PGCD d'Euclide et matrices (Wikipedia, Denise Vella-Chemla, 4.12.2018)

On veut calculer le plus grand commun diviseur (*pgcd*) de 9 et 6.

Les deux égalités obtenues par l'exécution de l'algorithme d'Euclide :

$$9 = 1 \times 6 + 3 \;\; (a = q_0 \times b + r_0)$$
$$6 = 2 \times 3 + 0 \;\; (b = q_1 \times r_0 + r_1)$$

sont codées par les matrices de la forme $\begin{pmatrix} q_i & 1 \\ 1 & 0 \end{pmatrix}$ suivantes $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$ et $\begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}$.

On effectue leur produit pour obtenir la matrice $M = \begin{pmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 3 & 1 \\ 2 & 1 \end{pmatrix}$.

L'inverse de M est $M^{-1} = \begin{pmatrix} m_{22} & -m_{12} \\ -m_{21} & m_{11} \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ -2 & 3 \end{pmatrix}$.

Le *pgcd* de 9 et 6 est ainsi trouvé en calculant le produit (dans lequel l'exposant de -1 est le nombre de matrices intervenant dans le produit calculant M ci-dessus) :

$$(-1)^2 \begin{pmatrix} 1 & -1 \\ -2 & 3 \end{pmatrix} \begin{pmatrix} 9 \\ 6 \end{pmatrix} = \begin{pmatrix} 3 \\ 0 \end{pmatrix}$$

Note : bien qu'on ait $pgcd(x, y) = pgcd(y, x)$, la multiplication des matrices, par exemple $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$ et $\begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}$ est non-commutative. Ainsi :

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 3 & 1 \\ 2 & 1 \end{pmatrix}$$

tandis que

$$\begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 3 & 2 \\ 1 & 1 \end{pmatrix}$$

On a :

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} \neq \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$$

On peut de cette manière voir les nombres premiers comme mettant en relation les nombres dont ils sont *pgcd*. Les nombres premiers sont les éléments minimaux de la relation d'ordre partiel induite sur les entiers par la relation de divisibilité.

Transcription de l'extrait de l'article de Wikipedia concernant le pgcd calculé par des matrices
L'identité de Bézout établit que le plus grand commun diviseur g de deux entiers a et b peut être représenté par une combinaison linéaire de a et b. En d'autres termes, on peut toujours trouver deux entiers s et t tels que $g = sa + tb$.

Les entiers solutions de l'identité de Bézout peuvent être trouvés en utilisant une méthode de calcul matriciel.
La séquence d'équations de l'algorithme d'Euclide

$$a = q_0 b + r_0$$
$$b = q_1 r_0 + r_1$$
$$\vdots$$
$$r_{N-2} = q_N r_{N-1} + 0$$

peut s'écrire comme un produit de matrices quotients de taille 2×2 multipliées par un vecteur colonne reste de deux lignes.

$$\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} q_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} b \\ r_0 \end{pmatrix} = \begin{pmatrix} q_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} r_0 \\ r_1 \end{pmatrix} = \cdots = \prod_{i=0}^{N} \begin{pmatrix} q_i & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} r_{N-1} \\ 0 \end{pmatrix}.$$

M représente le produit de toutes les matrices quotient.

$$\mathbf{M} = \begin{pmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{pmatrix} = \prod_{i=0}^{N} \begin{pmatrix} q_i & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} q_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} q_N & 1 \\ 1 & 0 \end{pmatrix}.$$

L'algorithme d'Euclide se simplifie ainsi en la forme :

$$\begin{pmatrix} a \\ b \end{pmatrix} = \mathbf{M} \begin{pmatrix} r_{N-1} \\ 0 \end{pmatrix} = \mathbf{M} \begin{pmatrix} g \\ 0 \end{pmatrix}.$$

Pour exprimer g comme une combinaison linéaire de a et b, les deux côtés de l'équation peuvent être multipliés par l'inverse de la matrice **M**. Le déterminant de **M** est égal à $(-1)^{N+1}$, puisqu'il est égal au produit des déterminants des matrices quotients, chacun de ces déterminants valant -1. Puisque le déterminant de **M** n'est jamais nul, le dernier vecteur des restes peut être calculé en utilisant l'inverse de **M**.

$$\begin{pmatrix} g \\ 0 \end{pmatrix} = \mathbf{M}^{-1} \begin{pmatrix} a \\ b \end{pmatrix} = (-1)^{N+1} \begin{pmatrix} m_{22} & -m_{12} \\ -m_{21} & m_{11} \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix}.$$

Puisque l'équation ci-dessus donne

$$g = (-1)^{N+1}(m_{22}a - m_{12}b),$$

les deux entiers solutions de l'identité de Bézout sont $s = (-1)^{N+1}m_{22}$ and $t = (-1)^{N}m_{12}$. La méthode par les matrices est aussi efficace que la méthode récursive, avec deux multiplications et deux additions à chaque étape de l'algorithme d'Euclide.