Université Paris 7 — 19 octobre 1994
U.F.R. de Mathématiques — B. Keller
D.E.U.G. Mathématiques : MT 282

L'algorithme d'Euclide–Bézout

Soient $a, b, c \in \mathbf{Z}$ tels que $(a, b) \neq (0, 0)$. L'algorithme suivant sert à calculer le PGCD (a, b) et la solution générale $(x, y) \in \mathbf{Z}^2$ de l'équation de Bézout

$$a\,x + b\,y = c.$$

L'algorithme se présente sous forme d'un tableau. Dans une première étape on remplit les deux premières lignes comme indiquées dans le tableau ci-dessous. Le coefficient q_1 n'est pas défini; le coefficient q_2 est le quotient de la division euclidienne de a par b. Les lignes suivantes se calculent chacune en fonction des deux précédentes comme indiquée ci-dessous.

k	r_k	q_k	x_k	y_k	
1	a	$*$	1	0	
2	b	q_2	0	1	$a = q_2\,b + r_3$ est une div. eucl.
3	r_3	...	...	...	
⋮					
$k-1$	r_{k-1}	q_{k-1}	x_{k-1}	y_{k-1}	
k	r_k	q_k	x_k	y_k	$r_{k-1} = q_k\,r_k + r_{k+1}$ est une div. eucl.
$k+1$	r_{k+1}	q_{k+1}	x_{k+1}	y_{k+1}	$x_{k+1} = x_{k-1} - q_k x_k$, $y_{k+1} = y_{k-1} - q_k y_k$
⋮					
N	r_N	q_N	x_N	y_N	
$N+1$	$r_{N+1} = 0$	$*$	x_{N+1}	y_{N+1}	

La première colonne contient donc les restes des divisions euclidiennes successives, la deuxième colonne les quotients et les deux dernières colonnes des coefficients x_k, y_k tels que $a\,x_k + b\,y_k = r_k$ (voir la démonstration ci-dessous).

Les coefficients de la première colonne forment une suite strictement décroissante de nombres positifs entiers. Par définition, N est le plus petit entier avec $r_{N+1} = 0$.

Théorème. *On a $r_N = PGCD(a, b)$. Si $PGCD(a, b)$ divise c, la solution générale de l'équation*

$$ax + by = c$$

est donnée par

$$\begin{aligned} x &= \frac{c}{PGCD(a,b)} x_N + l x_{N+1} \\ y &= \frac{c}{PGCD(a,b)} y_N + l y_{N+1} \end{aligned}$$

où $l \in \mathbf{Z}$. Si $PGCD(a, b)$ ne divise pas c, l'équation $ax + by = c$ n'admet pas de solution $(x, y) \in \mathbf{Z}^2$.

Exemple. Nous cherchons le PGCD $(198, 75)$ et toutes les solutions de l'équation $198x + 75y = \text{PGCD}\,(198, 75)$. Nous obtenons le tableau

k	r_k	q_k	x_k	y_k
1	198	$*$	1	0
2	75	2	0	1
3	48	1	1	-2
4	27	1	-1	3
5	21	1	2	-5
6	6	3	-3	8
7	3	2	11	-29
8	0	$*$	-25	66

Ainsi PGCD $(198, 75) = 3$ et la solution générale de l'équation $198x + 75y = 3$ est donnée par

$$\begin{aligned} x &= 11 - 25l \\ y &= -29 + 66l \end{aligned}$$

où $l \in \mathbf{Z}$.

Notons que $25 = 75/3$ et $66 = 198/3$. Notons aussi que les dernières deux colonnes sont des suites alternées et que les modules de x_k, y_k sont strictement croissants pour $k \geq 3$. En particulier, nous avons $0 \leq x_N < -(-25)$ et $-66 < y_N \leq 0$. La solution (x_N, y_N) est la seule avec ces propriétés. Les coefficients q_k apparaissent dans l'identité

$$\frac{198}{75} = 2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{2}}}}} \quad .$$

Voir les exercices après la démonstration.

Démonstration. Notons d'abord que l'algorithme s'arrête. En effet, r_{k+1} est le reste d'une division euclidienne par r_k. Donc r_{k+1} est compris entre 0 et $r_k - 1$. Les r_k forment donc une suite strictement décroissante de nombres positifs entiers. Une telle suite doit aboutir à zéro après un nombre fini d'étapes.

Montrons que $r_N = \text{PGCD}\,(a, b)$. Montrons d'abord que nous avons

$$\text{PGCD}\,(r_{k-1}, r_k) = \text{PGCD}\,(r_k, r_{k+1}).$$

En effet, par construction, nous avons une équation

$$r_{k-1} = q_k r_k + r_{k+1}.$$

Elle montre que l'ensemble des diviseurs communs à r_{k-1} et r_k est égal à l'ensemble des diviseurs communs à r_k et r_{k+1}. En particulier, les plus grands éléments de ces ensembles sont égaux. La formule pour r_N s'ensuit par récurrence :

$$\begin{aligned} \text{PGCD}\,(a, b) &= \text{PGCD}\,(b, r_3) = \ldots \\ &= \text{PGCD}\,(r_{N-1}, r_N) = \text{PGCD}\,(r_N, r_{N+1}) = \text{PGCD}\,(r_N, 0) = r_N. \end{aligned}$$

Pour montrer la deuxième affirmation, nous introduisons les matrices

$$S_k = \begin{bmatrix} x_k & x_{k+1} \\ y_k & y_{k+1} \end{bmatrix}, k \geq 1.$$

Nous avons

$$S_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \text{ et } S_{k+1} = S_k \begin{bmatrix} 0 & 1 \\ 1 & -q_{k+1} \end{bmatrix}.$$

Par récurrence, il s'ensuit que

$$[a \;\; b]S_k = [r_k \;\; r_{k+1}] \quad \text{et} \quad \text{dét}\, S_k = -(-1)^k.$$

En particulier, nous avons $[a \;\; b]S_N = [r_N \;\; 0]$ et la matrice

$$S_N^{-1} = -(-1)^N \begin{bmatrix} y_{N+1} & -x_{N+1} \\ -y_N & x_N \end{bmatrix}$$

est *à coefficients entiers*. Donc si nous posons

$$\begin{bmatrix} u \\ v \end{bmatrix} = S_N^{-1} \begin{bmatrix} x \\ y \end{bmatrix},$$

alors u, v sont des *entiers*. Nous avons

$$[a \;\; b] \begin{bmatrix} x \\ y \end{bmatrix} = [a \;\; b]S_N S_N^{-1} \begin{bmatrix} x \\ y \end{bmatrix} = [r_N \;\; 0] \begin{bmatrix} u \\ v \end{bmatrix}$$

de façon que l'équation

$$[a \;\; b] \begin{bmatrix} x \\ y \end{bmatrix} = c \quad (\text{resp. } ax + by = c)$$

est équivalente à l'équation

$$[r_N \;\; 0] \begin{bmatrix} u \\ v \end{bmatrix} = c \quad (\text{resp. } r_N u + 0\, v = c).$$

Or il est clair que cette dernière équation admet des solutions si et seulement si r_N divise c et que dans ce cas la solution générale est

$$\begin{bmatrix} u \\ v \end{bmatrix} = \begin{bmatrix} c/r_N \\ l \end{bmatrix},$$

où $l \in \mathbf{Z}$. Donc l'équation $ax + by = c$ admet des solutions si et seulement si r_N divise c et dans ce cas la solution générale est

$$\begin{bmatrix} x \\ y \end{bmatrix} = S_N \begin{bmatrix} u \\ v \end{bmatrix} = \begin{bmatrix} x_N & x_{N+1} \\ y_N & y_{N+1} \end{bmatrix} \begin{bmatrix} c/r_N \\ l \end{bmatrix} = \begin{bmatrix} \frac{c}{r_N} x_N + l x_{N+1} \\ \frac{c}{r_N} y_N + l y_{N+1} \end{bmatrix}.$$

Exercices. 1) Trouver toutes les solutions $(x, y) \in \mathbf{Z}^2$ des équations suivantes : a) $5x+3y = 2$, b) $4x+9y = 1$, c) $17x+68y = 3$, d) $20x+30y = 0$, e) $1789x+1994y = 1$ f) $1994x + 666y = 2$.

2) Avec les notations de l'algorithme d'Euclide-Bézout, montrer que

$$x_{N+1} = (-1)^N \frac{c}{\text{PGCD}\,(a,b)} \text{ et } y_{N+1} = -(-1)^N \frac{a}{\text{PGCD}\,(a,b)}.$$

Indication : On pourra utiliser l'identité

$$\begin{bmatrix} a & b \\ -y_N & x_N \end{bmatrix} S_N = \begin{bmatrix} r_N & 0 \\ 0 & -(-1)^N \end{bmatrix}.$$

3) Supposons $a > b > 0$. Avec les notations de l'algorithme d'Euclide-Bézout, montrer que

$$\frac{a}{b} = q_2 + \frac{r_3}{b} = q_2 + \frac{1}{q_3 + \dfrac{r_4}{r_3}} = q_2 + \frac{1}{q_3 + \dfrac{1}{q_4 + \dfrac{r_5}{r_4}}} = \dots$$

4) Nous allons caractériser la solution (x_N, y_N) fournie par l'algorithme d'Euclide-Bézout parmi toutes les solutions de l'équation de Bézout. Supposons, pour simplifier, que $a > b > 0$ et que $\text{PGCD}\,(a,b) = 1$.

a) Montrer qu'il existe une solution $(x_+, y_+) \in \mathbf{Z}^2$ de $ax + by = 1$ et une seule telle que $0 \leq x_+ < b$. Montrer qu'on a $-a < y_+ \leq 0$.

b) Montrer qu'il existe une solution $(x_-, y_-) \in \mathbf{Z}^2$ de $ax + by = 1$ et une seule telle que $-b < x_- \leq 0$. Montrer qu'on a $0 \leq y_+ < a$.

c) Montrer qu'on a $(x_N, y_N) = (x_+, y_+)$ si N est impair et $(x_N, y_N) = (x_-, y_-)$ si N est pair. Indication : on pourra commencer par montrer que les suites $-(-1)^k x_k$ et $(-1)^k y_k$ sont strictement croissantes pour $k \geq 3$.

5) Nous allons estimer le nombre d'étapes de l'algorithme d'Euclide-Bézout. Pour un couple d'entiers (a, b) avec $a > b \geq 0$ notons $N(a, b)$ le nombre N apparaissant comme nombre d'étapes de l'algorithme d'Euclide-Bézout appliqué à (a, b).

a) Montrer que $N(a, b) \leq 1 + \log_2 a$.

b) Soit $F_0 = 0$, $F_1 = 1$ et $F_n = F_{n-1} + F_{n-2}$ pour tout $n > 1$. Par définition, le nombre F_n est le *n-ième nombre de Fibonacci*. Montrer que $N(F_n, F_{n-1}) = n$, que $N(a, b) \leq n$ si $a \leq F_n$ et que l'égalité ne se présente que pour $a = F_n$ et $b = F_{n-1}$.