Une précision sur le pgcd

Daniel PERRIN

Dans cette note je montre comment prouver le théorème de Gauss sans utiliser ni la décomposition en facteurs premiers, ni le théorème de Bézout. Cette preuve est sans doute très proche celle que l'on donnait autrefois dans les cours de terminale[1]*. En vérité, elle est très proche de la méthode qui utilise Bézout.*

Dans ce qui suit, j'utilise le raisonnement par absurde et minimalité qui s'appuie sur le fait que toute partie non vide de $\mathbf{N}$ a un plus petit élément. Le principe d'utilisation de ce raisonnement est le suivant. Pour montrer qu'une propriété portant sur les entiers est vraie, on suppose qu'elle ne l'est pas. Il y a donc un ensemble non vide de contre-exemples. On choisit alors le plus petit contre-exemple et on tente d'aboutir à une contradiction.

On définit le pgcd de deux entiers $a, b \geq 0$, non tous deux nuls, comme le plus grand diviseur commun (au sens de l'ordre usuel) de $\mathbf{N}$. On rappelle la *comptine du* pgcd :

Remarque 1. Si d est le pgcd de a et b, il existe a' et b', premiers entre eux, tels que l'on ait $a = da'$ et $b = db'$.

Le point clé est de prouver la proposition suivante, qui montre que le pgcd est aussi le plus grand diviseur commun au sens de la divisibilité, sans utiliser le théorème de Bézout :

Proposition 2.
Si d est le pgcd *de a et b et si e est un diviseur de a et b, alors e* **divise** *d.*

Démonstration. On note d'abord que le cas où a ou b est nul est trivial. On raisonne par l'absurde et minimalité en choisissant un contre-exemple a, b, avec $a \leq b$, tel que a soit le plus petit possible et b le plus petit pour a fixé. On a $a > 0$. On considère alors a et $b - a$. Il est clair que les diviseurs communs à a et b sont les mêmes que ceux de a et $b-a$. En particulier, on a $d = \text{pgcd}\,(a, b) = \text{pgcd}\,(a, b-a)$ et e divise aussi a et $b - a$. Mais, comme $b - a$ est $< b$, le couple $(a, b - a)$ (ou $(b - a, a)$ si $b - a < a$) n'est plus un contre-exemple en vertu de l'hypothèse de minimalité. Il en résulte que e divise d et on a gagné.

Remarque 3.
On notera que l'astuce de cette démonstration (remplacer a, b par $a, b-a$) est très proche de l'algorithme d'Euclide, donc de la preuve de Bézout.

Corollaire 4.
Soient $a, b, c \in \mathbf{N}$ avec $c > 0$ et a, b non tous deux nuls. On a la formule : $\text{pgcd}\,(ac, bc) = c\,\text{pgcd}\,(a, b)$.

[1] Je vous parle d'un temps que les moins de vingt ans ne peuvent pas connaître.

Démonstration. Posons $d = \text{pgcd}\,(a, b)$ et $\delta = \text{pgcd}\,(ac, bc)$. Il est clair que cd est un diviseur commun de ac et bc. En vertu de la proposition 2, il divise donc δ. Inversement, c divise ac et bc, donc aussi leur pgcd (toujours par la proposition 2). On a donc $\delta = ce$, avec $e \in \mathbf{N}$. On écrit alors la comptine du pgcd avec ac et bc : on a $ac = \delta a'$, $bc = \delta b'$ avec a', b' premiers entre eux (mais ici cela ne sert pas). En remplaçant δ par ce, on obtient $a = ea'$, $b = eb'$, de sorte que e est un diviseur commun de a, b, donc divise d (encore la proposition 2). Mais alors $\delta = ce$ divise cd et, en définitive, on a $cd = \delta$.

Corollaire 5 (théorème de Gauss).
Soient a, b, c des entiers naturels avec a, b non tous deux nuls. On suppose que a divise bc et que a est premier avec b. Alors a divise c.

Démonstration. L'hypothèse $\text{pgcd}\,(a, b) = 1$ implique, en vertu du corollaire 4, $\text{pgcd}\,(ac, bc) = c$. Mais comme a divise ac et bc, il divise leur pgcd en vertu de la proposition 2.