

Sur l'unicité de la décomposition d'un entier en facteurs premiers

La méthode usuelle suppose préalablement acquise la théorie du P.G.C.D. et le fameux théorème de Gauss, effroi des candidats au bachot : si $a|bc$ et si $(a, b) = 1$ alors $a|c$.

Elève, je m'étonnais de ce que je considérais comme un détour — et fort long — pour atteindre un but que je trouvais « intuitivement » proche.

Plus tard, j'ai eu la satisfaction d'apprendre une méthode qui se base sur un strict minimum de connaissances. Le mérite en revient à ZERMELO, célèbre pour son *axiome du choix*. J'ignore si des manuels la proposent aux étudiants, enfin, la voici.

S'il existe des nombres admettant plusieurs factorisations distinctes leur ensemble possède nécessairement un premier élément, plus petit que tous les autres. Soit a ce nombre. Il est susceptible d'au moins deux factorisations distinctes, j'appelle m et p les plus petits facteurs premiers figurant respectivement dans chaque factorisation. On peut donc écrire : $a = mn$, $a = pq$ en précisant que m est différent

de p , que m ne divise pas q et que p ne divise pas n , sans quoi $\frac{a}{m}$ ou $\frac{a}{p}$ qui sont inférieurs à a auraient deux factorisations distinctes contrairement à la définition de a .

Si l'on suppose par exemple $m < p$ on a alors $n > q$ et comme d'autre part $p < q$ on a : $mp < pq = a$. Formons alors le nombre positif $a - mp$,

$$a - mp = mn - mp = m(n - p),$$

$$a - mp = pq - mp = p(q - m),$$

m qui ne divise pas q ne divise pas $(q - m)$ et de même p ne divise pas $(n - p)$. Donc le nombre $(a - mp)$, qui est inférieur à a , admet deux factorisations distinctes, ce qui est une contradiction. Le théorème d'unicité est démontré.

Remarque : Le lecteur qui s'intéresse à l'*Algèbre moderne* verra que la démonstration s'étend aussitôt à tous les anneaux euclidiens, en particulier aux entiers de Gauss, de la forme $a + bi$ (a et b entiers) et aux polynômes à une variable sur le corps des réels.

André LENTIN,
Professeur au Lycée Buffon.