Bezout, à la recherche d'une solution minimale

par Patrick TELLER

version beta

Avertissement 1.

Dans tout ce qui suit la notation $\|(u_1, ..., u_n)\|$ (ou le terme « norme) représentera la norme $\sum_{k=1}^{n} |u_i|$.

Il est bien connu que le Théorème de Bezout appliqué à n entiers naturels (x_1,..,x_n) dont le plus grand diviseur commun est d, établit l'existence d' entiers relatifs (u_1,..u_n) tels que $\sum_{i=1}^{n} u_i x_i = d$.

L'ensemble des n-uplets solutions possède un (ou plusieurs) élément (s) de norme minimale.

1 n=2, tout va bien

Le Théorème de Bezout appliqué à deux entiers naturels a et b établit que si d est leur plus grand diviseur commun il existe des entiers relatifs (u,v) tels que au+bv=d; l'algorithme d'Euclide étendu permet d'en trouver un couple.

q	r	u	v	
	$r_{-1} = a$	1	0	
	$r_0 = b$	0	1	
q_1	r_1	$u_1 = 1$	$v_1 = -q_1$	
q_2	r_2	$u_2 = -q_2$	$v_2 = 1 + q_1 q_2$	
...	...	...	...	(*)
q_p	r_p	u_p	v_p	
q_{p+1}	r_{p+1}	u_{p+1}	v_{p+1}	
q_{p+2}	r_{p+2}	$u_{p+2} = u_p - q_{p+2} u_{p+1}$	v_{p+2}	
.....	.....	.....	....	
q_n	$r_n = d$	u_n	v_n	
q_{n+1}	0	u_{n+1}	v_{n+1}	

Proposition 2. *Les suites (u_k) et (v_k) sont de signes alternés, de valeurs absolues croissantes et strictement croissantes pour k>1; $u_{n+1} = (-1)^n \frac{b}{d}$ et $v_{n+1} = (-1)^{n+1} \frac{a}{d}$ [1].*

Démonstration.

Les q_k sont strictement positifs, les signes de u_1 et u_2 sont connus, ainsi que la relation de récurrence $u_{p+2} = u_p - q_{p+2} u_{p+1}$; ce qui établit les deux premières affirmations pour (u_k), il en est de même pour (v_k).

De plus $r_{p+1} u_{p+2} - r_{p+2} u_{p+1} = r_{p+1}(u_p - q_{p+2} u_{p+1})$-$(r_p$-$q_{p+2} r_{p+1})u_{p+1}$=-$(r_p u_{p+1}$-$r_{p+1} u_p)$=...=$(-1)^{p+2}(r_{-1} u_0$-$r_0 u_{-1})$=$(-1)^{p+2}$(a.0-b.1)=$(-1)^{p+1} b$.

Par suite en posant p+2=n+1 on en déduit $d.u_{n+1}$-$0.u_n$=$(-1)^n$b, c'est à dire u_{n+1}=$(-1)^n \frac{b}{d}$ et, par suite, v_{n+1}=$(-1)^{n+1} \frac{a}{d}$.

On remarque aussi que, comme r_n=d est le pgcd il divise r_{n-1} (et ne lui est pas égal) donc $q_{n+1}>1$, or $u_{n+1}=u_{n-1}-q_{n+1}u_n$, d'où $|u_n|=\frac{|u_{n+1}-u_{n-1}|}{q_{n+1}}$, comme u_{n+1} et u_{n-1} sont de même signe ceci entraîne que $|u_n|<\frac{|u_{n+1}|}{2}=\frac{b}{2d}$ et de même $|v_n|<\frac{|v_{n+1}|}{2}=\frac{a}{2d}$ □

Théorème 3.

L'algorithme d'Euclide étendu fournit deux entiers relatifs u_n et v_n tels que $au_n+bv_n=d$ avec $|u_n|<\frac{b}{2d}$ et $|v_n|<\frac{a}{2d}$.

Démonstration.

Comme $r_n=d$ est le pgcd il divise r_{n-1} (et ne lui est pas égal) donc $q_{n+1}>1$, or $u_{n+1}=u_{n-1}-q_{n+1}u_n$, d'où $/u_n/=\frac{|u_{n+1}-u_{n-1}|}{q_{n+1}}$, comme u_{n+1} et u_{n-1} sont de même signe ceci entraîne que $|u_n|<\frac{|u_{n+1}|}{2}=\frac{b}{2d}$ et de même $|v_n|<\frac{|v_{n+1}|}{2}=\frac{a}{2d}$. □

Définition 4.

Un couple (u^*,v^*), solution de l'équation $ax+by=d$, sera dit minimal lorsque quelle que soit la solution (u,v) on a $|u^*|+|v^*|\leqslant|u|+|v|$

Théorème 5.

Le couple (u_n,v_n) fourni par l'algorithme d'Euclide étendu est la solution minimale.

Démonstration.

Il est bien connu que si le couple (u^*,v^*) vérifie la relation $au+bv=d$ l'ensemble des solutions de l'équation $ax+by=d$ est l'ensemble $\left\{\left(u^*+k\frac{b}{d},v^*-k\frac{a}{d}\right),k\in\mathbb{Z}\right\}$.donc l'ensemble des solutions est $\left\{\left(u_n,v_n\right)+k\left(\frac{b}{d},-\frac{a}{d}\right),k\in\mathbb{Z}\right\}$.

On voit aisément que

i) si k est du signe de u_n $\left|u_n+k\frac{b}{d}\right|>\frac{b}{d}>|u_n|$.

ii) soit k de signe opposé à celui de u_n on déduit de la remarque à la fin de la démonstration de la proposition 1 que $\left|u_n+k\frac{b}{d}\right|\geqslant\left||u_n|-|k|\frac{b}{d}\right|=|k|\frac{b}{d}-|u_n|>|u_n|$.

On démontre de manière analogue que $\forall k\in\mathbb{Z}^*,\left|v_n-k\frac{a}{d}\right|>|v_n|$ □

Remarque 6.

On montrerait de même que $\forall p\in[\![1,n]\!],\forall k\in\mathbb{Z}^*,\left|u_p+k\frac{a}{d}\right|>|u_p|$ et $\forall p\in[\![1,n]\!],\forall k\in\mathbb{Z}^*,\left|v_p-k\frac{a}{d}\right|>|v_p|$.

Donc pour tout $p\in[\![1,n]\!]$ la solution minimale de l'équation ax+by=r_p est le couple (u_p,v_p).

2 La fonction D

Définition 7.

Deux entiers a et b étant donnés on désignera pour tout entier x le minimum de $\{|u|+|v|,\ au+bv=x\}$ par D(x) (si nécessaire on écrira $D_{(a,b)}(x)$).

Proposition 8.

Soit le tableau (*) de l'algorithme d'Euclide étendu associé aux entiers a et b

i) pour tout $p \in [\![1, n]\!]$ *D(*r_p *)=*$|u_p| + |v_p|$

ii) soit $x \in [\![a \wedge b, \max(a, b)]\!]$, $\exists(\alpha_1, ..., \alpha_n) \in \mathbb{N}^n, x = \sum_{p=1}^n \alpha_p r_p \Rightarrow D(x) \leqslant \sum_{p=1}^n \alpha_p D(r_p)$.

Démonstration.

i) découle de la remarque 6.

ii) supposons $x = \sum_{p=1}^n \alpha_p r_p$, alors $x = \sum_{p=1}^n \alpha_p(\mathrm{au}_p + \mathrm{bv}_p) = a\sum_{p=1}^n \alpha_p u_p + \mathrm{b}\sum_{p=1}^n \alpha_p v_p$, par suite $\mathrm{D(x)} \leqslant \sum_{p=1}^n \alpha_p |u_p| + \sum_{p=1}^n \alpha_p |v_p| \leqslant \sum_{p=1}^n \alpha_p D(r_p)$. □

Par suite le calcul des valeurs de D se fonde sur le tableau de l'algorithme d'Euclide étendu pour les valeurs de x qui appartiennent à $\{r_p\}$; pour les autres on posera $x = \sum_{p=1}^n \alpha_p(\mathrm{au}_p + \mathrm{bv}_p) = \mathrm{ua} + \mathrm{bv}$ et on comparera $|u| + |v|$ avec $|u + \varepsilon b| + |v - \varepsilon a|$ (où $\varepsilon = \pm 1$) et on corrigera (autant de fois que nécessaire le couple (u,v) en $(\mathrm{u} + \varepsilon b, v - \varepsilon a)$.

Exemple 9.

x	23	16	$D(x)$
23	1	0	1
16	0	1	1
7	1	−1	2
2	−2	3	5
1	7	−10	17
0	−16	23	

Pour les autres valeurs de x :

9=7+2, donc 9=(1-2)*23+(-1+3)*16, il n'y a pas mieux donc $\mathrm{D}(9) = |-1| + |2| = 3$

8=7+1, donc 8=(1+7)*23+(-1-10)*16, D(8)=8+11=19.

6=2+2+2, D(6)=6+9=15

5=2*2+1, donc D(5)=3+4=7

D(4)=4+6=10

D(3)=5+7=12

D(11)=3+5=8

D(13)=5+8=13....

d'ou la fonction D

x	$D(x)$
13	13
12	9
11	8
10	14
9	3
8	19
7	2
6	15
5	9
4	10
3	12
2	5
1	17

3 Le cas général

Le Théorème de Bezout établit que si (x_1,..,x_n) sont des entiers naturels et si d est leur plus grand diviseur commun il existe des entiers relatifs (u_1,..u_n) tels que $\sum_{i=1}^{n} u_i x_i = d$; nous désirons trouver une solution de norme minimale.

L'idée naïve consiste à calculer pas à pas: $x_1 \wedge x_2 = u_{11}x_1 + u_{12}x_2$, ($x_1 \wedge x_2) \wedge x_3 = u_{21}x_1 + u_{22}x_2 + u_{23}x_3$.....cependant l'expérience montre que les coefficients peuvent croître rapidement.

Exemple 10. (2618,6204,24132)

12=494*6204-127*24312

2=-218*12+1*2618

d'où 2=1*2618-107692*6204+27686*24132

ou bien, en commençant 2618∧6204, 22=-109*2618+46*6204

2=1097*22-24132

d'où 2=-119573*2618+50462*6204-1*24132

On remarque que la norme de la solution est « assez grande » (sic !) et si on se souvient que la croissance des coefficients est dûe aux quotients (cf Proposition 1) il existe un moyen de les réduire: on conviendra d'effectuer chaque fois des divisions euclidiennes impliquant le plus « petit » quotient possible.

3.1 Un algorithme d'Euclide n-étendu

Soient les entiers $(x_1, x_2, ..., x_n)$

I. Préparation matrice:

Création de la matrice: M sera une matrice à n lignes et 1+n colonnes numérotées de 0 à n

1. $\forall i \in \{1, ..., n\}$, M[i,0]:=$x_i$

2. $\forall i \in \{1, ..., n\}$ M[i,i]:=1

tous les autres sont nuls

II. Tant que les M[i,0] ne sont pas tous $\neq 0$

Soient a=max({M[i,0],i=1...n}), s tel que a=M[s,0] est maximal et b=max{M[i,0],i$\neq s$}, t tel que b=M[t,0] (pour a comme pour b, au cas où il y aurait plusieurs candidats on choisira le plus « ancien », suivant la règle FIFO)

si b>0 alors effectuer Réduction(s,t)

si b=0 alors

i. pgcd=M[s,0]

ii. Bezout=(M[s,1],..,M[s,n]

Procédure Réduction (s,t)

1. Soient (q,r) le quotient et le reste de la division euclidienne de M[s,0] par M[t,0]

2. $\forall j \in \{0, ..., n\}$ M[s,j]:M[s,j]-q*M[t,j]

On remarquera que, tout comme dans l'algorithme d'Euclide étendu, on conserve tout au long $\forall i \in \{0, ..., n\}$, $\sum_{j=1}^{n} M[i, j]x_j$=M[i,0]

et à la fin $\sum_{j=1}^{n} M[s, j]x_j$=M[s,0] (qui est le pgcd).

Remarque 11.

On peut aussi convenir qu'à chaque étape les lignes sont réécrites suivant l'ordre décroissant de la première coordonnée , avec en cas d'égalité application de la règle FIFO.

Exemple 12. (suite)

avec les données de l'exemple au-dessus et l'algorithme proposé

	24132	6204	2618
21432	1	0	0
6204	0	1	0
2618	0	0	1

$\longrightarrow$

	24132	6204	2618
6204	0	1	0
5520	1	−3	0
2618	1	0	0

$\longrightarrow$

	24132	6204	2618
5520	1	−3	0
2618	0	0	1
684	−1	4	0

$\longrightarrow$

	24132	6204	2618
2618	0	0	1
684	−1	4	0
284	1	−3	−2

$\longrightarrow$

	24132	6204	2618
684	−1	4	0
566	3	−12	1
284	1	−3	−2

$\longrightarrow$

	24132	6204	2618
566	3	−12	1
284	1	−3	−2
118	−4	16	−1

$\longrightarrow$

	24132	6204	2618
284	1	−3	−2
282	2	−9	3
118	−4	16	−1

$$
\begin{array}{cccc}
 & 24132 & 6204 & 2618 \\
\longrightarrow 282 & 2 & -9 & 3 \\
118 & -4 & 16 & -1 \\
2 & -1 & 6 & -5
\end{array}
\qquad (*)
$$

$$
\begin{array}{cccc}
 & 24132 & 6204 & 2618 \\
\longrightarrow 118 & -4 & 16 & -1 \\
46 & 10 & -41 & 5 \\
2 & -1 & 6 & -5
\end{array}
$$

$$
\begin{array}{cccc}
 & 24132 & 6204 & 2618 \\
\longrightarrow 46 & 10 & -41 & 5 \\
26 & -24 & 98 & -11 \\
2 & -1 & 6 & -5
\end{array}
$$

$$
\begin{array}{cccc}
 & 24132 & 6204 & 2618 \\
\longrightarrow 26 & -24 & 98 & -11 \\
20 & 34 & -139 & 16 \\
2 & -1 & 6 & -5
\end{array}
$$

$$
\begin{array}{cccc}
 & 24132 & 6204 & 2618 \\
\longrightarrow 20 & 34 & -139 & 16 \\
6 & -58 & 237 & -27 \\
2 & -1 & 6 & -5
\end{array}
$$

$$
\begin{array}{cccc}
 & 24132 & 6204 & 2618 \\
\longrightarrow 6 & -58 & 237 & -27 \\
2 & -1 & 6 & -5 \\
2 & 208 & -850 & 97
\end{array}
$$

$$
\begin{array}{cccc}
 & 24132 & 6204 & 2618 \\
\longrightarrow 2 & -1 & 6 & -5 \\
2 & 208 & -376 & 97 \\
0 & \ldots & \ldots & \ldots
\end{array}
$$

$$
\begin{array}{cccc}
 & 24132 & 6204 & 2618 \\
\longrightarrow 2 & 208 & -376 & 97 \\
0 & \ldots & \ldots & .... \\
0 & \ldots & \ldots &
\end{array}
$$

D'où

2=208*24132+(-850)*6204+97*2618

mais

2=-5*2618+6*6204+(-1)*24132 (que nous avions croisée en *) est incomparablement meilleure.

Exemple 13.

$$
\begin{array}{cccc}
142 & 1 & 0 & 0 \\
67 & 0 & 1 & 0 \\
14 & 0 & 0 & 1
\end{array}
$$

$$
\begin{array}{cccc}
 & 8 & 1 & -2 & 0 \\
\longrightarrow & 67 & 0 & 1 & 0 \\
 & 14 & 0 & 0 & 1
\end{array}
$$

$$
\begin{array}{cccc}
 & 8 & 1 & -2 & 0 \\
\longrightarrow & 11 & 0 & 1 & -4 \\
 & 14 & 0 & 0 & 1
\end{array}
$$

$$\begin{array}{cccc} & 8 & 1 & -2 & 0 \\ \longrightarrow & 11 & 0 & 1 & -4 \\ & 3 & 0 & -1 & 5 \end{array}$$

$$\begin{array}{cccc} & 8 & 1 & -2 & 0 \\ \longrightarrow & 3 & -1 & 3 & -4 \\ & 3 & 0 & -1 & 5 \end{array}$$

; la règle FIFO tranche: on réduit la ligne 1 par la ligne 3, plus ancienne que la ligne 2.

$$\begin{array}{cccc} & 2 & 1 & 0 & -10 \\ \longrightarrow & 3 & -1 & 3 & -4 \\ & 3 & 0 & -1 & 5 \end{array}$$

; à nouveau la règle FIFO tranche: on réduit la ligne 3 par la ligne 2.

$$\begin{array}{cccc} & 2 & 1 & 0 & -10 \\ \longrightarrow & 3 & -1 & 3 & -4 \\ & 0 & 1 & -4 & 9 \end{array}$$

$$\begin{array}{cccc} & 2 & 1 & 0 & -10 \\ \longrightarrow & 1 & -2 & 3 & 6 \\ & 0 & 1 & -4 & 9 \end{array}$$

d'où (-2)*142+3*67+6*14=1 et le triplet (-2,3,6) semble minimal.

3.2 A la recherche d'une solution minimale

L'étude d'un grand nombre de cas suggère que l'algorithme décrit au-dessus fournit souvent, mais pas toujours (exemple 12), une solution minimale.

Il semble donc nécessaire, au vu de la fonction qu'on désire optimiser, d'envisager une démarche en deux temps:

i. Détermination d'une solution de « taille acceptable », par exemple avec l'algorithme ci-dessus.

ii. Maintenant que la situation est « bornée » recherche d'un élément minimal, avec application du principe de Bellman (programmation dynamique).

3.2.1 Exemple dans le cas n=3

Soient 3 entiers naturels a>b>c de plus grand diviseur commun d, trois entiers relatifs (u',v',w') tels que au'+bv'+cw'=d et h=$|u'|+|v'|+|w'|$.

On pose H=$[\![-h+1,....,h-1]\!]$.

Pour tout x$(w)\in\{1-4\,w, w\in H\}$, le minimum recherché est $|w|+D(x(w))$.

Exemple 14. 13>8>4

i. $\begin{array}{cccc} & 23 & 16 & 4 \\ 23 & 1 & 0 & 0 \\ 16 & 0 & 1 & 0 \\ 4 & 0 & 0 & 1 \end{array} \rightarrow \begin{array}{cccc} & 23 & 16 & 4 \\ 16 & 0 & 1 & 0 \\ 7 & 1 & -1 & 0 \\ 4 & 0 & 0 & 1 \end{array} \longrightarrow \begin{array}{cccc} & 23 & 16 & 4 \\ 7 & 1 & -1 & 0 \\ 4 & 0 & 0 & 1 \\ 2 & -2 & 3 & 0 \end{array} \rightarrow \begin{array}{cccc} & 23 & 16 & 4 \\ 4 & 0 & 0 & 1 \\ 3 & 1 & -1 & -1 \\ 2 & -2 & 3 & 0 \end{array} \rightarrow \begin{array}{cccc} & 23 & 16 & 4 \\ 3 & 1 & -1 & -1 \\ 2 & -2 & 3 & 0 \\ 1 & -1 & 1 & 2 \end{array}$; d'où (u',v'w')=(-1,1,2) et h=4 et H=[-3,-2,-1,0,1,2,3].

x décrit $\{1-12, 1-8, 1-4, 1, 1+4, 1+8, 1+12\}$={-11,-7,-3,1,5,9,13}

ii. Etude de $D_{(23,16)}$(x) pour les valeurs x(w)

x	$D(x)$
13	13
12	9
11	8
10	14
9	3
8	19
7	2
6	15
5	9
4	10
3	12
2	5
1	17

(cf exemple 9)

d'où

x	$D(x)$
13	13
9	3
5	9
1	17
-3	12
-7	2
-11	8

et

w	$x(w)$	$D(x(w))$	$x(w)+D(x(w))$
-3	13	1	14
-2	9	3	12
-1	5	7	8
0	1	17	18
1	-3	12	13
2	-7	2	4
3	-11	4	7

d'ou le triplet minimal est (-1,1,2) de norme 4.

Le cas général, de taille n, se traitant suivant les principes de la programmation dynamique.

Question 15.

Il est décevant de ne pouvoir exhiber une méthode directe pour édterminer une solution minimale mais cela semble cohérent vue la nature « transverse » du problème: arithmétique d'une part et géométrie des nombres avec une norme peu commode.

Mais existe-t-il une méthode directe pour trouver une solution minimale ?

Bibliographie:

[1] M. Demazure, Cours d'Algèbre, Cassini, 1997.

Paris, décembre 2017.