

Appendice:

Considérons $\mathbb{N} = \{0, 1, 2, 3, \dots\}$
avec les opérations $+$, $\times$.

On peut comparer $u, v \in \mathbb{N}$ en
disant $u < v \iff \exists d \in \mathbb{N} \text{ t.q.}$
 $u + d = v$

Propriétés: 1) $\forall u \in \mathbb{N}, u \leq u$

2) $\forall u, v \in \mathbb{N}, u \leq v \text{ et } v \leq u, \text{ alors } u = v$

3) $\forall u, v, p \in \mathbb{N}, u \geq v, v \geq p, \text{ alors } u \geq p$

4) $\forall E \subset \mathbb{N}, E \neq \emptyset \text{ alors, } E \text{ possède un}$
élément minimal.

On dit que $\leq$ est un bon ordre sur
 $\mathbb{N}$

Def: Un nombre $p \in \mathbb{N}^*$ est dit premier

ssi $\forall a, b \in \mathbb{N}, \text{ si } ab = p \text{ alors}$

$\uparrow$
soit $a = 1$ soit $b = 1$

"si et seulement si"

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41,

, ..., 73

Combien y a-t-il de nombres premiers?
(une infinité)

Thm fondamental de l'arithmétique:

Tout nombre $n \geq 2$ s'écrit comme un produit de nombres premiers et ce produit est unique (à l'ordre des facteurs près).

Exemples: $6 = 2 \cdot 3$, $12 = 2 \cdot 2 \cdot 3$
 $= 2 \cdot 3 \cdot 2$

$7 = 7$, $5 = 5$, $120 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 5$

Preuve: l'existence d'une telle factorisation est claire, prouvons l'unicité.

Posons $E \subset \mathbb{N}$, l'ensemble des nombres avec plusieurs factorisations en premiers.

Supposons $E \neq \emptyset$.

Puisque $\mathbb{N}$ est bien ordonné, E possède un élément minimal, disons m .

On a alors

$$m = p_1 \cdot p_2 \cdots p_k = q_1 \cdot q_2 \cdots q_\ell$$

avec $p_1, \dots, p_k, q_1, \dots, q_e$ premiers

Par minimalité de m ,

$$\{p_1, \dots, p_k\} \cap \{q_1, \dots, q_e\} = \emptyset$$

En particulier, $p_1 \neq q_1$

On peut supposer que $p_1 < q_1$, donc

$$p_1 + d = q_1$$

Donc

$$m = p_1 p_2 \dots p_k = (p_1 + d) q_2 \dots q_e$$

$$\Rightarrow p_1 (p_2 \dots p_k - q_2 \dots q_e) = \underbrace{d q_2 \dots q_e}_{< m}$$

Donc, p_1 divise $d q_2 \dots q_e < m$

Par unicité de la factorisation pour

$d q_2 \dots q_e < m$, p_1 doit diviser d

Mais alors, p_1 divise $p_1 + d = q_1 \nmid$
 $\square$

Thm: Il existe un nombre infini de nombres premiers.

preuve: Supposons qu'il existe un nombre fini

de nombres premiers. On a donc la liste
des premiers : $\{p_1, p_2, p_3, \dots, p_n\}$

Considétons

$$N = (p_1 \times p_2 \times \dots \times p_n) + 1$$

$N \in \mathbb{N}_{\geq 2}$ qui, d'après TFAr, s'écrit
comme un produit sur ses facteurs premiers.
Comme $u_1 p_1, u_2 p_2, \dots, u_n p_n$ ne
divise N , celui-ci doit être premier lui-
même et $\{p_1, \dots, p_n\}$ n'est pas complète. $\square$





