Algorithmes pour l'arithmétique II
Cours 4

Julien Lavauzelle

Université Paris 8

Master 2 ACC et CSSD – Algorithmes pour l'arithmétique

15/12/2020

Motivation

Aujourd'hui :

Factorisation de polynômes dans les corps finis

Applications :

- cryptographie : logarithmes discrets
- décodage algébrique
- calcul de racines de polynômes : $X - a \mid P(X) \iff P(a) = 0$
- on peut aussi dériver des tests d'irréductibilité, ...

Plan

Le problème

Définition. Soit $P \in \mathbb{F}_q[X]$ de degré $n \geq 1$. Une factorisation de P en polynômes irréductibles est une écriture

$$P = \alpha \prod_{i=1}^{k} P_i^{m_i}$$

où les $P_i \in \mathbb{F}_q[X]$ sont unitaires et premiers entre eux, $m_i \geq 1$ est la multiplicité du facteur P_i, et $\alpha \in \mathbb{F}_q$ est le coefficient dominant de P.

Cette factorisation est unique à l'ordre près des facteurs.

Remarque. Si $m_i = 1$ pour tout $1 \leq i \leq k$, on dit que P est sans carré (*square-free*).

But : Étant donné un polynôme $P \in \mathbb{F}_q[X]$ de degré n dont une factorisation en polynômes irrédictibles est $\alpha \prod_{i=1}^{k} P_i^{m_i}$, calculer efficacement tous les couples (P_i, m_i).

Mesure de complexité :

- en fonction de la taille de l'entrée $n \log_2 q$,
- en nombre d'opérations élémentaires sur $\mathbb{F}_q$.

La stratégie

Définition. On dit que $Q \in \mathbb{F}_q[X]$ est un diviseur propre de $P \in \mathbb{F}_q[X]$, si Q divise P et si $1 \leq \deg Q \leq \deg P - 1$.

Stratégie. Étant donné $P = \alpha \prod_{i=1}^{k} P_i^{m_i} \in \mathbb{F}_q[X]$:

1. On élimine le scalaire $\alpha \neq 1$ (facile).
2. On élimine la multiplicité dans les facteurs.
3. Lorsque P est sans carré, on cherche **un** diviseur propre Q de P, puis on itère le procédé sur P/Q et Q.

Notation. Dans toute la suite, on note p la caractéristique de $\mathbb{F}_q$.

Plan

Élimination des facteurs carrés

Objectif : calculer efficacement

$$\prod_{i=1}^{k} P_i^{m_i} \quad \longrightarrow \quad \prod_{i=1}^{k} P_i$$

Idée importante : dériver P. On a

$$P'(X) = \sum_{i=1}^{k} m_i P_i' \frac{P}{P_i}$$

Soit $D = \mathrm{pgcd}(P, P')$. Alors D s'écrit

$$D = \prod_{i=1}^{k} P_i^{\ell_i} \quad \text{avec } 0 \leq \ell_i \leq m_i$$

Attention ! On est en caractéristique positive. Donc, on remarque que

- $\ell_i \geq m_i - 1$, car $P_i^{m_i - 1} \mid \frac{P}{P_i}$,
- $p \mid m_i \implies m_i P_i' \frac{P}{P_i} = 0 \implies P_i^{m_i} \mid P' \implies \ell_i = m_i$.

Lemme. En définissant $\delta_i = 0$ si p divise m_i, et $\delta_i = 1$ sinon, on a :

$$D = \mathrm{pgcd}(P, P') = \prod_{i=1}^{k} P_i^{m_i - \delta_i}$$

Élimination des facteurs carrés

Soit $I = \{i \in \{1, \ldots, k\} \mid p \text{ divise } m_i\} = \{i \mid \delta_i = 0\}$. Alors,

$$U := \frac{P}{\operatorname{pgcd}(P, P')} = \prod_{i \notin I} P_i$$

Par ailleurs, si

$$V := \frac{P}{\operatorname{pgcd}(P, U^{\deg P})}$$

alors

$$V = \prod_{i \in I} P_i^{m_i} = \prod_{i \in I} P_i^{m_i} = \left(\prod_{i \in I} P_i^{m_i/p} \right)^p .$$

Conséquence. Si l'on sait calculer une racine p-ième d'un polynôme (en caractéristique p), alors on peut réitérer le procédé sur

$$Q = \prod_{i \in I} P_i^{m_i/p} .$$

Il reste donc à résoudre le problème suivant :

Problème. Étant donné $A(X) = B(X)^p \in \mathbb{F}_q[X]$, calculer $B(X)$.

Extraction de racine p-ème, où $p = \mathrm{char}(\mathbb{F}_q)$

Problème. Étant donné $A(X) = B(X)^p \in \mathbb{F}_q[X]$, calculer $B(X)$.

Soit $B = \sum_{i \in I} b_i X^{d_i}$, alors

$$A = B^p = \sum_{i \in I} b_i^p X^{pd_i}$$

Pour calculer B à partir de $A = \sum_{i \in I} a_i X^{m_i}$, il suffit donc de

1. diviser les exposants m_i par p,
2. calculer une racine p-ème de a_i... pour cela on calcule $a_i^{q/p} = b_i^q = b_i$.

Élimination des facteurs carrés : exemple

Dans $\mathbb{F}_3[X]$, on prend $P(X) = (X+1)^3(X+2)(X^2+1)^4$.

- Lors du premier appel :

$$P = X^{12} + 2\cdot X^{11} + X^{10} + 2\cdot X^8 + X^7 + 2\cdot X^5 + X^4 + 2\cdot X^2 + X + 2$$
$$P' = X^{10} + X^9 + X^7 + X^6 + X^4 + X^3 + X + 1$$
$$D = \mathrm{pgcd}(P, P') = X^9 + X^6 + X^3 + 1$$
$$U = \tfrac{P}{D} = X^3 + 2\cdot X^2 + X + 2$$
$$V = \frac{P}{\mathrm{pgcd}(P, U^{\deg P})} = X^3 + 1$$

  On a donc obtenu une partie de la décomposition en facteurs sans carré :

$$U = (X+2)(X^2+1)$$

  Comme $V \neq 1$, il faut en calculer une racine cubique. On obtient $V = (X+1)^3$.

- On relance l'algorithme avec un nouveau polynôme $P = X + 1$, ce qui donne :

$$P = X + 1$$
$$P' = 1$$
$$D = 1$$

  Comme $D = 1$, $X + 1$ est irréductible et on obtient le dernier facteur $X + 1$.

Plan

Factorisation sans carré : structure de l'anneau quotient

On peut maintenant supposer que $P = \prod_{i=1}^{k} P_i$ où les P_i sont unitaires, irréductibles dans $\mathbb{F}_q[X]$ et distincts. On note $n = \deg P$.

Objectif : calculer efficacement

$$P = \prod_{i=1}^{k} P_i \quad \longrightarrow \quad \text{au moins un diviseur propre de } P$$

Idée : un diviseur de P dans $\mathbb{F}_q[X]$ est un diviseur de 0 dans l'anneau quotient $\mathbb{F}_q[X]/(P)$. On va donc étudier cet anneau.

Lemme. L'anneau quotient $\mathbb{F}_q[X]/(P)$:

1. est aussi un espace vectoriel (donc une $\mathbb{F}_q$-algèbre) de dimension n sur $\mathbb{F}_q$;
2. se décompose comme

$$\mathbb{F}_q[X]/(P) \simeq \Big(\mathbb{F}_q[X]/(P_1)\Big) \times \cdots \times \Big(\mathbb{F}_q[X]/(P_k)\Big)$$

où les $\mathbb{F}_q[X]/(P_i)$ sont des extensions du corps $\mathbb{F}_q$, de degré $\deg P_i$.

Preuve laissée en exercice.

Factorisation sans carré : algèbre de Berlekamp

Soit

$$\begin{array}{rccc} \phi : & \mathbb{F}_q[X]/(P) & \to & \mathbb{F}_q[X]/(P) \\ & A & \mapsto & A^q - A \end{array}$$

et son application induite

$$\tilde{\phi} : \mathbb{F}_q[X]/(P) \to \mathbb{F}_q[X]/(P_1) \times \cdots \times \mathbb{F}_q[X]/(P_k)$$

Question. Que dire de $\ker \phi$?

On a

$$\phi(A) = 0 \iff \forall i,\ A^q \equiv A \mod P_i$$

Dans le **corps** $\mathbb{F}_q[X]/(P_i)$ de cardinal $q^{\deg P_i}$, les solutions de $x^q = x$ sont les éléments du sous-corps $\mathbb{F}_q$.

Donc, $\tilde{\phi}$ s'annule exactement sur les éléments de la forme $(\lambda_1, \ldots, \lambda_k)$ où $\lambda_j \in \mathbb{F}_q$.

Lemme. On a donc

$$\dim \ker \phi = k\,.$$

Remarque. En réalité, $\ker \phi$ est une sous-algèbre de $\mathbb{F}_q[X]/(P)$, appelée algèbre de Berlekamp associée à P.

Factorisation sans carré : théorème de Berlekamp (1)

Une base de $\mathbb{F}_q[X]/(P)$ est $\{1, \alpha, \ldots, \alpha^{n-1}\}$ où $\alpha = [X]$, la classe de X modulo P.

Tout élement $B(\alpha) \in \ker \phi$ peut donc être identifié au polynôme $B \in \mathbb{F}_q[X]$.

On obtient alors le résultat suivant.

Théorème. (Berlekamp) Si $P(X) = \prod_{i=1}^{k} P_i(X)$ est un produit de polynômes irréductibles distincts, et $B(X) \in \mathbb{F}_q[X]$ de degré $< n$ est tel que $B(\alpha) \in \ker \phi$, alors :

$$P(X) = \prod_{\lambda \in \mathbb{F}_q} \operatorname{pgcd}(P(X), B(X) - \lambda)$$

Conséquence directe. Lorsque $k \geq 2$:

- on peut calculer $B \in \mathbb{F}_q[X]$ de degré ≥ 1 tel que $B(\alpha) \in \ker \phi$ (algèbre linéaire)
- en énumérant les $\lambda \in \mathbb{F}_q$, on obtient donc des diviseurs propres de P (comme $\deg B < n$)

On a donc un algorithme pour factoriser P **si l'on peut énumérer** efficacement $\mathbb{F}_q$.

Et sinon ?

Factorisation sans carré : théorème de Berlekamp (2)

Idée : lorsque $\mathbb{F}_q$ est trop grand pour être parcouru exhaustivement, on essaie de regrouper les diviseurs de la forme $\mathrm{pgcd}(P, B - \lambda)$.

Remarquons que pour tout $\beta \in \mathbb{F}_q$:

1. ou bien $\beta = 0$,
2. ou bien β est un carré non-nul dans $\mathbb{F}_q$, auquel cas $\beta^{(q-1)/2} - 1 = 0$,
3. ou bien β est un non-carré dans $\mathbb{F}_q$, auquel cas $\beta^{(q-1)/2} + 1 = 0$.

En considérant $\beta = B \mod P_i$, on peut donc considérer trois ensembles :

1. $I_1 := \{i \in \{1, \ldots, k\} \mid B \bmod P_i = 0\}$,
2. $I_2 := \{i \in \{1, \ldots, k\} \mid B^{(q-1)/2} - 1 \bmod P_i = 0\}$,
3. $I_3 := \{i \in \{1, \ldots, k\} \mid B^{(q-1)/2} + 1 \bmod P_i = 0\}$.

On démontre qu'avec une probabilité $\geq 1/2$ sur le choix de B (en pratique, cette probabilité est proche de 1), deux des ensembles I_1, I_2 et I_3 sont non-vides.

On obtient donc une factorisation non-triviale

$$P = \mathrm{pgcd}(P, B) \times \mathrm{pgcd}(P, B^{(q-1)/2} - 1) \times \mathrm{pgcd}(P, B^{(q-1)/2} + 1)\,.$$

Factorisation sans carré : théorème de Berlekamp (3)

Théorème. (Berlekamp) Si $P(X) = \prod_{i=1}^{k} P_i(X)$ est un produit de polynômes irréductible distincts, et $B(X) \in \mathbb{F}_q[X]$ de degré $< n$ est tel que $B(\alpha) \in \ker \phi$, alors :

$$P(X) = \prod_{\lambda \in \mathbb{F}_q} \operatorname{pgcd}(P(X), B(X) - \lambda)$$

Preuve.
L'élément $B(\alpha) \in \ker \phi$ s'écrit $(\beta_1, \ldots, \beta_k)$ dans $\mathbb{F}_q[X]/(P_1) \times \cdots \times \mathbb{F}_q[X]/(P_k)$.

Comme $B(\alpha) \in \ker \phi$, on a $\beta_i \in \mathbb{F}_q$ pour tout i, et $P_i(X)$ divise $B(X) - \beta_i$ dans $\mathbb{F}_q[X]$.

Pour $\lambda \in \mathbb{F}_q$, si l'on note $D_\lambda = \operatorname{pgcd}(P, B - \lambda)$, on remarque que

$$P_i \mid D_\lambda \iff \beta_i = \lambda$$

En effet :

- Si $\lambda = \beta_i$, alors P_i divise $B - \beta_i = B - \lambda$ donc divise aussi D_λ.
- Si P_i divise D_λ, alors P_i divise $B - \lambda$, puis $\beta_i = B \bmod P_i = \lambda$.

On en déduit :

$$D_\lambda = \prod_{i \mid \beta_i = \lambda} P_i \quad \text{puis} \quad P = \prod_{\lambda \in \mathbb{F}_q} D_\lambda \,.$$

Algorithme de Berlekamp pour $q = O(n^d)$, d petit

ALGORITHME DE BERLEKAMP EN PETITE CARDINALITÉ

Entrée : un polynôme $P = \prod_{i=1}^{k} P_i$ sans facteur carré
Sortie : un diviseur propre Q de P

1. Calculer la matrice $\boldsymbol{M}$ de ϕ dans la base polynomiale $(1, \alpha, \ldots, \alpha^{n-1})$.
2. Calculer un élément $(b_0 = 0, \ldots, b_{n-1})$ du noyau de $\boldsymbol{M}$ tel que $b_j \neq 0$ pour au moins un $j \geq 1$.
3. Construire $B(X) = \sum_{j=0}^{n-1} b_j X^j$
4. **Faire :**
   - Choisir un nouveau $\lambda \in \mathbb{F}_q$ — déterministe (énumération) ou probabiliste.
   - Calculer $Q(X) = \mathrm{pgcd}(P(X), B(X) - \lambda)$.

   tant que $Q(X) = 1$.
5. Retourner Q.

Complexité : en pire cas

- $O(n^2)$ pour le calcul de $\boldsymbol{M}$,
- $O(n^3)$ op. sur $\mathbb{F}_q$ pour le calcul de $\boldsymbol{b}$,
- pour chaque λ (au plus q fois) : $O(n^2)$ op. sur $\mathbb{F}_q$ pour le pgcd

Au **total** : $O(qn^2 + n^3) = O(n^{\max\{3, d+2\}})$ si $q = O(n^d)$.

Exemple

On reprend l'exemple précédent ($q = 3$, $P = (X+1)^3(X+2)(X^2+1)^4$), où l'on avait trouvé la partie sans carré $Q = (X+1)(X+2)(X^2+1) = X^4 + 2$.

On calcule la matrice des $X^{3i} - X^i \bmod Q$ dans la base $(1, X, X^2, X^3)$:

$$\boldsymbol{M} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 2 \end{pmatrix}$$

On calcule un $B \in \ker \boldsymbol{M}$ aléatoire, disons $B(X) = X^2 + 2$. On obtient :

λ	$D_\lambda = \mathrm{pgcd}(Q, B - \lambda)$
0	$X^2 + 2$
1	$X^2 + 1$
2	1

On a trouvé deux diviseurs propres de Q : $X^2 + 2$ et $X^2 + 1$.
On appelle récursivement l'algorithme sur ces deux polynômes ...

Algorithme de Berlekamp pour $q = \Omega(n^d)$ et d petit

Algorithme de Berlekamp en grande cardinalité ($p \neq 2$)

Entrée : un polynôme $P = \prod_{i=1}^{k} P_i$ sans facteur carré
Sortie : au moins deux diviseurs propres de P

1. Calculer la matrice $\boldsymbol{M}$ de ϕ dans la base polynomiale $(1, \alpha, \ldots, \alpha^{n-1})$.
2. **Faire :**
   - Calculer un aléatoirement un élément $(b_0 = 0, \ldots, b_{n-1})$ du noyau de $\boldsymbol{M}$ tel que $b_j \neq 0$ pour au moins un $j \geq 1$.
   - Construire $B(X) = \sum_{j=0}^{n-1} b_j X^j$.
   - Calculer $B^{(q-1)/2} - 1 \bmod P$ et $B^{(q-1)/2} + 1 \bmod P$.
   - Calculer $A_0 = \mathrm{pgcd}(P, B)$, $A_1 = \mathrm{pgcd}(P, B^{(q-1)/2} - 1)$ et $A_2 = \mathrm{pgcd}(P, B^{(q-1)/2} + 1)$.

   tant que l'un des A_i vaut P.
3. Retourner les A_i différents de 1.

Complexité : en moyenne

- $O(n^2)$ pour le calcul de $\boldsymbol{M}$,
- pour chaque choix de B (en moyenne un nombre constant de fois) : $O(n^3)$ op. sur $\mathbb{F}_q$ pour le calcul de $\boldsymbol{b}$, $O(n^2 \log_2 q)$ op. sur $\mathbb{F}_q$ pour les puissances de B modulo P, et $O(n^2)$ op. sur $\mathbb{F}_q$ pour le pgcd.

Au **total** : $O(n^3 + n^2 \log_2 q)$

Plan

Idée générale

On reprend :

Objectif : calculer efficacement

$$P = \prod_{i=1}^{k} P_i \quad \longrightarrow \quad \text{au moins un diviseur propre de } P$$

Stratégie :

1. *Factorisation en degrés distincts.* On factorise $P = Q_1 \times \cdots \times Q_d$, où Q_r est le produit de tous les facteurs P_i de degré r.
2. *Factorisation à degrés égaux.* Pour tout r tel que Q_r est non-irréductible, on calcule des diviseurs propres de Q_r.

Factorisation en degré distincts

Objectif : calculer efficacement, pour tout r,

$$P = \prod_{i=1}^{k} P_i \quad \longrightarrow \quad Q_r := \prod_{i \mid \deg P_i = r} P_i$$

Théorème. Soit $r \geq 1$. On note $\mathcal{P}_r \subset \mathbb{F}_q[X]$ l'ensemble des polynômes irréductibles dont le degré divise r. Alors on a :

$$X^{q^r} - X = \prod_{A \in \mathcal{P}_r} A(X)\,.$$

Preuve. En TD.

Question. Pour $r \geq 1$, comment utiliser ce résultat pour calculer Q_r à partir de P ?

On a :

$$\operatorname{pgcd}(P(X), X^{q^r} - X) = \prod_{A \in \mathcal{P}_r \text{ et } A \text{ divise } P} A = \prod_{d \mid r} Q_r(X)\,.$$

Factorisation en degré distincts : algorithme

ALGORITHME DE FACTORISATION EN DEGRÉ DISTINCTS

Entrée : $P \in \mathbb{F}_q[X]$
Sortie : la factorisation $P = Q_1 Q_2 \dots Q_s$ où Q_r est le produit de tous les diviseurs de P irréductibles et de degré r

1. Poser $Q \leftarrow P$, $S \leftarrow X$, et $i \leftarrow 1$
2. **Tant que** $Q \neq 1$
   - 2.1 Calculer $S \leftarrow S^q \mod P$
   - 2.2 Calculer $Q_i \leftarrow \text{pgcd}(Q, S - X)$
   - 2.3 Calculer $Q \leftarrow Q/Q_i$
   - 2.4 Incrémenter i
3. Retourner $Q_1, \dots, Q_{i-1}$.

Explication.

- À la fin du i-ème tour de boucle, le polynôme Q ne contient plus de diviseurs irréductibles de degré $\leq i$.
- Donc, dans le $(i+1)$-ème tour de boucle, Q_{i+1} est bien formé du produit des polynômes irréductibles divisant P et de degré **exactement** $i+1$.

Factorisation en degré distincts : exemple

Dans $\mathbb{F}_3[X]$, on prend

$$\begin{aligned} P(X) &= (X+1)(X^2+1)(X^2+2X+2)(X^3+X^2+2) \\ &= X^8+X^7+2\cdot X^6+X^3+2\cdot X+1 \end{aligned}$$

L'algorithme se déroule comme suit :

Q	$S-X$	Q_i
$X^8+X^7+2\cdot X^6+X^3+2\cdot X+1$	X^3-X	$X+1$
$X^7+2\cdot X^5+X^4+2\cdot X^3+2\cdot X^2+X+1$	X^9-X	$X^4+2\cdot X^3+2\cdot X+2$
X^3+X^2+2	$X^{27}-X$	X^3+X^2+2
1		

Factorisation à degré égal

ALGORITHME DE CANTOR-ZASSENHAUS : FACTORISATION À DEGRÉ ÉGAL

Entrée : $Q \in \mathbb{F}_q[X]$ un polynôme de degré $n = sr$, formé de s polynômes irréductibles $P_1, \ldots, P_s$, distincts de degré r
Sortie : des diviseurs propres de Q

1. **Faire :**
   - 1.1 Tirer uniformément $A(X)$ un polynôme non-nul de degré $\leq n-1$.
   - 1.2 Calculer $D_0 = \text{pgcd}(A, Q)$.
   - 1.3 Calculer $S = A^{(q^r-1)/2} \bmod Q$.
   - 1.4 Calculer $D_1 = \text{pgcd}(A-1, Q)$.

   tant que D_0 ou D_1 n'est pas un diviseur propre de Q.
2. Retourner les diviseurs propres obtenus parmi $Q/D_0, D_0, Q/D_1, D_1$

Factorisation à degré égal : explication

1. **Faire :**
   1.1 Tirer uniformément $A(X)$ un polynôme non-nul de degré $\leq n-1$.
   1.2 Calculer $D_0 = \mathrm{pgcd}(A, Q)$.
   1.3 Calculer $S = A^{(q-1)/2} \bmod Q$.
   1.4 Calculer $D_1 = \mathrm{pgcd}(S-1, Q)$.

   tant que D_0 ou D_1 n'est pas un diviseur propre de Q.
2. Retourner les diviseurs propres obtenus parmi $Q/D_0, D_0, Q/D_1, D_1$

Éléments de preuve.

- Si D_0 est un diviseur propre de Q, alors on retourne bien D_0 et Q/D_0.
- Sinon, cela signifie que A et premier avec Q, donc A est premier avec tous les P_j. Alors, on reprend $\mathbb{F}_q[X]/(Q) \simeq \left(\mathbb{F}_q[X]/(P_1)\right) \times \cdots \times \left(\mathbb{F}_q[X]/(P_s)\right)$ et
  - tous les $\mathbb{F}_q[X]/(P_j)$ sont des corps finis de même cardinal q^r,
  - comme A a été tiré uniformément dans $\mathbb{F}_q[X]/(Q)$, les éléments $a_j := A \bmod P_j$ sont des scalaires tirés uniformément dans $\mathbb{F}_{q^r} \setminus \{0\}$,
  - donc, les composantes du vecteur $(a_1^{(q^r-1)/2}, \ldots, a_s^{(q^r-1)/2})$ sont tirées uniformément dans $\{-1, 1\}$
  - donc, avec probabilité $\geq 1 - \frac{1}{2^{s-1}}$, ce vecteur n'est ni $(1, \ldots, 1)$, ni $(-1, \ldots, -1)$
  - l'image réciproque de $(a_1^{(q^r-1)/2} - 1, \ldots, a_s^{(q^r-1)/2} - 1)$, qui contient donc une composante nulle, forme un diviseur propre de Q

Exemple

Dans $\mathbb{F}_3[X]$, soit $P(X) = (X^3 + 2 \cdot X^2 + 2 \cdot X + 2)(X^3 + 2 \cdot X + 2)(X^3 + 2 \cdot X^2 + 1)$.

1. **1er appel :** avec P
   on a choisi aléatoirement $A = X^8 + X^6 + X^5 + X^4 + X^3 + X^2 + 2X + 1$
   on obtient la liste $[X^3 + 2X^2 + 1, X^6 + 2X^5 + X^4 + 2X^3 + 2X^2 + 2X + 1, 1, X^9 + X^8 + 2X^7 + 2X^6 + 2X^5 + X^4 + X^3 + X^2 + 2X + 1]$
   $\rightarrow$ on a 2 diviseurs propres (les deux premiers éléments)
2. **2nd appel :** avec $X^6 + 2X^5 + X^4 + 2X^3 + 2X^2 + 2X + 1$
   on a choisi aléatoirement $A = 2X^5 + 2X^3 + 2X + 1$
   on obtient la liste
   $[1, X^6 + 2X^5 + X^4 + 2X^3 + 2X^2 + 2X + 1, 1, X^6 + 2X^5 + X^4 + 2X^3 + 2X^2 + 2X + 1]$
   $\rightarrow$ échec
   on a choisi aléatoirement $A = X + 2$
   on obtient la liste
   $[1, X^6 + 2X^5 + X^4 + 2X^3 + 2X^2 + 2X + 1, 1, X^6 + 2X^5 + X^4 + 2X^3 + 2X^2 + 2X + 1]$
   $\rightarrow$ échec
   on a choisi aléatoirement $A = X^5 + 2X^4 + X^3 + X + 1$
   on obtient la liste
   $[X^3 + 2X^2 + 2X + 2, X^3 + 2X + 2, 1, X^6 + 2X^5 + X^4 + 2X^3 + 2X^2 + 2X + 1]$
   $\rightarrow$ on a 2 diviseurs propres

Plan

Exercice 1

Exercice 1. On souhaite démontrer le résultat suivant.

Lemme. Soit $P \in \mathbb{F}_q[X]$ irréductible. Alors, pour tout $\ell \geq 1$,

$$P \text{ divise } X^{q^\ell} - X \iff \deg P \text{ divise } \ell\,.$$

Soit $P \in \mathbb{F}_q[X]$ irréductible.

Question 1. Supposons que $\ell \mid d$ dans $\mathbb{Z}$. Démontrer que $q^\ell - 1$ divise $q^d - 1$.

Question 2. Démontrer que si $\deg P$ divise ℓ, alors P divise $X^{q^\ell} - X$.

Question 3. Démontrer que, pour tout polynôme $B(X) \in \mathbb{F}_q[X]$, on a $B(X)^{q^{\deg P}} \equiv B(X) \mod P$.

Question 4. En effectuant une division euclidienne de ℓ par $\deg P$, conclure.

Exercice 1

Soit $P \in \mathbb{F}_q[X]$ irréductible.

Question 1. Supposons que $d \mid \ell$ dans $\mathbb{Z}$. Démontrer que $q^d - 1$ divise $q^\ell - 1$.

Question 2. Démontrer que si $\deg P$ divise ℓ, alors P divise $X^{q^\ell} - X$.

Réponse 1. Si l'on note $\ell = dt$, alors on a

$$q^\ell - 1 = q^{dt} - 1 = \left(q^d - 1\right)\left(1 + q^d + (q^d)^2 + \cdots + (q^d)^{t-1}\right)$$

Réponse 2. Notons $d = \deg P$. Alors $\mathbb{F}_q[X]/(P)$ est un corps de cardinal q^d.
Donc la classe de X modulo P, notée α, vérifie

$$\alpha^{q^d - 1} = 1.$$

On a donc $\alpha^{q^\ell - 1} = \alpha^{k(q^d-1)} = 1^k = 1$. C'est-à-dire :

$$X^{q^\ell} \equiv X \mod P$$

Question 3. Démontrer que, pour tout polynôme $B(X) \in \mathbb{F}_q[X]$, on a

$$B(X)^{q^{\deg P}} \equiv B(X) \mod P\,.$$

Réponse 3. Si $B(X) = \sum_{i=0}^{m} b_i X^i$, alors on a :

$$B(X)^q = \sum_{i=0}^{m} b_i^q X^{iq} = \sum_{i=0}^{m} b_i X^{iq} \quad \text{car } b_i \in \mathbb{F}_q\,.$$

Notons $d = \deg P$. On a donc

$$B(X)^{q^d} = \sum_{i=0}^{m} b_i (X^{q^d})^i \equiv \sum_{i=0}^{m} b_i X^i \equiv B(X) \mod P$$

Exercice 1

Exercice 1. On souhaite démontrer le résultat suivant.

Lemme. Soit $P \in \mathbb{F}_q[X]$ irréductible. Alors, pour tout $\ell \geq 1$,

$$P \text{ divise } X^{q^\ell} - X \iff \deg P \text{ divise } \ell\,.$$

Question 4. En effectuant une division euclidienne de ℓ par $\deg P$, conclure.

Réponse 4. Supposons que $P(X)$ divise $X^{q^\ell} - X$. On vérifie alors (comme à la question précédente) que pour tout $B \in \mathbb{F}_q[X]$, on a $B(X)^{q^\ell} \equiv B(X) \mod P$.

Comme $\mathbb{F}_q[X]/(P)$ est un corps, on a donc $B(X)^{q^\ell - 1} \equiv 1 \mod P$.

Pour $d = \deg P$, on écrit ensuite $\ell = du + r$. Montrons que $r = 0$.

On a

$$q^\ell - 1 = q^{du+r} - 1 = (q^{du} - 1)q^r + q^r - 1$$

On sait que $q^d - 1$ divise $q^{du} - 1$ (cf. **Q1.**). Pour tout $B(X) \in \mathbb{F}_q[X]/(P)$, on a donc

$$1 \equiv B(X)^{q^\ell - 1} \equiv \underbrace{B(X)^{(q^{du}-1)q^r}}_{\equiv 1} B(X)^{q^r - 1} \equiv B(X)^{q^r - 1} \mod P$$

Si $r \neq 0$, tout élément non-nul de $\mathbb{F}_q[X]/(P)$ est solution de l'équation $Y^{q^r - 1} - 1$ qui admet au plus $q^r - 1$ solutions. C'est impossible, donc $r = 0$.

Exercice 2

Lors du dernier exercice, on a démontré :

Lemme. Soit $P \in \mathbb{F}_q[X]$ irréductible. Alors, pour tout $\ell \geq 1$,

$$P \text{ divise } X^{q^\ell} - X \iff \deg P \text{ divise } \ell\,.$$

Exercice 2. Soit $P(X) = X^{q^n} - X \in \mathbb{F}_q[X]$.

Question 1. Calculer $P'(X)$. Le polynôme $P(X)$ contient-il des facteurs carrés ?

Question 2. Démontrer le résultat suivant :

Lemme. Le polynôme $P(X) = X^{q^n} - X$ est le produit de tous les polynômes irréductibles dont le degré divise n.

Réponse 1. $P'(X) = q^n X^{q^n-1} - 1 = -1$ dans $\mathbb{F}_q[X]$.

Si $P = R^2 S$, alors $P' = 2RR'S + R^2 S' = R(2R'S + RS')$. Autrement dit R divise $P' = -1$. Donc, R n'est pas un facteur propre.

Réponse 2. D'après le lemme de l'**Exercice 1.**, tout polynôme irréductible apparaît dans la factorisation de $X^{q^n} - X$. D'après la **Q1.**, il n'y apparaît qu'une seule fois.

Exercice 3

Lors du dernier exercice, on a démontré :

Lemme. Le polynôme $P(X) = X^{q^n} - X$ est le produit de tous les polynômes irréductibles dont le degré divise n.

Exercice.

Question 1. Démontrer le lemme suivant

Lemme. Soit $P(X) \in \mathbb{F}_q[X]$ de degré d. Le polynôme P est irréductible si et seulement si les deux conditions suivantes sont satisfaites :

1. P divise $X^{q^d} - X$,
2. pour tout r diviseur strict de d, les polynômes P et $X^{q^r} - X$ sont premiers entre eux.

Question 2. En déduire un algorithme de test d'irréductibilité, et calculer sa complexité.