Une démonstration originale de l'infinité de l'ensemble des nombres premiers

L'idée essentielle de la démonstration est que, s'il n'y a qu'un ensemble fini de nombres premiers, alors il n'y a "pas assez" de décompositions possibles. Pour formaliser cette idée, il nous faut nous restreindre à un sous ensemble fini de $\mathbb{N}$. Nous allons en réalité montrer que, sous cette hypothèse, on ne peut plus décomposer tous les entiers de 1 à n pour n assez grand.

Soit P l'ensemble des nombres premiers. Si P est fini, P s'écrit $\{p_1, \ldots, p_r\}$.

Soit n un entier, désormais fixé. n s'écrit comme un produit de nombres premiers, c'est-à-dire sous la forme :

$$n = \prod_{i=1}^{r} p_i^{v_i(n)}$$

Une considération élémentaire sur les nombres p_i : ils sont tous supérieurs ou égaux à 2. Or pour tout $i \leq r$, on a $p_i^{v_i(n)}$ diviseur de n, donc $p_i^{v_i(n)} \leq n$. En passant aux logarithmes, on obtient :

$$v_i(n) \leq \frac{\log(n)}{\log(p_i)} \leq \frac{\log(n)}{\log(2)}$$

Cette majoration reste bien sûr valable pour un entier k plus petit que n : on a $v_i(k) \leq \frac{\log(k)}{\log(2)}$ donc $v_i(k) \leq \frac{\log(n)}{\log(2)}$.

Or décomposer un entier k ($k \leq n$) en un produit de nombre premier revient, dans le cadre de notre hypothèse P fini, à choisir un r-uplet $(v_1(k), \ldots, v_r(k))$. La majoration précédente nous assure que tous les éléments du r-uplet sont majorés par $\frac{\log(n)}{\log(2)}$, et donc il y a au plus $\left(\frac{\log(n)}{\log(2)}\right)^r$ tels r-uplets (cette majoration est très loin d'être optimale).

Enfin, comme le r-uplet $(v_1(k), \ldots, v_r(k))$ détermine l'entier k, tous ces r-uplets doivent être distincts. C'est-à-dire qu'aux entiers de 1 à n correspondent n r-uplets distincts.

Pour que tout ceci soit possible, il faut donc que $n \leq \left(\frac{\log(n)}{\log(2)}\right)^r$. Mais comme le rapport $\frac{\left(\frac{\log(n)}{\log(2)}\right)^r}{n}$ tends vers 0 lorsque n tends vers l'infini, il devient strictement plus petit que 1 à partir d'un certain rang, c'est-à-dire que l'on a :

$$\left(\frac{\log(n)}{\log(2)}\right)^r < n$$

Et l'on obtient la contradiction voulue : il n'y a alors pas assez de façons possibles pour décomposer tous les entiers de 1 à n comme produits distincts de puissances des r nombres premiers à notre disposition.

En conclusion, l'ensemble P des nombres premiers est infini.

□

N.B. Cette démonstration a l'intérêt de ne pas nécessiter d'« astuce » : on n'a pas, contrairement à beaucoup de démonstrations de ce résultat, à exhiber un nombre particulier qui va permettre de prouver qu'il y a un problème. Il suffit de dérouler les arguments, en majorant un maximum de quantités par des bornes naturelles.

On peut trouver des preuves plus courtes encore, reposant sur le même principe (s'il n'y a qu'une quantité fini de nombres premiers, alors il n'y a pas assez de décompositions possibles en facteurs premiers). Par exemple, la suivante :

Soient $p_1, \ldots, p_r$ une énumération des nombres premiers. Tout entier peut alors s'écrire comme un produit de la forme

$$n = \prod_{i=1}^{r} p_i^{v_i(n)}$$

Étant donné un entier n, et sa décomposition en facteurs premiers, si l'on isole le produit des nombres p_i pour lesquels $v_i(n)$ est impair, on obtient une écriture de la forme :

$$n = l \times m^2$$

où l est le produit que l'on a isolé. En effet le quotient n/l ayant des valences (les nombres $v_i(n/l)$) paires, il peut s'écrire comme un carré parfait.

Regardons maintenant le nombre de décompositions possibles pour les entiers de 1 à n :

- Le nombre de termes carrés possibles est majoré par $\sqrt{n}$.
- L'autre facteur s'écrit comme un produit de certain des p_i $(1 \leq i \leq r)$, soit 2^r possibilités (correspond au nombre de parties d'un ensemble à r éléments).

Au total, cela nous laisse donc $2^r \times \sqrt{n}$ possibilités. Là encore, comme $\left(2^r \times \sqrt{n}\right)/n$ tend vers 0 lorsque n tend vers l'infini, ce rapport devient strictement inférieur à 1 à partir d'un certain rang, ce qui veut dire qu'alors, il n'y a pas assez de décompositions possibles distinctes pour tous les entiers de 1 à n, ce qui est absurde.

□

Rappelons pour mémoire la démonstration "classique", la plus courante en tous cas, de ce résultat :

Reprennons les mêmes notations. Soit P l'ensemble des nombres premiers. Supposons que P est fini, c'est-à-dire que l'on peut écrire P sous la forme $\{p_1, \ldots, p_r\}$.

Soit n l'entier $1 + \prod_{i=1}^{r} p_i$. Alors la définition de l'entier n nous assure que :

$$\forall k \leq r, \quad n \wedge p_k = 1$$

En effet l'équation $n = 1 + \prod_{i=1}^{r} p_i$ s'écrit aussi $n - p_k \prod_{i \neq k} p_i = 1$. Ceci n'est rien d'autre qu'une relation de Bezout entre n et p_k, et donc n et p_k sont premiers entre eux.

Soit q un diviseur premier de n. D'après ce qui précède, q est distinct de tous les $p_i, i \leq r$, et l'on a construit un $(r+1)$ème nombre premier, ce qui est une contradiction avec l'hypothèse sur P.

Donc P est infini.

□

N.B. L'existence d'un diviseur premier de n est une conséquence directe du caractère factoriel de $\mathbb{Z}$, c'est-à-dire que tout entier s'écrit (de manière unique) comme produit de nombres premiers. Par ailleurs, ce résultat se démontre à la main assez facilement : si D_n désigne l'ensemble des diviseurs de n, D_n contient au moins deux éléments : 1 et n lui-même. On exhibe un diviseur premier de n en considérant le plus petit élément q de D_n différent de 1. Celui-ci ne peut avoir de diviseur strict, car un tel diviseur diviserait aussi n et contredirait la minimalité de q.