Le lemme d'Euclide

1 Les énoncés

Il s'agit du résultat suivant, proposition 30 du livre VII des Éléments d'Euclide :

1.1 Lemme. *Si le produit de deux facteurs admet un diviseur premier, ce dernier divise l'un des facteurs du produit.*

Ce lemme repose sur le suivant (proposition 20) :

1.2 Lemme. *Si l'on a une proportion* $\frac{a}{b}$ *et si* a, b *sont les plus petits dans ce rapport (c'est-à-dire si* $\frac{a}{b} = \frac{c}{d}$ *implique* $a \leq c$ *et* $b \leq d$*), alors on a* $c = ae$ *et* $d = be$*.*

2 Les preuves

Commençons par 1.2. On divise c par a et d par b : $c = ae + r$ et $d = bf + s$ avec $0 \leq r < a$ et $0 \leq s < b$. En écrivant $ad = bc$ on obtient $n := ad = abf + as = bc = abe + br$. Mais, comme on a $as < ab$ et $br < ab$, ces expressions sont deux divisions euclidiennes de n par ab et, par unicité du quotient et du reste, on a $f = e$ et $as = br$. Si r ou s est non nul, l'autre aussi et on a $\frac{a}{b} = \frac{r}{s}$ avec des nombres plus petits, ce qui est absurde. On a donc bien $c = ae$ et $d = be$.

Une conséquence de ce lemme (proposition 21) est le fait que si a, b sont premiers entre eux, ce sont les plus petits donnant la proportion $\frac{a}{b}$ (sinon, on en a une autre avec des plus petits et ils divisent a, b par 1.2).

Passons à la preuve de 1.1. On suppose que p premier divise ab et on écrit $ab = pc$. Si p ne divise pas a, il est premier avec a et on a $\frac{a}{p} = \frac{c}{b}\cdot$ Mais, comme a, p sont premiers entre eux (car p ne divise pas a), ils forment la plus petite proportion et donc, par 1.2, il existe e tel que $c = ae$ et $b = pe$, donc p divise b.

Euclide prouve ensuite que tout nombre entier admet un facteur premier, mais n'énonce pas l'existence et la décomposition d'un nombre en produit de facteurs premiers, même s'il est clair qu'il est en posture de prouver cela.