

L'algorithme d'Euclide étendu

Résolution de l'équation diophantienne $ax + by = 1$ (en supposant que $\text{pgcd}(a, b) = 1$).

Cette présentation commence par un tableau-exemple détaillé, justifié plus loin...

Un exemple : résolution de l'équation

$$95x + 14y = 1$$

quot.	$a, b...$	$x, y...$	$\pm$	pour remonter	solutions
	95	34	—		$14 \cdot 34 - 95 \cdot 5 = 1$
6	14	5	+	$6 \cdot 5 + 4 = 34$	$14 \cdot 4 - 11 \cdot 5 = 1$
1	11	4	—	$2 \cdot 4 + 1 = 5$	$3 \cdot 4 - 11 \cdot 1 = 1$
3	3	1	+	$3 \cdot 1 + 1 = 4$	$3 \cdot 1 - 2 \cdot 1 = 1$
1	2	1	—	$1 \cdot 1 + 0 = 1$	$1 \cdot 1 - 2 \cdot 0 = 1$
2	1	0	+	$2 \cdot 0 + 1 = 1$	$1 \cdot 1 - 0 \cdot 0 = 1$
—	0	1	—		

Description de l'algorithme

- On commence par descendre avec l'algorithme d'Euclide pour le PGCD, en notant les quotients dans la colonne de gauche et les restes successifs dans la seconde colonne. Pour deux éléments successifs descendants, on calcule le troisième par division : $a \text{ divisé par } b \rightarrow q \text{ reste } c$.
- Le processus s'arrête lorsqu'on obtient un reste nul, qui permet d'écrire dans la colonne 3, en face des deux derniers nombres obtenus, les nombres 0 et 1, dont les produits croisés avec la deuxième colonne ont une différence de 1. On peut les lire comme des déterminants valant alternativement 1 et -1 . (Voir page suivante).
- On remonte ensuite en construisant la troisième colonne avec l'égalité caractéristique de la division euclidienne : $x' = y' \cdot q + z'$, parallèlement à la première colonne. On note des traits obliques alternés pour indiquer dans quel sens la soustraction donne 1.
- A chaque ligne, on a par construction une solution d'une équation de la forme $ay - bx = \pm 1$, avec une alternance des signes. La ligne d'en haut fournit ainsi la solution de l'équation diophantienne initiale, les lignes suivantes celles d'équations diophantiennes réduites.

- Remarque : il n'est en pratique pas nécessaire de poursuivre la procédure jusqu'à la dernière ligne – ni d'écrire toutes les colonnes. Dès qu'on a une solution évidente, on peut s'arrêter et remonter. Dans cet exemple, on pourrait s'arrêter à la ligne du reste 3 avec l'égalité $3 \cdot 4 - 11 \cdot 1 = 1$, et remonter directement depuis là. Cela donne le tableau simplifié à 3 colonnes ci-dessous :

quot.	$a, b...$	$x, y...$
	95	34
6	14	5
1	11	4
	3	1

Une chaîne de déterminants

Le tableau construit peut aussi se lire avec des déterminants de valeurs alternativement $+1$ et -1 , et reconstruits de bas en haut par combinaisons linéaires (dont les coefficients sont chaque fois 1 et le quotient correspondants). Pour chaque déterminant, on a $l_1 = l'_1 \cdot q + l'_2$ et $l_2 = l'_1$. Cette observation explique pourquoi les déterminants ont des valeurs ± 1 alternées et donne ainsi une justification de l'algorithme.

quot.	a	x	déterminants	équation
	95	34	$\begin{vmatrix} 95 & 34 \\ 14 & 5 \end{vmatrix} = -1$	$\rightarrow 14 \cdot 34 - 95 \cdot 5 = 1$
6	14	5	$\begin{vmatrix} 14 & 5 \\ 11 & 4 \end{vmatrix} = +1$	$\rightarrow 14 \cdot 4 - 11 \cdot 5 = 1$
1	11	4	$\begin{vmatrix} 11 & 4 \\ 3 & 1 \end{vmatrix} = -1$	$\rightarrow 3 \cdot 4 - 11 \cdot 1 = 1$
3	3	1	$\begin{vmatrix} 3 & 1 \\ 2 & 1 \end{vmatrix} = +1$	$\rightarrow 3 \cdot 1 - 2 \cdot 1 = 1$
1	2	1	$\begin{vmatrix} 2 & 1 \\ 1 & 0 \end{vmatrix} = -1$	$\rightarrow 1 \cdot 1 - 2 \cdot 0 = 1$
2	1	0	$\begin{vmatrix} 1 & 0 \\ 0 & 1 \end{vmatrix} = 1$	$\rightarrow 1 \cdot 1 - 0 \cdot 0 = 1$
	0	1		

Note : si le pgcd n'était pas égal à 1, il suffirait de remplacer l'alternance ± 1 par une alternance $\pm d$, où $d = \text{pgcd}(a, b)$

Démonstration de l'algorithme

Pour mieux voir les correspondances qui se cachent derrière cet algorithme, posons l'équation à résoudre sous la forme

$$[1] \quad \boxed{ay - bx = 1}$$

Effectuons la division euclidienne de a par b de sorte que $a = b \cdot q + c$, et $c = a - b \cdot q$

Par substitution, l'équation devient $(b \cdot q + c)y - bx = 1$,

qui peut se réécrire sous la forme $b(qy - x) + cy = 1$, puis se réarranger sous la forme

$$b \underbrace{(x - qy)}_z - cy = -1$$

Ainsi donc, en posant $z = x - qy$ (ce qui donne $x = q \cdot y + z$), on a une nouvelle équation de forme analogue mais avec le signe opposé à droite

$$[2] \quad \boxed{bz - cy = -1}$$

Une solution de l'équation [2] fournit donc une solution de l'équation [1] par substitution au moyen de l'égalité

$$\boxed{x = q \cdot y + z} \quad \text{parallèle à} \quad \boxed{a = b \cdot q + c}$$

Cela justifie l'algorithme.

Justification par les déterminants

On peut aussi raisonner en terme de déterminants. L'équation [1] s'écrit alors

$$\begin{vmatrix} a & x \\ b & y \end{vmatrix} = 1$$

Par combinaison linéaires de lignes de la matrice sous-jacente, et avec le même changement de variables, on obtient l'équation [2] sous la forme :

$$\begin{vmatrix} (a - bq) & (x - qy) \\ b & y \end{vmatrix} = 1 \iff \begin{vmatrix} c & z \\ b & y \end{vmatrix} = 1 \iff \begin{vmatrix} b & y \\ c & z \end{vmatrix} = -1$$

Cette présentation fait apparaître à la fois le fonctionnement parallèle du changement de variable et de coefficients et la raison de l'alternance des signes – ainsi que la raison pour laquelle il faut arranger les variables comme ci-dessus pour faire apparaître le parallélisme.