# Résolution élémentaire du problème de Frobenius au moyen des bases standard

par Patrick Teller

***VERSION BETA.1***

Le problème de Frobenius consiste à déterminer pour chaque p-uplet ($a_1$,...,$a_m$) d'entiers premiers entre eux dans leur ensemble le plus grand entier qui ne peut s'écrire comme $\sum_{i=1}^{m} x_k a_k$ , où les $x_k$ sont des entiers naturels; il existe une littérature très riche sur le sujet et une grande variété de méthodes [1 ].

Nous allons montrer que l'on peut utiliser des bases standard, sous la forme que nous décrite dans [2], pour déterminer facilement ce nombre, souvent désigné comme nombre de Frobenius.

Il est vrai que la complexité de la construction des bases de Grobner est exponentielle mais il n'est pas sûr qu'il en soit ainsi dans le contexte « vectoriel » que nous avons choisi et qui est en soi un allègement du cas des binômes.

## 1. Les bases

## 1.1 La matrice-témoin

Soit la matrice A$\in\mathcal{M}_{1m}(\mathbb{N})$ et B$\in\mathbb{N}$ on désigne par (*) l'équation linéaire AX=B.

**Définition 1.** *La matrice témoin d'un système linéaire*

*Soit une matrice $A\in\mathcal{M}_{1m}(N)$ on appelera matrice témoin du système (*) la matrice* $\bar{A}=\begin{pmatrix} A \\ -I_m \end{pmatrix}=\begin{pmatrix} A_1 & A_2 & . & . & A_m \\ -1 & 0 & 0 & . & 0 \\ 0 & -1 & 0 & . & . \\ . & 0 & -1 & . & . \\ . & . & . & . & 0 \\ 0 & 0 & . & 0 & -1 \end{pmatrix}$.

**Proposition 2.** *La matrice témoin de l'équation linéaire AX=B permet de « tracer » la résolution*

Soit une matrice A$\in\mathcal{M}_{1m}(\mathbb{N})$ et $B\in\mathbb{N}$, il existe un vecteur colonne $X=\begin{pmatrix} x_1 \\ ... \\ x_m \end{pmatrix}\in\mathcal{M}_{m1}(\mathbb{N})$, tel que AX=B si seulement si, en considérant la matrice $\bar{A}=\begin{pmatrix} A \\ -I_m \end{pmatrix}=\begin{pmatrix} A_1 & A_2 & . & . & A_m \\ -1 & 0 & 0 & . & 0 \\ 0 & -1 & 0 & . & . \\ . & 0 & -1 & . & . \\ . & . & . & . & 0 \\ 0 & 0 & . & 0 & -1 \end{pmatrix}$, $\bar{A}$X$=\begin{pmatrix} B \\ -X \end{pmatrix}$, ce qui équivaut à $\begin{pmatrix} B \\ 0 \end{pmatrix}=\bar{A}X+\begin{pmatrix} 0 \\ X \end{pmatrix}$ (**).

Plutôt que résoudre le système (*) nous allons rechercher l'existence d'un vecteur $\begin{pmatrix} 0 \\ X \end{pmatrix}$ qui sera le « reste » de $\begin{pmatrix} B \\ 0 \end{pmatrix}$ modulo le semi-sous-groupe de $\mathbb{Z}^{1+m}$ engendré par les vecteurs colonnes ($\overline{A_1}$,..,$\overline{A_m}$).

Le problème c'est que ce « reste » dépend de la procédure employée, ce qui signifie que, si une réponse positive suffit, une réponse négative ne permet pas de conclure car il n'y a pas unicité du reste; nous allons substituer à la famille ($\overline{A_1}$, ...., $\overline{A_m}$) une base standard associée, pour laquelle nous établirons une telle unicité.

## 1.2. Les outils (inspirés des bases de Grobner)

Rappelons de manière succincte les définitions et propriétés des bases standard vectorielles qui ont été définies et établies dans [4]:

Nous désignerons par $\preccurlyeq$ la relation d'ordre (partiel) sur $\mathbb{N}^p$ définie comme suit $U=\begin{pmatrix} u_1 \\ ... \\ u_p \end{pmatrix} \preccurlyeq V=\begin{pmatrix} v_1 \\ ... \\ v_p \end{pmatrix} \Longleftrightarrow \forall i \in \{1,...,p\}, u_i \leqslant v_i$; on dira alors que U précède V, lorsque 0 précède U on dira que U est positif.

On désignera par $\alpha$ l'ordre lexicographique qui, lui, est un ordre total; lorsque $\begin{pmatrix} 0 \\ . \\ 0 \end{pmatrix} \alpha \begin{pmatrix} v_1 \\ ... \\ v_p \end{pmatrix}$ on dira que $\begin{pmatrix} v_1 \\ ... \\ v_p \end{pmatrix}$ est lex-positif , de meme on dira lex-strictement-positif pour lex-positif et non nul.

**Définition 3.** *Soit un p-uplet* $U=\begin{pmatrix} u_1 \\ ... \\ .; \\ u_p \end{pmatrix}$ *on notera, pour chaque i,* $u_i{}^+ = max\{u_i, 0\}$ *et* $u_i{}^- = \max\{0, -u_i\}$, $U^+=\begin{pmatrix} u_1^+ \\ ... \\ .; \\ u_p^+ \end{pmatrix}$ *et* $U^-=\begin{pmatrix} u_1^- \\ ... \\ .; \\ u_p^- \end{pmatrix}$, *d'où* $U=U^+-U^-$; *lorsque* $U \neq 0$ *on notera* $s(U)=min\{i \in [\![1,...,p]\!], u_i \neq 0\}$ *et* $U^*=U$ *lorsque* $u_{s(U)}>0$ *et* $U^*=-U$ *lorsque* $u_{s(U)}<0$; *un p-uplet U non nul, tel que* $u_{s(U)}>0$ *sera donc lex-strictement-positif.*

*On appellera support de U l'ensemble* $supp(U)=\{i, u_i \neq 0\}$ *et de même on pourra s'intéresser à* $supp(U^+)$ *et* $supp(U^-)$

*Par ailleurs on remarquera que si U est non nul alors* $U^*$ *est nécessairement lex-strictement positif.*

**Définition 4.** *Réduction d'un p uplet U par un p uplet V lex-strictement positif.*

Soit U et V deux p uplets tels que $V^+ \preccurlyeq U^{*+}$, soit $\beta = \max\left\{k \in \mathbb{N},\ 0 \preccurlyeq U^{*+} - kV^+\right\}$, d'où on posera $U=\varepsilon\beta V + W$ (où $\varepsilon = +1$ si $U^*=U, \varepsilon = -1$ si $U^* = -U$).

W sera appelé le reste de U modulo V.

Dans le cas U=0V+W on dira que U est irréductible par V.

**Exemple 5.**

$U=\begin{pmatrix} 4 \\ 3 \\ -3 \\ -2 \end{pmatrix}$, $V=\begin{pmatrix} 1 \\ 3 \\ -1 \\ -4 \end{pmatrix}$, $U=1V+ W=\begin{pmatrix} 3 \\ 0 \\ -2 \\ 2 \end{pmatrix}$, donc $U \overset{V}{\longmapsto} \begin{pmatrix} 3 \\ 0 \\ -2 \\ 2 \end{pmatrix}$

$U=\begin{pmatrix} -4 \\ -3 \\ 3 \\ 2 \end{pmatrix}$, $V=\begin{pmatrix} 1 \\ 3 \\ -1 \\ -4 \end{pmatrix}$, $U=(-1)V+W=\begin{pmatrix} -3 \\ 0 \\ 2 \\ -2 \end{pmatrix}$, donc $U \overset{V}{\longmapsto} \begin{pmatrix} -3 \\ 0 \\ 2 \\ -2 \end{pmatrix}$

$U=\begin{pmatrix} 0 \\ -3 \\ 3 \\ 2 \end{pmatrix}$, $V=\begin{pmatrix} 1 \\ 3 \\ -1 \\ -4 \end{pmatrix}$, $U^*=\begin{pmatrix} 0 \\ 3 \\ -3 \\ -2 \end{pmatrix}$ n'est pas précédé par V donc $U \overset{V}{\longmapsto} U$

**Proposition 6.** *Le processus de r*éduction *et les premières coordonnées*

***Démonstration.***

*1) Soit* $U=\begin{pmatrix} a \\ \cdots \\ \cdots \\ \cdots \end{pmatrix}$, *où* $a>0$; *il ne peut être réduit que par un vecteur lex-strictement positif* $V=\begin{pmatrix} b \\ \cdots \\ \cdots \end{pmatrix}$, *où* $0 \leqslant b \leqslant a$ *et alors* $U \overset{V}{\longmapsto} \begin{pmatrix} c \\ \cdots \\ \cdots \end{pmatrix}$, *où* $0 \leqslant c \leqslant a$.

*2) Soit* $U=\begin{pmatrix} 0 \\ a \\ \cdots \\ \cdots \end{pmatrix}$, *où* $a>0$; *il ne peut être réduit que par un vecteur lex-strictement positif* $V=\begin{pmatrix} 0 \\ b \\ \cdots \end{pmatrix}$, *où* $0 \leqslant b \leqslant a$ *et alors* $U \overset{V}{\longmapsto} \begin{pmatrix} 0 \\ c \\ \cdots \end{pmatrix}$, *où* $0 \leqslant c \leqslant a$.

*3) Soit* $U=\begin{pmatrix} 0 \\ a \\ \cdots \\ \cdots \end{pmatrix}$, *où* $a<0$; *alors* $U^*=\begin{pmatrix} 0 \\ -a \\ \cdots \\ \cdots \end{pmatrix}$*il ne peut être réduit que par un vecteur lex-strictement positif* $V=\begin{pmatrix} 0 \\ b \\ \cdots \end{pmatrix}$, *où* $0 \leqslant b \leqslant -a$ *et alors* $U \overset{V}{\longmapsto} \begin{pmatrix} 0 \\ c \\ \cdots \end{pmatrix}$. □

**Proposition 7.**

*Le reste d'un vecteur positif modulo un vecteur lex-strictement positif est positif*

***Démonstration.***

*Soit* $U=\begin{pmatrix} u_1 \\ \cdots \\ \cdots \\ u_p \end{pmatrix} \succcurlyeq 0$ *et* $V=\begin{pmatrix} v_1 \\ \cdots \\ \cdots \\ v_p \end{pmatrix}$, lex − strictement positif*;* si U n'est pas irréductible alors $\forall i$, $v_i > 0$,$u_i \geqslant v_i$ et le reste de U par V sera U-max$\{u_i/v_i, v_i>0\}$V, donc à coordonnées positives. □

**Définition 8.** *Réduction d'un p uplet U par un ensemble de p uplets lex-strictement positifs S*

*Soit le n+m–uplet U et un ensemble de p -uplets* $S=\{V_i, i \in I\}$ *on dira que U est réduit à W modulo S lorsqu'il existe un ensemble d'indices* $(i_1,..,i_q)$ *à valeurs dans I tel que* $U \overset{V_{i_1}}{\longmapsto} \overset{V_{i_2}}{\longmapsto} \ldots\ldots \overset{V_{i_q}}{\longmapsto} W$, *où W est irréductible par les différents* $V_i$*; W pourra être appelé « un reste » de U modulo S.*

**Théorème 9.** *Algorithme de construction de bases standard associée à un ensemble fini de p-uplets lex-strictement positifs* $S=\{V_i, i \in I\}$.

*On pose* $S:=\{V_i, i \in I\}$, $G:=\{\{V_i, V_j\}\}, V_i \neq V_j\}$

*tant que* $G \neq \varnothing$

*on prend* $\{V_i,\ V_j\} \in G$, *on pose* $G:=G-\{V_i,\ V_j\}$,$W:=$*une réduction de* $(V_i - V_j)$ *modulo S*

*si* $W \neq 0$ *on pose* $G:=G \cup \{\{V, W^*\}, V \in G\}, S := S \cup \{W^*\}$

*L'algorithme de Buchberger s'arrête en un temps fini.*

*On désigne par* $S_\infty$ *la famille obtenue, ce sera une base standard associée à S.*

**Exemple 10.**

On considère les trois uplets $\begin{pmatrix} 1 \\ 2 \\ -1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 3 \\ 4 \\ 0 \\ -1 \\ 0 \end{pmatrix}, \begin{pmatrix} 2 \\ 5 \\ 0 \\ 0 \\ -1 \end{pmatrix}$, l'application de l'algorithme produit les six uplets: $\begin{pmatrix} 1 \\ 0 \\ 2 \\ -1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 2 \\ 0 \\ -1 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \\ 0 \\ -1 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 2 \\ -3 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 7 \\ -1 \\ -2 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ -5 \\ 1 \\ 1 \end{pmatrix}$.

**Théorème 11.**

*Soit un ensemble fini de p uplets $S=\{V_i, i \in I\}$ et une base standard $S_\infty = \{W_j, j \in J\}$ associée à S; un n+m-uplet V appartient au sous-groupe engendré par S si et seulement il est réduit modulo $S_\infty$.*

**Théorème 12.** *Unicité du reste d'un p -uplet modulo $S_\infty$*

*Soit V un p-uplet, le reste de V modulo $S_\infty$ est unique (indépendant de la réduction appliquée).*

## 2. Application aux équations linéaires

Rappelons

**Définition 13.** *La matrice témoin d'une équation linéaire*

*Soit une matrice $A \in \mathcal{M}_{1m}(N)$ on appelera matrice témoin de l'équation la matrice* $\bar{A}=\begin{pmatrix} A \\ -I_m \end{pmatrix}=\begin{pmatrix} A1 & A2 & . & . & \mathrm{Am} \\ -1 & 0 & 0 & . & 0 \\ 0 & -1 & 0 & . & . \\ . & 0 & -1 & . & . \\ . & . & . & . & 0 \\ 0 & 0 & . & 0 & -1 \end{pmatrix}$.

**Proposition 14.** *La matrice témoin de l'équation linéaire AX=B permet de « tracer » la résolution*

Soit une matrice $A \in \mathcal{M}_{1m}(N)$ et $B \in N$, il existe un vecteur colonne $X = \begin{pmatrix} x1 \\ ... \\ \mathrm{xm} \end{pmatrix} \in \mathcal{M}_{m1}(N)$, tel que AX=B si seulement si, en considérant la matrice $\bar{A}=\begin{pmatrix} A \\ -I_m \end{pmatrix}=\begin{pmatrix} A1 & A2 & . & . & \mathrm{Am} \\ -1 & 0 & 0 & . & 0 \\ 0 & -1 & 0 & . & . \\ . & 0 & -1 & . & . \\ . & . & . & . & 0 \\ 0 & 0 & . & 0 & -1 \end{pmatrix}$, $\bar{A}\mathrm{X}=\begin{pmatrix} B \\ -X \end{pmatrix}$, ce qui équivaut à $\begin{pmatrix} B \\ 0 \end{pmatrix} = \bar{A}X + \begin{pmatrix} 0 \\ X \end{pmatrix}$ (*). Si on considère une base standard $\mathrm{S}_\infty$ associée à l'ensemble des colonnes $\bar{A}_1, ..., \bar{A}_m$ , l'égalité (*) est équivalente au fait que le reste de $\begin{pmatrix} B \\ 0 \end{pmatrix}$ modulo $\mathrm{S}_\infty$ est de la forme $\begin{pmatrix} 0 \\ X \end{pmatrix}$.

Or il a été montré plus haut (proposition 8) que le reste de $\begin{pmatrix} B \\ 0 \end{pmatrix}$ modulo $\mathrm{S}_\infty$ est nécessairement un 1+m uplet à coordonnées positives; donc la question se résume à savoir si la première coordonnée du reste est nulles ou pas; l'unicité du reste modulo $\mathrm{S}_\infty$ nous conduit donc à

**Théorème 15.**

*Soit* $\mathcal{F} = \{W_1, ..., W_t\}$ *une base standard du sous-groupe engendré par* $\left\{ \begin{pmatrix} A_1 \\ -1 \\ 0 \\ ... \\ ... \\ 0 \end{pmatrix}, \begin{pmatrix} A_2 \\ 0 \\ -1 \\ ... \\ ... \\ 0 \end{pmatrix}, ...., \begin{pmatrix} A_m \\ 0 \\ ... \\ .... \\ .... \\ -1 \end{pmatrix} \right\}$ *et* $V{:=}\begin{pmatrix} B \\ 0 \end{pmatrix} \in \mathcal{M}_{1+m,1}(\mathbb{N})$.

*V':=V*

*tant que* $V' \neq 0$

*s'il existe un* $i \in \{1, ..., t\}$ $W_i^+ \preccurlyeq V'$, *prendre* $j = min\{i, W_i^+ \preccurlyeq V'\}$

*alors si* $V' \xrightarrow{W_j} R$, $V' := R$

*Le reste de* $\begin{pmatrix} B \\ 0 \end{pmatrix}$ *modulo* $S_\infty$ *est le 1+m uplet R; si* $R = \begin{pmatrix} 0 \\ X \geqslant 0 \end{pmatrix}$ *X est solution (dans* $\mathbb{N}^m$*) de l'équation AX=B, si dans R la première coordonnée n'est pas nulle l'équation AX=B ne possède pas de solution dans* $\mathbb{N}^m$.

**Exemple 16.**

a=3, b=5, b=7

$\bar{A} = \begin{pmatrix} 3 & 5 & 7 \\ -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$; on obtient la base standard $\begin{pmatrix} 3 \\ -1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 5 \\ 0 \\ -1 \\ 0 \end{pmatrix}, \begin{pmatrix} 7 \\ 0 \\ 0 \\ -1 \end{pmatrix}, \begin{pmatrix} 2 \\ 1 \\ -1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ -2 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 2 \\ 0 \\ -1 \end{pmatrix}, \begin{pmatrix} 0 \\ 4 \\ -1 \\ -1 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \\ -1 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ -2 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 3 \\ 1 \\ -2 \end{pmatrix}, \begin{pmatrix} 0 \\ 2 \\ 3 \\ -3 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 5 \\ -4 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 7 \\ -5 \end{pmatrix}$

Montrons que l'équation x*3+y*5+z*7=19 a des solutions dans $\mathbb{N}^3$:

$\begin{pmatrix} 19 \\ 0 \\ 0 \\ 0 \end{pmatrix} \underset{\longrightarrow}{\begin{pmatrix} 7 \\ 0 \\ 0 \\ -1 \end{pmatrix}} \begin{pmatrix} 5 \\ 0 \\ 0 \\ 2 \end{pmatrix} \underset{\longrightarrow}{\begin{pmatrix} 5 \\ 0 \\ -1 \\ 0 \end{pmatrix}} \begin{pmatrix} 0 \\ 0 \\ 1 \\ 2 \end{pmatrix}$, donc 19=1*5+2*7.

**Exemple 17.** Montrons que l'équation x*3+y*5+z*7=4 n'a pas de solution

$\begin{pmatrix} 4 \\ 0 \\ 0 \\ 0 \end{pmatrix} \underset{\longrightarrow}{\begin{pmatrix} 3 \\ -1 \\ 0 \\ 0 \end{pmatrix}} \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix}$, qui n'est pas de la forme $\begin{pmatrix} 0 \\ + \\ + \\ + \end{pmatrix}$.

# 3. A la recherche du nombre de Frobenius

Soit $a_1 < a_2 \lessdot ..... < a_m$ des entiers naturels premiers entre eux dans leur ensemble et S une base standard associée à la famille $(\overline{A_1}, .., \overline{A_m})$.

On appelle nombre de Frobenius associé à un p-uplet d'entiers premiers entre eux le plus grand entier qui n'en est pas combinaison linéaire à coefficients entiers; on le notera F et on notera $L = \{x \in \mathbb{N}, \exists (x_1, ...., x_m) \in \mathbb{N}^m, x = \sum_{k=1}^{m} x_k a_k\}$; F=min(L)-1.

**Lemme 18.** *Soit* $a_1 < a_2 \lessdot ..... < a_m$ *des entiers naturels premiers entre eux dans leur ensemble et* $\forall x \in L, x + a_1 \in L$.

**Démonstration.**

Soit $x=\sum_{k=1}^{m} x_k a_k$ alors $x+a_1=(x_1+1)a_1+\sum_{k=2}^{m} x_k a_k$ □

Donc pour établir que x>F il suffit de montrer que $\{x, x+1, ..., x+a_1-1\} \subset L$, un tel entier sera appelé un pionnier de L.

**Définition 19.** *Socle d'une base standard de vecteurs de* $\mathbb{N}^n$

*Soit une base standard S on appelle socle de S la sous-famille de S formée par les vecteurs dont la première coordonnée est inférieure ou égale à 1.*

*Nous désignerons le socle de S par S'.*

*Il est facile de montrer que S' hérite de S les propriétés des bases standard: en particulier le reste modulo S' est indépendant de la procédure suivie.*

Soit un entier naturel x, $x \in L \iff \begin{pmatrix} x \\ 0 \\ . \\ 0 \end{pmatrix}$ est réduit modulo S à un vecteur de la forme (somme d'une combinaison linéaire à coefficients positifs de vecteurs de S) + $\begin{pmatrix} 0 \\ x_1 \\ ... \\ x_m \end{pmatrix}$ (coefficients positifs), alors $\begin{pmatrix} x+1 \\ 0 \\ ... \\ 0 \end{pmatrix} = \sum_{j \in J} y_j W_j + \begin{pmatrix} 1 \\ x_1 \\ ... \\ x_m \end{pmatrix}$; donc $x+1 \in L \iff \begin{pmatrix} 1 \\ x_1 \\ ... \\ x_m \end{pmatrix}$ est réduit modulo S à un vecteur de la forme $\begin{pmatrix} 0 \\ x'_1 \\ ... \\ x'_m \end{pmatrix}$ ( à coefficients positifs).

$\begin{pmatrix} 1 \\ x_1 \\ ... \\ x_m \end{pmatrix}$ est réduit modulo S à un vecteur de la forme $\begin{pmatrix} 0 \\ x'_1 \\ ... \\ x'_m \end{pmatrix}$ ( à coefficients positifs) si et seulement si le reste de $\begin{pmatrix} 1 \\ x_1 \\ ... \\ x_m \end{pmatrix}$ modulo S' est $\begin{pmatrix} 0 \\ x'_1 \\ ... \\ x'_m \end{pmatrix}$ ( à coefficients positifs).

**Définition 20.** *Soit un vecteur* $V \in Z^m$ *on désigne par S(V) (resp. S'(V)) son reste modulo S (resp. modulo S').*

D'où le

**Théorème 21.**

*Soit* $x \in N$

$$\{x, x+1, ..., x+a_1-1\} \subset L \iff \begin{cases} S\begin{pmatrix} x \\ 0 \\ 0 \\ ... \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ x_1 \geqslant 0 \\ ... \\ ... \\ x_m \geqslant 0 \end{pmatrix} \\ \text{si on pose } V_0 = \begin{pmatrix} 0 \\ x_1 \geqslant 0 \\ ... \\ ... \\ x_m \geqslant 0 \end{pmatrix}, \forall k \in \{0, ..., a_1-2\}, V_{k+1} = S'\left( V_k + \begin{pmatrix} 1 \\ 0 \\ 0 \\ ... \\ 0 \end{pmatrix} \right) \\ \forall k \in \{0, ..., a_1-2\}, V_{k+1} \text{ est de la forme } \begin{pmatrix} 0 \\ x'_1 \geqslant 0 \\ ... \\ ... \\ x'_m \geqslant 0 \end{pmatrix} \end{cases}$$

**Exemple 22.** Soit 5<8<11

La base standard (telle que la fournit l'algorithme vu plus haut):

$$S=\left(\begin{array}{c}5\\-1\\0\\0\end{array}\right),\left(\begin{array}{c}8\\0\\-1\\0\end{array}\right),\left(\begin{array}{c}11\\0\\0\\-1\end{array}\right),\left(\begin{array}{c}3\\1\\-1\\0\end{array}\right),\left(\begin{array}{c}2\\-2\\1\\0\end{array}\right),\left(\begin{array}{c}0\\1\\-2\\1\end{array}\right),\left(\begin{array}{c}1\\2\\0\\-1\end{array}\right)\left(\begin{array}{c}1\\-4\\1\\1\end{array}\right),\left(\begin{array}{c}2\\-1\\-1\\1\end{array}\right),\left(\begin{array}{c}1\\-5\\3\\0\end{array}\right),\left(\begin{array}{c}1\\1\\2\\-2\end{array}\right),\left(\begin{array}{c}0\\5\\1\\-3\end{array}\right),\left(\begin{array}{c}0\\6\\-1\\-2\end{array}\right),$$
$$\left(\begin{array}{c}1\\-3\\-1\\2\end{array}\right),\left(\begin{array}{c}0\\4\\3\\-4\end{array}\right),\left(\begin{array}{c}0\\3\\5\\-5\end{array}\right),\left(\begin{array}{c}0\\2\\7\\-6\end{array}\right),\left(\begin{array}{c}0\\1\\9\\7\end{array}\right),\left(\begin{array}{c}0\\0\\11\\-8\end{array}\right)$$

$$S'=\left(\begin{array}{c}0\\1\\-2\\1\end{array}\right),\left(\begin{array}{c}1\\2\\0\\-1\end{array}\right)\left(\begin{array}{c}1\\-4\\1\\1\end{array}\right),\left(\begin{array}{c}1\\-5\\3\\0\end{array}\right),\left(\begin{array}{c}1\\1\\2\\-2\end{array}\right),\left(\begin{array}{c}0\\5\\1\\-3\end{array}\right),\left(\begin{array}{c}0\\6\\-1\\-2\end{array}\right),\left(\begin{array}{c}1\\-3\\-1\\2\end{array}\right),\left(\begin{array}{c}0\\4\\3\\-4\end{array}\right),\left(\begin{array}{c}0\\3\\5\\-5\end{array}\right),\left(\begin{array}{c}0\\2\\7\\-6\end{array}\right),\left(\begin{array}{c}0\\1\\9\\-7\end{array}\right),\left(\begin{array}{c}0\\0\\11\\-8\end{array}\right)$$

Choisissons comme départ n=20

$\left(\begin{array}{c}20\\0\\0\\0\end{array}\right) \overset{S}{\longrightarrow} \left(\begin{array}{c}0\\4\\0\\0\end{array}\right)$ qui signifie que 4*5=20

$\left(\begin{array}{c}1\\4\\0\\0\end{array}\right)=\left(\begin{array}{c}1\\2\\0\\-1\end{array}\right)+\left(\begin{array}{c}0\\2\\0\\1\end{array}\right)$ donc $\left(\begin{array}{c}1\\4\\0\\0\end{array}\right) \overset{S'}{\longrightarrow} \left(\begin{array}{c}0\\2\\0\\1\end{array}\right)$

$\left(\begin{array}{c}1\\2\\0\\1\end{array}\right)=\left(\begin{array}{c}1\\2\\0\\-1\end{array}\right)+\left(\begin{array}{c}0\\0\\0\\2\end{array}\right)$ donc $\left(\begin{array}{c}1\\2\\0\\1\end{array}\right) \overset{S'}{\longrightarrow} \left(\begin{array}{c}0\\0\\0\\2\end{array}\right)$

$\left(\begin{array}{c}1\\0\\0\\2\end{array}\right)=\left(\begin{array}{c}1\\-3\\-1\\2\end{array}\right)+\left(\begin{array}{c}0\\3\\1\\0\end{array}\right)$ donc $\left(\begin{array}{c}1\\0\\0\\2\end{array}\right) \overset{S'}{\longrightarrow} \left(\begin{array}{c}0\\3\\1\\0\end{array}\right)$

$\left(\begin{array}{c}1\\3\\1\\0\end{array}\right)=\left(\begin{array}{c}1\\2\\0\\-1\end{array}\right)+\left(\begin{array}{c}0\\1\\1\\1\end{array}\right)$ donc $\left(\begin{array}{c}1\\3\\1\\0\end{array}\right) \overset{S'}{\longrightarrow} \left(\begin{array}{c}0\\1\\1\\1\end{array}\right)$

Donc 20,21,22,23,24 appartiennent à L, donc F<20.

Mais nous cherchons F=min(L)-1, il faut donc déterminer le plus petit x tel que $\{x, x+1, ..., x+a_1-1\} \subset L$, nous allons commencer par rechercher le plus petit multiple de $a_1$ qui soit un pionnier.

Considérons un pionnier de la forme $x=na_1$ alors l'appartenance à L de $x, x+1, ..., x+a_1-1$ et $x+a_1$ se traduit par $\left(\begin{array}{c}na_1+a_1\\0\\...\\...\\0\end{array}\right)=n\left(\begin{array}{c}a_1\\-1\\0\\...\\0\end{array}\right)+\left(\begin{array}{c}a_1\\n\\0\\...\\0\end{array}\right)$ et la réduction $\left(\begin{array}{c}a_1\\n\\0\\...\\0\end{array}\right)=\left(\begin{array}{c}1\\\sigma_{1,1}\\...\\...\\\sigma_{1,p+1}\end{array}\right)+\left(\begin{array}{c}1\\\sigma_{2,1}\\...\\...\\\sigma_{2,p+1}\end{array}\right)+....+$
$\left(\begin{array}{c}1\\\sigma_{a_1,1}\\...\\...\\\sigma_{a_1,p+1}\end{array}\right)+\left(\begin{array}{c}0\\n+1\\0\\.\\0\end{array}\right)$; ceci sera effectivement une réduction si et seulement si chaque étape est une réduction, ce qui ne dépend pas de n sauf en ce qui concerne la deuxième coordonnée pour laquelle il est nécessaire et suffisant que $\forall k \in \{1, ..., a_1-1\}$ n-$\sum_{i=1}^{k} \sigma_{k,1} \geqslant 0$.

D'où le

**Théorème 23.** *Détermination du plus petit multiple de $a_1$ qui soit un pionnier*

*1) Considérer $x=na_1$ assez grand pour que $x, x+1, ..., x+a_1-1$ et $x+a_1$ appartiennent à L.*

*(par exemple $x=(a_2-1)a_1$)*

*2) Extraire des éléments intervenant dans la réduction de* $\begin{pmatrix} a_1 \\ n \\ 0 \\ ... \\ 0 \end{pmatrix}$ *les coefficients de la deuxième ligne:* $\sigma_{1,1}$ , $\sigma_{2,1}$, ..., $\sigma_{a_1-1,1}$

*3) Soit* $N=max\{\sum_{i=1}^{k}\sigma_{k,1}, k=1,...,a_1-1\}$, $Na_1$ *est le plus petit multiple de* $a_1$ *qui soit un pionnier*

**Théorème 24.** *Détermination de F*

*Soit* $a_1<a_2<.....<a_p$ *des entiers naturels premiers entre eux dans leur ensemble, pour déterminer F*

*1. On détermine le plus petit multiple x de* $a_1$ *tel que* $\{x, x+1, ..., x+a_1-1\} \subset L$

*Soit* $\begin{pmatrix} x \\ 0 \\ . \\ ... \\ 0 \end{pmatrix} \overset{S}{\longrightarrow} \begin{pmatrix} 0 \\ x_1 \\ .... \\ x_m \end{pmatrix}$ *la réduction de* $\begin{pmatrix} x \\ 0 \\ ... \\ 0 \end{pmatrix}$ *modulo S; on pose* $V=\begin{pmatrix} 0 \\ x_1 \geqslant 0 \\ ... \\ ... \\ x_m \geqslant 0 \end{pmatrix}$

*2. Tant que la réduction de V modulo -S' est un vecteur de la forme* $W=\begin{pmatrix} 1 \\ x_1' \geqslant 0 \\ .... \\ x_m' \geqslant 0 \end{pmatrix}$ *on posera V=W-* $\begin{pmatrix} 1 \\ 0 \\ 0 \\ ... \\ 0 \end{pmatrix}$.

*Si* $V=\begin{pmatrix} 0 \\ v1 \\ .... \\ \text{vm} \end{pmatrix}$ $F=\sum_{i=1}^{m} v_i a_i$*-1.*

**Exemple 25.**

Poursuivons l'exemple précédent

V=$\begin{pmatrix} 0 \\ 4 \\ 0 \\ 0 \end{pmatrix}=\begin{pmatrix} -1 \\ 4 \\ -1 \\ -1 \end{pmatrix}+\begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \end{pmatrix}$; W=$\begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \end{pmatrix}$=, V=$\begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \end{pmatrix}$

$\begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \end{pmatrix}=\begin{pmatrix} -1 \\ -2 \\ 0 \\ 1 \end{pmatrix}+\begin{pmatrix} 1 \\ 2 \\ 1 \\ 0 \end{pmatrix}$; W=$\begin{pmatrix} 1 \\ 2 \\ 1 \\ 0 \end{pmatrix}$, V=$\begin{pmatrix} 0 \\ 2 \\ 1 \\ 0 \end{pmatrix}$

$\begin{pmatrix} 0 \\ 2 \\ 1 \\ 0 \end{pmatrix}$=impossible

impossible donc F=17.

En d'autres mots

**Notation 26.**

*Nous désignerons par T l'ensemble de m-vecteurs* $\left\{Z, \begin{pmatrix} 1 \\ -Z \end{pmatrix} \in S'\right\}$*; dans le cas de l'exemple ci-dessus* $T=\begin{pmatrix} -1 \\ 2 \\ -1 \end{pmatrix}, \begin{pmatrix} -2 \\ 0 \\ 1 \end{pmatrix}\begin{pmatrix} 4 \\ -1 \\ -1 \end{pmatrix}, \begin{pmatrix} 5 \\ -3 \\ 0 \end{pmatrix}, \begin{pmatrix} -1 \\ -2 \\ 2 \end{pmatrix}, \begin{pmatrix} -5 \\ -1 \\ 3 \end{pmatrix}, \begin{pmatrix} -6 \\ 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 3 \\ 1 \\ -2 \end{pmatrix}, \begin{pmatrix} -4 \\ -3 \\ 4 \end{pmatrix}, \begin{pmatrix} -3 \\ -5 \\ 5 \end{pmatrix}, \begin{pmatrix} -2 \\ -7 \\ 6 \end{pmatrix}, \begin{pmatrix} -1 \\ -9 \\ 7 \end{pmatrix}, \begin{pmatrix} 0 \\ -11 \\ 8 \end{pmatrix}$

D'où une formulation plus claire:

**Théorème 27.** *Détermination de F*

*Soit* $a_1 < a_2 \leqslant ..... < a_p$ *des entiers naturels premiers entre eux dans leur ensemble, pour déterminer F*

*1. On détermine le plus petit multiple x de* $a_1$ *tel que* $\{x, x+1, ..., x+a_1-1\} \subset L$

*Soit* $\begin{pmatrix} x \\ 0 \\ . \\ ... \\ 0 \end{pmatrix} \overset{S}{\longrightarrow} \begin{pmatrix} 0 \\ x_1 \\ .... \\ x_m \end{pmatrix}$ *la réduction de* $\begin{pmatrix} x \\ 0 \\ ... \\ 0 \end{pmatrix}$ *modulo S;* $V := \begin{pmatrix} x_1 \geqslant 0 \\ ... \\ ... \\ x_m \geqslant 0 \end{pmatrix}$

*2. Tant qu'il existe* $W \in T$, $V \geqslant W$ $V := V - W$

*Si* $V = \begin{pmatrix} v_1 \\ .... \\ v_m \end{pmatrix}$ $F = \sum_{i=1}^{m} v_i a_i - 1$.

# Conclusion

Pour déterminer le nombre de Frobenius associé aux entiers $a_1 < a_2 \leqslant ..... < a_m$ premiers entre eux dans leur ensemble nous proposons

1. Détermination d'une base standard associée aux vecteurs $(\overline{A_1}, .., \overline{A_m})$: cette partie est la plus lourde (complexité à évaluer) mais n'est sollicitée qu'une fois.

2. Détermination du plus petit multiple x de $a_1$ tel que $\{x, x+1, ..., x+a_1-1\} \subset$ L.

3. La « descente » vers F: une réduction modulo T.

**Remarque 28.**

De la méthode employée dans le Théorème 23 on pourrait aussi déduire une démonstration de l'existence de F.

Bibliographie:

[1] J.L.RamirezAlfonsin, The diophantine Frobenius Problem, Oxford lecture Series in Mathematics and Applications, 30

[2] P. Teller, Une version vectorielle des bases standard, www.lalgebrisant.fr

Paris 01/12/2016