Transcription d'un extrait d'Histoire d'algorithmes, du caillou à la puce
de Jean-Luc Chabert, Évelyne Barbin, Michel Guillemot,
Anne Michel-Pajus, Jacques Borowczyk, Ahmed Djebbar,
Jean-Claude Martzloff

L'identité de Bézout

(p. 139 et suivantes)
Comment résoudre en nombres entiers l'équation du premier degré :

$$ax - by = c$$

où x et y désignent les inconnues et a, b, c sont trois entiers donnés ? Ce problème a-t-il toujours une solution ? On sait en particulier que, lorsque les entiers a et b sont premiers entre eux, il est toujours possible de trouver deux entiers x_0 et y_0 tels que :

$$ax_0 - by_0 = 1,$$

relation que l'on appelle aujourd'hui l'*identité de Bézout*.

La méthode se trouve déjà exposée dans la deuxième édition de 1624 des *Problèmes plaisants et délectables* de Bachet de Méziriac [1]. La théorie réside dans sa proposition XVIII : "Deux nombres premiers étant donnés, trouver le moindre multiple de chacun d'iceux, surpassant de l'unité un multiple de l'autre.". L'auteur en donne une preuve distinguant selon la parité du nombre de divisions à effectuer dans l'algorithme d'Euclide pour obtenir le reste 1 et pratiquant sur des lettres une sorte de récurrence laborieuse et difficile à suivre.

Bachet propose des applications pratiques dans son Problème sixième, "*Deviner le Nombre que quelqu'un aura pensé*", et dans sa dixième "*Petite subtilité*" : "*Il y a 41 personnes en un banquet tant hommes que femmes et enfants qui en tout dépensent 40 sous, mais chaque homme paye 4 sous, chaque femme 3 sous, chaque enfant 4 deniers. Je demande combien il y a d'hommes, combien de femmes, combien d'enfants.*" Signalons que ce problème se rattache à la tradition médiévale des problèmes arabes, indiens et chinois dits "des 100 volailles" (cf. [2] et [3]).

Nous avons préféré présenter ici un texte de Bézout, extrait de son *Cours d'Algèbre* de 1766 [4], plus facile à lire que celui de Bachet. C'est en fait sur un exemple :

$$17x - 11y = 542$$

qu'il détaille la méthode. L'extrait ci-dessous illustre bien la façon dont Bézout procède dans tout son Cours : plutôt que d'exposer de façon dogmatique - à la façon d'Euclide - il préfère introduire ses explications par l'intermédiaire d'exemples numériques plus ou moins concrets, à partir desquels il est aisé d'induire des principes généraux. Les manuels de Bézout joueront d'ailleurs un rôle important dans l'enseignement des mathématiques.

aux Éditions Belin, Collection Regards sur la Science, 1994.

Le texte de Bézout

Extrait du *Cours de Mathématiques à l'usage des Gardes du Pavillon et de la Marine*, 6 vol., 1764-1769. Troisième Partie contenant l'Algèbre et l'Application de cette Science à l'Arithmétique et la Géométrie, Musier, Paris, 1766 (transcription des pages 118-121)

Des Problèmes indéterminés

Question première. *On demande en combien de manières on peut payer 542 livres, en donnant des pièces de 17 livres et recevant en échange des pièces de 11 livres.*

Représentons par x le nombre des pièces de 17 livres et par y celui des pièces de 11 livres ; en donnant x pièces de 17 livres, on payera x fois 17 livres ou $17x$: en recevant y pièces de 11 livres on recevra $11y$; par conséquent, on aura payé $17x - 11y$; et puisqu'on veut payer 542 livres, on aura $17x - 11y = 542$. Tirons la valeur de y, c'est à dire de l'inconnue qui a le moindre coefficient, et nous aurons $y = \dfrac{17x - 542}{11}$.

Comme on n'a que cette équation, on voit qu'en mettant arbitrairement pour x tel nombre qu'on voudra, on aura pour y une valeur qui satisfera sûrement à l'équation ; mais comme la question exige que x et y soient des nombres entiers, voici comment il faut s'y prendre pour y parvenir directement.

La valeur de $y = \dfrac{17x - 542}{11}$ se réduit, en faisant la division autant qu'il est possible, à $y = x - 49 + \dfrac{6x - 3}{11}$; il faut donc que $\dfrac{6x - 3}{11}$ soit un nombre entier : soit u ce nombre entier ; on aura $\dfrac{6x - 3}{11} = u$ et par conséquent $6x - 3 = 11u$ et $x = \dfrac{11u + 3}{6}$, ou, en faisant la division, $x = u + \dfrac{5u + 3}{6}$; il faut donc que $\dfrac{5u + 3}{6}$ fasse un nombre entier ; on aura $\dfrac{5u + 3}{6} = t$, et par conséquent $5u + 3 = 6t$ et $u = \dfrac{6t - 3}{5} = t + \dfrac{t - 3}{5}$; il faut donc que $\dfrac{t - 3}{5}$ fasse un nombre entier : soit s ce nombre entier, on aura $\dfrac{t - 3}{5} = s$ et par conséquent $t = 5s + 3$: l'opération est terminée ici, parce qu'il est évident qu'en prenant pour s tel nombre entier qu'on voudra, on aura toujours pour t un nombre entier tel que l'exige la question, puisqu'il n'y a plus de dénominateur.

Remontons maintenant aux valeurs de x et y : puisqu'on a trouvé $u = \dfrac{6t - 3}{5}$; en mettant pour t la valeur $5s + 3$, on aura $u = \dfrac{30s + 18 - 3}{5} = 6s + 3$: et puisqu'on a trouvé $x = \dfrac{11u + 3}{6}$, en mettant pour u sa valeur, on aura $x = \dfrac{66s + 33 + 3}{6} = 11s + 6$: enfin, puisqu'on a trouvé $y = \dfrac{17x - 542}{11}$, en substituant pour x sa valeur, on aura $y = \dfrac{187s + 102 - 542}{11} = 17s - 40$; ainsi les valeurs correspondantes de x et de y sont $x = 11s + 6$ et $y = 17s - 40$. Par la première, on est libre de prendre pour s tel nombre entier qu'on voudra ; mais la seconde ne permet pas de prendre s plus petit que 3 ; en effet, y devant être positif, il faut que $17s$ soit plus grand que 40, ou que s soit plus grand que $\frac{40}{17}$, c'est-à dire plus grand que 2.

On peut donc satisfaire à cette question d'une infinité de manières différentes, qu'on aura toutes en mettant dans les valeurs de x et de y, au lieu de s, tous les nombres entiers positifs imaginables depuis 3 jusqu'à l'infini ; ainsi, posant successivement $s = 3, s = 4, s = 5, s = 6, s = 7$, etc., on aura les valeurs correspondantes de x et de y comme il suit :

$$\begin{array}{llll} x & = 39\ldots & y & = 11 \\ & = 50 & & = 28 \\ & = 61 & & = 45 \\ & = 72 & & = 62 \\ & = 83, \text{etc.} & & = 79 \end{array}$$

dont chacune est telle qu'en donnant le nombre de pièces de 17 livres désigné par x et recevant le nombre correspondant de pièces de 11 livres désigné par y, on payera 542 livres.

Pour décrire l'algorithme de résolution en nombres entiers d'une équation :

$$ax - by = c$$

on introduit aujourd'hui une étape intermédiaire. Cette première étape consiste à trouver une solution particulière de l'équation :

$$ax - by = d$$

où d désigne le plus grand commun diviseur de a et b. La deuxième étape en déduit aisément toutes les solutions de l'équation initiale - qui est effectivement résoluble si et seulement si c est un multiple de d. D'une certaine façon, on retrouve au cours de cette première étape la procédure d'abord descendante, puis remontante de Bézout. Reprenons en effet l'exemple étudié.

Première étape. Trouver une solution particulière (x_0, y_0) de l'équation :

(1) $$17x - 11y = 1.$$

En effectuant les divisions euclidiennes successives à partir de 17 et 11 :

$$17 = 11.1 + 6, \qquad 11 = 6.1 + 5, \qquad 6 = 5.1 + 1,$$

on obtient un reste 1, le plus grand commun diviseur de 11 et 17 est 1 et les nombres 11 et 17 sont premiers entre eux. En remontant la procédure à partir du dernier reste 1 :

$$1 = 6 - 5 = 6 - (11 - 6) = 2.6 - 11 = 2(17 - 11) - 11 = 2.17 - 3.11,$$

on obtient la solution particulière $(x_0, y_0) = (2, 3)$ de l'équation (1).

Deuxième étape. Trouver toutes les solutions de l'équation :

(2) $$17x - 11y = 542.$$

Remarquant que $(x_1, y_1) = (542.2, 542.3)$ est une solution particulière de l'équation (2), on voit que (x, y) est solution de (2) si et seulement si (x, y) est solution de l'équation :

(3) $$17(x - x_1) = 11(y - y_1).$$

Ainsi, 17 et 11 n'ayant pas de facteurs communs, 17 divise $(y - y_1)$ et y est de la forme $y_1 + 17k$ où k désigne un entier. Par report dans (3), on voit que x est de la forme $x_1 + 11k$. Inversement, quel que soit l'entier k, le couple $(x_1 + 11k, y_1 + 17k)$ est solution de (2). Ainsi, les solutions de (2) sont de la forme : $x = (2 \times 542) + 11k, y = (3 \times 542) + 17k$, où k est

entier.

Pour que la solution (x, y) soit formée de nombres entiers naturels, il faut et il suffit que k vérifie à la fois : $(2 \times 542) + 11k > 0$ et $(3 \times 542) + 17k > 0$, c'est à dire : $k > -95.6$; d'où : $k = -95,\ x = 39,\ y = 1$; $k = -94,\ x = 50,\ y = 28, \ldots$ ou encore :

$$x = 39 + 11h, \quad y = 1 + 17h \quad \text{où } h \text{ est un entier naturel.}$$

Comme nous l'avons suggéré, les calculs effectués par Bézout reviennent aussi à une utilisation de l'algorithme d'Euclide.

En effet, Bézout pose successivement :

$$u = (\underline{6}x - 3)/\mathbf{11} \ ; \ t = (\underline{5}u + 3)/\mathbf{6} \ ; \ s = (\underline{1}t - 3)/\mathbf{5}.$$

or les nombres en gras correspondent aux diviseurs et les nombres soulignés aux restes dans les divisions euclidiennes successives que nous avons effectuées.

Cependant, la preuve de l'algorithme sous-tendu par la technique de Bézout est relativement complexe puisque, en écriture littérale, on peut lire la construction d'au moins trois suites dans la résolution de $ax - by = c$. L'initialisation du processus chez Bézout permet de comprendre la genèse de ces trois suites. En effet, de l'équation à résoudre, il tire $y = (ax + c)/b$ qui, tout comme x, doit prendre une valeur entière ; d'où l'idée de faire apparaître le reste a_2 dans la division de $a = a_0$ par $b = a_1$ et le reste c_2 dans la division de $c = c_1$ par $b = a_1$, de sorte que :

$$y = (ax + c)/b = (a_0x + c_1)/a_1 \equiv (a_2x + c_2)/a_1 \pmod 1;$$

puis l'idée d'introduire la quantité $u = (a_2x + c_2)/a_1$ qui, tout comme y, doit prendre une valeur entière. Ceci s'écrit encore :

$$a_2x - a_1u = -c_2,$$

et on peut itérer le processus en tirant $x = (a_1u - c_2)/a_2$. On est ainsi conduit naturellement à considérer :

- la suite strictement décroissante d'entiers $(a_n)_{0 \le n \le k+1}$ des restes dans l'algorithme d'Euclide relatif au couple (a, b) : si $a_0 = a$ et $a_1 = b$, alors a_{n+1} désigne le reste de a_{n-1} dans la division par a_n ;
  par suite, $a_{n+1} \equiv a_{n-1} \pmod{a_n}, a_{k+1} = 0$ et $a_k = \text{P.G.C.D.}(a, b)$;
- la suite décroissante d'entiers $(c_n)_{1 \le n \le k+1}$ où $c_1 = c$ et c_{n+1} désigne le reste de c_n dans la division par a_n ; par suite, $c_{n+1} \equiv c_n \pmod{a_n}$;
- une suite de lettres $(x_n)_{0 \le n \le k+1}$ où $x_0 = y$ et $x_1 = x$ et dont les valeurs sont liées entre elles par la relation de récurrence :

$$a_nx_{n+1} - a_{n+1}x_n = (-1)^n c_{n+1} \ \text{ pour } \ n \ge 0.$$

Par construction même, si la valeur de x_n est entière, alors la différence $x_{n+1} - x_{n-1}$ est un entier. En effet,

$$x_{n+1} = (a_{n+1}x_n + (-1)^n c_{n+1})/a_n \equiv (a_{n-1}x_n + (-1)^n c_n)/a_n = x_{n-1} \pmod 1.$$

Par suite, on vérifie aisément par récurrence que, si les valeurs de x et y sont entières, alors les valeurs de $x_2, \ldots, x_{k+1}$, sont elles aussi entières.

Or, $a_{k+1} = 0$, donc $x_{k+1} = (-1)^k c_{k+1}/a_k$ n'est entier que si a_k divise c_{k+1}, d'où $c_{k+1} = 0$ et le P.G.C.D. de a et b divise c.

Inversement, supposons que le P.G.C.D. de a et b divise c, alors a_k divise c_k, $c_{k+1} = 0$ et $x_{k+1} = 0$. Par suite, à toute valeur entière de x_k correspondent, en remontant la récurrence, des valeurs entières pour $x_{k-1}, \ldots, x_2, x_1 = x$ et $x_0 = y$.

Commentaire

L'écriture du P.G.C.D. 1 de 11 et 17 sous la forme d'une combinaison de 11 et 17 à coefficients entiers :

$$1 = 2 \times 17 - 3 \times 11$$

est appelée *identité de Bézout*.

Une telle identité a lieu non seulement dans l'anneau des entiers $\mathbb{Z}$, mais aussi dans l'anneau $\mathrm{K}[X]$ des polynômes à coefficients dans un corps K, comme l'anneau $\mathbb{R}[X]$ (cf. le commentaire souligné p. 156[a]), en fait dans tout anneau euclidien (cf. le commentaire souligné p. 133[b]). Ainsi, si P et Q sont deux polynômes étrangers entre eux, il existe deux polynômes U et V tels que :

$$PU + QV = 1$$

L'obtention de U et V s'effectue par la même méthode, c'est à dire l'utilisation de l'algorithme d'Euclide pour déterminer le P.G.C.D. de P et Q.

Plus généralement, on appelle aujourd'hui *anneau de Bézout* un anneau dont tout idéal de type fini est principal. Deux éléments a et b y possèdent un P.G.C.D. à savoir un élément d tel que $\mathrm{A}d$ soit l'idéal engendré par a et b et l'identité de Bézout y a bien lieu puisque :

$$\mathrm{A}a + \mathrm{A}b = \mathrm{A}d.$$

Mais on ne dispose plus nécessairement de l'algorithme d'Euclide pour déterminer un tel P.G.C.D., d.

[a] On trouve p. 156 une remarque concernant le théorème de Sturm dont il est noté qu'il est quant à lui applicable dans tout anneau de polynômes à coefficients dans un corps K, et dont on cherche des racines dans le corps K, pourvu que l'on y puisse appliquer le théorème des valeurs intermédiaires. A cet effet, il faut tout d'abord pouvoir munir K d'un ordre compatible avec les opérations, c'est la notion de *corps réel* ou ordonnable - caractérisé par le fait que -1 ne peut y être somme de carrés -, il faut ensuite des conditions affirmant l'existence de racines dans K - en fait, que $K(i)$ soit un corps algébriquement clos -, le corps réel K est alors appelé *corps réel clos* ou corps ordonné maximal.

[b] Le commentaire en question est : "On appelle aujourd'hui *anneau euclidien* [5] un anneau A muni d'un "*algorithme euclidien*", c'est à dire d'une application g de A dans $\mathbb{N}$ telle que : étant donnés deux éléments a et b de A, b étant non nul, il existe deux éléments q et r de A vérifiant :

$$a = bq + r \quad \text{et} \quad g(r) < g(b).$$

Par exemple : $A = \mathbb{Z}$ avec $g(a) = |a|$ (plus petit reste en valeur absolue) ou encore $A = \mathbb{R}[X]$ avec $g(P(X)) = 1 + d^{\circ}(P(X))$ et $g(0) = 0$."

Références

[1] Cl.-G. Bachet, Sieur de Méziriac, *Problèmes plaisans et délectables qui se font par les nombres*, 1ère éd. 1612, 2ème éd. 1624 chez P. Rigaud, à Lyon ; éd. simplifiée Blanchard, Paris, 1959.

[2] J.-C. Martzloff, *Histoire des mathématiques chinoises*, Masson, Paris, 1987.

[3] A. Youschkevitch, *Les mathématiques arabes (VIIIe-XVe siècles)*, trad. M. Cazenave et K. Jaouiche, Vrin, Paris, 1976.

[4] E. Bézout, *Cours de mathématiques à l'égard des Gardes du Pavillon et de la Marine, tome III, Algèbre*, Musier, Paris, 1766.

[5] P. Samuel, *About euclidean rings*, Journal of Algebra, t. 19 (1971), 282-301.