Arithmétique : PGCD, Bézout et Gauss
Problème de recherche : les vases de Bachet

Dans ses *Problèmes plaisants et délectables qui se font par les nombres* (1612), Claude-Gaspard Bachet de Méziriac pose le problème suivant : partager en deux moitiés 8 pintes de vin contenues dans un vase de 8 pintes, en ne disposant que de deux vases vides de 5 et 3 pintes, sans graduation. On ne peut que transvaser un vase dans un autre jusqu'à ce que le premier soit vide ou le second plein.

La mission

1. Résoudre le problème de Bachet. On décrira chaque étape par le contenu des trois vases.
2. On dispose maintenant d'une fontaine et de deux récipients non gradués de a et b litres (a, b entiers naturels non nuls). On peut remplir un récipient à la fontaine, le vider, ou transvaser l'un dans l'autre. Démontrer qu'à tout moment, la quantité d'eau contenue dans chaque récipient est de la forme $au+bv$ avec u et v entiers relatifs.
3. En déduire qu'avec des récipients de 6 L et de 9 L, on ne peut pas mesurer 4 L.
4. Avec des récipients de 9 L et 7 L, on veut obtenir exactement 1 L. Trouver des entiers u et v tels que $9u-7v=1$, puis en déduire une suite d'opérations qui fournit 1 L.

Pour aller plus loin

Quelle condition sur a, b et l'entier c est nécessaire pour pouvoir mesurer c litres ? Peut-on mesurer 5 L avec des récipients de 10 L et 15 L ? avec 6 L et 9 L ?

Coups de pouce

Bloqué ? Des indices progressifs sont disponibles en ligne. N'en ouvrir qu'un à la fois, et seulement après avoir cherché !

Éléments de correction

1. Le partage de Bachet

On note (vase de 8 ; vase de 5 ; vase de 3). Une solution en 7 transvasements :

$$(8;0;0) \to (3;5;0) \to (3;2;3) \to (6;2;0) \to (6;0;2) \to (1;5;2) \to (1;4;3) \to (4;4;0).$$

On remplit le 5, on le verse dans le 3, on reverse le 3 dans le 8, on passe les 2 pintes restantes dans le 3, on remplit à nouveau le 5, on complète le 3 (il manquait 1 pinte), on reverse le 3 dans le 8.

2. Les quantités possibles

Au départ, les deux récipients contiennent $0 = a \times 0 + b \times 0$. Supposons qu'à un moment les contenus soient $x = au + bv$ et $y = au' + bv'$. Remplir ou vider un récipient le fait passer à a, b ou 0, qui sont de la forme voulue. Un transvasement de quantité t donne $x - t$ et $y + t$; or t vaut soit x (on vide le premier), soit ce qu'il fallait pour remplir le second, $b - y$ par exemple. Dans tous les cas, les nouveaux contenus s'écrivent encore $au'' + bv''$ avec u'', v'' entiers. Par récurrence sur le nombre d'opérations, la propriété est toujours vraie.

3. Avec 6 L et 9 L

Toute quantité mesurée est de la forme $6u + 9v = 3(2u + 3v)$: c'est un multiple de 3, et 4 n'en est pas un. On ne peut pas mesurer 4 L. Plus généralement, toute quantité mesurée est un multiple de $\text{PGCD}(a, b)$.

4. Avec 9 L et 7 L

$\text{PGCD}(9, 7) = 1$. L'algorithme d'Euclide : $9 = 7 + 2$, $7 = 3 \times 2 + 1$, d'où $1 = 7 - 3 \times 2 = 7 - 3(9 - 7) = 4 \times 7 - 3 \times 9$. Ou, plus pratique ici : $9 \times 4 - 7 \times 5 = 36 - 35 = 1$, soit $u = 4$ et $v = 5$.

Interprétation : on remplit 4 fois le récipient de 9 L et on vide 5 fois celui de 7 L. On répète : remplir le 9, le verser dans le 7, vider le 7 dès qu'il est plein.

$$(9;0) \to (2;7) \to (2;0) \to (0;2) \to (9;2) \to (4;7) \to (4;0) \to (0;4) \to (9;4)$$
$$\to (6;7) \to (6;0) \to (0;6) \to (9;6) \to (8;7) \to (8;0) \to (1;7) \to (1;0).$$

On a rempli 4 fois le 9 et vidé 5 fois le 7 : il reste **1** L dans le récipient de 9 L.

Pour aller plus loin

Condition nécessaire : $\text{PGCD}(a, b)$ divise c (et $c \leqslant \max(a, b)$ pour que la quantité tienne dans un récipient). Avec 10 L et 15 L, PGCD = 5 divise 5 : c'est possible (remplir le 15, le verser dans le 10, il reste 5 L). Avec 6 L et 9 L, 3 ne divise pas 5 : c'est impossible.

On peut démontrer (enrichissement) que la condition est aussi suffisante, avec la méthode répétitive de la question 4.

Enrichissement historique : dans l'édition de 1624 de son livre, Bachet démontre que si deux entiers sont premiers entre eux, il existe une combinaison $au - bv$ égale à 1 ; Étienne Bézout étendra ce résultat aux polynômes au XVIIIe siècle.

Ce qu'on a utilisé du chapitre

— PGCD, algorithme d'Euclide.
— Identité de Bézout ; tout entier de la forme $au + bv$ est multiple du PGCD.