

La méthode matricielle de Blankinship pour déterminer une solution particulière d'une équation diophantienne linéaire

BAKIR FARHI

Département de Mathématiques

Université de Béjaia

Algérie

bakir.farhi@gmail.com

<http://farhi.bakir.free.fr/>

Béjaia, le 14 avril 2017

1 Introduction

Soit à résoudre dans $\mathbb{Z}^2$ une équation diophantienne linéaire :

$$ax + by = c \quad (\star)$$

(avec $a, b \in \mathbb{Z}^*$ et $c \in \mathbb{Z}$).

On sait que la condition nécessaire et suffisante pour que $(\star)$ possède des solutions est « pgcd(a, b) divise c ». On sait aussi que, sous cette condition, une solution particulière de l'équation $(\star)$ permet de déterminer immédiatement sa solution générale (en utilisant le lemme de Gauss). Lorsque les entiers a et b sont “petits” en valeurs absolues, une solution particulière de $(\star)$ peut être trouvée de tête (i.e., par tâtonnement) ; mais lorsque a et b sont assez grands, une méthode de recherche d'une telle solution s'impose. En fait, l'algorithme d'Euclide (calculant pgcd(a, b)) permet de déterminer une solution particulière de $(\star)$ (on écrit chaque reste des divisions de l'algorithme en fonction du divisant et du diviseur de la même division en commençant de la dernière division à la première). La méthode de Blankinship [1] permet de réaliser le même objectif mais d'une façon plus apaisante en utilisant les matrices de $\mathcal{M}_{2 \times 3}(\mathbb{Z})$.

2 Description de la méthode de Blankinship

Supposons que l'équation $(\star)$ possède des solutions dans $\mathbb{Z}^2$, c'est-à-dire qu'on a $\text{pgcd}(a, b)/c$. La méthode de Blankinship pour déterminer une solution particulière de $(\star)$ consiste en ce qui suit :

On démarre de la matrice :

$$A_0 := \begin{pmatrix} 1 & 0 & a \\ 0 & 1 & b \end{pmatrix}$$

et on lui applique une succession de transformations matricielles où chaque transformation consiste à remplacer une des deux lignes L_i ($i = 1$ ou 2) par un vecteur ligne de la forme $L_i + kL_j$ (avec $k \in \mathbb{Z}$), où $j \in \{1, 2\}$ et $j \neq i$. Par exemple, la ligne L_1 peut être remplacée par $(L_1 - 3L_2)$; de même, la ligne L_2 peut être remplacée par $(L_2 + 5L_1)$, etc. Le but de ces transformations est de réduire (en valeurs absolues) les entiers a et b . Ainsi, l'entier k qu'on utilise lorsqu'on arrive à une matrice

$$A_i = \begin{pmatrix} * & * & \alpha \\ * & * & \beta \end{pmatrix},$$

en supposant $\alpha > \beta > 0$ par exemple, est simplement égale à l'opposé du résultat de la division euclidienne de α sur β ; de sorte que $(\alpha + k\beta)$ soit égale au reste de la division euclidienne de α sur β et soit donc strictement plus petit que β . On poursuit ces transformations matricielles jusqu'à l'obtention d'une matrice dont l'un des coefficients de la troisième colonne vaut c ou divise c (ceci est toujours possible d'après l'algorithme d'Euclide du calcul de $\text{pgcd}(a, b)$). La dernière matrice qu'on obtient nous fournira alors une solution particulière de $(\star)$, comme le précise la proposition suivante et le corollaire qui la suit :

Proposition 1. Soient $a, b \in \mathbb{Z}^*$. En partant de la matrice $A_0 := \begin{pmatrix} 1 & 0 & a \\ 0 & 1 & b \end{pmatrix}$, toute matrice A intervenant dans l'algorithme de Blankinship vérifie :

$$A \begin{pmatrix} a \\ b \\ -1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}.$$

Démonstration. Désignons par A_i ($i \in \mathbb{N}$) la $i^{\text{ème}}$ matrice intervenant dans l'algorithme de Blankinship. Nous montrons alors le résultat de la proposition par récurrence sur i .

- Pour $i = 0$: on a

$$A_0 \begin{pmatrix} a \\ b \\ -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & a \\ 0 & 1 & b \end{pmatrix} \begin{pmatrix} a \\ b \\ -1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix},$$

comme il fallait le prouver.

- Soit $i \in \mathbb{N}$. Supposons que $A_i \begin{pmatrix} a \\ b \\ -1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$ et montrons que $A_{i+1} \begin{pmatrix} a \\ b \\ -1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$. D'après

la description de l'algorithme de Blankinship, la matrice A_{i+1} s'obtient à partir de la matrice A_i de l'une des deux façons suivantes :

- Ou bien, on remplace la 1^{ère} ligne L_1 de A_i par $(L_1 + kL_2)$, avec $k \in \mathbb{Z}$ et L_2 est la 2nde ligne de A_i . Ce qui revient à écrire :

$$A_{i+1} = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} A_i.$$

- Ou bien, on remplace la 2nde ligne L_2 de A_i par $(L_2 + kL_1)$, avec $k \in \mathbb{Z}$. Ce qui revient à écrire :

$$A_{i+1} = \begin{pmatrix} 1 & 0 \\ k & 1 \end{pmatrix} A_i.$$

On voit que dans les deux cas, on a :

$$A_{i+1} = MA_i \quad (\text{avec } M \in \mathcal{M}_2(\mathbb{Z})).$$

Il s'ensuit de cela qu'on a :

$$\begin{aligned} A_{i+1} \begin{pmatrix} a \\ b \\ -1 \end{pmatrix} &= (MA_i) \begin{pmatrix} a \\ b \\ -1 \end{pmatrix} = M \left(A_i \begin{pmatrix} a \\ b \\ -1 \end{pmatrix} \right) \\ &= M \begin{pmatrix} 0 \\ 0 \end{pmatrix} \quad (\text{d'après notre hypothèse de récurrence}) \\ &= \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \end{aligned}$$

comme il fallait le prouver.

Ceci achève cette récurrence et confirme le résultat de la proposition. $\square$

Corollaire 2. Soient $a, b \in \mathbb{Z}^*$ et $c \in \mathbb{Z}$ tels que $\text{pgcd}(a, b)/c$. On considère l'algorithme de Blankinship débutant par la matrice $\begin{pmatrix} 1 & 0 & a \\ 0 & 1 & b \end{pmatrix}$ et s'achevant par une matrice $\begin{pmatrix} x_0 & y_0 & d \\ x_1 & y_1 & d' \end{pmatrix}$ tel que l'un au moins des deux entiers d et d' divise c .

Alors si d/c , le couple $(x_0 \frac{c}{d}, y_0 \frac{c}{d})$ est une solution particulière (dans $\mathbb{Z}^2$) de l'équation diophantienne $ax + by = c$ et si d'/c , le couple $(x_1 \frac{c}{d'}, y_1 \frac{c}{d'})$ est une solution particulière (dans $\mathbb{Z}^2$) de la même équation.

Démonstration. D'après la proposition 1, on a :

$$\begin{pmatrix} x_0 & y_0 & d \\ x_1 & y_1 & d' \end{pmatrix} \begin{pmatrix} a \\ b \\ -1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}.$$

Ce qui donne :

$$ax_0 + by_0 = d \quad (1)$$

$$ax_1 + by_1 = d' \quad (2)$$

Il suffit alors de multiplier les deux membre de (1) par $\frac{c}{d}$ (lorsque d/c) et les deux membres de (2) par $\frac{c}{d'}$ (lorsque d'/c) pour obtenir les solutions particulières énoncées par le corollaire pour l'équation diophantienne $ax + by = c$. La démonstration est achevée. $\square$

Remarque : Pour déterminer une solution particulière (dans $\mathbb{Z}^2$) d'une équation diophantienne $ax + by = c$ (avec $a, b \in \mathbb{Z}^*$, $c \in \mathbb{Z}$ et $\text{pgcd}(a, b)/c$) en utilisant l'algorithme de Blankinship, il est plus commode (en pratique) de partir de la matrice

$$A_0 = \begin{pmatrix} 1 & 0 & |a| \\ 0 & 1 & |b| \end{pmatrix}.$$

L'application du résultat de la proposition 1 à la dernière matrice que l'on obtient fournit immédiatement une solution particulière de l'équation en question.

3 Exemples

Exemple 1. Déterminons, par la méthode de Blankinship, une solution particulière (dans $\mathbb{Z}^2$) à l'équation diophantienne :

$$38x - 141y = 1.$$

Pour ce faire, on prend comme matrice de départ :

$$A_0 = \begin{pmatrix} 1 & 0 & 38 \\ 0 & 1 & 141 \end{pmatrix}.$$

La division euclidienne de 141 sur 38 donne 3 et reste 27. Ce qui suggère d'utiliser la transformation $L_2 \rightarrow L_2 - 3L_1$, qui transforme A_0 en :

$$A_1 = \begin{pmatrix} 1 & 0 & 38 \\ -3 & 1 & 27 \end{pmatrix}.$$

La division euclidienne de 38 sur 27 donne 1 et reste 11. Ce qui suggère d'utiliser la transformation $L_1 \rightarrow L_1 - L_2$, qui transforme A_1 en :

$$A_2 = \begin{pmatrix} 4 & -1 & 11 \\ -3 & 1 & 27 \end{pmatrix}.$$

La division euclidienne de 27 sur 11 donne 2 et reste 5. Ce qui suggère d'utiliser la transformation $L_2 \rightarrow L_2 - 2L_1$, qui transforme A_2 en :

$$A_3 = \begin{pmatrix} 4 & -1 & 11 \\ -11 & 3 & 5 \end{pmatrix}.$$

La division euclidienne de 11 sur 5 donne 2 et reste 1. Ce qui suggère d'utiliser la transformation $L_1 \rightarrow L_1 - 2L_2$, qui transforme A_3 en :

$$A_4 = \begin{pmatrix} 26 & -7 & 1 \\ -11 & 3 & 5 \end{pmatrix}.$$

Nous pouvons nous arrêter là puisque le premier coefficient de la 3^{ème} colonne de A_4 (égale à 1) divise le second membre de l'équation proposée (à savoir 1). D'après la proposition 1, on a :

$$A_4 \begin{pmatrix} 38 \\ 141 \\ -1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix},$$

c'est-à-dire :

$$\begin{pmatrix} 26 & -7 & 1 \\ -11 & 3 & 5 \end{pmatrix} \begin{pmatrix} 38 \\ 141 \\ -1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}.$$

Ce qui entraîne (en particulier) que :

$$26 \times 38 - 7 \times 141 - 1 = 0$$

et montre que le couple $\boxed{(26, 7)}$ est une solution particulière de l'équation proposée. $\square$

Exemple 2. Déterminons, en utilisant la méthode de Blankinship, une solution particulière (dans $\mathbb{Z}^2$) pour l'équation diophantienne :

$$116x + 37y = 6.$$

On part de la matrice

$$A_0 = \begin{pmatrix} 1 & 0 & 116 \\ 0 & 1 & 37 \end{pmatrix}.$$

Par $L_1 \rightarrow L_1 - 3L_2$, on transforme A_0 en

$$A_1 = \begin{pmatrix} 1 & -3 & 5 \\ 0 & 1 & 37 \end{pmatrix}.$$

Ensuite, par $L_2 \rightarrow L_2 - 7L_1$, on transforme A_1 en

$$A_2 = \begin{pmatrix} 1 & -3 & 5 \\ -7 & 22 & 2 \end{pmatrix}.$$

Nous pouvons nous arrêter là puisque le second coefficient de la dernière colonne de A_2 (qui vaut 2) divise le second membre de l'équation proposée (à savoir 6). D'après la proposition 1, on a :

$$A_2 \begin{pmatrix} 116 \\ 37 \\ -1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix},$$

c'est-à-dire

$$\begin{pmatrix} 1 & -3 & 5 \\ -7 & 22 & 2 \end{pmatrix} \begin{pmatrix} 116 \\ 37 \\ -1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}.$$

Ceci entraîne en particulier :

$$-7(116) + 22(37) - 2 = 0,$$

i.e.,

$$116(-7) + 37(22) = 2.$$

En multipliant par 3, il vient que

$$116(-21) + 37(66) = 6.$$

Ce qui montre que le couple $\boxed{(-21, 66)}$ est une solution particulière de l'équation proposée. $\square$

Références

- [1] W.A. BLANKINSHIP. A new version of the Euclidean algorithm, *Amer. Math. Monthly*, **70** (1963), p. 742-745.