

Le théorème fondamental de l'arithmétique

Définition. Un nombre $p \in \mathbb{N}$ est dit **premier** si $p \geq 2$ et $\forall m, n \in \mathbb{N}$,

$$nm = p \Rightarrow n = 1 \text{ ou } m = 1.$$

Le **théorème fondamental de l'arithmétique**, où TFA affirme que tout nombre naturel supérieur ou égal à 2 peut s'écrire comme un produit de nombres premiers. On appelle cela la **factorisation** des nombres naturels en premiers.

De plus, ce théorème affirme que la factorisation est unique à l'ordre des facteurs près. Par exemple, $10 = 2 \times 5 = 5 \times 2$, ou encore que $12 = 2 \times 3 \times 2 = 2 \times 2 \times 3$. Si on impose l'ordre croissant sur les facteurs, on aura alors les factorisations uniques $10 = 2 \times 5$ et $12 = 2 \times 2 \times 3 = 2^2 \times 3$.

La factorisation d'un nombre premier est le nombre premier lui-même, par exemple $7 = 7$ ou $23 = 23$.

L'énoncé du TFA se présente donc comme suit :

Tout nombre naturel $n \geq 2$ se factorise sur les nombres premiers de manière unique à l'ordre des facteurs près.

La preuve de ce théorème présentera deux parties : une qui montre l'existence de cette factorisation et une qui montre son unicité.

Existence : On forme l'ensemble $E \subset \mathbb{N} \setminus \{0, 1\}$ des nombres naturels sans factorisation. On suppose par absurde cet ensemble non vide. Puisqu'on a un bon ordre sur $\mathbb{N}$, cet ensemble E doit posséder un plus petit élément, disons m .

m ne peut être premier, puisqu'alors sa factorisation s'écrirait comme $m = m$. Puisque m n'est pas premier, il doit exister deux nombre $p, q \neq 1$ tels que $m = pq$. Mais alors, $p, q < m$ et donc $p, q \notin E$ par minimalité de m . Cela implique l'existence de factorisations en premiers

$$p = p_1 \times p_2 \times \dots \times p_k \text{ et } q = q_1 \times q_2 \times \dots \times q_l.$$

Mais alors $m = pq = p_1 \times p_2 \times \dots \times p_k \times q_1 \times \dots \times q_l$ est une factorisation de m et $m \notin E$, d'où contradiction. E n'a donc pas d'élément minimal et doit donc être vide.

Unicité : On forme l'ensemble $E \subset \mathbb{N} \setminus \{0, 1\}$ des nombres naturels avec plusieurs factorisations. On suppose par absurde cet ensemble non vide. Puisqu'on a un bon ordre sur $\mathbb{N}$, cet ensemble E doit posséder un plus petit élément, disons m . On aurait alors

$$m = p_1 \times p_2 \times \dots \times p_k = q_1 \times q_2 \times \dots \times q_l,$$

où $p_1 \leq p_2 \leq \dots \leq p_k$, $q_1 \leq q_2 \leq \dots \leq q_l$ et où au moins un des premiers p_i serait différent de tous les premiers q_j .

On remarque en fait que tous les p_i doivent être différents de tous les q_j , car si cela

n'était pas le cas, on pourrait simplifier les deux factorisations par le premier en commun, ce qui donnerait deux factorisations différentes d'un nombre plus petit que m , contredisant la minimalité de ce dernier. En effet, si $p_1 = q_1$ par exemple, alors

$$p_2 \times \dots \times p_k = q_2 \times \dots \times q_l < m,$$

et m ne serait pas le plus petit nombre de E . On a donc que tous les p_i sont différents de tous les q_j .

Sans pertes de généralités, on peut maintenant supposer que $p_1 < q_1$. Il doit donc exister un nombre naturel d tel que $p_1 + d = q_1$. Mais alors

$$p_1 \times p_2 \times \dots \times p_k = q_1 \times q_2 \times \dots \times q_l = (p_1 + d) \times q_2 \times \dots \times q_l$$

et

$$d \times q_2 \times \dots \times q_l < q_1 \times q_2 \times \dots \times q_l = m.$$

Mais on a aussi que

$$d \times q_2 \times \dots \times q_l = p_1 \times (p_2 \times \dots \times p_k - q_2 \times \dots \times q_l)$$

ce qui montre que le nombre $d \times q_2 \times \dots \times q_l$ est divisible par p_1 . Or, aucun des q_j n'est égal à p_1 et d n'est pas divisible par p_1 non plus, car sinon $q_1 = p_1 + d$ serait aussi divisible par p_1 , contredisant le fait que q_1 est un premier. On a donc que

$$m > d \times q_2 \times \dots \times q_l = p_1 \times r,$$

où r , étant un nombre naturel, possède une factorisation en premier aussi. On a donc que le nombre $d \times q_2 \times \dots \times q_l$ posséderait deux factorisations distinctes, une sans le facteur p_1 et une avec ce facteur. m ne peut donc être le plus petit élément de E et ce dernier ensemble doit être vide. $\square$