Cours d'Arithmétique

Identité de Bezout

Oumar D. Mbodj[1], Augustin P. Sarr[1]

[1]Université Gaston Berger
{oumar.mbodj, augustin.sarr}@ugb.edu.sn

UFR SAT, UGB 2014

Plan

Auteurs et Institutions

Oumar D. Mbodj
oumar.mbodj@ugb.edu.sn
UFR SAT UGB

Augustin P. Sarr
augustin.sarr@ugb.edu.sn
UFR SAT, UGB

Objectifs

Objectif général :
L'objectif de cette séquence est de présenter un second algorithme de calcul du pgcd et des coefficients de Bezout de deux entiers. Nous verrons qu cet algorithme, connu sous le nom d'algorithme d'Euclide étendu, est beaucoup plus puissant que le premier.

Faiblesse de l'algorithme

Rappel sur un exemple du premier algorithme d'Euclide : Soit $a = 450$ et $b = 153$ deux entiers. Déterminons leur pgcd d et les coefficients u et v de Bezout. Les divisions euclidiennes successives donnent :

$$\begin{aligned} 450 &= 2 * 153 + 144 \\ 153 &= 1 * 144 + 9 \\ 144 &= 16 * 9 \end{aligned}$$

Par suite $d = 9$ et en remontant les calculs nous obtenons $9 = (-1) * 450 + 3 * 153$. D'où $u = -1$ et $v = 3$.

Exercice. Déterminer le pgcd de $a = 57996$ et de $b = 5015$ en effectuant une suite de divisions euclidiennes comme celles ci-dessus. Le calcul des coefficients de Bezout n'est pas demandé.

Faiblesse de l'algorithme

Cet algorithme a un grand inconvénient. Il faudra mémoriser tous les calculs intermédiaires pour pouvoir, par la suite, les réutiliser afin d'obtenir les coefficients u et v intervenant dans la formule de Bezout. Ce qui peut poser un problème de mémoire et influer sur la vitesse surtout si les étapes intermédiaires sont nombreuses.

Algorithme d'Euclide étendu

Posons $r_{-1} = a$ et $r_0 = b$ effectuons les divisions euclidiennes successives. On s'arrête au premier reste nul :

$$\begin{aligned} r_{-1} &= q_0 r_0 + r_1 \\ r_0 &= q_1 r_1 + r_2 \\ &\vdots \\ r_{i-1} &= q_i r_i + r_{i+1} \end{aligned}$$

La dernière formule permet d'écrire l'égalité matricielle :

$$\begin{pmatrix} r_i \\ r_{i+1} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_i \end{pmatrix} \begin{pmatrix} r_{i-1} \\ r_i \end{pmatrix} \quad (1)$$

Exercice. Justifier l'égalité matricielle ci-dessus.

Algorithme d'Euclide étendu

L'égalité (1) et $(r_{-1}, r_0) = (a, b)$ montrent que l'on peut poser :

$$\begin{pmatrix} r_{i-1} \\ r_i \end{pmatrix} = \begin{pmatrix} s_i & t_i \\ u_i & v_i \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} \tag{2}$$

et que nous avons :

$$\begin{pmatrix} s_0 & t_0 \\ u_0 & v_0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \tag{3}$$

Exercice. Justifier chacune des égalités matricielles précédentes.

Algorithme d'Euclide étendu

Les relations (1) et (2) montrent que :

$$\begin{pmatrix} s_{i+1} & t_{i+1} \\ u_{i+1} & v_{i+1} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_i \end{pmatrix} \begin{pmatrix} s_i & t_i \\ u_i & v_i \end{pmatrix} \tag{4}$$

Il s'ensuit $s_{i+1} = u_i$, $t_{i+1} = v_i$ et donc :

$$\begin{pmatrix} s_i & t_i \\ u_i & v_i \end{pmatrix} = \begin{pmatrix} u_{i-1} & v_{i-1} \\ u_i & v_i \end{pmatrix} \tag{5}$$

On voit aussi, simplement, $u_{i+1} = u_{i-1} - q_i u_i$ et $v_{i+1} = v_{i-1} - q_i v_i$.

Algorithme d'Euclide étendu

Si le premier reste nul est r_{k+1} alors le pgcd d est égal à r_k et la formule (2) montre que l'égalité de Bezout est donnée par $d = r_k = u_k a + v_k b$ c'est à dire $u = u_k$ et $v = v_k$.

Nous avons, maintenant, tout ce qu'il faut pour procéder à l'écriture de l'algorithme. Soit a et b deux entiers dont on veut calculer le pgcd d et les coefficients u et v intervenant dans l'identité de Bezout.

Algorithm 1 Identité de Bezout

Initialization

$$\begin{pmatrix} s & t \\ u & v \end{pmatrix} \leftarrow \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

while $b \neq 0$ **do**
  $q \leftarrow a \div b$
  $r \leftarrow a - qb$
  if $r \neq 0$ **then**
    $a \leftarrow b$
    $b \leftarrow r$

$$\begin{pmatrix} s & t \\ u & v \end{pmatrix} \leftarrow \begin{pmatrix} u & v \\ s - qu & t - qv \end{pmatrix}$$

  end if
end while

Après exécution b contient le pgcd et u et v contiennent les coefficients de Bezout.

i	q	r	a	b	s	t	u	v
0			450	153	1	0	0	1
1	2	144	153	144	0	1	1	-2
2	1	9	144	9	1	-2	-1	-3
3	16	0						

A l'étape 3 l'algorithme s'arrête. On a alors $d = 9$, $u = -1$ et $v = 3$.

Exercice. Exécuter, sur un tableau similaire, l'algorithme avec $a = 126$ et $b = 35$.

Exercice. Exécuter, sur un tableau similaire, l'algorithme avec $a = 57996$ et $b = 5015$.

Références

- ✓ Joachim von zur Gathen, Jürgen Gerhard, Modern Computer Algebra, Cambridge University Press, 2003.
- ✓ Cours d'Arithmétique sur `http://uel.unisciel.fr`, (consulté le 11 juillet 2013).