Six preuves de l'infinité de l'ensemble des nombres premiers

Chapitre 1

Il est bien naturel de commencer ces notes avec la Preuve probablement la plus ancienne du Grand Livre, habituellement attribuée à Euclide (*Éléments* IX, 20). Elle montre que la suite des nombres premiers est infinie.

■ **La preuve d'Euclide.** Étant donné un ensemble fini $\{p_1, \ldots, p_r\}$ de nombres premiers, considérons le nombre $n = p_1 p_2 \cdots p_r + 1$. Ce nombre n a un diviseur premier p. Cependant p n'est pas l'un des p_i sinon p serait un diviseur de n, du produit $p_1 p_2 \cdots p_r$, et donc aussi de la différence $n - p_1 p_2 \ldots p_r = 1$, ce qui est impossible. Ainsi, un ensemble fini $\{p_1, \ldots, p_r\}$ ne peut constituer la collection de *tous* les nombres premiers. □

Avant de poursuivre, fixons quelques notations. $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$ est l'ensemble des entiers naturels, $\mathbb{N}^* = \mathbb{N} \setminus \{0\}$ l'ensemble des entiers naturels non nuls, $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ l'ensemble des entiers relatifs et $\mathbb{P} = \{2, 3, 5, 7, \ldots\}$ l'ensemble des nombres premiers.

Dans ce qui suit, nous allons exposer quelques autres démonstrations (choisies parmi bien d'autres) de ce résultat ; nous espérons que le lecteur les appréciera autant que nous. Bien qu'elles utilisent des points de vue différents, elles utilisent toutes les résultats suivants : les entiers naturels croissent au-delà de toute borne, et tout entier naturel $n \geq 2$ admet un diviseur premier. Ensemble, ces deux faits contraignent $\mathbb{P}$ à être infini. Les trois preuves suivantes viennent du folklore, la cinquième a été proposée par Harry Fürstenberg, et la dernière est attribuée à Paul Erdős.

Les deuxième et troisième preuves utilisent des suites particulières d'entiers bien connues.

■ **Deuxième preuve.** Examinons tout d'abord les *nombres de Fermat* $F_n = 2^{2^n} + 1$ où $n = 0, 1, 2, \ldots$ Nous allons montrer que deux nombres de Fermat (distincts) sont premiers entre eux ; en conséquence, il doit y avoir un nombre infini de nombres premiers*. À cet effet, vérifions la formule de récurrence :

$$\prod_{k=0}^{n-1} F_k \;=\; F_n - 2 \qquad (n \geq 1)$$

à partir de laquelle on déduit immédiatement notre assertion. En effet, si m est, par exemple, un diviseur de F_k et F_n $(k < n)$ alors m divise 2, et, par conséquent, $m = 1$ ou $m = 2$. Mais $m = 2$ est impossible puisque tous les nombres de Fermat sont impairs.

$$\begin{aligned} F_0 &= 3 \\ F_1 &= 5 \\ F_2 &= 17 \\ F_3 &= 257 \\ F_4 &= 65537 \\ F_5 &= 641 \times 6700417 \end{aligned}$$

Les premiers nombres de Fermat

*N.d.T. : puisque chaque nombre de Fermat comporte dans sa décomposition en facteurs premiers au moins un facteur qu'on ne retrouve pas dans la décomposition des autres.

Le théorème de Lagrange

Si G est un groupe (multiplicatif) fini et U un sous-groupe de G, alors $|U|$ divise $|G|$.

■ **Preuve.** Considérons la relation binaire :

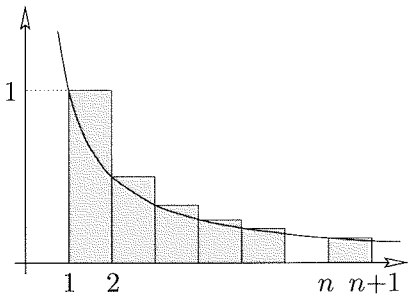
$$a \sim b : \Longleftrightarrow ba^{-1} \in U$$

On déduit des axiomes de groupe que $\sim$ est une relation d'équivalence. La classe d'équivalence qui contient l'élément a est exactement la classe :

$$Ua = \{xa : x \in U\}$$

Puisque l'on a clairement $|Ua| = |U|$, on en déduit que G se décompose en classes d'équivalence ayant toutes le même cardinal $|U|$, et que, par conséquent, $|U|$ divise $|G|$. □

Dans le cas particulier où U est un sous-groupe cyclique $\{a, a^2, \ldots, a^m\}$, on trouve que m (le plus petit entier positif tel que $a^m = 1$, appelé *l'ordre* de a) divise le cardinal $|G|$ du groupe.



Escalier au dessus de la fonction $f(t) = \frac{1}{t}$

Pour montrer la formule, nous faisons un raisonnement par récurrence sur n. Pour $n = 1$, nous avons $F_0 = 3$ et $F_1 - 2 = 3$. Nous constatons ensuite que :

$$\prod_{k=0}^{n} F_k = \Big(\prod_{k=0}^{n-1} F_k\Big) F_n = (F_n - 2)F_n =$$
$$= (2^{2^n} - 1)(2^{2^n} + 1) = 2^{2^{n+1}} - 1 = F_{n+1} - 2 \qquad \square$$

■ **Troisième preuve.** Supposons que $\mathbb{P}$ soit fini et que p soit le plus grand nombre premier. Considérons le *nombre de Mersenne* $2^p - 1$ et montrons que tout facteur premier q de $2^p - 1$ est plus grand que p, ce qui implique la conclusion désirée. Soit q un nombre premier qui divise $2^p - 1$. Nous avons donc $2^p \equiv 1 \pmod{q}$. Puisque p est un nombre premier, cela signifie que l'élément 2 est d'ordre p dans le groupe multiplicatif $\mathbb{Z}_q \backslash \{0\}$ du corps $\mathbb{Z}_q$. Ce groupe a $q - 1$ éléments. Grâce au théorème de Lagrange (voir encadré), nous savons que l'ordre de chaque élément divise le cardinal du groupe, c'est-à-dire que $p \mid q - 1$, et par conséquent $p < q$. □

Penchons-nous maintenant sur une preuve qui utilise l'analyse.

■ **Quatrième preuve.** Soit $\pi(x) := \#\{p \leq x : p \in \mathbb{P}\}$ le cardinal de l'ensemble des nombres premiers qui sont inférieurs ou égaux au nombre réel x. Énumérons les nombres premiers $\mathbb{P} = \{p_1, p_2, p_3, \ldots\}$ dans l'ordre croissant. Considérons le logarithme naturel $\ln x$, défini par $\ln x = \int_1^x \frac{1}{t} dt$. Comparons maintenant l'aire qui se trouve sous le graphe de $f(t) = \frac{1}{t}$ avec une fonction en escalier qui se trouve au dessus (voir aussi l'appendice en page 11 à propos de cette méthode). Si $n \leq x < n + 1$ nous avons :

$$\ln x \leq 1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{n-1} + \frac{1}{n}$$
$$\leq \sum \frac{1}{m} \quad \text{où la somme s'étend à tous les } m \in \mathbb{N}^* \text{ qui n'ont que des diviseurs premiers } p \leq x.$$

Puisque chaque m s'écrit de manière *unique* comme un produit de la forme $\prod_{p \leq x} p^{k_p}$, nous voyons que la dernière somme est égale à :

$$\prod_{\substack{p \in \mathbb{P} \\ p \leq x}} \Big(\sum_{k \geq 0} \frac{1}{p^k}\Big)$$

La somme qui se trouve à l'intérieur est une série géométrique de raison $\frac{1}{p}$, et par conséquent :

$$\ln x \leq \prod_{\substack{p \in \mathbb{P} \\ p \leq x}} \frac{1}{1 - \frac{1}{p}} = \prod_{\substack{p \in \mathbb{P} \\ p \leq x}} \frac{p}{p-1} = \prod_{k=1}^{\pi(x)} \frac{p_k}{p_k - 1}$$

Il est maintenant clair que $p_k \geq k+1$, donc :

$$\frac{p_k}{p_k - 1} = 1 + \frac{1}{p_k - 1} \leq 1 + \frac{1}{k} = \frac{k+1}{k}$$

et par suite :

$$\ln x \leq \prod_{k=1}^{\pi(x)} \frac{k+1}{k} = \pi(x) + 1$$

Tout le monde sait que $\ln x$ n'est pas borné. On en conclut que $\pi(x)$ est également non borné, et qu'il existe une infinité de nombres premiers. □

■ **Cinquième Preuve.** Après l'analyse, la topologie ! Considérons la curieuse topologie définie de la manière suivante sur l'ensemble $\mathbb{Z}$ des entiers. Pour $a, b \in \mathbb{Z}$, $b > 0$, posons :

$$N_{a,b} = \{a + nb : n \in \mathbb{Z}\}$$

Chaque ensemble $N_{a,b}$ est une progression arithmétique infinie des deux côtés. Nous disons qu'un ensemble $O \subseteq \mathbb{Z}$ est *ouvert* si O est vide, ou si pour chaque $a \in O$ il existe $b > 0$ tel que $N_{a,b} \subseteq O$. Il est clair qu'une réunion d'ensembles ouverts est encore un ouvert. Si O_1, O_2 sont ouverts, et que $a \in O_1 \cap O_2$ vérifie $N_{a,b_1} \subseteq O_1$ et $N_{a,b_2} \subseteq O_2$, alors $a \in N_{a,b_1 b_2} \subseteq O_1 \cap O_2$. Il en résulte que toute intersection finie d'ensembles ouverts est encore ouverte. Cette famille d'ouverts induit donc une véritable topologie sur $\mathbb{Z}$.

Notons les deux résultats suivants :
(A) Tout ensemble ouvert non vide est infini.
(B) Tout ensemble $N_{a,b}$ est fermé.
Le premier résultat est une conséquence de la définition. Pour le deuxième, on observe que :

$$N_{a,b} = \mathbb{Z} \setminus \bigcup_{i=1}^{b-1} N_{a+i,b}$$

ce qui prouve que $N_{a,b}$ est le complémentaire d'un ensemble ouvert et qu'il est donc fermé.

Jusqu'à présent, les nombres premiers n'interviennent pas, mais ils arrivent ici. Puisque tout nombre $n \neq 1, -1$ a un diviseur premier p, et qu'il est donc contenu dans $N_{0,p}$, nous pouvons affirmer que :

$$\mathbb{Z} \setminus \{1, -1\} = \bigcup_{p \in \mathbb{P}} N_{0,p}$$

Toutefois, si $\mathbb{P}$ était fini, $\bigcup_{p \in \mathbb{P}} N_{0,p}$ serait une réunion finie d'ensembles fermés (d'après le résultat (B)), et serait donc fermé. Par conséquent, $\{1, -1\}$ serait un ensemble ouvert, ce qui contredit le résultat (A). □

"Jeter des galets, indéfiniment"

■ **Sixième Preuve.** Cette dernière preuve représente un pas en avant considérable car elle démontre non seulement qu'il y a une infinité de nombres

premiers, mais aussi que la série $\sum_{p\in\mathbb{P}} \frac{1}{p}$ diverge. La première preuve de ce résultat important a été donnée par Euler (elle est intéressante en elle-même), mais la preuve donnée ici, inventée par Erdős, est d'une irrésistible beauté.

Soit $p_1, p_2, p_3, \ldots$ la suite des nombres premiers écrite dans l'ordre croissant. Supposons que $\sum_{p\in\mathbb{P}} \frac{1}{p}$ converge. Il doit donc y avoir un entier naturel k tel que $\sum_{i\geq k+1} \frac{1}{p_i} < \frac{1}{2}$. Appelons $p_1, \ldots, p_k$ les *petits* nombres premiers, et $p_{k+1}, p_{k+2}, \ldots$ les *grands* nombres premiers. Si N est un entier naturel arbitraire, nous avons donc :

$$\sum_{i\geq k+1} \frac{N}{p_i} \;<\; \frac{N}{2} \tag{1}$$

Soit N_b le nombre d'entiers positifs $n \leq N$ divisibles par un grand nombre premier au moins, et N_s le nombre d'entiers positifs $n \leq N$ qui n'ont que des petits diviseurs premiers. Nous allons montrer que pour un N convenable :

$$N_b + N_s \;<\; N$$

ce qui aboutira à la contradiction souhaitée, puisque par définition $N_b + N_s$ devrait être égal à N.

Pour estimer N_b, notons que $\lfloor \frac{N}{p_i} \rfloor$ dénombre les entiers positifs $n \leq N$ qui sont des multiples de p_i. Par conséquent, d'après (1) on obtient :

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

Examinons maintenant N_s. Écrivons chaque $n \leq N$ n'ayant que des petits diviseurs premiers sous la forme $n = a_n b_n^2$, où a_n est le facteur sans carré. Chaque a_n est ainsi un produit de petits nombres premiers *différents*. On en déduit qu'il y a exactement 2^k facteurs sans carré différents. Par ailleurs, comme $b_n \leq \sqrt{n} \leq \sqrt{N}$, il y a au plus $\sqrt{N}$ facteurs différents qui sont des carrés . Ainsi :

$$N_s \;\leq\; 2^k \sqrt{N}$$

Puisque l'on a établi l'inégalité (2) pour *tout* N, il reste à déterminer un nombre N tel que $2^k\sqrt{N} \leq \frac{N}{2}$, c'est-à-dire $2^{k+1} \leq \sqrt{N}$. $N = 2^{2k+2}$ convient. □

Bibliographie

[1] B. ARTMANN : *Euclid — The Creation of Mathematics,* Springer-Verlag, New York 1999.

[2] P. ERDŐS : *Über die Reihe* $\sum \frac{1}{p}$, Mathematica, Zutphen B **7** (1938), 1-2.

[3] L. EULER : *Introductio in Analysin Infinitorum,* Tomus Primus, Lausanne 1748 ; Opera Omnia, Ser. 1, Vol. 8.

[4] H. FÜRSTENBERG : *On the infinitude of primes,* Amer. Math. Monthly **62** (1955), 353.