi le problème de factorisation des polynômes est facile (en temps polynôme) tandis que le problème de factorisation des entiers reste difficile, les meilleurs algorithmes connus étant sous-exponentiels. Soient

$$f = \prod_{i=1}^t g_i^{e_i} \in \mathbb{F}_p[x] \text{ et } N = \prod_{i=1}^t p_i^{e_i} \in \mathbb{Z},$$

la factorisation en premiers (dits irréductibles dans le cadre des polynômes). Alors par le théorème chinois,

$$\mathbb{F}_p[x]/(f) \cong \prod_{i=1}^t \frac{\mathbb{F}_p[x]}{(g_i^{e_i})} \text{ et } \mathbb{Z}/N\mathbb{Z} \cong \prod_{i=1}^t \frac{\mathbb{Z}}{p_i^{e_i}\mathbb{Z}}.$$

En regardant les groupes d'unités, on a

$$|(\mathbb{F}_p[x]/(f))^*| = \prod_{i=1}^t (p^{d_i} - 1)p^{d_i(e_i-1)} \text{ et } |(\mathbb{Z}/N\mathbb{Z})^*| = \prod_{i=1}^t (p_i - 1)p_i^{e_i-1}.$$

où $d_i = \deg(g_i)$. Si f and N sont sans facteur carré, c'est à dire que $e_i = 1$ pour tout i , on a

$$|(\mathbb{F}_p[x]/(f))^*| = \prod_{i=1}^t (p^{d_i} - 1) \text{ et } |(\mathbb{Z}/N\mathbb{Z})^*| = \prod_{i=1}^t (p_i - 1)$$

Remarque. On note que les valeurs possibles pour les groupes d'unités des quotients sont discrètes dans le cadre des polynômes :

$$p - 1, p^2 - 1, p^3 - 1, \dots, p^d - 1 < p^{\deg(f)}.$$

Or, les espaces entre les premiers successifs

$$2, 3, 5, 7, 11, \dots, p < N$$

sont au moyenne $\log(p)$ autour d'un premier p . Alors ils sont plus nombreux, autour de $N/\log(N)$ en nombre, et plus équidistribués dans l'intervalle $[[1, N]]$.

Algorithme de factorisation dans $\mathbb{F}_p[x]$

L'algorithme dominant pour factorisation se base sur un algorithme probabiliste de Cantor-Zassenhaus. Les données d'entrée consistent d'un polynôme f sans facteur carré, dont tous les facteurs irréductibles ont le même degré d (qui fait partie des données). On décrit un algorithme complet en trois étapes, algorithmes **A**, **B**, et **C**, pour la factorisation des polynômes, dont **C** est l'algorithme de Cantor-Zassenhaus. Les algorithmes **A** et **B** sont déterministes et rapides, servant à décomposer un polynôme générale en polynôme f satisfaisant les conditions sur les données d'entrée de l'algorithme **C**. De la même façon, l'algorithme **A** produit des polynôme sans facteur carré, condition nécessaire pour les données d'entrée de l'algorithme **B**.

Remarque. Dans la suite, on écrit f ou $f(x)$ pour un polynôme dans $\mathbb{F}_p[x]$. En effet, l'évaluation d'un polynôme f au variable x est tautologiquement lui-même.

Algorithme A. Algorithme pour décomposition en polynômes sans facteur carré.

Entrée : La donnée d'entrée est un polynôme $f \in \mathbb{F}_p[x]$.

Sortie : Les données de sortie consistent de deux polynômes $g, h \in \mathbb{F}_p[x]$ tels que

$$g(x)h(x^p) \mid f(x) \mid g(x)^e h(x^p),$$

où g est un polynôme sans facteur carré. Le polynôme g sera envoyé en Algorithme **B** et le polynôme h en Algorithme **A**.

Remarque. L'exposant e est inconnu, mais après la décomposition complète de g , on peut déterminer rapidement l'exposant e_i de chaque diviseur g_i irréductible de g . Alors l'entier minimal e est $\max(\{e_i\})$.

Algorithme. On suppose que $f(x) = \prod_i g_i(x)^{e_i}$. On calcule $s = \text{pgcd}(f, f')$, où f' est la dérivée formelle de f :

$$f'(x) = \sum_{k=1}^n k a_k x^{k-1} \text{ où } f(x) = \sum_{k=0}^n a_k x^k.$$

Par la règle du product (de Leibniz), en termes de la factorisation de f , on a

$$f' = \sum_{i=1}^t e_i \frac{f}{g_i} g'_i = \sum_{i=1}^t e_i (g_1^{e_1} \cdots g_i^{e_i-1} \cdots g_t^{e_t}) \cdot g'_i.$$

Comme g_i est irréductible, $\text{pgcd}(g_i, g'_i) = 1$, et on peut vérifier que

$$g_i^{e_i-1} \mid \text{pgcd}(g_i^{e_i}, s) \mid g_i^{e_i},$$

avec égalité $g_i^{e_i-1} = \text{pgcd}(g_i^{e_i}, s)$ si et seulement si $e_i \neq 0 \pmod p$. Par conséquent, on en déduit que

$$g = \frac{f}{s} = \prod_{\substack{i=1 \\ p \nmid e_i}}^t g_i.$$

Par des pgcd successifs $[f \leftarrow f/\text{pgcd}(f, g)]$, on se reduit à une factorisation

$$g(x)h(x^p) \mid f(x) \mid g(x)^e h(x^p).$$

On envoie le polynôme $g(x)$ en Algorithme **B** et le polynôme $h(x)$ en Algorithme **A** pour extraire la partie sans facteur carré.

Algorithme B. Algorithme pour décomposition d'un polynôme sans facteur carré en produit d'irréductibles de degrés égaux.

Entrée : La donnée d'entrée est un polynôme $f \in \mathbb{F}_p[x]$ sans facteur carré.

Sortie : Les données de sortie consistent des polynômes $g_r \in \mathbb{F}_p[x]$ divisant f , qui sont les produits des diviseurs irréductibles de f du même degré r .

Par conséquent de la forme de f , par le théorème chinois, on a l'isomorphisme :

$$\frac{\mathbb{F}_p[x]}{(f(x))} \cong \prod_{i=1}^t \frac{\mathbb{F}_p[x]}{(p_i(x))}$$

où les polynômes $p_i(x)$ sont irréductibles, donc l'anneau est isomorphe à un produit de corps. Dans cette étape, on fait une factorisation partielle $f = g_1 g_2 \cdots g_d$ tel que les p_i du même degré r sont les diviseurs du polynôme g_r . Il suit que

$$d = \deg(f) = \sum_{r=1}^d \deg(g_r) = \sum_{r=1}^d m_r r.$$

L'algorithme extrait les facteurs de degré r par le pgcd de f avec $x^{p^r} - x$ (pourquoi?). Tout polynôme irréductible de degré r divisent $x^{p^r} - x$ et dans les étapes précédentes on élimines les diviseurs de degrés inférieur. On arrive donc au procédé suivante :

```
def fact_degre_egal(f):
    g = {}
    d = f.degree()
    p = f.parent().base_ring().characteristic()
    for r = range(1,d+1):
        y = power_mod(x,p^r,f)
        g[r] = pgcd(y - x, f); f /= g[r]
        if deg(f) == 0: break
    return g
```

Attention : Il est très important de calculer d'abord le polynôme x^{p^r} modulo f , par une exponentiation rapide (par `power_mod` en Sage), car le degré de $x^{p^r} - x$ est exponentiel en $r \log(p)$. On a donc l'égalité mathématique des l'expression :

$$\text{pgcd}(x^{p^r} - x, f) = \text{pgcd}(y - x, f) \text{ où } y = x^{p^r} \text{ mod } f.$$

bien que computationnellement les deux côtés de l'égalité ne sont pas équivalentes. Évidemment, dans le calcul de $\text{pgcd}(a, b)$ on peut remplacer a ou b par sa réduction modulo l'autre, sans changer le résultat, et en effet, c'est la méthode utilisée pour son calcul.

Exemple. En utilisant l'algorithme précédent, on peut faire une décomposition du polynôme $x^{27} - x$ dans $\mathbb{F}_3[x]$ en polynômes dont les degrés des diviseurs irréductibles sont 1 et 3.

```
sage: p = 3; d = 3
sage: P.<x> = FiniteField(p)[x]
sage: f = x^(p*d) - x
sage: g = fact_degre_egal(f)
sage: for r in g.keys(): print("%s: %s" % (r, g[r]))
1: x^3 + 2*x
2: 1
3: x^24 + x^22 + x^20 + x^18 + x^16 + x^14 + x^12 + x^10 + x^8 + x^6 + x^4 + x^2 + 1
```

Le polynôme g_1 est $x^3 - x = x(x-1)(x+1)$, et le polynôme g_3 de degré 24 est produit de 8 polynômes de degré 3. Par sa construction, on peut factoriser g_1 et g_3 en produits de polynômes cyclotomiques :

$$g_1 = x\Phi_1(x)\Phi_2(x) \text{ et } g_3 = \Phi_{13}(x)\Phi_{26}(x).$$

Les polynômes $\Phi_{13}(x)$ et $\Phi_{26}(x)$ sont de degré 12 et chacun factorise en 4 polynômes irréductibles de degré 3.

Les polynômes g_r sortant de l'algorithme **B** servent comme donnée d'entrée pour l'algorithme **C**, qui complète la factorisation.

Algorithme C. Pour compléter la factorisation, on décrit l'algorithme probabiliste de Cantor-Zassenhaus pour scinder les polynômes qui sont produits de polynômes irréductibles de degrés égaux. On suppose dans la suite que le caractère p est impair.

Entrée : Un polynôme $f(x) = p_1(x) \cdots p_t(x)$, où les polynômes irréductibles p_i sont deux à deux distincts et $\deg(p_i) = r$ (degré r donné), et $t > 1$.

Sortie : Une couple (g_1, g_2) donnant une factorisation $f(x) = g_1(x)g_2(x)$, qui est non triviale avec probabilité $\varepsilon \geq 1/2$.

N.B. Par itération de l'algorithme sur les polynômes g_i de degré $\geq r$, on obtient la liste complète des diviseurs irréductibles $(p_1, \dots, p_t)$.

Idée : Par le théorème chinois,

$$\frac{\mathbb{F}_p[x]}{(f(x))} \cong \frac{\mathbb{F}_p[x]}{(p_1(x))} \times \cdots \times \frac{\mathbb{F}_p[x]}{(p_t(x))} \cong (\mathbb{F}_{p^r})^t,$$

car les polynômes sont irréductibles du même degré. On définit une application donnée par l'exponentiation :

$$N : B = \frac{\mathbb{F}_p[x]}{(f(x))} \longrightarrow \frac{\mathbb{F}_p[x]}{(f(x))}$$

$$\alpha \longmapsto \alpha \cdot \alpha^p \cdots \alpha^{p^{r-1}} = \alpha^{1+p+\cdots+p^{r-1}}$$

et on note l'image directe de N par $A = N(B)$. L'inclusion $A \subset B$ de l'image correspond au sous-anneau $(\mathbb{F}_p)^t \subset (\mathbb{F}_{p^r})^t$, sous l'isomorphisme du théorème chinois. En effet, par l'écriture

$$N(\alpha) = \alpha^{1+p+\dots+p^{r-1}} = \alpha \cdot \alpha^p \dots \alpha^{p^{r-1}}$$

on voit que $\phi(N(\alpha)) = N(\alpha)^p = N(\alpha)$, alors son image dans chaque facteur $\mathbb{F}_{p^r}$ est le sous-corps $\mathbb{F}_p$ fixé par Frobenius.

Une autre manière de montrer la même chose est de considérer le sous-groupe B^* des éléments inversibles. Encore, il suffit de regarder l'image de N restreint à chaque quotient $\mathbb{F}_{p^r}^*$. Ce dernier groupe est cyclique d'ordre $p^r - 1$, dont le sous-groupe $\mathbb{F}_p^*$ est l'unique sous-groupe d'ordre $p - 1$.

Par la factorisation

$$p^r - 1 = (p^{r-1} + \dots + p + 1)(p - 1),$$

on obtient

$$N(\alpha)^{p-1} = \alpha^{(1+p+\dots+p^{r-1})(p-1)} = \alpha^{p^r-1} = 1,$$

alors l'image est dans $\mathbb{F}_p^*$. En effet, si α est un générateur de $\mathbb{F}_{p^r}^*$, d'ordre $p^r - 1$, alors $N(\alpha)$ est un générateur de $\mathbb{F}_p^*$, d'ordre $p - 1$, donc l'application $N : \mathbb{F}_{p^r} \rightarrow \mathbb{F}_p$ est surjective. En conclusion, l'image $A = N(B)$ est isomorphe au produit $(\mathbb{F}_p)^t$. En composant N avec l'application

$$\begin{array}{ccc} \chi : A & \longrightarrow & A \\ a & \longmapsto & a^{(p-1)/2} \end{array}$$

par le même argument on voit que sur chaque projection de A^* à $\mathbb{F}_p^*$, l'application χ induit l'unique surjection $\chi : \mathbb{F}_p^* \rightarrow \{\pm 1\}$. (Cette application s'appelle le caractère de Legendre, et distingue si a est un carré ($\chi(a) = 1$) ou pas ($\chi(a) = -1$)).

En conclusion la composition $\chi \circ N$ est donné par $(\chi \circ N)(\alpha) = \alpha^m$, où

$$m = (1 + \dots + p^{r-1})(p - 1)/2 = (p^r - 1)/2,$$

et qui induit le diagramme des morphismes de groupes :

$$\begin{array}{ccccc} B^* & \xrightarrow{N} & A^* & \xrightarrow{\chi} & U \\ \downarrow \cong & & \downarrow \cong & & \downarrow \cong \\ (\mathbb{F}_{p^r}^*)^t & \longrightarrow & (\mathbb{F}_p^*)^t & \longrightarrow & \{\pm 1\}^t \end{array}$$

où les applications verticales sont données par le théorème chinois. En particulier l'image de $\chi \circ N$ dans B^* est le sous-groupe $U = A^*[2] = B^*[2]$ des éléments d'ordre 2 (ou l'identité).

Algorithme. On choisit $\alpha \in B^* = \mathbb{F}_p[x]/(f(x))^*$ au hasard.

N.B. En pratique on prends un élément α aléatoire dans B , par rapport à une base additive. Si α n'est pas inversible, on découvre une factorisation par le calcul du pgcd(α, f) $\neq 1$. Le nombre d'éléments dans le complément $B \setminus B^*$ est négligible en général.

On calcule $u = \alpha^m = (\chi \circ N)(\alpha) \in B^*[2]$. Si $u = \pm 1$, on retourne au choix de $\alpha \in B^*$. Sinon, le $\text{pgcd}(u - 1, f) = g_1$ est un diviseur non trivial de f . En effet, la factorisation

$$f = \text{pgcd}(u^2 - 1, f) = \text{pgcd}(u - 1, f)\text{pgcd}(u + 1, f) = g_1 g_2,$$

est non triviale car $u \neq \pm 1$. On retourne les diviseurs (g_1, g_2) .

L'application récursive d'algorithme C à tout diviseur non irréductible (de degré $> r$) complète la factorisation en polynômes irréductibles (de degré r).

Remarque. Il suffit d'observer que pour $t > 1$ (f non irréductible), la probabilité de tomber sur un élément $u \in B^*[2] = A^*[2] \cong \{\pm 1\}^t$ différent que ± 1 est

$$\frac{2^t - 2}{2^t} = 1 - \frac{1}{2^{t-1}} > \frac{1}{2},$$

avec égalité si et seulement si $t = 2$.

Conclusion. Un algorithme complet pour factorisation suit de l'application des Algorithmes **A**, **B**, et **C** en succession. Les premiers deux algorithmes sont déterministes, avec complexité polynomiale, et le troisième est probabiliste avec espérance mathématiques de temps de calcul polynomial.

Exercices

1. Soit p un premier et $r \in \mathbb{N}^*$. Montrer que $x^{p^r} - x$ est le produit de tous les polynômes irréductibles de $\mathbb{F}_p[x]$ de degré divisant r .

Indication. On rappelle que

$$x^{p^r} - x = \prod_{\alpha \in \mathbb{F}_{p^r}} (x - \alpha).$$

Or le polynôme minimal de chaque $\alpha \in \mathbb{F}_{p^r}$ est de degré divisant r .

2. Soit $f(x) = x^5 + x + 1 \in \mathbb{F}_3[x]$.
- a. Construire la matrice de l'endomorphisme de Frobenius ϕ , agissant sur l'anneau quotient $A = \mathbb{F}_3[x]/(f(x))$, dans la base $\{1, x, x^2, x^3, x^4\}$.
 - b. Déterminer $\dim_{\mathbb{F}_3}(\ker(\phi - 1))$. Combien de diviseurs irréductibles a-t-il $f(x)$?
 - c. Factoriser $f(x)$.
3. Soit $f(x) = x^4 + x + 1 \in \mathbb{F}_3[x]$ et poser $A = \mathbb{F}_3[x]/(f(x))$.
- a. Factoriser $f(x)$, en notant que 1 est une racine.
 - b. Déterminer la structure de $A^*[2]$.
 - c. Calculer des générateurs de $A^*[2]$ en utilisant le théorème chinois.
4. Soit $f(x) = x^4 + 1 \in \mathbb{F}_3[x]$ et poser $A = \mathbb{F}_3[x]/(f(x))$.
- a. Décrire la forme de la factorisation de $f(x)$, en notant que $f(x) = \Phi_8(x)$.
 - b. Déterminer la structure de $A^*[2]$ (sans factoriser $f(x)$).
 - c. Calculer des générateurs de $A^*[2]$, sachant la forme de la factorisation de $f(x)$.
 - d. Factoriser $f(x)$ à l'aide des éléments de $A^*[2]$.
5. Soit $f(x) = x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \in \mathbb{F}_2[x]$.
- a. Décrire la forme de la factorisation de $f(x)$, en observant que

$$f(x) = (x^9 - 1)/(x - 1).$$

b. Factorization $f(x)$ en utilisant le pcgd avec des polynômes adaptés.

6. Soit $f(x) = x^8 + x^7 + x^5 + x^4 + x^3 + x + 1 = \Phi_{15}(x) \in \mathbb{F}_2[x]$ et poser $A = \mathbb{F}_2[x]/(f(x))$.
- a. Décrire la forme de la factorisation de $f(x)$.
 - b. Pour $i = 0, 1, 2, \dots$, calculer

$$\text{Tr}(x^i) = \sum_{j=0}^3 x^{ip^j} \text{ mod } f(x) \in A.$$

Pour est-ce qu'on obtient le même résultat pour $i = 1, 2, 4, 8 \dots$?

- c. Expliquer pourquoi ces éléments appartient à un sous-anneau $B \cong \mathbb{F}_2 \times \dots \times \mathbb{F}_2$.
- d. En déduire la factorisation de $f(x)$.