Option C : Factorisation des polynômes sur $\mathbb{F}_p$

cours du 20 octobre 2020

D. Kohel

Factorisation des polynômes (et entiers)

Objectif : Montrer qu'il existe un algorithme probabiliste pour la factorisation dans $\mathbb{F}_p[X]$ avec complexité polynôme (= espérance mathématique) sur $\mathbb{F}_p$

Idée : Utiliser la structure du groupe $(\mathbb{F}_p[X]/(f(X)))^*$ des unités. En particulier, on veut produire des éléments a tel que $a^2 = 1$. On dit des éléments de 2-torsion.

Rappel Pour un groupe G, on écrit $G[\ell] = \{x \in G \mid x^\ell = e\}$.

Théorème. Soit $\mathbb{F}_q$ un corps fini. Alors $\mathbb{F}_q^* \simeq (\mathbb{Z}/(q-1)\mathbb{Z}, +)$.

Preuve. Idée : un groupe abélien fini G est cyclique ssi $G[\ell]$ est cyclique pour tout ℓ premier, $\ell \mid |G|$.

Pour le groupe $G = \mathbb{F}_q^*$, on utilise 2 le fait que

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

car γ est une racine de $x^\ell - 1$, et tout racine γ est dans $G[\ell]$. Or $\deg(x^\ell - 1) = \ell = |G[\ell]|$, donc $G[\ell]$ est cyclique (ℓ premier), $t = 1$. $\mathrm{IIS}\ (\mathbb{Z}/\ell\mathbb{Z})^t$

Problème de factorisation :

(i) $f(x) \in \mathbb{F}_p[x]$ $\quad \mathbb{F}_p[x]/(f(x)) \simeq \prod \mathbb{F}_p[x]/(p_i(x)^{e_i})$

(ii) $N \in \mathbb{Z}$ $\quad \mathbb{Z}/N\mathbb{Z} \simeq \prod \mathbb{Z}/(p_i^{e_i}\mathbb{Z})$.

par le théorème chinois.

(i) $\left|\left(\mathbb{F}_p[x]/(f(x))\right)^*\right| = \prod (p^{d_i} - 1)\, p^{d_i(e_i - 1)}$

où $d_i = \deg(p_i(x))$.

en effet $\left(\frac{\mathbb{F}_p[x]}{p_i(x)^{e_i}}\right)^* = \frac{\mathbb{F}_p[x]}{(p_i(x)^{e_i})} \setminus \frac{p_i(x)\mathbb{F}_p[x]}{(p_i(x)^{e_i})}$

$\ast\ p^{d_i e_i} - p^{d_i(e_i - 1)}$

Attention. Les ordres possibles sont dans une liste finie.

(ii) $\left|(\mathbb{Z}/N\mathbb{Z})^*\right| = \prod \left|(\mathbb{Z}/p_i^{e_i}\mathbb{Z})^*\right|$

$= \prod (p_i^{e_i} - p^{e_i-1}) = \prod (p_i - 1) p^{e_i - 1}$.

Si on suppose que $\qquad =: \varphi(N)$

$f(x)$ et N sont sans facteur carré,

càd que $e_i = 1$ pour tout i, on a

$$\left|\left(\mathbb{F}_p[x]/(f(x))\right)^*\right| = \prod (p^{d_i} - 1), \quad \left|(\mathbb{Z}/N\mathbb{Z})^*\right| = \prod (p_i - 1)$$

(i) (ii)

Les nombres (i) sont discrets (p fixé) :

$p-1, p^2-1, p^3-1, \ldots, p^d - 1$ ($d = \deg(f)$)

Les nombres (ii) sont inconnus,

car il y a $\sim \frac{N}{\log(N)}$ premiers inférieurs à N.

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

A) Algorithme pour décomposition en polynôme(s) sans facteur carré

B) Algorithme pour décomposition en produit d'irreductibles de degrés égaux

C) Algorithme pour la décomposition complète (des produits d'irreductibles distincts de degrés égaux)

Algorithme A

Donnés : $f(x) \in \mathbb{F}_p[x]$

Donnés de sortie : $g(x), h(x)$ tels que

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

avec $g(x)$ sans facteur carré.

N.B. $g(x)$ passe en Algo B, $h(x)$ en Algo A

Algo A

On suppose que $f(x) = \prod p_i(x)^{e_i}$.

On calcule

$$r(x) = \text{pgcd}(f, f').$$

On note que :

$$f'(x) = \sum_{i=1}^{t} e_i \frac{f(x)}{p_i(x)} \cdot p_i'(x),$$

alors

$$r(x) = \left(\prod_{i=1}^{t} p_i(x)^{e_i - 1}\right) \prod_{p \mid e_i} p_i$$

$$= \left(\prod_{p \nmid e_i} p_i^{e_i - 1}\right)\left(\prod_{p \mid e_i} p_i^{e_i}\right)$$

car $\text{pgcd}(p_i(x), p_i'(x)) = 1$.

On pose $g(x) = \dfrac{f(x)}{r(x)} = \prod_{e_i \nmid p} p_i$

Pour $h(x)$, on pose $h(x) = r(x)$,

et pendant que $\text{pgcd}(h(x), g(x)) \neq 1$,

on remplace $h(x)$ avec

$$h(x) / \text{pgcd}(h(x), g(x))$$

Alors $h(x) = h_0(x)^p = h_0(x^p)$.

$\exists h_0(x) \in \mathbb{F}_p[x]$

Résumé : On retourne $g(x)$, $h_0(x)$;
$g(x)$ est sans facteur carré $\Rightarrow$ Algo B
$h_0(x)$ n'a pas de contrainte $\Rightarrow$ Algo A.

Algorithme B.

Donnés d'entrée : $f(x)$ sans facteurs carré.

Donc :

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

Donnés de sortie : pour $r = 1, \ldots,$
un polynôme $g_r(x) \mid f(x)$ $\deg f(x) = d$
tel que tous les diviseurs irreds
de $g_r(x)$ sont de degré r.

Avec $f(x) = g_1(x)\, g_2(x) \cdots g_d(x)$.

N.B. On a

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

Algo B

for r = 1 à d :

$g_r(x) = \text{pgcd}(x^{p^r} - x, f(x))$ (*)

$f(x) = f(x) / g_r(x)$ (**)

if $\deg(f(x)) = 0$:

break

Remarque. On note que $x^{p^r} - x$ est le produit dans $\mathbb{F}_p[x]$ de tous les polynômes irreductibles de degré divisant r. Alors

(*) = l'extraction des facteurs de $f(x)$ qui sont produits de polynômes irreds de degré divisant r

(**) mais on a déjà éliminé les diviseurs de degré inferieur à r.

Par conséquent, l'algorithme est correct ($g_r(x)$ = produit des polynômes irreds de degré r divisant $f(x)$).

Remarque: Calcul du $\gcd(x^{p^r}-x, f)$.
Le dégré de $x^{p^r}-x$ est énorme.
Naïvement on va exploser le temps de calcul avec le pgcd.
On note que

$$\gcd(x^{p^r}-x, f) = \gcd((x^{p^r}-x) \bmod f, f)$$

et on peut calculer

$$(x^{p^r}-x) \bmod f = (x^{p^r} \bmod f) - x$$

Le calcul de $x^{p^r} \bmod f$ est une exponentiation modulaire.
On peut le faire avec complexité $(r \log p)$ multiplications dans $\mathbb{F}_p[x]/(f(x))$.

donc avec complexité dans

$$O(r\log(p)\cdot d^2\log(p)^2) \subseteq O(d^3\log(p)^3)$$

↑ mult naïve dans $\mathbb{F}_p[x]/(f(x))$

À la sortie de l'algorithme, on envoie $g_1(x), \dots, g_d(x)$ (plusieurs égals à 1) en Algo C.

Algorithme C.

Donnés : $f(x) = p_1(x)\cdots p_t(x)$, $\deg p_i = r$.

N.B. On suppose que r est donné.

Sortie : $(p_1, \dots, p_t)$.

Idée : Par le théorème chinois

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

L'application $N : \frac{\mathbb{F}_p[x]}{(f(x))} \longrightarrow \frac{\mathbb{F}_p[x]}{(f(x))}$ donné par

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

a image dans $(\mathbb{F}_p)^t \subseteq (\mathbb{F}_{p^r})^t$ sous l'application du théorème chinois :

$$\begin{array}{ccc} B = \dfrac{\mathbb{F}_p[x]}{(f(x))} & \xrightarrow{\cong} & (\mathbb{F}_{p^r})^t \\ \downarrow N & & \downarrow N \\ \mathrm{Im}(N) = A & \xrightarrow{\cong} & (\mathbb{F}_p)^t \\ \cap & & \cap \\ B & & (\mathbb{F}_{p^r})^t \end{array}$$

<u>Preuve</u> : On note que $N : (\mathbb{F}_{p^r})^t \longrightarrow (\mathbb{F}_{p^r})^t$ est définie par $(\alpha_1, \dots, \alpha_t) \longmapsto (N(\alpha_1), \dots, N(\alpha_t))$, où

$$\begin{array}{ccc} N : \mathbb{F}_{p^r} & \longrightarrow & \mathbb{F}_{p^r} \\ \alpha & \longmapsto & \alpha^{(1+\dots+p^{r-1})} \end{array}$$

Pour montrer que l'image est dans $\mathbb{F}_p$ il suffit de noter que N est multiplicative $N(\alpha\beta) = N(\alpha)N(\beta)$, alors elle induit un homomorphisme

$N : \mathbb{F}_{p^r}^* \longrightarrow \mathbb{F}_{p^r}^*$.

Comme $\mathbb{F}_{p^r}^*$ est un groupe cyclique, le sous-groupe $\mathbb{F}_p^*$ est l'unique sous-groupe (cyclique) d'ordre $p-1$ $(= \mathbb{F}_{p^r}^*[p-1])$.

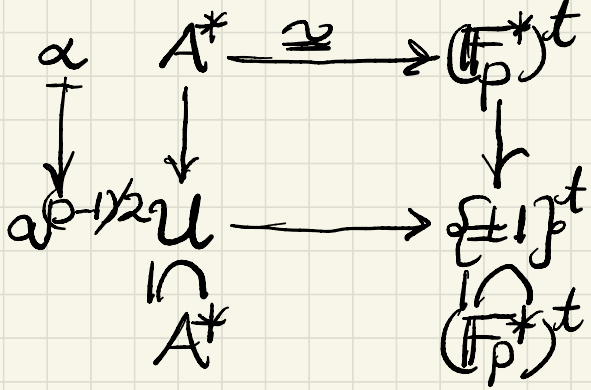
Mais
$$N(\alpha)^{p-1} = \alpha^{(1+\cdots+p^{r-1})(p-1)}$$
$$= \alpha^{p^r-1} = 1,$$
alors l'image est dans $\mathbb{F}_p^*$.

N.B. On peut le montrer autrement, en observant que
$$\mathbb{F}_p^* = \{\beta \in \mathbb{F}_{p^r}^* \mid \beta^p = \beta\}.$$
Il suffit de montrer que $N(\alpha)^p = N(\alpha)$, en utilisant la forme :
$$(\alpha \cdot \alpha^p \cdot \cdots \cdot \alpha^{p^{r-1}})^p = \alpha^p \cdot \alpha^{p^2} \cdots \alpha^{p^r},$$
notant que $\alpha^{p^r} = \alpha$.

Ensuite on va composer N avec l'application (aussi homomorphisme de groupe) $A \longrightarrow A$

$$\alpha \longmapsto \alpha^{(p-1)/2}$$

qui envoie tout α à un élément γ tel que $\gamma^2 = 1$. À droite du théorème chinois :



l'image U correspond à $\{\pm 1\}^t$.

En conclusion, exponentiation par $m = (1 + \cdots + p^{r-1})(p-1)/2$

$= (p^r - 1)/2$ ∈ composition des deux homomorphismes donne une application surjectif $B^* \longrightarrow B^*[2] \simeq \{\pm 1\}^t$.

Algo C

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

N.B. Aléatoire dans $\mathbb{F}_p[x]/(f(x))$, mais si α n'est pas inversible, on découvre une factorisation par le $\text{pgcd}(\alpha, f) \neq 1$.

On calcule $r = \alpha^m = N(\alpha)^{(p-1)/2} \in B^*[2]$.

Si $r = 1$ ou -1, on retourne au choix de $\alpha \in B^*$.

Sinon, $\text{pgcd}(r-1, f) = g \neq 1, \neq f$.

En effet

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

mais par hypothèse ($r \neq \pm 1$), cette factorisation est non triviale. On répète l'algo C

avec les facteurs

$\gcd(T-1, f)$ et $\gcd(T+1, f)$

jusqu'à déterminer tous le diviseurs irreds (de degré r).

<u>Conclusion</u>. On a décrit un algo en temps polynôme

Algo A, Algo B } déterministe

Algo C } probabiliste

Il suffit d'observer que pour $t>1$, la probabilité de tomber sur un élément $\gamma \in B^*[2] = A^*[2] \cong \{\pm 1\}^t$ different que ± 1

$(\pm 1 \mapsto \{(1,\dots,1),(-1,\dots,-1)\} \subseteq \{\pm 1\}^t)$

est $\frac{2^t-2}{2^t} = 1 - \frac{1}{2^{t-1}} \geq \frac{1}{2}$ (égalité si $t=2$).