Agrégation de mathématiques

par JEAN-LOUIS NICOLAS

Épreuve de mathématiques et informatique

6634

Ce problème étudie des algorithmes de factorisations de polynômes. On pourra trouver des informations sur ce sujet dans les livres de D.E. KNUTH, *Seminumerical algorithms*, vol 2, et M. MIGNOTTE, *Mathématiques pour le calcul formel*.

La partie III traite de la factorisation des polynômes à deux variables et n'est pas présentée dans les livres ci-dessus. La méthode suivie est celle de P.S. WANG, « *An improved multivariate polynomial factoring algorithm* », *Mathematics of Computation*, 1978, p. 1215-1231.

Les toutes premières questions étaient des applications directes du cours. Sur 138 copies, environ les deux tiers ont su écrire les deux facteurs de x^5+x+1 sur les corps à deux éléments. Seulement 42 % ont donné les polynômes irréductibles de degré ≤ 4 sur ce même corps. Le nombre d'opérations élémentaires nécessitées par la division euclidienne de deux polynômes sur un corps quelconque a été traité correctement par 57 % des copies, mais le coût du PGCD de deux polynômes n'a été obtenu que dans 4 copies. Enfin, le rang d'une matrice 5×5 sur le corps à deux éléments et la détermination des vecteurs propres correspondant à la valeur propre 1 (question **I 3°***a*)) n'ont fait l'objet d'une réponse juste que dans 36 % des copies. L'origine des erreurs est quelquefois une faute de calcul, ou un calcul effectué sur les réels, mais souvent aussi des lacunes en algèbre linéaire.

Très peu de copies ont abordé de façon significative la deuxième ou la troisième partie. Les candidats qui ont traité correctement la première partie ont obtenu 30/40. Quelques très bons candidats ont dominé le sujet, mais très peu ont su factoriser le polynôme à une variable de degré 5 de la deuxième partie, et personne n'a su factoriser le polynôme à deux variable de la fin.

I

1° *a)* Ce polynôme n'a pas de racines dans $\mathbb{F}_2$. Le seul polynôme irréductible de degré 2 est x^2+x+1, et par division, on voit que :

$$x^5+x+1 = (x^2+x+1)(x^3+x^2+1).$$

b) Degré 1 : x et $x+1$.

Degré 2 : x^2+x+1.

Degré 3 : Pour ne pas avoir de racines, le polynôme doit être de la forme $x^3+a\,x^2+b\,x+1$ avec $a\neq b$. Il y a donc x^3+x+1 et x^3+x^2+1.

Degré 4 : De même les polynômes sans racines sont x^4+x^3+1, x^4+x^2+1, x^4+x+1, $x^4+x^3+x^2+x+1$. Il faut enlever le second, qui est le carré de x^2+x+1.

2° *a)* Le nombre de termes du quotient est $\leq m-n+1$. Pour déterminer chacun de ses termes, on fait une division, $(n+1)$ multiplications, et $(n+1)$ soustractions dans K, soit $(2n+3)$ opérations.

b) Posons $A = R_1$, $B = R_2$. L'algorithme d'EUCLIDE s'écrit :

$$R_i = R_{i+1}+Q_{i+1}+R_{i+2},\ 1\leq i\leq k$$

avec $R_{k+2}=0$. Posons $r_i =$ degré R_i. On peut supposer que $m\geq n$, sinon après la division de A par B, dans l'algorithme on effectue l'algorithme d'EUCLIDE sur B et A.

On a : $r_1=m, r_2=n, r_3\leq n-1,\ldots, r_i\leq n-i+2$. À la dernière étape, $R_{k+2}=0$, et $r_{k+1}\geq 0$. On a donc :

$$0\leq r_{k+1}\leq n-(k+1)+2,$$

ce qui donne $k\leq n+1\leq m+1$.

D'après **2° *a)***, le nombre d'opérations est inférieur ou égal à :

$$\sum_{i=1}^{k}(r_i-r_{i+1}+1)(2r_{i+1}+3)\leq(2n+3)\sum_{i=1}^{k}(r_i-r_{i+1}+1)$$

$$=(2n+3)(k+r_1-r_{k+1})\leq(2n+3)(2m+1)=O(mn)$$

3° *a)* On a :

$$M-I=\begin{pmatrix}0&0&0&0&0\\0&1&0&1&0\\0&1&1&1&0\\0&0&0&1&1\\0&0&1&0&0\end{pmatrix}$$

Le rang de cette matrice est aussi celui de la matrice obtenue en rayant la première ligne et la première colonne :

$$\begin{pmatrix}1&0&1&0\\1&1&1&0\\0&0&1&1\\0&1&0&0\end{pmatrix}$$

Par la méthode du pivot de GAUSS, cette matrice devient :

$$\begin{pmatrix}1&0&1&0\\0&1&0&0\\0&0&1&1\\0&1&0&0\end{pmatrix}\ \text{et}\ \begin{pmatrix}1&0&1&0\\0&1&0&0\\0&0&1&1\\0&0&0&0\end{pmatrix}$$

qui est de rang 3.

Le système d'équations pour trouver les vecteurs propres est :

$$\begin{cases}x_2+x_4=0\\x_2+x_3+x_4=0\\x_4+x_5=0\\x_3=0\end{cases}$$

Il y a pour solutions : x_1 quelconque, $x_3=0$, $x_2=x_4=x_5$. Il y a trois vecteurs propres :

$$\begin{pmatrix}1\\0\\0\\0\\0\end{pmatrix}\quad\begin{pmatrix}0\\1\\0\\1\\1\end{pmatrix}\quad\begin{pmatrix}1\\1\\0\\1\\1\end{pmatrix}$$

b) Il y a 2^n choix possibles pour un vecteur dans $\mathbb{F}_2^n$, et on doit écarter le vecteur nul, soit $2^n - 1$. Le choix d'un deuxième vecteur doit écarter les deux vecteurs du sous-espace engendré par v_1 ; le choix du r-ième vecteur doit écarter les 2^{r-1} vecteurs du sous-espace engendré par $v_1, \ldots, v_{r-1}$. Le nombre demandé est donc

$$(2^n - 1)(2^n - 2)(2^n - 4)\ldots(2^n - 2^{r-1})$$

Notons que ce nombre compte le nombre de matrices à n lignes et r colonnes qui sont de rang r. Si l'on veut déterminer le nombre d'ensembles à r vecteurs qui forment une famille libre, il faut le diviser par $r!$, ce qui fournit une propriété de divisibilité non évidente.

4° *a)* Observons d'abord que le PGCD dans $\mathbb{Q}$ de deux polynômes de $\mathbb{Q}[x]$, est le même que dans $\mathbb{C}$, par l'algorithme d'EUCLIDE. Le PGCD de F et F' dans $\mathbb{Q}$ va évidemment diviser F dans $\mathbb{Q}[x]$, et donc $G \in \mathbb{Q}[x]$. De plus, si

$$F = a_n (x - x_1)^{\alpha_1} \ldots (x - x_r)^{\alpha_r}$$

on a :

$$\mathrm{PGCD}(F, F') = (x - x_1)^{\alpha_1 - 1} \ldots (x - x_r)^{\alpha_r - 1}$$

et G sera bien sans facteurs carrés.

b) Si F est sans facteur carré, on a $C_1 = 1$, la boucle *tant que* n'est pas exécutée, et l'on a :

$$k = 1, \quad P_1 = F.$$

Si $F = x^3 (x-1)^2 (x+1)^2 (x^2+1)$, on obtient :

$$\begin{aligned} C_1 &= x^2 (x-1)(x+1) \\ D_1 &= x(x-1)(x+1)(x^2+1) \\ C_2 &= x \\ D_2 &= x(x-1)(x+1) \\ P_1 &= x^2 + 1 \\ C_3 &= 1 \\ D_3 &= x \\ P_2 &= (x-1)(x+1) \\ k &= 3 \quad ; \quad P_3 = x. \end{aligned}$$

Tout polynôme $F \in \mathbb{Q}[x]$ s'écrit comme un produit de polynômes irréductibles dans $\mathbb{Q}[x]$. Or un polynôme P irréductible sur $\mathbb{Q}$ est sans facteur carré. Sinon le PGCD de P et P' serait différent de 1 et serait un facteur de P de degré $\leq$ degré P' = degré $P - 1$.

On peut alors écrire :

$$F = P_1 P_2^2 \ldots P_k^k$$

où $P_2, \ldots, P_k$ sont unitaires, et P_i est le produit des polynômes irréductibles qui divisent F avec exactement l'exposant i. L'algorithme précédent calcule $P_1, P_2, \ldots, P_k$. Les variables intermédiaires sont

$$C_i = P_{i+1} P_{i+2}^2 \ldots P_k^{k-i}$$

$$D_i = P_i P_{i+1} \ldots P_k.$$

5° *a)* Montrons d'abord l'unicité. Supposons que

$$A_1 U + B_1 V = S$$

$$A_2 U + B_2 V = S.$$

On aurait

$$(A_1 - A_2) U = (B_2 - B_1) V.$$

Par le lemme de GAUSS, U divise $(B_2 - B_1) V$ et est premier avec V, il doit diviser $B_2 - B_1$.
Mais $d°(B_2 - B_1) < n = d°V$, donc $B_1 = B_2$ et il s'ensuit que $A_1 = A_2$.

L'existence résulte de la relation de BÉZOUT : il existe C et D tels que

$$CU + DV = 1.$$

Multiplions par S :

$$CSU + DSV = S.$$

La division euclidienne de CS par V donne :

$$CS = VQ + R \quad d°R < d°V = m$$

$$RU + (QU + DS) V = S.$$

On choisit $A = R$, $B = QU + DS$, et l'on a :

$$d°(BV) = d°(S - RU) < m + n$$

d'où, $d°B < n$.

Application numérique. De façons évidente : $A = 1$, $B = -x$ conviennent pour $S = 1$, et $A = s_0 + s_1 x$, $B = -x(s_0 + s_1 x)$ conviennent pour $S = s_0 + s_1 x$.

b) Posons $A(x) = a_{m-1} x^{m-1} + \ldots + a_0$,

$$B(x) = b_{n-1} x^{n-1} + \ldots + b_0$$

$$S(X) = s_{m+n-1} s^{m+n-1} + \ldots + s_0,$$

et Z la matrice colonne :

$$Z = \begin{pmatrix} a_{m-1} \\ \vdots \\ a_0 \\ b_{n-1} \\ \vdots \\ b_0 \end{pmatrix}.$$

Le i-ième terme du produit RZ vaut

$$\sum_{j=1}^{m} u_{n+j-i} a_{m-j} + \sum_{j=m+1}^{m+n} v_{j-1} b_{n+m-j}$$

et c'est le coefficient de x^{n+m-i} dans $AU + BV$. L'égalité polynomiale $AU + BV = S$ est donc équivalente à :

$$RZ = \begin{pmatrix} s_{m+n-1} \\ \vdots \\ s_0 \end{pmatrix}$$

Si U et V sont premiers entre eux, il y a une solution et une seule pour tout S, l'application linéaire associée à R est surjective, et R est inversible. Si U et V ne sont pas premiers entre eux, pour $S = 1$, il n'y a pas de solution et R n'est pas inversible.

On a :

$$Z = \begin{pmatrix} a_{m-1} \\ \vdots \\ a_0 \\ b_{n-1} \\ \vdots \\ b_0 \end{pmatrix} \qquad R^{-1} = \begin{pmatrix} s_{m+n-1} \\ \vdots \\ s_0 \end{pmatrix}$$

Application numérique. On a

$$R^{-1} \begin{pmatrix} 8 \\ 8 \\ 20 \\ 10 \\ 7 \end{pmatrix} = \begin{pmatrix} 4 \\ 5 \\ 0 \\ -1 \\ 2 \end{pmatrix}$$

soit $A = 4x+5$, $B = -x+2$.

6° ***a)*** Posons $u_{-1} = u_{n+1} = 0$. Il vient

$$(x-\alpha)\,U(x) = \sum_{k=-1}^{n} (u_k - \alpha u_{k+1})\,x^{k+1}$$

et

$$N(g)^2 = \sum_{k=-1}^{n} (u_k - \alpha u_{k+1})(\overline{u}_k - \overline{\alpha}\,\overline{u}_{k+1})$$

$$= \sum_{k=-1}^{n} |u_k|^2 + |\alpha u_{k+1}|^2 - \alpha \overline{u}_k u_{k+1} - \overline{\alpha} u_k \overline{u}_{k+1}$$

On a de même :

$$(\overline{\alpha}x - 1)\,U(x) = \sum_{k=-1}^{n} (\overline{\alpha} u_k - u_{k+1})\,x^{k+1}$$

et

$$N(h)^2 = \sum_{k=-1}^{n} |\alpha u_k|^2 + |u_{k+1}|^2 - \alpha \overline{u}_k u_{k+1} - \overline{\alpha}\,\overline{u}_{k+1} u_k.$$

Comme $u_{-1} = u_{n+1} = 0$, on a bien $N(g)^2 = N(h)^2$, soit $N(g) = N(h)$.

b) Soit $x_1, \ldots, x_r$ les racines vérifiant $|x_i| > 1$. On a :

$$M(U) = |u_n x_1 x_2 \ldots x_r|.$$

Par ailleurs le polynôme

$$V(x) = u_n (\overline{x}_1 x - 1) \ldots (\overline{x}_r x - 1)(x - x_{r+1}) \ldots (x - x_n)$$

vérifie $N(U) = N(V)$ en appliquant r fois la question précédente.

Si l'on écrit $V(x) = v_n x^n + \ldots + v_0$, on a :

$$N(V) = (|v_n|^2 + \ldots + |v_0|^2)^{1/2} \geq |v_n| = M(U),$$

ce qui prouve $M(U) \leq N(U)$.

À l'aide des relations entre les coefficients et les racines, on a pour : $1 \leq j \leq n$

$$(-1)^j u_{n-j} = \sum_{1 \leq i_1 \ldots < i_j \leq n} u_n x_{i_1} x_{i_2} \ldots x_{i_j}$$

ce qui donne

$$|u_{n-j}| \leq \binom{n}{j} M(U) = \binom{n}{n-j} M(U)$$

c) La question précédente nous donne

$$|v_i| \leq \binom{d}{i} M(V) \leq \binom{d}{\lfloor d/2 \rfloor} M(V).$$

Comme V divise U dans $\mathbb{Z}[x]$, v_d divise u_n dans $\mathbb{Z}$, et donc $|v_d| \leq |u_n|$. Par ailleurs, soit $I \subset \{1, 2, \ldots, n\}$ tel que $i \in I \Leftrightarrow x_i$ racine de V. On a :

$$\prod_{i \in I} \max(1, |x_i|) \leq \prod_{1 \leq i \leq n} \max(1, |x_i|)$$

et donc $M(V) \leq M(U)$.

Par la question précédente, $M(U) \leq N(U)$, ce qui achève la preuve.

Application numérique. $N(U) = 64{,}17$. Un polynôme de degré 2 vérifiera $|v_i| \leq 128$, de degré 3, $|v_i| \leq 192$, de degré 4, $|v_i| \leq 385$.

II

1° C'est le théorème chinois. Montrons l'unicité de F : s'il existait F_1 et F_2 vérifiant $F_1 \equiv F_2 \equiv A_i \bmod U_i$, $F_1 - F_2$ serait divisible par le produit des U_i, et comme

$$d^0(F_1 - F_2) < \sum_{i=1}^{r} d^0 U_i$$

$$F_1 - F_2 = 0.$$

Posons $M_i = \prod_{j \neq i} U_j$ · U_i et M_i sont premiers entre eux, et il existe B_i et C_i tels que

$$B_i M_i + U_i C_i = 1.$$

Le polynôme $B_i M_i$ est solution du système de congruences

$$B_i M_i \equiv 1 \bmod U_i \quad B_j M_j \equiv 0 \bmod U_j \quad j \neq i,$$

et par conséquent

$$F = \sum_{i=0}^{r} A_i B_i M_i$$

est une solution de la congruence demandée. En divisant F par $U_1 U_2 \ldots U_r$,

$$F = (U_1 U_2 \ldots U_r) Q + R$$

le reste R est aussi une solution de cette congruence, et son degré est $< \sum_{i=1}^{r} d^0(U_i)$.

Ceci fournit un algorithme de calcul : les B_i sont calculés par l'algorithme d'EUCLIDE étendu.

2° Dans $\mathbb{F}_p[x]$, on a l'identité :

$$X^p - X = X(X-1)\dots(X-p+1)$$

ce qui donne

$$V(x)^p - V(x) = V(x)(V(x)-1)\dots(V(x)-(p-1)).$$

Comme $U(x)$ divise le membre de gauche, il doit diviser le membre de droite, et chaque U_i doit diviser un polynôme de la forme $V(x) - s_i$, car U_i est irréductible. (Il ne peut en diviser 2). Il existe donc $s_1, s_2, \dots, s_r$ tel que $V(x)$ vérifie

$$V(x) \equiv s_i \bmod U_i \quad 1 \le i \le r.$$

Réciproquement, pour tout choix $s_1, \dots, s_r$ d'éléments de $\mathbb{F}_p$ (soit p^r choix) la solution des congruences ci-dessus vérifie

$$V(x)^p \equiv V(x) \bmod U$$

et il y a donc p^r tels polynômes. Notons que ces polynômes forment un espace vectoriel, et il y a donc p^{r-1} polynômes unitaires répondant à la question. L'énoncé comportait une coquille : il fallait supprimer « unitaire » devant « V ».

Application numérique. On observe d'abord que, dans $\mathbb{F}_5$,

$$1 + x + x^2 + x^3 = (x-2)(x-3)(x-4)$$

mais que $1 + x + x^2$ est irréductible. On a donc $r = 4$, et l'on doit résoudre

$$\begin{cases} V(x) \equiv s_1 \bmod (x-2) \\ V(x) \equiv s_2 \bmod (x-3) \\ V(x) \equiv s_3 \bmod (x-4) \\ V(x) \equiv s_4 \bmod (x^2+x+1) \end{cases}$$

Les solutions sont

$$V(x) = (ax^2 + bx + c)(x^2 + x + 1) + s_4$$

où a, b, c, s_4 sont 4 éléments quelconques de $\mathbb{F}_5$.

3° De façon générale, si U et $V \in K[x]$, les applications de $K[x]$ dans lui même :

$$V(x) \mapsto V(x^p)$$

et

$$V(x) \mapsto V(x) \bmod U(x)$$

sont linéaires. La restriction à $\mathbb{F}_p^{(n-1)}[x]$ lorsque $K = \mathbb{F}_p$ est bien contenue dans $\mathbb{F}_p^{(n-1)}[x]$, puisque $d^0 U = n$.

La matrice M a ses colonnes égales aux coefficients de $X^{jp} \bmod U(X)$, $0 \le j \le n-1$. La 1re colonne vaut :

$$\begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

Ensuite, on calcule $X^p \bmod U$, puis de proche en proche :

$$\left(X^{(j-1)p} \bmod U\right)(X^j \bmod U) \bmod U,$$

de façon à calculer sur des polynômes de degré aussi bas que possible.

Dans $\mathbb{F}_p[x]$, on a $V(x)^p = V(x)$. Par conséquent, les p^r polynômes solutions de $V(x)^p \equiv V(x) \bmod U(x)$ constituent le sous-espace propre associé à la valeur propre 1. La dimension de ce sous-espace est donc r, d'après 2.

Application numérique. On a mod U, $x^6 \equiv x^2 + x$, $x^8 \equiv x^4 + x^3$, et la matrice M est celle du **3° *a)***.
La dimension du sous-espace propre est 2, montrant que le polynôme $x^5 + x + 1$ a deux facteurs irréductibles dans $\mathbb{F}_2[x]$.

4° Les instructions affectant une valeur à W_j sont :

$$\begin{aligned} W_1 &: = U; \\ D &: = \mathrm{PGCD}(W_j, V_i - s); \\ W_\ell &: = D; \\ W_j &: = W_j / D; \end{aligned}$$

Ceci montre que D et W_j sont des diviseurs de U.

On remarque ensuite que le produit des polynômes

$$W_1 W_2 \dots W_\ell$$

est toujours égal à U.

En effet, quand on crée le polynôme $W_\ell := D$, on divise le polynôme W_j par D (et $j \le k \le \ell$) gardant ainsi ce produit constant ; or il vaut U au début.

Ensuite aucun des polynômes W_j n'est égal à 1, puisque avant les affectations $W_\ell := D$ et $W_j := W_j / D$, on suppose $D \ne 1, D \ne W_j$.

D'après la question **II 2°** pour chaque V_i, il existe $t_i^{(j)}$ tel que U_j divise $V_i - t_i^{(j)}$, et $t_i^{(j)} \in \mathbb{F}^p$, et ceci de façon unique. Nous allons d'abord montrer la propriété :

$$\text{Pour } j \ne j' \quad \text{il existe} \quad i, 1 \le i \le r \quad \text{avec} \quad t_i^{(j)} \ne t_i^{(j')}.$$

Supposons le contraire ; on aurait pour tout vecteur propre V :

$$V = \lambda_1 V_1 + \dots + \lambda_r V_r$$

les relations :

$$V \equiv \sum_{i=1}^{r} \lambda_i t_i^{(j)} \bmod U_j$$

et

$$V \equiv \sum_{i=1}^{r} \lambda_i t_i^{(j')} \bmod U_{j'}.$$

En posant $s = \sum_{i=1}^{r} \lambda_i t_i^{(j)} = \sum_{i=1}^{r} \lambda_i t_i^{(j')}$, on aurait :

$$V \equiv s \bmod U_j \text{ et } V \equiv s' \bmod U_{j'}.$$

Or, en résolvant les congruences du 2 par le théorème chinois, on a su trouver des vecteurs V tels que

$$V \equiv s \bmod U_j \text{ et } V \equiv s' \bmod U_{j'}$$

avec $s \ne s'$.

Soit i_0 tel que l'on ait $t_{i_0}^{(j)} \ne t_{i_0}^{(j')}$. Dans l'exécution du programme, lorsque $i = i_0$ et $s_0 = t_{i_0}^{(j)}$, on a :

$$W_1 W_2 \dots W_k = U$$

et supposons que l'un des polynômes, par exemple W_1, soit divisible par U_j et $U_{j'}$. Alors le PGCD $(W_1, V_{i_0} - s_0)$ sera divisible par U_j, mais pas par $U_{j'}$, donc D sera différent de 1 et de W_1, et il y aura création d'un nouveau W_ℓ.
On voit ainsi qu'à la fin de l'algorithme, un même W_i ne peut pas être multiple de deux polynômes U_j et $U_{j'}$.

5° Supposons construits f_{n-1} et g_{n-1}. On écrit :

$$f_n = f_{n-1} + p^{n-1} h \quad , \quad g_n = g_{n-1} + p^{n-1} k$$

où h et k sont à déterminer. On doit avoir :

$$f_n g_n \equiv f_{n-1} g_{n-1} + p^{n-1} (h g_{n-1} + k f_{n-1}) \equiv U \bmod p^n$$

soit

$$\frac{U - f_{n-1} g_{n-1}}{p^{n-1}} \equiv h g_{n-1} + k f_{n-1} \bmod p$$

$$\equiv h g_1 + k f_1 \bmod p$$

Comme U, f_{n-1} et g_{n-1} sont unitaires, $d^\circ(U - f_{n-1} g_{n-1}) < d^\circ U$, et par **I 5° *a)***, on peut déterminer h et k dans $\mathbb{Z}_p[x]$, et donc aussi dans $\mathbb{Z}[x]$, avec $d^\circ h < d^\circ f_1 = d^\circ f_{n-1}$, $d^\circ k < d^\circ g_{n-1}$ ce qui assure $d^\circ f_n = d^\circ f_1$ et $d^\circ g_n = d^\circ g_1$.

Application numérique. On a

$$f_1 g_1 = 1 + 2x + 3x^2 + 3x^3 + 2x^4 + x^5$$

$$U - f_1 g_1 = -25x^3 + 50x^2 - 30x + 5$$

$$\frac{U - f_1 g_1}{p} \equiv -x + 1 \bmod 5$$

D'après **I 5° *a)***, on peut choisir $h = -x(-x+1)$ et $k = -x+1$ pour avoir

$$h g_1 + k f_1 \equiv -x + 1 \bmod 5.$$

On a donc

$$f_2 = 1 - 4x + 6x^2 + x^3 \quad g_2 = 6 - 4x + x^2$$

On a ensuite $f_2 g_2 = U$, et donc $f_3 = f_2$, $g_3 = g_2$ conviennent.

6° Soit $R : R(U, U')$ la matrice définie en **I 5° *b)***. On a : $\det R \in \mathbb{Z}^*$ et soit p un nombre premier ne divisant pas $\det R$. Alors d'après **I 5° *b)***, U et U' sont premiers entre eux dans $\mathbb{F}_p[x]$.

On choisit p aussi petit que possible, avec la propriété ci-dessus. On factorise U dans $\mathbb{F}_p[x]$, en déterminant la matrice M, et la dimension r du sous-espace propre définie en **3°**. Si $r = 1$, U est irréductible dans $\mathbb{F}_p[x]$, et donc aussi dans $\mathbb{Z}[x]$. Si $r \neq 1$, on calcule une base de vecteurs propres V_i, et on applique l'algorithme du **4°**.

On utilise ensuite la question **I 6° *c)*** en calculant

$$B = \begin{pmatrix} n \\ \lfloor n/2 \rfloor \end{pmatrix} N(U) \quad , \quad n = d^\circ U.$$

Soit maintenant, pour $a \in \mathbb{Z}$, $\hat{a}$ l'image de a dans $\mathbb{F}_p$ par l'application canonique. Pour $f \in \mathbb{Z}[x]$, $f = \sum_{i=0}^{n} a_i x^i$, on définit $\hat{f} = \sum_{i=0}^{n} \hat{a}_i x^i$. Si U s'écrit $U = fg$ dans $\mathbb{Z}[x]$ alors $\hat{U} = \hat{f}\hat{g}$ et il existe $I \subset \{1, 2, \dots, r\}$ tel que $f = \prod_{i \in I} U_i$.

Pour tous les ensembles I possibles, on pose

$$f_1 = \prod_{i \in I} U_i \quad , \quad g_1 = \prod_{i \notin I} U_i$$

et l'on calcule (cf. **5°**) f_n et g_n pour n tel que $p^n > 2B$.

Ou bien on a $U = f_n g_n$ dans $\mathbb{Z}[x]$, et on a trouvé une factorisation de U, ou bien $U \neq f_n g_n$, et alors la factorisation $\hat{U} = f_1 g_1$ ne se relève pas dans $\mathbb{Z}[x]$. Lorsque l'on a trouvé une factorisation de U, on recommence à partir de chacun des facteurs déjà trouvés, et en utilisant les facteurs U_i de U dans $\mathbb{F}_p[x]$.

Application numérique. Nous avons vu au **5°** que $U(x) = f_3 g_3$ avec $g_3 = 6 - 4x + x^2$ et $f_3 = 1 - 4x + 6x^2 + x^3$. Mais g_3 est irréductible car $1 + x + x^2$ est irréductible sur $\mathbb{F}_5$. La théorie ci-dessus voudrait que l'on regarde pour f_3 les 3 factorisations possibles de $1 + x + x^2 + x^3$ dans $\mathbb{F}_5[x]$, soit

$$(x-2)(x^2-2x+2) \quad (x-3)(x^2-x+3) \quad (x-4)(x^2+1)$$

et qu'on applique à chacune d'elles la méthode exposée ci-dessus.

En fait, f_3 est irréductible sur $\mathbb{Z}[x]$: si f_3 avait une racine dans $\mathbb{Z}$, ce ne pourrait être que ± 1.

7° Soit $U(x) = A(x) B(x)$ avec $A(x) = \sum_{i=0}^{d} a_i x^i$ et $B(x) = \sum_{j=0}^{n-d} b_j x^j$. On doit avoir $u_n = a_d b_{n-d}$ et on a $u_n U = (b_{n-d} A)(a_d B)$.

Supposons maintenant que p ne divise pas u_n. On peut démontrer la question **5°** ci-dessus en supposant que les coefficients dominants de f_n et g_n sont égaux à u_n, et vérifient :

$$u_n U \equiv f_n g_n \bmod p^n,$$

qui assure que le terme de degré n s'en va dans la différence $u_n U - f_n g_n$.

On procède de même qu'en **5°** en choisissant p ne divisant pas u_n. On factorise dans $\mathbb{F}_p[x]$ le polynôme unitaire $(u_n^{-1} \bmod p) U$, et à partir d'une factorisation AB de ce polynôme, on pose $f_1 = u_n A$, $g_1 = u_n B$ et $u_n U \equiv f_1 g_1 \bmod p$. Le reste de la méthode est similaire pour factoriser $u_n U$. Il reste à calculer le PGCD des coefficients de chacun des facteurs pour obtenir la factorisation de U.

III

1° *a)* Soit $P(x) = \sum_{i=0}^{n} p_i x^i$. On a

$$P(a + bc) = \sum_{i=0}^{n} p_i (a + bc)^i = P(a) + \lambda bc$$

avec $\lambda \in \mathbb{Z}$, et

$$\frac{1}{b} P(a + bc) = 1 + \lambda c,$$

ce qui montre, par la relation de BÉZOUT que,

$$\mathrm{PGCD}\left(c, \frac{1}{b} P(a + bc) \right) = 1.$$

b) Supposons qu'il existe k nombres premiers $p_1, \dots, p_k$, tels que pour tout n, $P(n)$ s'écrive $p_1^{\alpha_1} \dots p_k^{\alpha_k}$ avec $\alpha_i \geq 0$. Choisissons $a \in \mathbb{Z}$, tel que $P(a) = b \neq 0$, et $c_0 = p_1 p_2 \dots p_k$. Pour tout t entier, le polynôme

$$Q(t) = \frac{1}{b} P(a + b c_0 t)$$

prend des valeurs qui sont, d'après *a)*, non divisibles par $p_1, p_2, \dots, p_k$. Comme il n'y a qu'un nombre fini de valeurs de t telles que $|Q(t)| = 1$, il existe t_0 tel que $Q(t_0)$ soit divisible par $p \neq p_1, p_2, \dots, p_k$ et $P(n)$ avec $n = a + b c_0 t_0$ sera multiple de p, ce qui contredit notre hypothèse.

c) F_1 et F_2 sont irréductibles dans $\mathbb{Q}[X]$, et distincts, donc ils sont premiers entre eux. Par la relation de BÉZOUT, il existe A_1 et A_2 dans $\mathbb{Q}[X]$ tels que $A_1 F_1 + A_2 F_2 = 1$. Soit N un dénominateur commun des coefficients de A_1 et A_2. On pose $G_1 = NA_1$, $G_2 = NA_2$.

2° *a)* Par la question **1° *c)***, il existe des entiers $N_{i,j}$ et des polynômes G_i et G_j tels que

$$F_i G_i + F_j G_j = N_{ij}$$

Soit $\mathscr{P}$ l'ensemble des nombres premiers divisant N_{ij} et Ω. Nous allons choisir $d_1, d_2, \dots, d_k$ premiers, et non dans $\mathscr{P}$.

Choix de d_1, y_1. D'après **1° *b)***, il existe $y_1 \in \mathbb{Z}$ et d_1 premier non dans $\mathscr{P}$ tel que d_1 divise $F_1(y_1)$. Comme d_1 ne divise aucun $N_{i,j}$, cela assure que d_1 ne divisera pas $F_j(y_1)$ pour $j \neq 1$.

Choix de d_i, y_i. Supposons choisis d_{i-1}, y_{i-1}. Soit $P(t) = F_i(y_{i-1} + d_1 d_2 \dots d_{i-1} t)$. Il existe t_i et d_i, $d_i \notin \mathscr{P} \cup \Gamma_j \neq \Gamma_i$ avec $j < i$, tel que d_i divise $P(t_i)$ et l'on pose $y_i = y_{i-1} + d_1 d_2 \dots d_{i-1} t_i$. On pose $y_0 = y_k$, et $d_1, \dots, d_k, y_0$ ont la propriété cherchée car « d_1 divise $F_1(y_1)$ » est équivalent à « d_1 divise $F_1(y_1 + \lambda d_1)$ » pour $\lambda \in \mathbb{Z}$.

b) Construisons d'abord la fonction div (*a*, *b*) qui retourne le plus grand diviseur de *a* premier avec *b* :

```
fonction div ( a, b ) ;
c := a ;
répéter
    r := pgcd ( c, b ) ;
    c := c / r ;
jusqu'à ce que r = 1 ;
div := c ;
fin ;
```

L'algorithme s'écrira alors de la façon suivante :

```
d0 := |Ω| ; B := vrai;
Pour i = 1 à k tant que B faire
    q := Fi ( Y0 ) ;
    Pour j = 1 à k tant que B faire
        Si j ≠ i alors
            q := div ( q, dj ) ;
            Si q = 1 alors B := faux ;
    fin pour ;
    di := q ;
fin pour ;
fin ;
```

Application numérique. $\Omega = 1$, $F_1 = y$, $F_2 = y + 1$, $e_1 = 2$, $e_2 = 1$. L'algorithme retourne $d_1 = 2$ et $d_2 = 3$.

c) Soit pour $1 \leq j \leq e_i$, $\gamma_i^{(j)}$ la plus grande puissance de d_i qui divise $F_i^j(y_0)$. Comme d_i divise $F_i(y_0)$, $\gamma_i^{(j)}$ est strictement croissante en j. (En général, $\gamma_i^{(j)} = j\gamma_i^{(1)}$, mais ce n'est pas toujours le cas, par exemple si $F_i(y_0) = 0$ et $d_1 = 4$, on a $\gamma_i^{(1)} = 1$, $\gamma_i^{(2)} = 3$.)

On doit avoir :

$$H_i = \omega_\ell \prod_{i=1}^{k} F_i^{\varepsilon(\ell,i)},\ 1 \leq \ell \leq r$$

avec $\omega_1 \omega_2 \dots \omega_r = \Omega$ et $\sum_{\ell=1}^{r} \varepsilon(\ell, i) = e_i$, et

$$\alpha_\ell = \omega_\ell \prod_{i=1}^{k} F_i(y_0)^{\varepsilon(\ell,i)}.$$

Quelle est la plus grande puissance de d_1 divisant α_ℓ ? C'est $\gamma_1^{\varepsilon(\ell,i)}$ puisque d_1 est premier avec ω_ℓ et $F_i(y_0)$ pour $i \geq 2$.

On peut ainsi déterminer $\varepsilon(\ell, i)$ pour tout ℓ et tout i. On calcule alors :

$$\omega_\ell = \alpha_\ell / \prod_{i=1}^{k} F_i(y_0)^{\varepsilon(\ell,i)}.$$

Application numérique. $H_1(y) = y(y+1)$; $H_2(y) = y$.

3° *a)* Pour satisfaire (IV), il suffit de choisir y_0 non racine du polynôme en y, $R(U, \partial U/\partial X)$.
Par le même raisonnement qu'en **1° *c)***, il existe des polynômes $A_0, \dots, A_n$ dans $\mathbb{Z}[Y]$ tels que :

$$A_0 V_0 + \dots + A_n V_n = M \in \mathbb{Z}$$

et le contenu de $U(x, y_0)$ sera un diviseur de M. On peut alors faire le même raisonnement qu'en **2° *a)***, en mettant dans P les facteurs premiers de M.
De même, l'algorithme de **2° *b)*** on pourra être adapté en posant $d_0 = |\Omega|$ (contenu de $U(x, y_0)$).

b) On a $V_n(y) = A_k(y) B_\ell(y)$, et par la méthode de **2° *c)***, $A_k(y)$ et $B_\ell(y)$, peuvent être déterminés puisque l'on connaît $A_k(y_0)$ et $B_\ell(y_0)$, qui sont les coefficients dominants de $A(x, y_0)$ et de $B(x, y_0)$.
Il vient ensuite :

$$U = AB = (A_k(y) x^k + S)(B_\ell(y) x^\ell + T)$$

avec

$$S = S_0(x) + \dots + S_s(x)(y - y_0)^s$$

et

$$T = T_0(x) + \dots + T_t(x)(y - y_0)^t.$$

Les S_i et T_i sont donnés par la fonction de TAYLOR, et on a $s \leq d^\circ A$ en $y \leq d^\circ U$ en y et de même $t \leq d^\circ U$ en y.

On pose

$$\tilde{U} = U - A_k(y) B_\ell(y) x^{k+\ell} = A_k(y) x^k T + B_\ell(y) x^\ell S + ST.$$

On développe chacun de ces termes par rapport à $(y - y_0)$:

$$A_k(y) = \alpha_0 + \alpha_1 (y - y_0) + \dots$$

$$B_\ell(y) = \beta_0 + \beta_1 (y - y_0) + \dots$$

$$\tilde{U} = \tilde{U}(x, y_0) + \frac{\partial \tilde{U}}{\partial y}\Big|_{y=y_0} (y - y_0) + \frac{1}{2} \frac{\partial^2 \tilde{U}}{\partial y^2}\Big|_{y=y_0} (y - y_0)^2 + \dots$$

et on identifie les termes de même degré en y_0.

On a :

$$A(x, y_0) = A_k(y_0)x^k + S_0(x)$$

$$B(x, y_0) = B_\ell(y_0)x^\ell + T_0(x)$$

ce qui donne S_0 et T_0. En degré 1,

$$\frac{\partial \tilde{U}}{\partial y}\Big|_{y=y_0} = \alpha_0 T_1 x^k + \alpha_1 T_0 x^k + \beta_0 S_1 x^\ell + \beta_1 S_0 x^\ell + S_0 T_1 + S_1 T_0,$$

soit

$$A(x, y_0)T_1 + B(x, y_0)S_1 = \frac{\partial \tilde{U}}{\partial y}\Big|_{y=y_0} - \alpha_1 T_0 x^k - \beta_1 S_0 x^\ell.$$

Or le deuxième membre est de degré $\leq k + \ell - 1$, car $d^\circ T_0 \leq \ell - 1$, $d^\circ S_0 \leq k - 1$ et $d_x^\circ \tilde{U} \leq k + \ell - 1$. Donc S_1 et T_1 sont déterminés par cette relation puisque, $U(x, y_0)$ étant sans facteurs carrés, $A(x, y_0)$ et $B(x, y_0)$ sont premiers entre eux.

En degré 2,

$$\frac{1}{2}\frac{\partial^2 \tilde{U}}{\partial y^2}\Big|_{y=y_0} = \alpha_0 T_2 x^k + \alpha_1 T_1 x^k + \alpha_2 T_0 x^k + \beta_0 S_2 x^\ell + \beta_1 S_1 x^\ell + \beta_2 S_0 x^\ell + S_0 T_2 + S_1 T_1 + S_2 T_0,$$

ce qui donne :

$$A(x, y_0)T_2 + B(x, y_0)S_2 = \frac{1}{2}\frac{\partial^2 \tilde{U}}{\partial y^2}\Big|_{y=y_0} - (\alpha_1 T_1 + \alpha_2 T_0)x^k - (\beta_1 S_1 + \beta_2 S_0)x^k - S_1 T_1,$$

ce qui fournit S_2 et T_2, etc.

Application numérique. On a $k = 3, \ell = 2, y = 2$;

$y = y_0 + (y - y_0)$ donne $\alpha_0 = 2, \alpha_1 = 1$.

$y(y+1) = y_0(y_0+1) + (2y_0+1)(y-y_0) + (y-y_0)^2$

donne $\beta_0 = 6, \beta_1 = 5, \beta_2 = 1$.

$A(x, y_0) = 2x^3 + x^2 + x + 1$, $S_0(x) = x^2 + x + 1$

$B(x, y_0) = 6x^2 + x + 1, T_0(x) = x + 1$

$$\frac{\partial \tilde{U}}{\partial y}\Big|_{y=2} = 14x^4 + 14x^3 + 25x^2 + 10x + 7$$

Les termes de degré 1 fournissent :

$$A(x, y_0)T_1 + B(x, y_0)S_1 = 8x^4 + 8x^3 + 20x^2 + 10x + 7,$$

ce qui donne (cf. I 5° ***b)***) : $T_1 = 4x + 5$ et $S_1 = -x + 2$.

$$\frac{1}{2}\frac{\partial^2 \tilde{U}}{\partial y^2}\Big|_{y=2} = 7x^4 + 4x^3 + 9x^2 + 5x + 11.$$

Les termes de degré 2 fournissent :

$$A(x, y_0)T_2 + B(x, y_0)S_2 = 2x^4 + 3x^3 + 2x^2 + 2x + 1$$

ce qui donne $T_2 = x + 1$ et $S_2 = 0$.

Comme U est de degré 3 en y et que $A_k(y)$ est de degré 1 et $B_\ell(y)$ de degré 2, on voit que $d_y^\circ(S) \leq 1$ et $d_y^\circ(T) \leq 2$, d'où $S_2 = 0$ et $S_i = T_i = 0$ pour $i \geq 3$. On obtient

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

$$= yx^3 + x^2 - (y-3)x + (2y-3)$$

et

$$B(x, y) = y(y+1)x^2 + x + 1 + (y-2)(4x+5) + (y-2)^2(x+1)$$

$$= y(y+1)x^2 + (y^2-3)x + y^2 + y - 5.$$

c) On commence par factoriser $V = V_n(y)$. Il faut ensuite chercher $y_0, d_1, \ldots, d_k$. On utilise pour cela l'algorithme 2° ***b)*** revu pour tenir compte de (V), (cf. ci-dessus 3° ***a)***) en testant $y_0 = 0$, $y_0 = \pm 1$, ... jusqu'à trouver un y_0 correct. On factorise alors $U(x, y_0)$ et on en déduit toutes les écritures possibles

$$U(x, y_0) = A(x, y_0)B(x, y_0).$$

On essaie alors de « remonter » ces factorisations en

$$U(x, y) = A(x, y)B(x, y)$$

par la méthode du 3° ***b)*** : on détermine $A_k(y)$ et $B_\ell(y)$, puis les S_i et les T_i avec $i \leq d^\circ A(x, y_0)$ et $j \leq d^0 B(x, y_0)$.

Il reste à vérifier que l'on a bien $U(x, y) = A(x, y)B(x, y)$.