Algorithme d'Euclide étendu

L'**algorithme d'Euclide étendu** est une variante de l'algorithme d'Euclide qui permet, à partir de deux entiers a et b, de calculer non seulement leur plus grand commun diviseur (PGCD), mais aussi un de leurs couples de coefficients de Bézout (deux entiers u et v tels que $au + bv = \mathrm{PGCD}(a, b)$). Quand a et b sont premiers entre eux, u est alors l'inverse pour la multiplication de a modulo b, et v est de la même façon l'inverse pour la multiplication de b modulo a. ce qui est un cas particulièrement utile.

Exemple introductif[modifier | modifier le code]

Considérons par exemple le calcul du PGCD de 120 et 23 avec l'algorithme d'Euclide :

120 ÷ 23 = 5 reste 5
23 ÷ 5 = 4 reste 3
5 ÷ 3 = 1 reste 2
3 ÷ 2 = 1 reste 1
2 ÷ 1 = 2 reste 0

Dans ce cas, le reste obtenu à l'avant dernière ligne donne le PGCD égal à 1 ; c'est-à-dire que 120 et 23 sont premiers entre eux. Maintenant présentons autrement les divisions précédentes :

Reste	= Dividende	- Quotient	× Diviseur
5	= **120**	- 5	× **23**
3	= **23**	- 4	× 5
2	= 5	- 1	× 3
1	= 3	- 1	× 2
0	= 2	- 2	× 1

Observons que 120 et 23 apparaissent sur les deux premières lignes. D'autre part, la valeur la plus à droite dans chaque ligne (à partir de la 2e ligne du tableau) est le reste de la ligne précédente, et le dividende est — dans chaque égalité à partir de la 3e ligne — le reste obtenu deux lignes plus haut. Nous pouvons ainsi calculer progressivement chaque reste successif comme combinaison linéaire des deux valeurs initiales 120 et 23.

Cependant cette méthode n'est pas la plus efficace. On écrit d'abord ces calculs de façon à faire apparaître un algorithme plus direct :

r				**= u × A + v × b**
120				= 1 × 120 + 0 × 23
23				= 0 × 120 + 1 × 23
5	= 120 - 5 × 23			= 1 × 120 + -5 × 23
3	= 23 - 4 × 5	= 1×23	- 4 × (1×120 - 5×23)	= -4 × 120 + 21 × 23
2	= 5 - 1 × 3	= (1×120 - 5×23)	- 1 × (-4×120 + 21×23)	= 5 × 120 + -26 × 23

$1 = 3 - 1 \times 2 = (-4\times120 + 21\times23) - 1 \times (5\times120 - 26\times23) = -9 \times 120 + 47 \times 23$

Remarquons que la dernière ligne donne $1 = -9\times120 + 47\times23$, et nous fournit exactement ce que nous voulons : $u = -9$ et $v = 47$. Ceci signifie que -9 est l'inverse pour la multiplication de 120 modulo 23, parce que $1 = -9 \times 120 \pmod{23}$. De même 47 est l'inverse, pour la multiplication modulo 120, de 23.

On a en bleu les calculs successifs qui conduisent au pgcd par reste de la division des deux nombres précédents (algorithme d'Euclide ordinaire). On a noté en jaune les quotients correspondants. Les deux colonnes vertes donnent les calculs successifs qui aboutissent aux coefficients de Bezout (u et v). On peut vérifier que ces coefficients se calculent à partir des deux coefficients les précédant dans la même colonne, à l'aide des quotients de la colonne jaune.