

Et si on étendait Euclide étendu ?

PAR PATRICK TELLER

L'algorithme d'Euclide étendu permet de trouver deux entiers (u,v) tels que $au+bv=d$, où d est le plus grand diviseur commun des entiers a et b ; cet algorithme se prête aussi à une présentation facile sous forme de tableau (pour « travailler à la main ») ou de matrice (dans le cas d'un calcul formel); Euclide au service de Bezout !

Mais le même théorème de Bezout affirme qu'il existe des entiers (u_1, \dots, u_n) tels que $\sum_{i=1}^n u_i x_i = d$, où d est le plus grand diviseur commun de (x_1, \dots, x_n) , nous allons voir une présentation sous forme de tableau qui le permet.

On trouvera au-dessous une présentation sous forme de tableau de l'algorithme d'Euclide étendu, dans le cas de n entiers.

1 L'algorithme

Nous noterons (comme Maxima) le quotient de deux entiers $\text{quotient}(b,a)$

Soient les entiers $x_1 < x_2 < \dots < x_n$

M sera une matrice à $1+n$ lignes et $1+n$ colonnes numérotées de 0 à n

1. $\forall i \in \{1, \dots, n\}, M[0,i] := x_i$
2. $\forall i \in \{1, \dots, n\} M[i,i] := 1$
3. $i := 1$

Tant que $M[i,0] > 0$ $\text{Li-1:Li+1}; \text{Li+1:Li, Li:Li-1-quotient}(M[i-1,0], M[i+1,0]) * \text{Li+1}; i := i+1$

fin.

Alors $\sum_{j=1}^n M[n, j] x_j = M[n,0]$ (qui est le pgcd).

Exemple 1.

Soient $(4,7,18,24)$ dont le pgcd est égal à 1; nous classons les entiers par ordre croissant.

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 4 & 1 & 0 & 0 & 0 \\ 7 & 0 & 1 & 0 & 0 \\ 18 & 0 & 0 & 1 & 0 \\ 24 & 0 & 0 & 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 7 & 0 & 1 & 0 & 0 \\ 3 & -1 & 1 & 0 & 0 \\ 4 & 1 & 0 & 0 & 0 \\ 18 & 0 & 0 & 1 & 0 \\ 24 & 0 & 0 & 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 4 & 1 & 0 & 0 & 0 \\ 1 & 2 & -1 & 0 & 0 \\ 3 & -1 & 1 & 0 & 0 \\ 18 & 0 & 0 & 1 & 0 \\ 24 & 0 & 0 & 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 3 & -1 & 1 & 0 & 0 \\ 0 & 7 & 4 & 0 & 0 \\ 1 & 2 & -1 & 0 & 0 \\ 18 & 0 & 0 & 1 & 0 \\ 24 & 0 & 0 & 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 3 & -1 & 1 & 0 & 0 \\ 18 & 0 & 0 & 1 & 0 \\ 0 & 0 & -18 & 1 & 0 \\ 1 & 2 & -1 & 0 & 0 \\ 24 & 0 & 0 & 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 3 & -1 & 1 & 0 & 0 \\ 18 & 0 & 0 & 1 & 0 \\ 24 & 0 & 0 & 0 & 1 \\ 0 & -48 & 24 & 0 & 1 \\ 1 & 2 & -1 & 0 & 0 \end{pmatrix}$$

d'où $1=2*4 + (-1)*7$

Exemple 2.

$$\begin{pmatrix} 0 & 0 & 0 & 0 \\ 4 & 1 & 0 & 0 \\ 6 & 0 & 1 & 0 \\ 15 & 0 & 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 6 & 0 & 1 & 0 \\ 2 & -1 & 1 & 0 \\ 4 & 1 & 0 & 0 \\ 15 & 0 & 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 4 & 1 & 0 & 0 \\ 0 & 3 & -2 & 0 \\ 2 & -1 & 1 & 0 \\ 15 & 0 & 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 4 & 1 & 0 & 0 \\ 15 & 0 & 0 & 1 \\ 1 & 7 & -7 & 1 \\ 2 & -1 & 1 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 4 & 1 & 0 & 0 \\ 2 & -1 & 1 & 0 \\ 0 & -15 & 15 & -2 \\ 1 & 7 & -7 & 1 \end{pmatrix}$$

d'où $1=7*4-7*6+1*15$

Paris le 28/11/2016