Autour du pgcd

2.1 L'anthyphérèse

Chez Euclide, ce que nous appelons l'algorithme d'Euclide est avant tout une méthode géométrique pour trouver une plus grande commune mesure, si elle existe, à deux grandeurs de même nature.

Considérons par exemple deux segments de droites, AB et CD qui admettent pour commune mesure un segment EF, ce qui signifie que l'unité EF est contenue un nombre entier de fois dans AB et CD. Supposant $AB > CD$, on commence par retrancher autant de fois qu'il est possible le segment CD du segment AB. S'il ne reste rien, c'est que CD était une commune mesure, et c'est manifestement la plus grande possible. S'il reste quelque chose, que nous notons GH, alors toute commune mesure à AB et CD est aussi une commune mesure à CD et GH. On peut donc continuer le processus. Comme GH est strictement plus petit que CD, le nombre de fois que EF est contenu dans GH est inférieur au nombre de fois qu'il est contenu dans CD. Ainsi le processus s'arrête après un nombre fini d'étapes et fournit une commune mesure, nécessairement multiple entier de EF.

Voici donc un résultat qui n'était pas a priori évident : la commune mesure trouvée est multiple de toute autre commune mesure.

Si maintenant on raisonne avec les nombres entiers a et b qui mesurent AB et CD par rapport à l'unité EF, le processus devient un calcul avec des entiers positifs qui fournit un commun diviseur g de a et b, et tout autre diviseur commun de a et b divise g, donc est plus petit que g.

Ceci démontre que le plus grand commun diviseur de a et b est multiple de tout autre diviseur commun.

Ce processus de soustractions alternées (on retranche autant de fois qu'on peut CD de AB, puis autant de fois qu'on peut GH de CD, puis ...) s'appelle l'anthyphérèse dans les textes anciens.

Plus que pour chercher une commune mesure quand il en existe une, ce procédé était surtout utilisé pour montrer l'impossibilité d'une commune mesure entre deux grandeurs données, lorsqu'on montre que l'anthyphérèse ne peut aboutir en un nombre fini d'étapes.

Voyons ceci sur l'exemple du coté et de la diagonale du carré (figure 2.1).

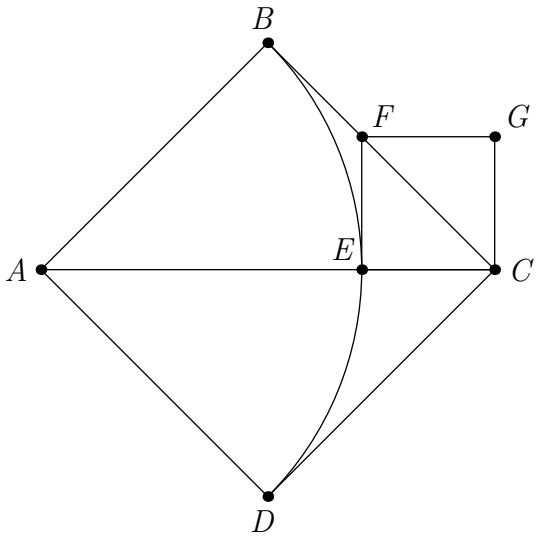

FIG. 2.1 – L'anthyphérèse de la diagonale et du coté du carré

On démarre avec le coté et la diagonale d'un carré $ABCD$. Le cercle de centre A passant par B coupe la diagonale AC en E, de sorte que $AB = AE$. On retranche le coté AB de la diagonale AC et l'on obtient EC. On considère alors le carré $EFGC$. On a $FB = FE = EC$, la première égalité parce que FB et FE sont les deux tangentes au cercles menéees depuis le point F. Ainsi une commune mesure à AB et AC est aussi une commune mesure à AB et EF, donc à BC et $BF = EF$, donc à FC et EF : la diagonale et le coté du carré $EFGC$. Le processus va se répéter à l'identique en remplaçant le carré $ABCD$ par le carré $EFGC$. Comme le coté EF est moindre que la moitié du coté AB, les cotés des carrés successifs deviendront moindre que tout segment donné par avance (axiome d'Archimède), et ceci montre qu'une commune mesure à AB et AC est impossible.

2.2 Le théorème du pgcd

Le théorème qui nous occupe est le suivant.

Théorème 2.2.1 *Si a et b sont deux entiers > 0, le plus grand diviseur commun $g > 0$ de a et b est multiple de tout autre diviseur commun.*

En fait on a découvert plus tard que le théorème 2.2.1 résulte du théorème suivant, qui concentre toute la difficulté du problème dans un énoncé simple, mais plus fort.

Théorème 2.2.2 *Si a et b sont deux entiers > 0, il existe un entier $g > 0$ de la forme $ua + vb$ avec $u, v \in \mathbb{Z}$, qui divise a et b.*
L'égalité $g = ua + vb$ s'appelle aussi une relation de Bezout entre a et b.

Démonstration que le théorème 2.2.2 implique le théorème 2.2.1. Soit h un diviseur commun de a et b : $a = ha_1$, $b = hb_1$ donc $g = au + bv = h(au_1 + bv_1)$. Ainsi g est à la fois plus grand que h et multiple de h. Le théorème 2.2.1 est bien satisfait. □

Le théorème doit donc être compris comme affirmant deux propriétés inattendues du plus grand des diviseurs communs à a et b.

- La première est que tout diviseur commun à a et b doit diviser g.
- La seconde est que g peut s'écrire sous la forme $ua + vb$ avec $u, v \in \mathbb{Z}$.

Nous envisageons maintenant deux preuves du théorème 2.2.2.

2.3 Une preuve abstraite classique

Tout d'abord on établit le lemme suivant :

Lemme 2.3.1 *Toute partie non vide de* $\mathbb{N}$ *admet un plus petit élément.*

Preuve du lemme. Si une partie V de $\mathbb{N}$ contient un élément c alors le plus petit élément de l'ensemble fini $V \cap [0, c]$ est aussi le plus petit élément de V. □

Preuve abstraite du théorème 2.2.2. On considère l'ensemble

$$V(a, b) = V = (a\mathbb{Z} + b\mathbb{Z}) \cap \mathbb{N}^* = \{x > 0 \mid \exists u, v \in \mathbb{Z},\ x = ua + vb\}\,.$$

L'ensemble V contient a et b : il est non vide. Soit $g = ua + vb$ le plus petit élément de V. Montrons par l'absurde qu'il divise a et b. Si ce n'était pas le cas, on aurait par exemple : g ne divise pas a. Alors en divisant a par g on obtiendrait un reste $r \in \{1, \ldots, g-1\}$ avec $a = gq + r$. On aurait alors

$$r = a - gq = a(1 - uq) + (-vq)b$$

et ceci montre que $r \in V$, ce qui contredit le fait que g est le plus petit élément de V. □

2.4 Une preuve par algorithme

Algorithme 2.4.1 ***Algorithme de calcul du pgcd.***
Entrée : Deux entiers naturels a et b, > 0.
Sortie : Leur pgcd g.
Début
  # boucle
  Tant que $b \neq 0$ **faire**
    Remplacer a et b par : b et le reste de la division de a par b ;
  fin tant que ;
  # fin de boucle
  $g \leftarrow a$
Fin.

On considère l'algorithme 2.4.1 qui est à peu près celui exposé par Euclide.

Nous affirmons que pour n'importe quelles valeurs entrées pour a et b, l'algorithme fournit un élément g qui satisfait les propriétés requises dans le théorème 2.2.2.

Sous une forme un peu plus précise, et sans détruire le contenu des identificateurs a et b donnés en entrée, l'algorithme se réécrit comme dans l'encadré 2.4.1 bis.

Preuve de terminaison. Nous vérifions tout d'abord que l'algorithme 2.4.1 bis s'arrête bien après un nombre fini d'étapes. Cela tient à ce que, à chaque exécution de la boucle, b' est remplacé par un nombre strictement plus petit dans $\mathbb{N}$. Il atteint donc nécessairement la valeur 0 (ce qui est le seul moyen de sortir de la boucle) en un nombre fini d'étapes.
Il faut également noter que l'instruction « $b'' \leftarrow$ reste de la division de a' par b' » est toujours exécutée avec un $b' > 0$ et qu'il n'y aura donc pas d'erreur (la division par 0 n'est pas définie) lors de l'exécution du programme. □

Preuve de correction. Notons a_k et b_k $(k = 0, 1, \ldots, n)$ les valeurs successives prises par a' et b' chaque fois qu'on fait le test « $b' = 0$? » en début de boucle. On démarre avec $a_0 = a$ et $b_0 = b$.

Algorithme 2.4.1 bis ***Algorithme de calcul du pgcd, plus précis.***
Entrée : Deux entiers naturels a et b, > 0.
Sortie : Leur pgcd g.
Variables locales : a', b', b'' : entiers ≥ 0 ;
Début
initialisation
$a' \leftarrow a$; $b' \leftarrow b$;
boucle
Tant que $b' > 0$ **faire**
$b'' \leftarrow$ reste de la division de a' par b' ;
$a' \leftarrow b'$; $b' \leftarrow b''$;
fin tant que ;
fin de boucle
$g \leftarrow a'$
Fin.

Si $b_k \neq 0$ la boucle est exécutée et l'on obtient $a_{k+1} = b_k$ et $b_{k+1} = a_k - q_k b_k$, en notant q_k le quotient dans la division. Alors on a par un calcul immédiat l'équivalence :

$$\forall\, x \in \mathbb{N} \quad \big(\ (x \text{ divise } a_k \text{ et } b_k) \iff (x \text{ divise } a_{k+1} \text{ et } b_{k+1})\ \big)$$

On a donc pour tout $x \in \mathbb{N}$:

$$(x \text{ divise } a_0 \text{ et } b_0) \iff (x \text{ divise } a_1 \text{ et } b_1) \iff \cdots \iff (x \text{ divise } a_n \text{ et } b_n)$$

La dernière valeur du couple (a', b') est (a_n, b_n) avec $a_n > 0$ et $b_n = 0$.
Or $a_n = b_{n-1}$ et $b_n = 0$ est le reste de la division de a_{n-1} par b_{n-1}. Cela signifie que a_n divise a_{n-1} et b_{n-1}, donc divise a et b.
Par ailleurs on a de proche en proche le fait que a_k et b_k sont tous de la forme $u_k a + v_k b$ avec $u_k, v_k \in \mathbb{Z}$. Ainsi $g = a_n$, qui est la sortie donnée par l'algorithme, vérifie les conclusions du théorème 2.2.2. □

2.5 Comparaison des deux preuves

On peut comparer les deux preuves proposées de différents points de vue. Élégance, rigueur, simplicité, facilité de compréhension, conviction de l'interlocuteur, effectivité du résultat annoncé.

Bien que ces critères, hormis le dernier, soient très subjectifs, et que les réponses dépendent beaucoup de notre éducation mathématique ils sont néanmoins très importants.

Une grande partie de l'activité de recherche en mathématiques consiste à essayer de simplifier ce qui a déjà été démontré. Souvent la première preuve trouvée pour un résultat important est obscure pour la plupart. La science mathématique ne pourrait pas progresser réellement sans l'activité continue de simplification des preuves.

La première preuve est appelée ici « classique » car c'est celle que l'on trouve désormais le plus souvent exposée[1].

Elle est particulièrement rapide et donne le sentiment d'aller droit au but. On peut la voir comme le résultat d'un effort de simplification de la preuve originelle, qui, dans la mesure où elle peut être pointée historiquement, ressemble beaucoup plus à la preuve par algorithme.

L'argument aussi est dans une certaine mesure plus simple que dans la deuxième preuve. Si l'on n'avait pas déjà la démonstration d'Euclide en tête, il aurait fallu de l'imagination pour trouver l'argument décisif :

$$\forall\, x \in \mathbb{N} \quad (\ (x \text{ divise } a_k \text{ et } b_k) \iff (x \text{ divise } a_{k+1} \text{ et } b_{k+1})\ ).$$

Par contre la première preuve ne semble pas fournir d'algorithme pour le calcul de u, v et g dont on affirme qu'ils existent. Certainement avant Cantor on n'aurait jamais écrit quelque chose qui ressemble à cela. Il faut une certaine audace pour dire « je les ai trouvés » quand on ne dit pas comment concrètement on peut les avoir. Il faut aussi un certain culot pour considérer l'ensemble infini $V(a,b) \subset \mathbb{N}$ comme objet central de la preuve et raisonner avec son plus petit élément.

A priori, si l'on cherche l'algorithme sous-jacent à la preuve abstraite on est tenté de penser qu'il va falloir examiner tous les éléments de $V(a,b) \cap [0,a]$ et prendre le plus petit d'entre eux. même si une telle recherche s'avère possible, elle semble très inefficace.

[1] En fait, dans un langage plus abstrait on trouve en général l'énoncé suivant : *tout idéal de $\mathbb{Z}$ est principal*, et on en déduit ensuite le théorème 2.2.1. Nous avons préféré ici donner un résumé de cette preuve classique pour mieux faire ressortir son caractère fulgurant.

2.6 La preuve classique cache-t-elle un algorithme ?

O U I ！

Voici en effet « une bonne rédaction » de la preuve classique.

Cette rédaction évite tout aussi bien les difficultés inhérentes à l'emploi du lemme 2.3.1 que celles inhérentes aux preuves par l'absurde.

Nous noterons $\mathrm{Rst}(x, y)$ le reste de la division euclidienne de x par y lorsque $x, y \in \mathbb{N}^*$.

Démonstration élégante et constructive. Remarquons que si nous trouvons un élément g dans $V(a, b) = V$ qui divise a et b, alors tout autre élément de V sera multiple de g. En effet, si $a = ga'$ et $b = gb'$ alors un z arbitraire de V s'écrit $z = ua + vb = g(ua' + vb')$. A fortiori, g doit être le plus petit élément de V.
On est donc amené à chercher un chemin dans V qui descende tant que l'on n'a pas atteint le but fixé. Or l'argument par l'absurde de la première preuve nous indique ce qu'il faut faire pour descendre plus bas dans V quand le but n'est pas atteint.
Définissons donc une suite g_n par récurrence comme suit.

- $g_0 = \inf(a, b)$. On remarque que $g_0 \in V$.
- Passage de n à $n + 1$:
  - Si g_n divise a et b, on arrête la suite (ou, au choix, on pose $g_{n+1} = g_n$).
  - Si g_n ne divise pas a, on pose $g_{n+1} = \mathrm{Rst}(a, g_n)$. On remarque que $g_{n+1} \in V$ et $g_{n+1} < g_n$.
  - Si g_n divise a mais ne divise pas b, on pose $g_{n+1} = \mathrm{Rst}(b, g_n)$. On remarque que $g_{n+1} \in V$ et $g_{n+1} < g_n$.

Cette suite est bien définie, et tous ses termes sont dans V. Tant qu'on n'aboutit pas au premier cas, la suite est strictement décroissante, donc on est certain d'aboutir au premier cas. □

Notez qu'on réalise ainsi de manière certaine l'objectif « trouver un diviseur commun à a et b dans l'ensemble $V(a, b)$ » mais qu'on ne se soucie pas de savoir si le nombre g obtenu est le minimum de $V(a, b)$. Cet « autre » objectif est atteint, comme dans l'algorithme d'Euclide, sans avoir été recherché en tant que tel.

Une légère variante de la démonstration correspond à l'algorithme 2.6.1.

Algorithme 2.6.1 ***Algorithme de calcul du pgcd, implicite dans la preuve classique.***

Entrée : Deux entiers naturels a et b, > 0.
Sortie : Leur pgcd g.
Variables locales : r, r' : entiers ≥ 0 ;
Début
  # initialisation
  $g \leftarrow \inf(a, b)$;
  # boucle
  Répéter
    $r \leftarrow$ le reste de la division de a par g ;
    Si $r > 0$ **alors** $g \leftarrow r$ **fin si** ;
    $r' \leftarrow$ le reste de la division de b par g ;
    Si $r' > 0$ **alors** $g \leftarrow r'$ **fin si** ;
  jusqu'à ce que $r = r' = 0$
  # fin de boucle
Fin.