Leçon 142 : PGCD, PPCM : Algorithme de calcul. Applications
Trinôme G : Anaïs WIDMER, Corentin FAIPEUR, Pierre-Jules BIENAYMÉ
Références : Perrin, Saux-Picart, Objectif Agreg, Hardy et Wright (Algo. fondamentaux)

On se place dans un anneau $A \neq \{0\}$ commutatif, unitaire et intègre.

I. Introduction à la notion de PGCD et PPCM

1. Divisibilité

déf 1 : L'ensemble des inversibles de A est $A^* = \{a \in A, \exists b \in A, ab = 1\}$

Ex 2 : A corps $\Rightarrow A^* = A \setminus \{0\}$; $\mathbb{Z}^* = \{\pm 1\}$

déf 3 : $a, b \in A$, $a | b \Leftrightarrow \exists c \in A$, $b = ac$

Prop 4 : $a, b \in A$, $a | b$ et $b | a \Leftrightarrow \exists u \in A^*$, $a = ub$.
Dans ce cas, on note $a \sim b$, et cela définit une relation d'équivalence.

déf 5 : Soit $p \in A$, p est irréductible si et seulement si $p \notin A^*$ et $(p = ab \Rightarrow a \in A^*$ ou $b \in A^*)$

Ex 6 : dans $\mathbb{Z}$, les irréductibles sont les nombres premiers

déf 7 : a et b sont premiers entre eux si $\forall d \in A$, $\begin{cases} d | a \\ d | b \end{cases} \Rightarrow d \in A^*$

2. Définition de PGCD, PPCM, dans un anneau factoriel.

déf 8 : L'anneau A est factoriel si :
$\forall a \in A \setminus \{0\}$, a s'écrit sous la forme $a = u \prod_{p \in \mathcal{P}} p^{v_p(a)}$, avec $u \in A^*$, $v_p(a) \in \mathbb{N}$ (tel que les $v_p(a)$ sont presque tous nuls), et $\mathcal{P}$ un système de représentants des irréductibles de A pour $\sim$.
De plus, cette écriture est unique.

Ex 9 : $\mathbb{Z}$ et $\mathbb{Z}[X]$ factoriels

Rq 10 : $a | b \Rightarrow v_p(a) \leq v_p(b)$, $\forall p \in \mathcal{P}$

Prop 11 (lemme d'Euclide) : Si p irréductible et p divise ab, alors p divise a ou b.

Prop 12 (théorème de Gauß) : si a divise bc, et a premier avec b, alors a divise c.

Rq 13 : les prop. 11 et 12 sont équivalentes à l'unicité de la décomposition est facteurs irréductibles.

déf-prop 14 : Soit $a = u \prod_{p \in \mathcal{P}} p^{v_p(a)}$, $b = v \prod_{p \in \mathcal{P}} p^{v_p(b)} \in A$, on pose $a \wedge b = \mathrm{pgcd}(a, b) = \prod_{p \in \mathcal{P}} p^{\min(v_p(a), v_p(b))}$
et $a \vee b = \mathrm{ppcm}(a, b) = \prod_{p \in \mathcal{P}} p^{\max(v_p(a), v_p(b))}$.
Ces définitions coïncident avec le plus grand diviseur et le plus petit multiple commun.

Rq 15 : • le pgcd et le ppcm sont définis aux inversibles près
• on définit par récurrence le pgcd / ppcm de plusieurs éléments : $\mathrm{pgcd}(a_1, \dots, a_n) = a_1 \wedge (\mathrm{pgcd}(a_2, \dots, a_n))$

Prop 16 : $a, b \in A$, $ab = (a \wedge b)(a \vee b)$

Ex 17 : • $(X^2-1) \wedge (X+1) = X+1$ dans $\mathbb{F}_2[X]$
• $\mathrm{pgcd}(0{,}42 ; 35000) = 7$ dans $\mathbb{D} = \mathbb{Z}[\frac{1}{10}]$
• $X \vee Y = XY$ dans $\mathbb{K}[X, Y]$

3. Idéaux et anneau principal

déf 18 : Un idéal I de A est premier si
• $A \neq I$ • $\forall a, b \in A$, $ab \in I \Rightarrow a \in I$ ou $b \in I$.

Ex 19 : $p\mathbb{Z}$, pour p premier, est un idéal premier de $\mathbb{Z}$

Prop 20 : • $a \in A^* \Leftrightarrow (a) = A$ • $a | b \Leftrightarrow (b) \subset (a)$
• p irréductible $\Leftrightarrow (p)$ premier
• $a \sim b \Leftrightarrow (a) = (b)$.

déf 21 : A est un anneau principal si tous les idéaux de A sont engendrés par un seul élément.

Prop 22 : un anneau principal est factoriel.

Contre-ex 23 : $A[X_1, \dots, X_n]$ est factoriel non principal.

Ex 24 : $\mathbb{K}[X]$ est principal

II. Théorèmes généraux

1. Contenu de Gauß

Th 25 (de Gauß) : A factoriel $\Rightarrow A[X]$ factoriel.

Déf 26 : Soit $P \in A[X]$, $P = \sum_{k=0}^{n} a_k X^k$, alors le contenu de P est $c(P) = \mathrm{pgcd}(a_0, \dots, a_n)$.

Lemme 27 (Gauß) : Soit $P, Q \in A[X]$, $c(PQ) = c(P)c(Q) \bmod A^*$

Prop 28 : Les polynômes irréductibles de $A[X]$ sont
- les constantes $p \in A$ irréductibles dans A
- les polynômes de degré ≥ 1, primitif (de contenu 1), irréductibles dans $Q(A)[X]$, avec $Q(A)$ le corps de fraction de A.

2. Théorème de Bézout

Th. 29 (de Bézout) : Soit A un anneau principal, $a, b \in A \setminus \{0\}$, $(a) + (b) = (a \wedge b)$.
En particulier, il existe $\lambda, \mu \in A$, $(a \wedge b) = \lambda a + \mu b$

On suppose désormais que A est un anneau principal.

Cor 30 : a et b premiers entre eux
$\iff (a) + (b) = (1) = A$
$\iff \exists \lambda, \mu \in A, \ \lambda a + \mu b = 1$

Contre-ex 31 : dans $\mathbb{K}[X,Y]$, $(X) + (Y) = (X,Y) \neq (1)$.

Appli 32 : Soit $n \geq 2$, $(\mathbb{Z}/n\mathbb{Z})^* = \{\overline{m} \in \mathbb{Z}/n\mathbb{Z}, \ m \wedge n = 1\}$
De plus, pour $\overline{m} \in (\mathbb{Z}/n\mathbb{Z})^*$, on a $\lambda m + \mu n = 1$, d'où $\overline{m}^{-1} = \overline{\lambda}$

3. Théorème chinois

Th. 33 : $a, b \in A$, tels que a et b sont premiers entre eux. Alors $A/(ab) \simeq A/(a) \times A/(b)$.
On peut généraliser à $a_1 \dots a_n$, où les (a_i) sont premiers entre eux deux à deux.

Appli 34 : Résolution de $\begin{cases} x \equiv a [m] \\ x \equiv b [n] \end{cases}$ $a, b \in \mathbb{Z}$, $m, n \in \mathbb{N}^*$

Ex 35 :
- $\begin{cases} x \equiv 2 \ [21] \\ x \equiv 11 \ [35] \end{cases}$ n'a pas de solution
- $\begin{cases} x \equiv 3 \ [21] \\ x \equiv 10 \ [35] \end{cases}$ a comme solution $\{45 + 105k, k \in \mathbb{Z}\}$

DEV 1.

III. Algorithme de calcul.

déf 36 : A est un anneau euclidien s'il est muni d'une division euclidienne, i.e il existe un stathme $v : A \setminus \{0\} \longrightarrow \mathbb{N}$, tq $\forall a, b \in A \setminus \{0\}$, $\exists q, r \in A$, $a = bq + r$ et ($r = 0$ ou $v(r) < v(b)$)

Ex 37 : $(\mathbb{Z}, |\cdot|)$, $(\mathbb{K}[X], \deg(\cdot))$, $(\mathbb{Z}[i], |\cdot|^2)$

Rq 38 : $\mathbb{Z}[X]$ n'est pas euclidien, mais on peut définir une division euclidienne $P_1 = QP_2 + R$, si P_2 est unitaire.

Th. 39 : un anneau euclidien est principal

Algo 40 (Euclide - étendu) :
Soit $a, b \in A$ un anneau euclidien.
Considérons la suite (W_i) définit par récurrence :
$$W_0 = \begin{pmatrix} a \\ 1 \\ 0 \end{pmatrix} ; \ W_1 = \begin{pmatrix} b \\ 0 \\ 1 \end{pmatrix} ; \ W_i = \begin{pmatrix} r_i \\ u_i \\ v_i \end{pmatrix} = W_{i-2} - q_i W_{i-1}$$
où (q_i, r_i) sont le couple quotient-reste de la division euclidienne de r_{i-2} par r_{i-1}
Il existe un rang maximal N tel que $r_N \neq 0$, on a alors $r_N = a \wedge b$. Et $a u_N + b v_N = r_N$.

Ex 41 : On applique l'algorithme à X^2+1 et X^3-1
$$W_0 = \begin{pmatrix} X^3-1 \\ 1 \\ 0 \end{pmatrix} \quad W_1 = \begin{pmatrix} X^2+1 \\ 0 \\ 1 \end{pmatrix}$$
$$\hookrightarrow W_2 = \begin{pmatrix} -X-1 \\ 1 \\ -X \end{pmatrix} \quad \rightarrow \quad W_3 = \begin{pmatrix} 2 \\ X-1 \\ -X^2+X+1 \end{pmatrix}$$
D'où $(X^2+1)(-X^2+X+1) + (X-1)(X^3-1) = 2$.

Prop 42 : Soit $a > b \in \mathbb{Z}$, $\mathcal{E}(a,b) :=$ nombre de divisions dans l'algorithme d'Euclide.
Alors $\mathcal{E}(a,b) \leq 2 \log_2(a)$.

• Soit $A, B \in \mathbb{K}[X]$, $\deg(B) \leq \deg(A)$.
Alors $\mathcal{E}(A,B) \leq \deg(B)$.

Prop 43: On considère la suite de Fibonacci (F_n)
$\forall z \in \mathbb{N}^*, \exists N_z \in \mathbb{N}, F_{N_z} \leq z \leq F_{N_z+1}$.
On a alors, pour $a > b > 0$, $\begin{cases} \mathcal{E}(a,b) \leq N_b - 1 \\ \mathcal{E}(a,b) \leq N_a - 2 \end{cases}$

On remarque de plus que $\mathcal{E}(F_{n+1}, F_{n+2}) = n$

Appli 44: équations diophantiennes:

• résolution de $ax + by = c$ (E_1), avec $a, b, c \in \mathbb{Z}$

(E_1) admet une solution ssi $a \wedge b \mid c$.
Dans ce cas, par Bézout, $\exists u, v \in \mathbb{Z}$, $au + bv = a \wedge b$.
Et, en posant $k = \frac{c}{a \wedge b}$, on obtient que (ku, kv) est solution

• résolution de $x^2 + y^2 = z^2$ (E_2) dans $\mathbb{Z}$.

Sans perdre de généralité, on peut supposer $x \geq 0$, $y \geq 0$, $z \geq 0$, $x \wedge y = 1$, x paire, y impaire.
Alors les solutions sont $\begin{cases} x = 2ab \\ y = a^2 - b^2 \\ z = a^2 + b^2 \end{cases}$ avec $a \geq b \geq 0$, $a \wedge b = 1$, a, b de différente parité.

Algo 45 (Binaire): Soit $a, b \in \mathbb{Z}$.

$$\operatorname{pgcd}(a,b) = \begin{cases} a & \text{si } a = b \\ 2\left(\frac{a}{2} \wedge \frac{b}{2}\right) & \text{si } a = b = 0\,[2] \\ a \wedge \frac{b}{2} & \text{si } b = 0\,[2],\ a = 1\,[2] \\ \frac{a}{2} \wedge b & \text{si } a = 0\,[2],\ b = 1\,[2] \\ (a-b) \wedge b & \text{si } a = b = 1\,[2],\ a > b \\ a \wedge (b-a) & \text{si } a = b = 1\,[2],\ b > a \end{cases}$$

Rq 46: la complexité de l'algorithme est de $O(\log^2(a))$, avec $a > b$.

Ex 47: Calcul du pgcd$(24, 18)$.
En base 2, 24 s'écrit 11000 et 18 s'écrit 10010.
On a alors
$$11000 \wedge 10010 = 10\,(1100 \wedge 1001) = 10\,(11 \wedge 1001) = 10\,(11 \wedge 110) = 10\,(11 \wedge 11) = 10 \times 11 = 110.$$
Et 110 correspond à 6 en base 10.

Lemme 48 (morphisme de Frobénius):
Soit p premier, $q = p^s$. Soit $P \in \mathbb{F}_q[X]$
$$S_p : \mathbb{F}_q[X]/(P) \longrightarrow \mathbb{F}_q[X]/(P)$$
$$Q(X) \longmapsto Q(X^q) = Q(X)^q$$
coïncide avec l'élévation à la puissance q.

Prop 49: Soit $P \in \mathbb{F}_q[X]$, $P \wedge P' = 1 \iff P$ sans facteur carré.

Algo 50: Soit $P \in \mathbb{F}_q[X]$, tq $P \wedge P' = 1$.

① Calcul de $\mathrm{Mat}_{\mathcal{B}}(S_p - Id)$, dans $\mathcal{B} = \{1, x, \dots, x^{\deg(P)-1}\}$

② Le nombre de facteurs irréductibles de P est $r = \dim(\operatorname{Ker}(S_p - Id))$

→ si $r = 1$, P est irréductible et l'algorithme s'arrête.

③ On choisit $V \in \mathbb{F}_q[X]$, tq $V \neq$ cste $[P]$ et $V[P] \in \operatorname{Ker}(S_p - Id)$, alors
$$P = \prod_{\alpha \in \mathbb{F}_q} P \wedge (V - \alpha).$$
→ on retourne en ① pour chaque facteurs non triviaux.

Prop 51: $P \wedge P' = P \Rightarrow P = R^p$, $R \in \mathbb{F}_q[X]$.

Généralisation 52: Pour $P \in \mathbb{F}_q[X]$, on calcule $P \wedge P'$:

* $P \wedge P' = 1 \Rightarrow$ on fait Berlekamp
* $P \wedge P' = P \Rightarrow P = R^p$, on calcule $R \wedge R'$
* $P \wedge P' = D \in \mathbb{F}_q[X]$

Développement : Système de congruences

Référence : CVA - 4.2.8

Au III$^{\text{è}}$ siècle avant J-C, le général chinois Han Xin demande au mathématicien Sun Zi[1] de compter son armée. Celui-ci décide de les ranger en colonnes : rangés en colonne de 3, il reste 2 soldats, en colonne de 5, il en reste 3 et en colonne de 7, il en reste 2. Les systèmes de congruences étaient nés...

Soient $n, m \in \mathbb{N}^*$, $a, b \in \mathbb{Z}$. On cherche à résoudre $(S) \begin{cases} x \equiv a\,[n] \\ x \equiv b\,[m] \end{cases}$ dans $\mathbb{Z}$.

On pose $\delta = \text{pgcd}(n,m)$ et $\mu = \text{ppcm}(n,m)$.

$\boxed{0}$ On observe que le morphisme $\left| \begin{array}{l} \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/s\mathbb{Z} \\ \overline{x}_n \mapsto \overline{x}_s \end{array} \right.$ [2] est bien défini ssi $s \mid n$

En effet si $s \mid n$, soient x et $y \in \mathbb{Z}$ / $x \equiv y\,[n]$. Alors $n \mid x-y$ donc $s \mid x-y$ donc $\overline{x}_s = \overline{y}_s$ d'où le fait que le morphisme est bien défini.

Réciproquement, si $\forall x, y \in \mathbb{Z}$ / $x \equiv y\,[n]$, on a $x \equiv y\,[s]$, alors en particulier pour $y = x+n$, on a $n \equiv 0\,[s]$ ie $s \mid n$.

$\boxed{1}$ On pose $\varphi : \left| \begin{array}{l} \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \\ x \mapsto (\overline{x}_n, \overline{x}_m) \end{array} \right.$. Mq $\ker \varphi = \mu\mathbb{Z}$

Soit $x \in \mathbb{Z}$. $x \in \ker\varphi \iff \overline{x}_n = 0$ et $\overline{x}_m = 0 \iff n \mid x$ et $m \mid x \iff \mu \mid x \iff x \in \mu\mathbb{Z}$

On a donc $\mathbb{Z}/\mu\mathbb{Z} \simeq \text{Im}(\varphi)$

$\boxed{2}$ On pose $\psi : \left| \begin{array}{l} \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/\delta\mathbb{Z} \\ (\overline{x}_n, \overline{y}_m) \mapsto \overline{x}_\delta - \overline{y}_\delta \end{array} \right.$

ψ est bien défini par $\boxed{0}$. Mq ψ est surjectif.

Soit $\alpha \in \mathbb{Z}/\delta\mathbb{Z}$. $\exists x \in \mathbb{Z}$ / $\overline{x}_n = \alpha$, et alors $\psi(\overline{x}_n, 0) = \alpha$. D'où $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} / \ker\psi \simeq \mathbb{Z}/\delta\mathbb{Z}$

$\boxed{3}$ Mq $\text{Im}(\varphi) = \ker(\psi)$

$\boxed{\subset}$: Soit $x \in \mathbb{Z}$. $\psi(\varphi(x)) = \psi(\overline{x}_n, \overline{x}_m) = \overline{x}_\delta - \overline{x}_\delta = 0$

$\boxed{\supset}$: On montre l'égalité des cardinaux grâce à la célèbre formule $\mu\delta = nm$

(1) : On oubliera pour le bien de l'histoire les cinq siècles qui les ont séparés.

(2) : On note $\overline{x}_s$ la réduction modulo s de x, pour s et x entiers

On a $\#\mathrm{Im}(\varphi) = p$ d'après [1], et $\dfrac{n \times m}{\#\ker(\psi)} = \delta$ d'après [2], d'où $\#\mathrm{Im}(\varphi) = \#\ker\psi$

[4] Revenons maintenant à nos soldats:

x est solution de (S) ssi $\varphi(x) = (\bar{a}, \bar{b})$

En particulier, une condition nécessaire pour que (S) admette une solution est $(\bar{a}, \bar{b}) \in \mathrm{Im}(\varphi)$ ie $(\bar{a}, \bar{b}) \in \ker(\psi)$ ie $a \equiv b\,[\delta]$

[5] On suppose donc que $a \equiv b\,[\delta]$ i.e. $\exists k \in \mathbb{Z} / a = b + k\delta$

Le théorème de Bézout nous donne l'existe d'entiers u et v tels que $un + vm = \delta$.

On pose $x_0 = \dfrac{unb + vma}{\delta}$. Alors $x_0 = b + kvm = a - kun$ donc $x_0 \in \mathbb{Z}$

et $x_0 \equiv a\,[n]$ et $x_0 \equiv b\,[m]$ ie x_0 est solution de (S)

[6] Finalement, x est solution de (S) ssi $\varphi(x) = \varphi(x_0)$ ssi $x - x_0 \in \ker(\varphi)$

ssi $x \in x_0 + p\mathbb{Z}$

L'ensemble des solutions de (S) est donc $\boxed{x_0 + p\mathbb{Z}}$

<u>Remarque</u>: A la fin de l'étape [1], si l'on suppose $n \wedge m = 1$, on a alors $p = nm$ et par égalité des cardinaux, on a prouvé le lemme chinois: $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \simeq \mathbb{Z}/nm\mathbb{Z}$ lorsque $n \wedge m = 1$

<u>Application</u>: Laissons les questions militaires à d'autres et occupons-nous de choses plus poétiques, qui auraient possiblement motivés les Chinois à étudier ces systèmes: l'astronomie et le calendrier.

Halloween est dans 10 jours, et c'est mieux avec la pleine lune non ?

La prochaine pleine lune est dans 21 jours. Quand sera le prochain Halloween sous la pleine lune ?

Il faut résoudre $\begin{cases} x \equiv 10\,[365] \\ x \equiv 21\,[29] \end{cases}$; $365 \times 12 - 151 \times 29 = 1$; $x_0 := 365 \times 12 \times 21 - 151 \times 29 \times 10$

$= 48190$

$\mathcal{S} = 48190 + 10585\mathbb{Z}$

La prochaine Halloween sous pleine lune sera donc dans 5850 jours, c-à-d en 2035.

Algorithme de Berlekamp

• Soit p un nombre premier, $s \in \mathbb{N}^*$, $q = p^s$ et $\mathbb{F}_q$ le corps fini à q éléments. $P \in \mathbb{F}_q[X]$ sans facteurs carrés, on l'écrit $P = \prod_{i=1}^{r} P_i$

L'algorithme de Berlekamp nous donne le nombre r de facteurs irréductibles et quand $r \geq 2$, il les donne explicitement.

<u>Lemme (admis)</u>: L'application $S_P : \mathbb{F}_q[X]/(P) \longrightarrow \mathbb{F}_q[X]/(P)$
$$Q(X) \bmod P \longmapsto Q(X^q) \bmod P$$
est bien définie et coïncide avec l'élévation à la puissance q dans $\mathbb{F}_q[X]/(P)$

<u>Théorème.</u> Le processus suivant s'arrête au bout d'un nombre fini d'étapes et donne la décomposition de P.

1/ On calcul la matrice de $S_P - Id$.

2/ Le nombre de facteur irréductibles de P est
$r = \dim(\mathrm{Ker}(S_P - Id)) = \deg(P) - \mathrm{rg}(S_P - Id)$.
Si $r = 1$, P est irréductible et sinon on passe en 3.

3/ On calcule un polynôme V non congru à un polynôme constant modulo P dans $\mathbb{F}_q[X]$, et tel que $V \in \mathrm{Ker}(S_P - Id)$
on calcul les pgcd $(P, V - \alpha)$ pour $\alpha \in \mathbb{F}_q$. On a alors
$P = \prod_{\alpha \in \mathbb{F}_q} \mathrm{pgcd}(P, V-\alpha)$ (*). On retourne en 1/ avec les facteurs non triviaux de (*).

<u>Preuve.</u> On pose $K_i := \mathbb{F}_q[X]/(P_i)$, $1 \leq i \leq r$. Le théorème chinois nous fourni l'isomorphisme: $\varphi : \mathbb{F}_q[X]/(P) \longrightarrow K_1 \times \cdots \times K_r$
$$Q \bmod P \longmapsto (Q \bmod P_1, \ldots, Q \bmod P_r)$$

<u>Montrons que $r = \dim(\mathrm{Ker}(S_P - Id))$.</u> On pose $\tilde{S}_P : \varphi \circ S_P \circ \varphi^{-1}$
$K_1 \times \cdots \times K_r \to K_1 \times \cdots \times K_r$. $\tilde{S}_P$ correspond à l'élévation à la puissance q composante par composante. Ainsi, $(x_1 \ldots x_r) \in \mathrm{Ker}(\tilde{S}_P - Id)$
$\Leftrightarrow \forall i \in [\![1, r]\!]$ $x_i^q = x_i$ dans K_i. Or, en considérant K_i comme une extension de $\mathbb{F}_q$, les éléments de K_i sont les éléments de $\mathbb{F}_q$.

En effet : soit $x \in \mathbb{F}_q^*$, par Lagrange $x^{q-1} = 1$ et $x^q = x$. Comme $0^q = 0$, on a $\forall x \in \mathbb{F}_q \subset K_i$. De plus, le polynôme $X^q - X$ possède q racines dans K_i ce sont les elements de $\mathbb{F}_q$ et il n'y en a pas d'autres.
Ainsi : $(x_1 \dots x_r) \in \mathrm{Ker}(\tilde{S}_P - Id) \Longleftrightarrow \forall i \in [\![1,r]\!]\ x_i \in \mathbb{F}_q$ d'où $\mathrm{Ker}(\tilde{S}_P - Id) = (\mathbb{F}_q)^r$. Or $\mathrm{Ker}(\tilde{S}_P - Id) = \varphi(\mathrm{Ker}(S_P - Id))$. Comme φ est un isomorphisme de $\mathbb{F}_q$ e.v on en conclut que $\dim \mathrm{Ker}(S_P - Id) = r$

- On suppose $r > 1$. On commence par remarquer que l'ensemble des $U \bmod P$ où U est un polynôme congru à un polynôme constant est la droite vectorielle de $\mathbb{F}_q[X]/(P)$ engendrée par 1 (donc de dimension 1). Comme $r = \dim(\mathrm{Ker}(S_P - Id)) > 1$, il existe $V \in \mathbb{F}_q[X]$ non congru à un polynôme constant tel que $V \bmod P \in \mathrm{Ker}(S_P - Id)$. Soit V un tel polynôme.

<u>Montrons que $P = \prod_{\alpha \in \mathbb{F}_q} \mathrm{pgcd}(P, V - \alpha)$</u>

On observe que $(V \bmod P) \in \mathrm{Ker}(S_P - Id) \Leftrightarrow (V \bmod P_1 \dots V \bmod P_r) \in (\mathbb{F}_q)^r$
Pour tout $i \in [\![1,r]\!]$, on note $\alpha_i = (V \bmod P_i) \in \mathbb{F}_q \subset K_i$; pour $\alpha \in \mathbb{F}_q$ montrons : $\mathrm{pgcd}(V, \alpha) = \prod_{\{i, \alpha_i = \alpha\}} P_i$.

- Comme $\mathrm{pgcd}(P, V-\alpha) \mid P$, $\mathrm{pgcd}(P, V-\alpha) = \prod_{i \in I_\alpha} P_i$ $\quad I_\alpha \subset [\![1,r]\!]$
Comme $\mathrm{pgcd}(P, V-\alpha) \mid V-\alpha$, et que les P_i sont premiers entre eux, on a que $\forall i \in \cancel{[\![1,r]\!]}\ I_\alpha$ $P_i \mid V-\alpha$ et donc $I_\alpha = \{ i \in [\![1,r]\!]$ tq $P_i \mid V - \alpha \}$. Or $P_i \mid V-\alpha \Longleftrightarrow V - \alpha \equiv 0 [P_i] \Leftrightarrow V \equiv \alpha [P_i]$ $\Leftrightarrow \alpha = \alpha_i$. D'où $I_\alpha = \{ i \ \alpha_i = \alpha \}$ et $\mathrm{pgcd}(P, V-\alpha) = \prod_{\{i, \alpha_i = \alpha\}} P_i$

Ainsi, en ecrivant $P = \prod_{i=1}^{r} P_i$, il vient $P = \prod_{\alpha \in \mathbb{F}_q} \left(\prod_{\{i, \alpha_i = \alpha\}} P_i \right)$
$$= \prod_{\alpha \in \mathbb{F}_q} \mathrm{pgcd}(V - \alpha, P).$$

- Le choix d'un V non congru à un polynôme constant assure que tout les facteurs de ⊛ sont differents de P. Ainsi on a deux facteurs non triviaux et donc chacun ont strictement moins que r facteurs irreductibles. Par ailleurs, les n̶ précédents polynômes etant diviseurs de P, ils sont bien sans facteurs carrés.

□