Nombres premiers... où se trouvent-ils?

On étudie les entiers naturels $\mathbb{N} = \{1, 2, 3, \ldots\}$

Définition : $a \in \mathbb{N}$ divise $b \in \mathbb{N}$ si et seulement si il existe $n \in \mathbb{N}$ avec $b = an$.
Notation : $a \mid b$

Définition : $p \in \mathbb{N},\ p > 1$ est un nombre premier si et seulement si il existe que deux entiers naturels qui divisent p : 1 et p lui-même.
Exemples : $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, \ldots$

Types de preuves

1. Preuve directe :
   On montre ce que l'on veut monter.
2. Preuve par induction (par récurrence) :
   On veut montrer un énoncé pour chaque $n \in \mathbb{N}$
   — initialisation : montrer l'énoncé pour l'exemple le plus petit ($n = 1$)
   — hérédité : monter que si l'énoncé est vrai pour n, alors il est vrai pour $n + 1$
3. Preuve par l'absurde :
   On veut montrer un énoncé. On suppose que l'énoncé est faux. On arrive à une contradiction, alors l'énoncé doit être vrai.

Théorèmes fondamentaux de l'arithmétique

Théorème : Chaque $n \in \mathbb{N},\ n > 1$ s'écrit comme un produit de nombres premiers de manière unique à l'ordre de facteurs près.

Preuve par induction de l'existence d'une décomposition

$n = 2$: $2 = 2$ (premier)

$2, \ldots, n \rightsquigarrow n + 1$: On suppose que $2, \ldots, n$ s'écrivent comme un produit de nombres premiers. On veut le montrer pour $n + 1$.

Cas 1 : $n + 1$ est premier

Cas 2 : $n + 1$ n'est pas premier, alors $n + 1 = ab$ pour $1 < a, b < n + 1$
Par hypothèse : $a = p_1 \cdot \ldots \cdot p_k$ $b = q_1 \cdot \ldots \cdot q_m$ pour $p_1 \cdot \ldots \cdot p_k \cdot q_1 \cdot \ldots \cdot q_m$ premiers.
Alors $n + 1 = p_1 \cdot \ldots \cdot p_k \cdot q_1 \cdot \ldots \cdot q_m$ ■

Preuve par l'absurde de l'unicité

On suppose qu'il existe des entiers naturels qui s'écrivent de manières différentes comme produit de nombres premiers.

Soit $s \in \mathbb{N}$ le plus petit entier naturel avec cette propriété

Soient $n + 1 = p_1 \cdot \ldots \cdot p_n = q_1 \cdot \ldots \cdot q_m$ deux factorisations différentes.

Alors $p_i \neq q_j$ pour tout i, j. (Sinon s n'est pas le plus petit nombre avec la propriété)

On peut supposer $p_1 < q_1$

Soient $P = p_2 \cdot \ldots \cdot p_n$ et $Q = q_2 \cdot \ldots \cdot q_m$.

Alors $s = p_1 P = q_1 Q$ et $Q < P$ (car $p_1 < q_1$)

Donc $p_1(P - Q) = s - p_1 Q = (q_1 - p_1)Q < s$
$p_1 \mid p_1(P - Q) \Rightarrow p_1 \mid (q_1 - p_1)Q$
$(q_1 - p_1)Q,\ (q_1 - p_1),\ Q < s$
et alors se factorisent de manière unique comme produit de nombres premiers.

Alors $p_1 \mid (q_1 - p_1)$ ou $p_1 \mid Q$.

Cas 1 : $p_1 \mid (q_1 - p_1) \Rightarrow q_1 - p_1 = np_1 \Rightarrow q_1 = (n+1)p_1 \Rightarrow p_1 \mid q_1$ $\lightning$

Cas 2 : $p_1 \mid Q \Rightarrow p_1 \in \{q_1, \ldots, q_m\}$ $\lightning$

Alors un tel s n'existe pas ! ■

Théorème : Il existe une infinité de nombres premiers.

Preuve

Soient $p_1, \ldots, p_n$ des nombres premiers.

Voilà une stratégie pour trouver un nombre premier p avec $p \notin \{p_1, \ldots, p_n\}$

Soit $P = p_1 \cdot \ldots \cdot p_n$ et $q = P + 1$

Cas 1 : Si q est premier alors $p = q$

Cas 2 : Si q n'est pas un nombre premier. Alors soit p un nombre premier avec $p \mid q$

Par l'absurde : On suppose $p \in \{p_1, \ldots, p_n\}$

Alors $p \mid P$ et $p \mid P + 1$

Donc $p \mid (P + 1) - P \Rightarrow p \mid 1 \Rightarrow p = 1$ $\lightning$

Alors p ne peut pas être dans $\{p_1, \ldots, p_n\}$ ■

Théorème : Soit $p_1 < p_2 < p_3 < \ldots$ la suite des nombres premiers. La somme de cette suite est infinie.

$$\sum_{i=1}^{\infty} \frac{1}{p_i} = +\infty$$

Définition : $\sum_{i=1}^{\infty} a_i = +\infty$ si et seulement si pour tout $R > 0$ on trouve $N(R)$ tel que $\sum_{i=1}^{n} a_i > R$ dès que $n \geq N(R)$

Notation alternative : $\sum_{i=1}^{\infty} a_i = \sum_{i \geq 1} a_i$

Preuve par l'absurde

Supposons que $\sum_{i=1}^{\infty} \frac{1}{p_i} \neq +\infty$

Alors il existe $k \in \mathbb{N}$ tel que $\sum_{i \geq k+1} \frac{1}{p_1} < \frac{1}{2}$

Alors pour $N \in \mathbb{N}$: $\sum_{i \geq k+1} \frac{N}{p_1} < \frac{N}{2}$

Notation : $p_1, \cdots, p_k$ premiers petits
$p_{k+1}, \cdots$ premiers grands

Pour $N \in \mathbb{N}$:

$N_b = \#\{n \leq N : n \text{ est divisible par un premier grand}\}$

$N_s = \#\{n \leq N : n \text{ n'est pas divisible par un premier grand}\}$

Alors $N_b + N_s = N$

Estimons N_b et N_s

1. $\left\lfloor \frac{N}{p_i} \right\rfloor = \#\{n \leq N : n = p_i \cdot m \text{ pour } m \in \mathbb{N}\} = \#\{n \leq N : p_i \mid n\}$

   Alors $N_b \leq \sum_{i \geq k+1} \left\lfloor \frac{N}{p_1} \right\rfloor < \frac{N}{2}$

2. pour $n \leq \mathbb{N}$ avec que des facteurs premiers petits on écrit $n = a_n \cdot b_n^2$ où a_n n'est pas divisible par un carré d'un nombre premier.

   — a_n est un produit de $p_1, \ldots, p_k$ deux-à-deux distincts.
   $\rightsquigarrow 2^k$ possibilités pour a_n
   — $b_n < \sqrt{n} \leq \sqrt{N}$
   $\rightsquigarrow \sqrt{N}$ possibilités pour b_n

   Alors $N_s \leq 2^k \cdot \sqrt{N}$

Pour $N = 2^{2k+2}$: $N_b + N_s < \frac{N}{2} + 2^k \cdot \sqrt{2^{2k+2}} = \frac{N}{2} + 2^{2k+1} = \frac{N}{2} + \frac{N}{2} = N$ ↯

Alors $\sum_{i=1}^{\infty} \frac{1}{p_i} = +\infty$ ■

Symboles mathématiques

Symbole	Nom	Indications supplémentaires
$\mathbb{N}$	Entiers naturels	$\mathbb{N} = \{1, 2, 3, 4, 5, \ldots\}$
$\mid$	Divise	$a \mid b \iff b = an \quad (a, b, n \in \mathbb{N})$
$\sum$	Somme	$\sum_{i=1}^{5} i = 1 + 2 + 3 + 4 + 5 = 15$
$\#$	Nombre d'éléments	$\#\{-1, 0, 1\} = 3$
↯	Contradiction	$2 + 2 = 5$ ↯
■	*quod erat demonstrandum*	Indique la fin d'une preuve