

Le but de l'algorithme augmenté est de calculer en même temps le PGCD de deux éléments ainsi que les coefficients de Bézout. On peut l'utiliser dans  $\mathbf{Z}$  ou dans  $\mathbf{K}[X]$ .

Rappelons pour commencer le principe (en l'écrivant dans l'anneau  $\mathbf{Z}$ ) : On considère deux éléments  $a$  et  $b$  non nuls de  $\mathbf{Z}$ . On veut calculer le PGCD  $d = a \wedge b$ , ainsi que des coefficients de Bézout, c'est-à-dire deux entiers  $u$  et  $v$  tels que

$$au + bv = d$$

Le principe de l'algorithme est de construire trois suites  $(u_n)$ ,  $(v_n)$  et  $(r_n)$  d'éléments de  $\mathbf{Z}$  telles que

$$\forall n \in \mathbf{N}, au_n + bv_n = r_n$$

On notera  $X_n = (u_n \quad v_n \quad r_n)$ .

Après plusieurs itérations, on trouvera un entier  $p$  tel que  $r_p = d$  et alors  $u_p$  et  $v_p$  seront les coefficients de Bézout cherchés.

On initialise en posant  $u_0 = 1, v_0 = 0$  puis  $u_1 = 0, v_1 = 1$ . Pour assurer la relation ci-dessus, on prend donc  $r_0 = a$  et  $r_1 = b$ .

Ensuite, tant que  $r_n \neq 0$ , on réalise la division euclidienne de  $r_{n-1}$  par  $r_n$ ; on note  $q_n$  le quotient et  $r_{n+1}$  le reste :

$$r_{n-1} = q_n r_n + r_{n+1}$$

On pose alors

$$X_{n+1} = X_{n-1} - q_n X_n$$

c'est-à-dire

$$u_{n+1} = u_{n-1} - q_n u_n \text{ et } v_{n+1} = v_{n-1} - q_n v_n$$

On a bien aussi  $r_{n+1} = r_{n-1} - q_n r_n$ .

Par exemple pour  $a = 32$  et  $b = 23$  on a :

	$u_n$	$v_n$	$r_n$	$q_n$		
$X_0$	1	0	32			
$X_1$	0	1	23	1	$(32 = 1 \times 23 + 9)$	
$X_2$	1	-1	9	2	$(23 = 2 \times 9 + 5)$	$X_2 = X_0 - X_1$
$X_3$	-2	3	5	1	$(9 = 1 \times 5 + 4)$	$X_3 = X_1 - 2X_2$
$X_4$	3	-4	4	1	$(5 = 1 \times 4 + 1)$	$X_4 = X_2 - X_3$
$X_5$	-5	7	1	4	$(4 = 4 \times 1 + 0)$	$X_5 = X_3 - X_4$
$X_6$	23	32	0			$X_6 = X_4 - 4X_5$

Comme dans l'algorithme d'Euclide standard, on s'arrête au premier reste non nul.

Traisons maintenant un exemple dans  $\mathbf{K}[X]$ .

Calculons de PGCD de  $P = X^5 + X^4 + 2X^3 + X^2 + X + 2$  et  $Q = X^4 + 2X^3 + X^2 - 4$  ainsi que les coefficients de Bézout.

On pose donc  $U_0 = 1, V_0 = 0; U_1 = 0, V_1 = 1$  de sorte que  $R_0 = P$  et  $R_1 = Q$ .

— On effectue la division euclidienne de  $R_0$  par  $R_1$  :

$$X^5 + X^4 + 2X^3 + X^2 + X + 2 = (X - 1) \times (X^4 + 2X^3 + X^2 - 4) + 3X^3 + 2X^2 + 5X^2 - 2$$

On pose donc  $R_2 = 3X^3 + 2X^2 + 5X^2 - 2$ . On peut alors calculer  $U_2$  et  $V_2$  par les formules

$$U_2 = U_0 - (X - 1)U_1 = 1$$

et

$$V_2 = V_0 - (X - 1)V_1 = -(X - 1)$$

.

— On effectue la division euclidienne de  $R_1$  par  $R_2$  :

$$X^4 + 2X^3 + X^2 - 4 = \frac{1}{9}(3X + 4) \times (3X^3 + 2X^2 + 5X^2 - 2) - \frac{14}{9}(X^2 + X + 2)$$

On pose donc  $R_3 = -\frac{14}{9}(X^2 + X + 2)$ . On peut alors calculer  $U_3$  et  $V_3$  par les formules

$$U_3 = U_1 - \frac{1}{9}(3X + 4)U_2 = -\frac{1}{9}(3X + 4)$$

et

$$V_3 = V_1 - \frac{1}{9}(3X + 4)V_2 = 1 + \frac{1}{9}(3X + 4)(X - 1) = \frac{1}{9}(3X^2 + X + 5)$$

. Pour éviter d'avoir une fraction dans le reste  $R_3$ , on peut tout multiplier par  $-\frac{9}{14}$  pour obtenir

$$R_3 = X^2 + X + 2 \quad ; \quad U_3 = \frac{1}{14}(3X + 4) \quad ; \quad V_3 = -\frac{1}{14}(3X^2 + X + 5)$$

— On effectue la division euclidienne de  $R_2$  par  $R_3$  :

$$3X^3 + 2X^2 + 5X^2 - 2 = (3X - 1) \times (X^2 + X + 2) + 0$$

On vient de trouver un reste nul.

On remonte donc au dernier reste non nul.

Le PGCD est le dernier reste non nul normalisé. Ici,  $P \wedge Q = X^2 + X + 2$ .

De plus,

$$X^2 + X + 2 = -\frac{1}{14}(3X^2 + X + 5)Q + \frac{1}{14}(3X + 4)P.$$