Infinité des nombres premiers

Lionel Vidal

Où quelques démonstrations de l'infinité des nombres premiers servent de prétextes à des digressions mathématiques que l'on espère, c'est le seul enjeu, esthétiques.

1. Euclide. La plus ancienne démonstration connue de l'infinité des nombres premiers est due à Euclide : s'il n'y a qu'un nombre fini r de nombres premiers, et sachant qu'il en existe au moins un, on peut construire le nombre $n = p_1 \dots p_r + 1$. Ce nombre est supérieur à 1, donc il admet un diviseur premier p. Mais si p était l'un des p_i, il diviserait le produit $p_1 \dots p_r$ et n, donc 1, ce qui est absurde.

Le nombre $p_1 \dots p_r + 1$ n'est pas nécessairement premier (par exemple $2 \times \dots \times 13 + 1 = 30031 = 59 \times 509$), mais est premier avec chaque premier de l'ensemble supposé fini. De multiples constructions d'un tel nombre sont possibles et proposent de nouvelles démonstrations se ramenant *in fine* à l'idée originelle d'Euclide.

Par exemple,[1] si les nombres premiers sont en nombre fini :

$$0 < \prod_p \sin\left(\frac{\pi}{p}\right) = \prod_p \sin\left(\frac{\pi(1 + 2\prod_{p'} p')}{p}\right) = 0 \,.$$

L'inégalité est vraie car les facteurs du produit sont strictement positifs ; la première égalité est vraie car le produit de tous les premiers p' est divisible par p et donc l'argument du sinus est congru à π/p modulo 2π ; et la dernière égalité est vraie car l'entier au numérateur est divisible par un nombre premier et donc au moins un terme du produit est nul !

Un formalisme élégant[2] peut éviter une construction explicite : on définit sur $\mathbb{Z}$ une topologie en considérant comme ouverts l'ensemble vide et tout ensemble d'entiers $\mathcal{O}$, tel que pour tout $a \in \mathcal{O}$, il existe une progression arithmétique $\mathcal{A}$ telle que $a \in \mathcal{A} \subset \mathcal{O}$. En effet :

- l'ensemble vide et $\mathbb{Z} = 0 + 1\mathbb{Z}$ sont ouverts ;
- une union d'ouverts est trivialement ouverte ;
- une intersection finie d'ouverts est ouverte car si $a \in \bigcap_{i=1}^n \mathcal{O}_i$, il existe n entiers $m_i \in \mathbb{N}^*$, tel que $a + m_i\mathbb{Z} \subset \mathcal{O}_i$, et donc $a + m_1 \dots m_n\mathbb{Z} \subset \bigcap_{i=1}^n \mathcal{O}_i$.

Pour cette topologie, les progressions arithmétiques sont évidemment ouvertes mais aussi fermées :

$$\forall a \in \mathbb{Z}, \forall m \in \mathbb{N}^*, a + m\mathbb{Z} = \mathbb{Z} \setminus \bigcup_{i=1}^{m-1} (a + i + m\mathbb{Z}) \,.$$

Si les nombres premiers sont en nombre fini, alors l'ensemble $\bigcup p\mathbb{Z}$ est fermé comme union finie de fermés. Mais comme tout nombre différent de 1 et -1 admet un diviseur premier, le complémentaire de cet ensemble est $\{-1; 1\}$ qui n'est pas un ouvert.

Le point clé de cette preuve est le fait que $\bigcap_p (\mathbb{Z} \setminus p\mathbb{Z}) = \{-1; 1\}$ ne contient pas de progression arithmétique. Si les nombres premiers étaient en nombre fini r, cet ensemble contiendrait la progression $(1 + p_1 \dots p_r)\mathbb{Z}$, chaque p_i étant premier avec $1 + p_1 \dots p_r$: on retrouve Euclide !

2. Pierre de Fermat. Une autre idée est de construire une suite infinie de nombres premiers entre eux deux à deux : chacun de ces nombres admet alors au moins un facteur premier qui n'est commun à aucun des autres, et on en déduit l'existence d'une infinité de nombres premiers.

1. Preuve de S. Northshield, *American Mathematical Monthly* (2015).
2. Preuve de H. Furstenberg, *American Mathematical Monthly* (1955).

Par exemple, les nombres de Fermat $\mathrm{F}_n = 2^{2^n} + 1$ sont premiers entre eux deux à deux. En effet, pour $n \geqslant 1$:

$$\mathrm{F}_n = \prod_{d=0}^{n-1} \mathrm{F}_d + 2 \, .$$

Mais alors, si p est un diviseur premier commun de F_d et F_n, p divise 2, donc vaut 2, ce qui contredit l'imparité des F_n.

La formule précédente se montre par une récurrence très simple : $\mathrm{F}_1 = 5 = \mathrm{F}_0 + 2$ et

$$\prod_{d=0}^{n} \mathrm{F}_d = \left(\prod_{d=0}^{n-1} \mathrm{F}_d \right) \mathrm{F}_n = (\mathrm{F}_n - 2)\mathrm{F}_n = (2^{2^n} - 1)(2^{2^n} + 1) = 2^{2^{n+1}} - 1 = \mathrm{F}_{n+1} - 2 \, .$$

Toute démonstration aurait été inutile si, comme le pensait Fermat, les F_n étaient tous premiers. C'est vrai pour $\mathrm{F}_0 = 3$, $\mathrm{F}_1 = 5$, $\mathrm{F}_2 = 17$, $\mathrm{F}_3 = 257$ et $\mathrm{F}_4 = 65\,537$, mais $\mathrm{F}_5 = 641 \times 6\,700\,417$. On ne connait d'ailleurs, à ce jour, aucun nombre de Fermat premier autre que ceux juste cités.

3. Marin Mersenne et Joseph-Louis Lagrange. À partir d'un nombre premier quelconque, si l'on parvient à exhiber un autre premier strictement plus grand, on aura prouvé l'infinité de ces nombres. Soit donc p un nombre premier et q un facteur premier du nombre de Mersenne $2^p - 1$. On a donc $2^p \equiv 1 \ (q)$, et comme p est premier, 2 est d'ordre p dans le sous-groupe multiplicatif $(\mathbb{Z}/q\mathbb{Z})^*$ du corps $\mathbb{Z}/q\mathbb{Z}$. Mais d'après le théorème de Lagrange, l'ordre de l'élément d'un groupe divise l'ordre de ce groupe, soit $p \mid (q-1)$. Et donc $p < q$.

4. Leonhard Euler. En 1737, Euler montre que la série des inverses des nombres premiers,

$$\frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{11} + \cdots$$

est divergente, ce qui montre bien plus que l'infinité des nombres premiers : cela donne une idée de leur *densité* dans l'ensemble des entiers. Ils sont plus denses par exemple que les carrés, au sens où la série des inverses des carrés converge.

Pour tout entier $n \geqslant 2$, notons :

$$\mathrm{P}_n \coloneqq \prod_{p \leqslant n} \frac{1}{1 - \frac{1}{p}} = \prod_{p \leqslant n} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \cdots \right) \, .$$

Comme tout entier naturel non nul se décompose de manière unique, à l'ordre près, en produit de facteurs premiers, les termes du développement de P_n comprennent l'inverse de chaque entier $k \leqslant n$; en notant q le plus grand premier inférieur ou égal à n, il vient :

$$\begin{aligned} \mathrm{P}_n &= \left(1 + \frac{1}{2} + \frac{1}{2^2} + \cdots \right) \left(1 + \frac{1}{3} + \frac{1}{3^2} + \cdots \right) \ldots \left(1 + \frac{1}{q} + \frac{1}{q^2} + \cdots \right) \\ &= 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{2 \times 2} + \frac{1}{5} + \frac{1}{2 \times 3} + \frac{1}{7} + \cdots > \sum_{k=1}^{n} \frac{1}{k} > \int_1^n \frac{dx}{x} = \log n \, . \end{aligned}$$

D'où $\lim\limits_{n \to +\infty} \mathrm{P}_n = +\infty$, et donc déjà l'infinité des nombres premiers ! De plus :

$$\log(\log n) < \log \mathrm{P}_n = \sum_{p \leqslant n} \log \left(1 + \frac{1}{p} + \frac{1}{p^2} + \cdots \right) \leqslant \sum_{p \leqslant n} \left(\frac{1}{p} + \frac{1}{p^2} + \cdots \right) = \sum_{p \leqslant n} \frac{1}{p} + \mathrm{R}_n \, ,$$

où R_n est défini par :

$$\begin{aligned} \mathrm{R}_n &\coloneqq \sum_{p \leqslant n} \left(\frac{1}{p^2} + \cdots \right) = \sum_{p \leqslant n} \frac{1}{p^2} \left(1 + \frac{1}{p} + \cdots \right) = \sum_{p \leqslant n} \frac{1}{p^2} \frac{1}{1 - \frac{1}{p}} = \sum_{p \leqslant n} \frac{1}{p(p-1)} \\ &\leqslant \sum_{k=2}^{n} \frac{1}{k(k-1)} = \sum_{k=2}^{n} \left(\frac{1}{k-1} - \frac{1}{k} \right) = 1 - \frac{1}{n} < 1 \, . \end{aligned}$$

D'où finalement : $\log(\log n) - 1 < \sum\limits_{p \leqslant n} \frac{1}{p}$, ce qui montre que la série $\sum \frac{1}{p}$ diverge.

5. Euler encore, revu par Paul Erdős. Donnons une autre belle preuve, inventée par Erdős, de la divergence de la série des inverses des nombres premiers.

Soient p_1, p_2, ..., les nombres premiers en ordre croissant. Supposons que la série de leurs inverses soit convergente. Il existe alors un entier naturel k tel que :

$$\sum_{i\geqslant k+1} \frac{1}{p_i} < \frac{1}{2} .$$

On appellera p_1, ..., p_k, les *petits* nombres premiers, et p_{k+1}, p_{k+2}, ..., les *grands* nombres premiers. Soit N un nombre entier naturel non nul. On note G le nombre d'entiers naturels $n \leqslant \mathrm{N}$ divisibles par au moins un grand nombre premier et P le nombre d'entiers naturels $n \leqslant \mathrm{N}$ qui n'ont que des petits diviseurs premiers (ainsi 0 est compté dans G et 1 n'est pas compté).

Majorons alors G et P.

D'une part, $\lfloor \mathrm{N}/p_i \rfloor$ dénombre les entiers $n \leqslant \mathrm{N}$ qui sont des multiples de p_i. D'où :

$$\mathrm{G} \leqslant \sum_{i\geqslant k+1} \left\lfloor \frac{\mathrm{N}}{p_i} \right\rfloor \leqslant \sum_{i\geqslant k+1} \frac{\mathrm{N}}{p_i} < \frac{\mathrm{N}}{2} .$$

D'autre part, tout entier $n \leqslant \mathrm{N}$ qui n'admet que des petits diviseurs premiers peut s'écrire $n = a_n b_n^2$, où a_n est sans facteur carré et donc produit, éventuellement vide, de petits nombres premiers deux à deux distincts. Il y a donc 2^k facteurs possibles pour a_n, et comme $b_n \leqslant \sqrt{\mathrm{N}}$:

$$\mathrm{P} \leqslant 2^k \sqrt{\mathrm{N}} .$$

D'où : $\mathrm{G} + \mathrm{P} = \mathrm{N} < \dfrac{\mathrm{N}}{2} + 2^k\sqrt{\mathrm{N}}$, soit $\sqrt{\mathrm{N}} < 2^{k+1}$, ce qui contredit le choix arbitraire de N.

6. Euler toujours, et la fonction de Zéta de Bernhard Riemann.

$$\prod_p \frac{1}{1-\frac{1}{p^2}} = \zeta(2) = \frac{\pi^2}{6}$$

Le membre de droite est irrationnel, donc le produit de gauche a un nombre infini de termes !

La fonction Zéta de Riemann est définie sur $]1, +\infty[$ par $\zeta(x) := \displaystyle\sum_{n=1}^{+\infty} \frac{1}{n^x}$. Comme pour $s > 1$,

$$\frac{1}{1-\frac{1}{p^s}} = 1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \frac{1}{p^{3s}} + \cdots ,$$

en considérant tous les nombres premiers p inférieurs à un nombre premier q fixé :

$$\left| \zeta(s) - \prod_{p\leqslant q} \frac{1}{1-\frac{1}{p^s}} \right| < \sum_{n=q+1}^{+\infty} \frac{1}{n^s} .$$

En effet, comme chaque entier se décompose de façon unique en produit de facteurs premiers, le produit partiel, une fois développé en utilisant la relation précédente, ne comprend que des termes de type n^{-s}, où n est un produit de premiers au plus égaux à q. Donc seuls les entiers plus grands que q peuvent ne pas apparaître dans le produit partiel, ce qui justifie l'inégalité. La valeur absolue précédente tend vers 0 quand q tend vers l'infini, et donc pour tout $s > 1$:

$$\prod_p \frac{1}{1-\frac{1}{p^s}} = \zeta(s) .$$

Déterminons maintenant la valeur de $\zeta(2)$. Pour une preuve courte, sortons l'artillerie lourde : dans l'espace de Hilbert $\mathrm{L}^2[0,1]$ muni de la base orthonormée $(e_n(x) = \exp(2i\pi nx))_{n\in\mathbb{Z}}$, on applique à la fonction identité la formule de Parseval :

$$\langle f, f\rangle = \sum_{n\in\mathbb{Z}} |\langle f, e_n\rangle|^2 \text{ , où } \langle f, g\rangle := \int_0^1 f\bar{g} .$$

On calcule très facilement :

$$\langle f, f\rangle = \int_0^1 x^2\,dx = \frac{1}{3}\,, \quad \langle f, e_0\rangle = \int_0^1 x\,dx = \frac{1}{2}\,,$$

$$\text{et pour } n \text{ non nul, } \langle f, e_n\rangle = \int_0^1 xe^{-2i\pi nx}\,dx = \left[x\frac{e^{-2i\pi nx}}{-2i\pi n}\right]_0^1 - \underbrace{\int_0^1 \frac{e^{-2i\pi nx}}{-2i\pi n}\,dx}_{=0} = -\frac{1}{2i\pi n}\,.$$

D'où $\dfrac{1}{3} = \dfrac{1}{4} + \displaystyle\sum_{n\in\mathbb{Z}^*} \frac{1}{4\pi^2 n^2}$, et donc : $\zeta(2) = \displaystyle\sum_{n=1}^{+\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$.

Pour être complet, il faudrait encore démontrer que π^2 est irrationnel… ce qui sera admis ici !

7. Dénombrement. Peut-être la démonstration la plus naturelle : on compte le nombre de décompositions possibles en produit de facteurs premiers plus petits qu'un entier donné. Si on note $\pi(n)$ le nombre de nombres premiers inférieurs ou égaux à n, et p_1, p_2, ..., les nombres premiers en ordre croissant, tout entier k, $0 < k \leqslant n$, s'écrit :

$$k = \prod_{i=1}^{\pi(n)} p_i^{e_i}\,, \text{ où pour tout } i,\ e_i \text{ est un entier naturel.}$$

D'où : $\displaystyle\sum_{i=1}^{\pi(n)} e_i \log p_i \leqslant \log n$, et grossièrement, $e_i \leqslant \dfrac{\log n}{\log p_i} \leqslant \log_2 n$. En dénombrant alors toutes les décompositions, chaque p_i offre au plus $\log_2 n$ choix, et donc $n \leqslant (\log_2 n + 1)^{\pi(n)}$. On en déduit :

$$\pi(n) \geqslant \frac{\log n}{\log(\log_2 n + 1)}\,, \quad \text{et donc :} \quad \lim_{n\to+\infty} \pi(n) = +\infty\,.$$

8. Richard Dedekind. Pour finir, montons de quelques barreaux sur l'échelle de Jacob…
Beaucoup d'anneaux d'entiers de corps de nombres ne sont pas factoriels, et leurs éléments n'admettent donc pas une unique décomposition en produit de facteurs premiers. Pour pallier cet inconvénient, dans le cadre de travaux sur l'équation de Fermat, Dedekind développe la notion d'anneau, dit de Dedekind, plus général qu'un anneau principal :

> *un anneau de Dedekind est un anneau Nœthérien, intégralement clos, dans lequel tout idéal premier non nul est maximal.*

On montre que dans un tel anneau, tous les *idéaux* admettent une unique décomposition en *idéaux premiers*, et que tout anneau d'entiers de corps de nombres est un anneau de Dedekind.

Considérons alors un anneau de Dedeking R qui n'admette qu'un nombre fini d'idéaux premiers non nuls, $\mathfrak{p}_1$, ..., $\mathfrak{p}_n$, et montrons que dans ce cas, R est principal.

En notant $\mathrm{R}_{\mathfrak{p}_1}$ le localisé de R en $\mathfrak{p}_1$, comme le module $\mathfrak{p}_1\mathrm{R}_{\mathfrak{p}_1}$ est non nul, d'après le lemme de Nakayama, $\mathfrak{p}_1^2\mathrm{R}_{\mathfrak{p}_1} \subsetneq \mathfrak{p}_1\mathrm{R}_{\mathfrak{p}_1}$, et donc $\mathfrak{p}_1^2 \subsetneq \mathfrak{p}_1$. Soit alors $y_1 \in \mathfrak{p}_1 \setminus \mathfrak{p}_1^2$.

Remarquons que si $\mathfrak{a}$ et $\mathfrak{m}$ sont des idéaux de R, tels que $\mathfrak{a} \not\subset \mathfrak{m}$ et que $\mathfrak{m}$ soit maximal, alors $\mathfrak{a} + \mathfrak{m} = \mathrm{R}$ et les idéaux $\mathfrak{a}$ et $\mathfrak{m}$ sont premiers entre eux. Comme $\mathfrak{p}_2$, ..., $\mathfrak{p}_n$ sont maximaux, les idéaux $\mathfrak{p}_1^2$, $\mathfrak{p}_2$, ..., $\mathfrak{p}_n$ sont donc premiers entre eux deux à deux. D'après le lemme des restes chinois, il existe alors $x_1 \in \mathrm{R}$, tel que $x_1 \equiv y_1\ (\mathfrak{p}_1^2)$, et $x_1 \equiv 1\ (\mathfrak{p}_k)$, pour $2 \leqslant k \leqslant n$.

Comme R est de Dedekind, $\langle x_1\rangle$ se décompose en $\langle x_1\rangle = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_n^{e_n}$, où e_1, ..., e_n sont des entiers naturels. Mais pour $2 \leqslant k \leqslant n$, $x_1 \notin \mathfrak{p}_k$, donc $e_k = 0$. De plus, comme $x_1 \in \mathfrak{p}_1 \setminus \mathfrak{p}_1^2$, on a $e_1 = 1$. D'où $\mathfrak{p}_1 = \langle x_1\rangle$ et $\mathfrak{p}_1$ est donc principal. On montre de même que $\mathfrak{p}_2$, ..., $\mathfrak{p}_n$ sont principaux.

Mais tout idéal $\mathfrak{a}$ de R se décompose en $\mathfrak{a} = \mathfrak{p}_1^{a_1} \dots \mathfrak{p}_n^{a_n} = \langle x_1\rangle^{a_1} \dots \langle x_n\rangle^{a_n} = \langle x_1^{a_1} \dots x_n^{a_n}\rangle$, et l'anneau R est donc principal.

Considérons alors l'anneau $\mathbb{Z}[\sqrt{-5}]$, anneau de Dedekind des entiers de $\mathbb{Q}[\sqrt{-5}]$. L'élément $1+\sqrt{-5}$ est irréductible, car la norme d'un de ses diviseurs non trivial devrait être un diviseur non trivial de sa norme 6, et les équations $a^2+5b^2=2$ et $a^2+5b^2=3$ n'ont pas de solution dans $\mathbb{Z}$.

Mais comme $(1+\sqrt{-5})(1-\sqrt{-5}) = 2\times 3$, l'anneau $\mathbb{Z}[\sqrt{-5}]$ n'est pas principal, car sinon l'élément $1+\sqrt{-5}$ irréductible diviserait 2 ou 3, et en prenant les normes, 6 diviserait 4 ou 9.

Donc d'après ce qui précède, les nombres premiers sont en nombre infini !

C'est ma preuve préférée : moralement, il est nécessaire que les nombres premiers soient en nombre infini pour que la théorie des nombres soit aussi intéressante et complexe !