Une infinité de nombres premiers

Nous rassemblons ici plusieurs preuves du théorème suivant :

Théorème : *(d'Euclide)* Notons $\mathbb{P}$ l'ensemble des nombres premiers. Alors $\mathbb{P}$ est infini.

Démonstration α

Raisonnons par l'absurde, et supposons qu'il existe un nombre fini de nombres premiers ; indexons alors l'ensemble des nombres premiers par un ensemble fini I.

Posons $N = 1 + \prod_{i \in I} p_i$. Or N admet nécessairement un diviseur premier, que nous noterons p_k. Comme p_k divise N et $\prod_{i \in I} p_i$, on en déduit que p_k divise $N - \prod_{i \in I} p_i = 1$, ce qui est impossible puisque p_k est un nombre premier. □

Nota Bene : On aurait également pu poser $N = \prod_{i \in I} p_i - 1$.

Démonstration β

Soient $n \in \mathbb{N}_{\geq 2}$ [1] et $k \in [\![2, n]\!]$. Supposons que k divise $n! + 1$. Clairement, k divise $n!$, donc k divise $1 = (n! + 1) - n!$ ce qui est contradictoire avec $k > 1$. Ainsi, $n! + 1$ ne possède pas de diviseur compris entre 2 et n. Cependant, $n! + 1$ admet un diviseur premier p, donc nécessairement $p > n$.

On en déduit que l'ensemble des nombres premiers n'est pas borné, et qu'il est donc infini. □

Démonstration γ

Supposons par l'absurde que $\mathbb{P}$ soit fini. Notons p le plus grand nombre premier. Soit q un facteur premier du nombre de Mersenne $2^p - 1$. Alors $2^p \equiv 1[q]$. Remarquons que q ne peut pas diviser $2^{p-1} - 1$, sans quoi il diviserait $1 = (2^p - 1) - 2(2^{p-1} - 1)$. On en déduit que 2 est d'ordre p dans le groupe multiplicatif $(\mathbb{Z}/q\mathbb{Z})^\times$. D'après le théorème de Lagrange, p divise ainsi le cardinal de $(\mathbb{Z}/q\mathbb{Z})^\times$, à savoir $\varphi(q) = q - 1$ [2] (puisque q est un nombre premier), ce qui implique $p \leq q - 1$ ou $q > p$, d'où une contradiction avec la définition de p. □

1. Pour tout entier k, $\mathbb{N}_{\leq k} = \{n \in \mathbb{N} \mid n \leq k\}$ et $\mathbb{N}_{\geq k} = \{n \in \mathbb{N} \mid n \geq k\}$.
2. Ici, φ est la fonction indicatrice d'Euler.

Démonstration δ

Soit $x \in \mathbb{N}^*$. Notons $\pi(x) = \text{card}\left(\mathbb{P} \cap [\![1, x]\!]\right)$ [3]. Par comparaison série-intégrale, on obtient $\ln(x) \leq \sum_{k \in A} \frac{1}{k}$ où la sommation se fait sur l'ensemble des entiers dont les diviseurs premiers sont inférieurs à x. Or chacun de ces entiers s'écrit de manière unique comme le produit de puissance de nombres premiers inférieurs à x, donc la somme précédente peut être écrite sous la forme $\sum_{(k_i)_i \in \mathbb{N}^{\pi(x)}} \prod_{p \in \mathbb{P}_{\leq x}} \frac{1}{p^{k_p}} = \prod_{p \in \mathbb{P}_{\leq x}} \sum_{k \geq 0} \frac{1}{p^k}$.

Reconnaissant une série géométrique, on obtient $\ln(x) \leq \prod_{p \in \mathbb{P}_{\leq x}} \frac{p}{p-1} = \prod_{p \in \mathbb{P}_{\leq x}} \left(1 + \frac{1}{p-1}\right)$.
En écrivant $\mathbb{P}_{\leq x} = \{p_1, p_2, ..., p_x\}$, puis en remarquant que pour tout $k \in [\![1, \pi(x)]\!]$, $p_k \geq k+1$, on obtient : $\ln(x) \leq \prod_{k=1}^{\pi(x)} \left(1 + \frac{1}{k}\right) = \prod_{k=1}^{\pi(x)} \frac{k+1}{k}$.

Finalement, $\ln(x) \leq \pi(x) + 1$. On en déduit que $\pi(x) \underset{x \to +\infty}{\longrightarrow} +\infty$, c'est-à-dire que $\mathbb{P}$ est infini. $\square$

Démonstration ϵ

$\mathbb{P}$ étant au plus dénombrable, on peut écrire $\mathbb{P} = \{p_1, p_2, ...\}$. Supposons par l'absurde que la série $\sum_{k \geq 1} \frac{1}{p_k}$ converge (ce qui est le cas si $\mathbb{P}$ est fini). Alors il existe un entier k tel que $\sum_{i \geq k+1} \frac{1}{p_i} < \frac{1}{2}$. En particulier, pour tout $N \in \mathbb{N}$, $\sum_{i \geq k+1} \frac{N}{p_i} < \frac{N}{2}$.

Appelons les $p_1, ..., p_k$ les *petits nombres premiers* et les $p_{k+1}, p_{k+2}, ...$ les *grands nombres premiers*. Soit $N \in \mathbb{N}$. Notons N_b le nombre d'entiers inférieurs à N admettant au moins un grand nombre premier comme diviseur et N_s le nombre d'entiers inférieurs à N dont les diviseurs premiers ne sont que des petits nombres premiers. Clairement, $N = N_b + N_s$.

Remarquons que pour tout nombre premier p, $\lfloor \frac{N}{p} \rfloor$ donne le nombre d'entiers inférieurs à N qui sont divisibles par p. On en déduit que $N_b \leq \sum_{i \geq k+1} \lfloor \frac{N}{p_i} \rfloor \leq \sum_{i \geq k+1} \frac{N}{p_i} < \frac{N}{2}$.

Soit un entier $n \leq N$ dont les diviseurs premiers sont des petits nombres premiers. On peut écrire $n = a_n b_n^2$, où a_n n'est divisible par aucun facteur premier au carré. En particulier, a_n est un produit de petits nombres premiers différents. Il y a donc 2^k choix sur a_n (ce qui correspond au cardinal de l'ensemble des parties de l'ensemble des petits nombres premiers). Ensuite, remarquons que $b_n \leq \sqrt{n} \leq \sqrt{N}$. On en déduit que $N_s \leq 2^k \sqrt{N}$.

Pour trouver une contradiction avec $N_s + N_b = N$, il suffit donc de trouver un entier N tel que $2^k \sqrt{N} \leq \frac{N}{2}$. Or $N = 2^{2k+2}$ convient. $\square$

Nota Bene : On a en fait montrer un résultat plus fort que l'infinité de nombres premiers, la divergence de la série $\sum_{p \in \mathbb{P}} \frac{1}{p}$.

3. Pour tout entier $n \leq m$, $[\![n, m]\!] = [n, m] \cap \mathbb{N}$.

Démonstration ζ

Supposons par l'absurde que $\mathbb{P}$ est fini. Écrivons alors $\mathbb{P} = \{p_1, ..., p_r\}$. Soit $N \in \mathbb{N}$. Notons N_c le nombre d'entiers inférieurs à N admettant au moins un facteur premier au carré, et N_s le nombre d'entiers inférieurs à N n'admettant pas de tel facteur. N_s correspond donc au nombre de produits de nombres premiers deux à deux distincts, c'est-à-dire que $N_s = 2^r$. Ensuite, pour tout nombre premier p, $\lfloor \frac{N}{p^2} \rfloor$ correspond au nombre d'entiers inférieurs à N et divisible par p^2, donc $N_c \leq \sum_{i=1}^{r} \lfloor \frac{N}{p_i^2} \rfloor \leq N \sum_{i=1}^{r} \frac{1}{p_i^2}$.

On a ainsi, $N = N_c + N_s \leq 2^r + N\zeta(2)$, en notant $\zeta(2) = \sum_{i=1}^{+\infty} \frac{1}{i^2}$. On peut montrer rapidement la convergence de cette série : pour tout $s \in \mathbb{N}_{\geq 2}$, $\sum_{i=1}^{s} \frac{1}{i^2} \leq 1 + \sum_{i=2}^{s} \frac{1}{i(i-1)} = 1 + \sum_{i=2}^{s} \left(\frac{1}{i-1} - \frac{1}{i} \right) = 2 - \frac{1}{s}$, d'où $\zeta(2) \leq 2$.

Maintenant, supposons $N > \frac{2^r}{1-\zeta(2)}$. Alors $\frac{2^r}{1-\zeta(2)} < N < 2^r + 2^r \frac{\zeta(2)}{1-\zeta(2)} = \frac{2^r}{1-\zeta(2)}$, d'où une contradiction. □

1 Démonstration η

Pour tout $a, b \in \mathbb{Z}$, notons $V_{a,b} = \{a + nb, n \in \mathbb{Z}\}$. Définissons ensuite $\mathcal{T} \subset \mathcal{P}(\mathbb{Z})$ par : pour tout $U \in \mathcal{P}(\mathbb{Z})$, $U \in \mathcal{T}$ si, et seulement si, pour tout $a \in U$, il existe $b \in \mathbb{Z}^*$ tel que $V_{a,b} \subset U$.

Alors $(\mathbb{Z}, \mathcal{T})$ est un espace topologique. En effet, $\emptyset, \mathbb{Z} \in \mathcal{T}$, $\mathcal{T}$ est stable par union quelconque, et on peut montrer que $\mathbb{T}$ est stable par intersection finie en remarquant que pour tout $(a, b, d) \in \mathbb{Z} \times \mathbb{Z}^* \times \mathbb{Z}^*$, $V_{a,b} \cap V_{a,d} \supset V_{a,bd}$. On remarque notamment que tout ouvert est nécessairement infini.

Soient $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$. Alors pour tout $u \in \mathbb{Z} \backslash V_{a,b}$, $\mathbb{Z} \backslash V_{a,b} \supset V_{u,b}$, puisque nécessairement b ne divise pas $u - a$. Ainsi, les $V_{a,b}$ sont à la fois fermé et ouvert.

Supposons par l'absurde que $\mathbb{P}$ soit fini. Alors $\mathbb{Z} \backslash \{-1, 1\} = \bigcup_{p \in \mathbb{P}} V_{0,p}$ est fermé, donc $\{-1, 1\}$ est ouvert, ce qui est impossible puisque nous avons vu qu'un ouvert est nécessairement de cardinal infini. □

Démonstration θ

Pour tout $n \in \mathbb{N}$, notons $F_n = 2^{2^n} + 1$ le n-ième nombre de Fermat. On montre facilement par récurrence que pour tout $n \in \mathbb{N}^*$, $\prod_{k=1}^{n-1} F_k = F_n - 2$.

Soient deux entiers distincts $m, n \in \mathbb{N}$ et p un diviseur de F_m et F_n. Sans perte de généralité, on supposera $m > n$. Alors p divise $2 = F_m - \prod_{k=1}^{m-1} F_k$, c'est-à-dire que

$p \in \{1, 2\}$. Or les nombres de Fermat sont tous impairs, donc nécessairement $p = 1$, c'est-à-dire que les nombres de Fermat sont deux à deux premiers entre eux.

Pour tout nombre de Fermat F_n, il existe donc un nombre premier $\phi(n)$ divisant F_n et aucun autre nombre de Fermat. L'application $\phi : \mathbb{N} \to \mathbb{P}$ est alors injective, montrant que $\mathbb{P}$ est infini. □

Démonstration ι

On a vu dans la démonstration θ qu'il suffit d'exhiber une suite de nombres premiers entre eux deux à deux pour montrer le théorème d'Euclide. Les nombres de Fermat en sont un exemple, considérons maintenant la suite $(S_n)_n$ définie par : S_0 est un nombre impair et pour tout $n \in \mathbb{N}$, $S_{n+1} = S_n^2 - 2$.

Une première remarque est que les termes de cette suite sont tous impairs. Ensuite, on peut montrer par récurrence que pour tout $n \in \mathbb{N}$, pour tout $m \in \mathbb{N}_{<n}$, il existe un polynôme P tel que $S_n = S_m P(S_m) \pm 2$ (en fait, le cas où l'on a un $-$ correspond uniquement à $m = n - 1$).

Soient deux entiers distincts $n, m \in \mathbb{N}$. Notons $d = S_n \wedge S_m$ [4]. Sans perte de généralité, supposons $n > m$. Alors il existe un polynôme P tel que $S_n = S_m P(S_m) \pm 2$, donc d divise $\pm 2 = S_n - S_m P(S_m)$. Or on sait que S_n et S_m sont des nombres impairs, donc $d \neq 2$. Par conséquent, $d = 1$ c'est-à-dire que $(S_n)_n$ est bien suite de nombres deux à deux premiers entre eux. □

2 Démonstration κ

Soient deux entiers S_0 et a premiers entre eux. Posons, pour tout $n \in \mathbb{N}$, $S_{n+1} = S_n(S_n - a) + a$. Montrons $(S_n)_n$ est une suite de nombres premiers entre eux deux à deux, ce qui prouvera le théorème d'Euclide d'après la remarque faite à la démonstration précédente.

De même que dans la démonstration θ, on montre par récurrence que pour tout $n \in \mathbb{N}^*$, $\prod_{k=0}^{n-1} S_k = S_n - a$. En remarquant que pour tout $n \in \mathbb{N}$, $S_{n+1} = S_n^2 + a(1 - S_n)$, on montre également par récurrence que les éléments de la suite $(S_n)_n$ sont premiers avec a.

Soient deux entiers distincts $n, m \in \mathbb{N}$ (sans perte de généralité, supposons que $m > n$). Notons $d = S_n \wedge S_m$. Alors d divise S_n et $a = S_m - \prod_{k=0}^{m-1} S_k$, donc d divise $S_n \wedge a = 1$. Par conséquent, S_n et S_m sont bien premiers entre eux. □

Nota Bene : Pour $a = 2$ et $S_0 = 3$, on retrouve la suite des nombres de Fermat.

Démonstration λ

D'après la fin de la démonstration θ, s'il est possible de construire une suite arbitrairement longue de nombres premiers entre eux deux à deux, alors il est possible de constuire une suite arbitrairement longue de nombres premiers distincts, c'est-à-dire que $\mathbb{P}$ ne sera alors pas borné, et donc infini.

4. Pour tout entier a et b non nuls, $a \wedge b$ désigne le pgcd de a et b.

Soit $n \in \mathbb{N}^*$. Les nombres $1+i.n!$ et $1+j.n!$, où $i, j \in [\![1, n]\!]$ (distincts), sont premiers entre eux. En effet, notons d leur pgcd. Alors d divise $(1 + i.n!) - (1 + j.n!) = (i - j)n!$ ce qui implique $d \leq n$ et donc que d divise $n!$. Dans ce cas, d divise également $1 = (1+j.n!)-j.n!$, donc on a bien $d = 1$. On obtient ainsi une suite de longueur n de nombres premiers entre eux deux à deux : $(1 + k.n!)_{1 \leq n \leq k}$. □

Démonstration μ

Soit $n_1 \in \mathbb{N}_{\geq 2}$. Définissons par récurrence la suite $(n_k)_{k \geq 2}$ par : pour tout $k \in \mathbb{N}_{\geq 2}$, $n_{k+1} = n_k(n_k + 1)$. Sachant que pour tout entier $m \in \mathbb{N}^*$, m et $m + 1$ sont premiers entre eux, on montre facilement par récurrence que pour tout $k \in \mathbb{N}_{\geq 2}$, n_k possède au moins k facteurs premiers distincts deux à deux ; remarquons également que les facteurs premiers de n_k sont également facteurs premiers de n_{k+1}. Si l'on note pour tout $k \in \mathbb{N}_{\geq 2}$, l'ensemble A_k des facteurs premiers de n_k, on trouve alors que $(A_k)_{k \geq 1}$ est une suite croissante et non bornée de parties de $\mathbb{P}$. Donc $\mathbb{P}$ est infini. □

Démonstration ν

On a $\displaystyle\prod_{p \in \mathbb{P}} \frac{1}{1 - 1/p} = \prod_{p \in \mathbb{P}} \sum_{k=0}^{\infty} \frac{1}{p^k} = \sum_{n \in \mathbb{N}^*} \frac{1}{n}$. Or la série harmonique diverge, donc nécessairement $\mathbb{P}$ doit être infini. □

Démonstration ξ

Supposons par l'absurde que $\mathbb{P}$ est fini. Écrivons alors $\mathbb{P} = \{p_1, ..., p_r\}$. Soit $n \in \mathbb{N}^*$. Alors $\displaystyle n = \prod_{i=1}^{r} p_i^{v_{p_i}(n)}$. En particulier, pour tout $i \in [\![1, r]\!]$, $p_i^{v_{p_i}(n)} \leq n$ ou en passant au logarithme : $\displaystyle v_{p_i}(n) \leq \frac{\ln(n)}{\ln(p_i)} \leq \frac{\ln(n)}{\ln(2)}$.

On sait que tout entier inférieur à n s'écrit de manière unique comme un produit de puissances des p_i ($i \in [\![1, r]\!]$). D'après ce qui précède, il y au plus $\displaystyle\frac{\ln(n)}{\ln(2)}$ choix sur chacune des puissances. On en déduit que $\displaystyle n = \text{card}([\![1, n]\!]) \leq \left(\frac{\ln(n)}{\ln(2)}\right)^r$.

Cette inégalité doit être vraie pour tout $n \in \mathbb{N}^*$. Or, par croissance comparée, $\displaystyle\frac{1}{n}\left(\frac{ln(n)}{\ln(2)}\right)^r \underset{n \to +\infty}{\longrightarrow} 0$, donc pour n suffisamment grand, $\displaystyle\left(\frac{\ln(n)}{\ln(2)}\right)^r \leq \frac{n}{2}$, ce qui est contradictoire. □

Démonstration o

Supposons par l'absurde que $\mathbb{P}$ est fini. Écrivons alors $\mathbb{P} = \{p_1, ..., p_r\}$. Soit $n \in \mathbb{N}^*$. Tout entier $k \leq n$ s'écrit sous la forme $k = ab^2$, où a ne possède pas de facteurs premiers au carré. Il est clair que $b \leq \sqrt{k} \leq \sqrt{n}$. Ensuite, a s'écrit comme un produit de nombres premiers distincts, donc il y a au plus 2^r choix sur a. On en déduit que $n = \text{card}([\![1, n]\!]) \leq 2^r\sqrt{n}$, ce qui est faux pour n suffisamment grand (dès que $n > 2^{2r}$). □

Références

Raisonnements divins, M. Aigner et G. M. Ziegler, Springer Editions (2006).

An introduction to the theory of numbers, G. H. Hardy et E. M. Wright, Oxford University Press (1980).

Il y aurait une infinité de nombres premiers...

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