Les Nombres premiers, entre l'ordre et le chaos

Gérald Tenenbaum
Professeur à l'université de Lorraine

Michel Mendès France
Professeur émérite de l'université de Bordeaux

DUNOD

Une précédente version de cet ouvrage a été publiée
en 1997 aux Presses Universitaires de France
dans la collection « Que sais-je ? », rééditée en 2000.

ISBN : 978-2-10-070656-3

Ce livre est dédié à la mémoire de Paul Erdős, qui nous a quittés en septembre 1996, au moment même où nous achevions la rédaction de la première édition. Il fut pour nous un oncle (ainsi que l'appelaient ses amis) et un maître. Un géant des mathématiques a disparu, mais son empreinte marquera bien des siècles à venir.

Table des matières

Avant-propos

Issu de notre ouvrage *Les Nombres premiers*, paru dans la collection *Que sais-je ?* et à présent épuisé, ce petit livre représente un pari sans doute ambitieux : fournir au grand public scientifique une description concise de la théorie analytique moderne des nombres premiers — à l'exclusion toutefois des apports de la théorie des formes modulaires.

Répondant à des questions posées depuis l'Antiquité — y a-t-il beaucoup de nombres premiers ?, comment se répartissent-ils ?, etc. —, ce domaine connaît depuis un siècle un essor sans précédent, dû notamment aux interactions avec la théorie des probabilités. Les tables de nombres premiers mettent en évidence un aspect chaotique, dont le désordre apparent s'accorde finalement avec des modèles aléatoires classiques, issus, par exemple, de phénomènes physiques. Là est précisément l'objet de cet opuscule : décrire, puis tenter de comprendre, comment une suite aussi hautement déterminée que celle des nombres premiers peut renfermer une telle part de hasard.

Insistons un peu sur ce point. Le hasard total, le chaos, c'est la complexité infinie. Par ailleurs, la complexité d'un nombre entier croît manifestement avec sa taille, et répondre à des questions de base devient souvent difficile : le nombre $2^{57885161} - 1$ est-il premier ?[1] Combien de fois son développement décimal contient-il le chiffre 7 ? etc. Au voisinage de l'infini, la suite des nombres entiers, et partant celle des nombres premiers, mime le hasard. Les directions modernes de la théorie analytique des nombres tentent de rendre compte des modalités de cette tendance.

1. Oui, d'après Curtis Cooper (2013).

Physiciens et philosophes discutent encore de l'hypothétique « variable cachée », malgré les travaux convaincants d'Alain Aspect, qui semblent en proscrire l'existence. L'école de Copenhague, avec Niels Bohr, défend la thèse que le monde subatomique est régi par le hasard. Einstein, quant à lui, rêve d'une explication sub-subatomique totalement déterministe. La suite des nombres premiers ne pourrait-elle servir de modèle aux idées d'Einstein, lui qui prétendait que Dieu ne joue pas aux dés au moment même où Mark Kac, éminent arithméticien, professait l'opinion que les nombres premiers s'adonnent secrètement au jeu de pile ou face ?

La dialectique ordre/désordre occupe les théoriciens des nombres depuis que Legendre et Gauss ont conjecturé une répartition harmonieuse des nombres premiers, à savoir que le n-ième nombre premier p_n est proche de $n \ln n$.[1] Une telle régularité dans l'aléatoire ne doit pas surprendre : quoi de plus imprévisible que le jet d'une pièce de monnaie alors que la probabilité qui régit l'événement, constamment égale à $\frac{1}{2}$, prévoit une tendance à l'équilibre entre les piles et les faces ? Tous ceux qui ont observé la suite des nombres premiers ont remarqué à la fois l'irrégularité et la régularité de leur distribution. À l'instar du jeu de pile ou face, le comportement en moyenne est régulier alors que les fluctuations locales, ici le passage de p_n à p_{n+1}, demeure très complexe.

Nous avons choisi de décrire ces phénomènes de répartition en nous appuyant sur le cheminement historique et l'évolution graduelle de la philosophie — c'est-à-dire la représentation archétypale — des nombres premiers. Les Chapitres 1, 2 et 4 sont principalement consacrés aux résultats de régularité, alors que le Chapitre 3 traite surtout des aspects aléatoires de la répartition. Au Chapitre 5, nous décrivons les conjectures principales qui sous-tendent la théorie et nous comprenons, *in fine*, que cette dichotomie n'est qu'apparente : hasard et nécessité se conjuguent harmonieusement pour produire de la structure, chacune des

1. Cette assertion, qui porte aujourd'hui le nom de *théorème des nombres premiers*, a été démontrée par Jacques Hadamard et Charles de La Vallée-Poussin en 1896.

deux perspectives éclairant et expliquant l'autre ; compte-tenu des contraintes liées à la structure d'ordre des entiers, la répartition des nombres premiers s'avère aussi harmonieuse que possible.

La présente édition diffère notablement des précédentes. Nous avons, en particulier, significativement enrichi les introductions des différents chapitres de manière à fournir au non-spécialiste une description aussi fidèle que possible du contenu mathématique et des idées-forces sous-jacentes. Ces développements, largement métaphoriques, peuvent, en toute rigueur, être omis par un lecteur rompu au langage mathématique et aux notions principales utilisées dans le texte : logarithmes, congruences, nombres complexes, convergences, interversion de sommations, etc. En revanche, ils peuvent constituer l'essentiel de l'apport pour celui qui ne possède pas (ou pas encore) le bagage scientifique nécessaire au décryptage des démonstrations. Notre espoir est qu'ils recèlent également un intérêt pour le scientifique chevronné, soit en fournissant une piste de vulgarisation — les scientifiques parlent aussi aux profanes —, soit en mettant en évidence une « philosophie mathématique » implicite.

Nous avons également tenu compte des récentes avancées de la théorie en incluant la recension de deux résultats remarquables.

Le premier, dû à Goldston, Pintz et Yıldırım, affirme que, pour tout $\varepsilon > 0$, la différence $p_{n+1} - p_n$ entre deux nombres premiers consécutifs est inférieure à $\varepsilon \ln p_n$ pour une infinité d'indices n.[1] On est loin de la conjecture des nombres premiers jumeaux selon laquelle cette différence est infiniment souvent égale à 2, mais cela représente un saut qualitatif considérable.

Le second résultat est dû à Green et Tao. Il confirme une importante conjecture d'Erdős selon laquelle la suite des nombres premiers contient des progressions arithmétiques arbitrairement longues. Ainsi $\{3, 5, 7\}$ est une progression de raison 2 et de longueur 3, alors que

1. Plus précisément, ces auteurs établissent que, pour une constante convenable c, on a

$$p_{n+1} - p_n \leqslant c\sqrt{\ln p_n}(\ln \ln p_n)^2$$

pour une infinité d'indices n.

{199, 409, 619, 829, 1039, 1249, 1459, 1669, 1879, 2089} est une progression de raison 210 et de longueur 10. On sait dorénavant qu'il en existe de longueur supérieure à toute borne donnée par avance.

Nous ne donnerons pas les preuves de ces résultats. Elles sont longues et profondes et les détailler nous conduirait loin hors du cadre de cet ouvrage. Nous tenterons toutefois de satisfaire la curiosité du lecteur en fournissant des indications aussi précises que possible sur les idées essentielles. Signalons que Terence Tao a été récompensé en 2006 par la Médaille Fields, la plus haute distinction internationale pour les mathématiques.

Nous avons cru intéressant de parsemer cette édition d'illustrations de mathématiciens cités ici. Si le texte nous fait plonger dans une abstraction souvent exigeante, les portraits apportent une dimension sensible à l'exposé : les mathématiciens sont des êtres humains et voir leurs visages permet d'approcher leurs personnalités. Derrière leurs regards, on pourra peut-être deviner ce minuscule décalage qui souvent détermine une vie entière.

Tout choix est par nature restrictif : notre parti pris narratif a aussi ses dangers et ses désavantages. Rompant délibérément (certains diront scandaleusement) avec une tradition séculaire dans ce type d'ouvrage, nous ne fournissons pas de table de nombres premiers[1] et nous ne donnons pas notre démonstration favorite de la loi de réciprocité quadratique. Plus grave, les divers aspects de la théorie du crible sont seulement esquissés, bien que cette approche ait fourni de remarquables avancées, et nous n'abordons pas les diverses et profondes généralisations des nombres premiers en algèbre commutative : idéaux premiers des corps de nombres, polynômes irréductibles sur un anneau ou un corps fini, etc. On consultera à cet effet les ouvrages classiques disponibles en français.[2] Nous occultons aussi, quasi totalement, l'aspect « diviseurs » des nombres

1. Une carence à laquelle suppléeront aisément les calculatrices de bureau.

2. Voir, par exemple : Samuel, *Théorie algébrique des nombres,* Hermann, 1967 ; Borevitch & Chafarevitch, *Théorie des nombres*, Gauthier–Villars, 1967 ; Serre, *Corps locaux*, Hermann, 1968.

premiers qui fournit pourtant aux méthodes probabilistes de la théorie des nombres un champ d'investigation privilégié.[1] Enfin, nous ne faisons qu'aborder très succinctement (au § 1.5) les aspects cryptographiques et algorithmiques de la théorie, dont les saisissantes applications ont franchi, depuis plusieurs décennies, les frontières de la médiatisation grand public.[2]

La science en général, et, en son sein, les mathématiques, constitue une part sans cesse grandissante de la culture générale. Par ailleurs, les ouvrages « plaisants et délectables »[3] consacrés aux aspects spectaculaires des nombres premiers ne manquent pas, et certains sont d'ailleurs tout à fait remarquables.[4] Nous avons donc choisi d'assumer notre différence, selon une expression aujourd'hui consacrée, en visant un peu plus haut qu'il n'est d'usage dans un ouvrage de vulgarisation. Nous sommes conscients que certains développements pourront sembler ardus — ils le sont. Nous avons parfois préféré un court calcul (le dessin des mathématiciens) à de longues explications, et le style est volontairement dense, voire, de place en place, allusif. Cela nous a paru nécessaire à la mise en évidence des arguments essentiels. Ainsi, nous espérons qu'un lecteur assidu et tenace verra sa curiosité satisfaite par des preuves localement complètes — c'est en particulier avec ce souci que nous avons rédigé le Chapitre 4, essentiellement autonome. Mais nous encourageons aussi le lecteur plus pressé, ou moins désireux d'entrer dans les détails, à lire cet opuscule « en diagonale », tant il est vrai que seules les définitions comptent, pourvu qu'on les comprenne, et avec elles l'émergence d'une logique/musique

1. Ce point de vue est développé dans quelques ouvrages à présent classiques, en particulier : Elliott, *Probabilistic number theory* (2 vol.), Springer Verlag, 1979-1980 ; Hall & Tenenbaum, *Divisors*, Cambridge University Press, 1988 ; Montgomery & Vaughan, *Multiplicative number theory I*, Cambridge University Press, 2007 ; Tenenbaum, *Introduction à la théorie analytique et probabiliste des nombres*, Belin 2008.

2. Pour en savoir plus, voir par exemple les ouvrages de Robin, de Menezes, van Oorschot & Vanstone, et de Koblitz, cités dans la bibliographie.

3. Selon l'expression de Bachet (1612).

4. L'exhaustif *Nombres premiers : mystères et records* (PUF, 1994) de Ribenboim, et le lumineux *Merveilleux nombres premiers* (Belin, 2000) de Delahaye en font partie.

intrinsèque où elles s'appellent mutuellement. Le reste n'est que bavardage.

À la lecture analytique scolaire consistant à ne lire la ligne $n+1$ que lorsque l'on a compris et assimilé la ligne n, nous voulons opposer (ce qui est rendu possible précisément par la relative tension de l'exposé), une lecture synthétique, un *glissando*, où le fil directeur est sans cesse apparent. La synthèse faite, rien n'empêche (et, on l'aura compris, c'est en fait nécessaire pour progresser encore) de reprendre la lecture plume en main et d'affronter la rigueur, voire la rugosité, des démonstrations. Le jeu en vaut la chandelle.

Ce livre n'est donc pas facile, mais nous espérons qu'empreint de mystère, il engendrera une discrète poésie. De la complexité naît le rêve. Ni Stéphane Mallarmé ni Umberto Eco ne nous contrediront.

La maison Dunod, que nous avons plaisir à remercier ici, s'est engagée à nos côtés pour maintenir, sous une forme attrayante, la disponibilité de notre texte initial, qui a connu un certain succès depuis 1997, avec notamment la reconnaissance de l'Académie des Sciences,[1] une traduction anglaise,[2] et une traduction chinoise.[3]

Pour cette édition nous tenons évidemment à exprimer notre gratitude tous ceux qui nous ont aidé dès 1997 : Jean-Paul Allouche, Jean-Philippe Anker, Michel Balazard, Daniel Barlet, Régis de la Bretèche, Éric Charpentier, Hédi Daboussi, Cécile Dartyge, Jean-Marc Deshouillers, Jean-Claude Fort, Andrew Granville, Jerzy Kaczorowski, Bernard Landreau, Pierre Marchand, Gérard Mathieu, Jean-Louis Nicolas, Emmanuel Pedon, Patrick Sargos, Jacques Sicherman, André Sef, Jie Wu, et Paul Zimmermann.

1. Prix Paul Doistau-Émile Blutet de l'information scientifique 1999.

2. *The prime numbers and their distribution*, Student mathematical library 6, American Mathematical Society, 2000

3. *Les nombres premiers,* Mathematics series for graduate students 9, Tsinghua University Press, 2007.

À cette liste, il convient à présent d'ajouter Vitaly Bergelson, Daniel Goldston, Guillaume Hanrot, Charles Mozzochi, János Pintz, Jia-Yan Yao et Cem Yıldırım pour leurs précieux conseils. Régis de la Bretèche, Cécile Dartyge, et Jie Wu se sont à nouveau amicalement et efficacement mobilisés pour améliorer la présente édition.

Nancy et Bordeaux, mai 2010,
G. T. & M. M.F.

Rendue nécessaire par un accueil favorable du lectorat et une rapide indisponibilité de la première, cette seconde édition diffère de la précédente par la correction d'inévitables coquilles, voire d'erreurs, et l'inclusion de résultats récents.

La liste des erreurs véritables ne contient en fait, à notre connaissance, qu'un élément : celui de l'inclusion initiale d'un portrait du mathématicien Adrien-Marie Legendre, qui s'est révélé, après deux siècles de bons et loyaux services dans nombre d'ouvrages spécialisés, être en réalité celui de l'homonyme Louis Legendre, un homme politique contemporain du mathématicien. Il n'existe actuellement aucun portrait de ce dernier, hormis une caricature récemment retrouvée dans un album de Julien Léopold Boilly, datant de 1820. Par respect pour l'homme, nous n'avons pas souhaité reproduire cette caricature dans cet ouvrage. On ne s'étonnera donc pas de ne pas retrouver d'illustration relative à Legendre dans cette nouvelle mouture.

Au chapitre des découvertes récentes, qui furent particulièrement nombreuses et spectaculaires en théorie des nombres depuis quelques années, mentionnons le théorème de Yitang Zhang (2013) qui met la conjecture des nombres premiers jumeaux à portée de main, fût-ce une main de géant, et celui de Harald Helfgott, qui parachève le théorème de Vinogradov, dernier arrêt avant la conjecture de Goldbach.

AVANT-PROPOS

En 1921, le grand G.H. Hardy s'adressait ainsi aux membres rassemblés de la société mathématique de Copenhague : *Si quelqu'un produisait une preuve élémentaire du théorème des nombres premiers, il montrerait [...] qu'il est temps de mettre les livres à l'écart et de réécrire la théorie.* Peut-être l'édition suivante de ce petit ouvrage nécessitera-t-elle une refonte complète, en raison d'une preuve tant attendue de la conjecture de Riemann ? En dépit du travail que cela représenterait, nous l'espérons avec avidité.

Nous avons le plaisir de remercier ici Régis de la Bretèche et Sacha Zvonskine pour leur aide lors de la préparation de cette seconde édition.

Nancy et Bordeaux, août 2013
G.T. & M.M.F

Notations et conventions

Nous indiquons ici les principales notations et conventions utilisées dans l'ensemble de l'ouvrage. Celles qui n'apparaissent que dans un chapitre ou un paragraphe sont définies localement.

La lettre $\mathbb{N}$ désigne l'ensemble des entiers naturels $\{1, 2, \ldots\}$ et $\mathcal{P}$ celui des nombres premiers. Les ensembles des entiers relatifs, des nombres réels et des nombres complexes sont désignés respectivement par $\mathbb{Z}$, $\mathbb{R}$, et $\mathbb{C}$. La lettre p, avec ou sans indice désigne toujours un élément de $\mathcal{P}$. On écrit $a \mid b$ (resp. $a \nmid b$) pour signifier que a divise (resp. ne divise pas) b et $p^\nu \| a$ indique que $p^\nu \mid a$ et $p^{\nu+1} \nmid a$.

Le pgcd de deux entiers $a,\ b$ est noté (a, b). Lorsque $(a, b) = 1$, on dit que a et b sont premiers entre eux. Le nombre d'éléments d'un ensemble fini A est désigné, selon les circonstances, par $|A|$ ou $\sum_{a\in A} 1$. On désigne par $P^+(a)$ (resp. $P^-(a)$) le plus grand (resp. le plus petit) facteur premier d'un entier $a \in \mathbb{N}$, avec la convention $P^+(1) = 1$, $P^-(1) = \infty$.

Le logarithme népérien est noté ln.[1] Les itérés ln ln, ln ln ln, etc., sont notés $\ln_2$, $\ln_3$, etc. La constante d'Euler γ est définie comme la limite

$$\gamma = \lim_{N\to\infty} \Big(\sum_{n\leqslant N} 1/n - \ln N \Big).$$

On a $\gamma \approx 0,577215664$. Il est à noter, cependant, que nous suivrons l'usage traditionnel en désignant également par γ, au chapitre II, la partie imaginaire d'un zéro générique non trivial de la fonction zêta de Riemann. Aucune confusion ne sera à craindre.

1. $\ln a$ est donc, pour $a \geqslant 1$, l'aire du domaine plan limité par les axes $x = 1$, $x = a$, $y = 0$ et la courbe $y = 1/x$. On a, lorsque a est « grand », $\ln a \sim \sum_{n\leqslant a} 1/n$.

La partie entière et la partie fractionnaire d'un nombre réel x sont notées respectivement $\lfloor x \rfloor$ et $\langle x \rangle$. Ainsi

$$\lfloor 5/3 \rfloor = 1, \quad \langle -3{,}15 \rangle = 0{,}85.$$

Le signe d'affectation $:=$ indique que le membre de gauche d'une égalité est défini par celui de droite.

La fonction *logarithme intégral* est définie par

$$\mathrm{li}(x) := \int_2^x \frac{\mathrm{d}t}{\ln t} \qquad (x \geqslant 2).$$

Lorsque la lettre s désigne un nombre complexe, nous définissons implicitement ses parties réelle et imaginaire par $s = \sigma + i\tau$.

Étant données des fonctions f, g, de variable réelle ou complexe, nous employons indifféremment la notation de Landau $f = O(g)$ ou celle de Vinogradov $f \ll g$ pour signifier qu'il existe une constante positive C telle que $|f| \leqslant Cg$ dans le domaine de définition commun à f et g. Une éventuelle dépendance de C en fonction d'un paramètre α pourra être indiquée sous la forme $f = O_\alpha(g)$, ou $f \ll_\alpha g$. La notation de Landau $f = o(g)$ est utilisée dans son sens habituel de $\lim f/g = 0$.[1]

Nous désignons par *fonction indicatrice* d'un ensemble A la fonction qui vaut 1 sur A et 0 sur son complémentaire. Enfin, $\mathcal{C}^k[a, b]$ désigne l'espace des fonctions k fois continûment dérivables sur l'intervalle $[a, b]$.

Par ailleurs, nous utiliserons souvent la manipulation suivante pour estimer une moyenne pondérée par des coefficients complexes a_n $(n \in \mathbb{N})$ d'une somme aux valeurs entières d'une fonction $f \in \mathcal{C}^1[1, x]$:

$$\begin{aligned}\sum_{1\leqslant n\leqslant x} a_n f(n) &= \sum_{1\leqslant n\leqslant x} a_n \Big\{ f(x) - \int_n^x f'(t)\,\mathrm{d}t \Big\} \\ &= f(x) \sum_{1\leqslant n\leqslant x} a_n - \int_1^x f'(t) \Big\{ \sum_{1\leqslant n\leqslant t} a_n \Big\}\,\mathrm{d}t.\end{aligned}$$

1. Ainsi $O(1)$ désigne une quantité bornée alors que $o(1)$ dénote une quantité qui tend vers 0.

Index des notations

Chapitre 1

La genèse : d'Euclide à Tchébychev

1. Introduction

Compter, c'est d'abord compter sur soi. Au sens figuré, bien sûr, mais aussi au sens propre : compter sur ses doigts, sur ses pieds, sur ses épaules, sur ses genoux, etc. L'étymologie des noms de nombres fait en effet apparaître qu'ils sont des vestiges de langues très anciennes dans lesquelles ils désignaient les différentes parties du corps. Archétypes de notre représentation du monde, les nombres font, au sens le plus fort, partie de nous. À tel point que l'on peut légitimement se demander si l'objet d'étude de l'arithmétique n'est pas l'esprit humain lui-même. De là, naît une étrange fascination : comment ces nombres, que nous portons si profond, engendrent-ils des énigmes aussi redoutables ? Parmi ces mystères, celui des nombres premiers est sans doute l'un des plus anciens et des plus résistants. Notre objectif dans ce petit livre est d'initier le lecteur à quelques-unes des méthodes inventées par l'homme pour appréhender cette récalcitrante intimité. Puisse-t-il mesurer notre ignorance à l'aune de ces arcanes imbriqués et en concevoir un insatiable appétit de connaissance.

Il y a, fondamentalement, deux manières de conjuguer les entiers. On peut les ajouter et les multiplier. Mais alors que, par l'addition, on peut retrouver chaque entier fixé à l'avance à l'aide d'entiers plus petits, on s'aperçoit rapidement que, pour la multiplication, il est nécessaire d'introduire, de-ci de-là, des éléments nouveaux, irréductibles à ceux qui les précèdent. Ces éléments sont appelés des nombres premiers et, depuis la nuit des temps, l'humanité cherche à préciser le « de-ci de-là »...

L'ensemble des nombres premiers débute donc ainsi :

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, . . ., 571, . . .

Il y a près de vingt-trois siècles, Euclide démontrait l'infinitude de l'ensemble des nombres premiers. D'une grande beauté et d'une grande simplicité, sa preuve, avec les notations modernes, tient en quatre caractères :

$$n! + 1.$$

En effet, ce nombre n'est divisible par aucun entier d tel que $2 \leqslant d \leqslant n$; il ne possède donc que des facteurs premiers excédant n. Cela établit l'existence d'au moins un nombre premier plus grand que toute limite fixée à l'avance.

Pour tout nombre réel $x > 0$, on note $\pi(x)$ le nombre des nombres premiers p qui ne dépassent pas x, soit

$$\pi(x) := \sum_{p \leqslant x} 1.^{(1)}$$

Le résultat d'Euclide signifie que $\pi(x)$ tend vers l'infini avec x. Le problème se pose donc d'étudier la vitesse de croissance de cette fonction.

Il faut attendre Euler, au dix-huitième siècle, pour qu'une véritable percée soit faite dans ce domaine. Il découvre la formule

1. Cette écriture signifie simplement que l'on compte 1 pour chaque nombre premier n'excédant pas x. La notation peut sembler étrange à première vue, mais elle a fait ses preuves, notamment parce qu'elle se prête à diverses manipulations analogues à celles des intégrales.

fondamentale

$$\zeta(\sigma) := 1 + \frac{1}{2^\sigma} + \frac{1}{3^\sigma} + \cdots \\ = \frac{1}{1-1/2^\sigma}\frac{1}{1-1/3^\sigma}\frac{1}{1-1/5^\sigma}\cdots \quad (\sigma > 1),$$

qui relie une somme étendue à tous les entiers à un produit infini portant sur tous les nombres premiers. La formule n'est pas valable pour $\sigma = 1$, mais Euler n'hésitait pas à lui donner le sens suivant[1]

$$\prod_p \big(1 - 1/p\big) := \big(1-1/2\big)\big(1-1/3\big)\big(1-1/5\big)\cdots = 0.$$

Sachant que $\ln(1-1/p)$ est de l'ordre de $-1/p$, Euler en concluait que la somme des inverses des nombres premiers diverge :

$$\sum_p \frac{1}{p} := \frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{11} + \cdots = \infty.$$

Ce calcul sera justifié et précisé au § 7.

Gauss (1792), puis Legendre (1798, 1808) conjecturent que l'on a, lorsque x tend vers l'infini,

$$\pi(x) \sim x/\ln x.^{(2)}$$

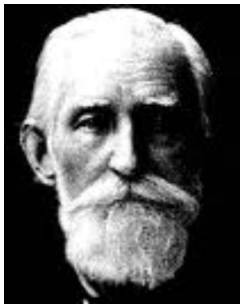
Carl Friedrich Gauss
(1777–1855)

Quelques décennies plus tard, en 1852, Tchébychev établit une forme faible de cette conjecture : il existe des constantes strictement positives a et b telles que l'on ait

$$ax/\ln x < \pi(x) < bx/\ln x \qquad (x \geqslant 2).$$

1. Qu'en langage moderne on pourrait qualifier de prolongement par continuité.
2. Il est utile de garder à l'esprit que cela équivaut à la validité de la formule asymptotique $p_n \sim n \ln n$, où p_n désigne le n-ième nombre premier.

Numériquement, le résultat constitue un argument très convaincant en faveur de la conjecture de Gauss-Legendre : pour x assez grand, on peut choisir $a = 0{,}921$ et $b = 1{,}106$.



Pafnouti Tchébychev
(1821–1894)

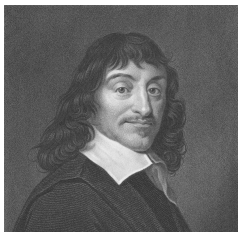
Un petit détour est nécessaire pour décrire le progrès suivant, dû à Riemann.

Le lecteur a sans doute, sinon une connaissance précise, du moins une certaine idée de ces nombres particuliers, qualifiés d'« imaginaires » par Descartes, et inventés par les mathématiciens italiens du XV^{e} siècle pour résoudre les équations de degré 3 et 4. Toute l'histoire consiste à admettre l'existence de racines carrées de nombres négatifs et à constater que le calcul formel fonctionne. Ainsi, selon Cardan, si l'on note $i = \sqrt{-1}$, les solutions de l'équation $x(10 - x) = 40$ sont $5 \pm i\sqrt{15}$: par exemple

$$\begin{aligned}(5 + i\sqrt{15})(5 - i\sqrt{15}) &= 25 - (i\sqrt{15})^5 \\ &= 25 - i^2 15 = 25 + 15 = 40.\end{aligned}$$

Le trouble vient de ce qu'on sait depuis toujours que le carré d'un nombre réel est nécessairement positif, et donc qu'il n'existe aucun nombre réel dont le carré soit négatif. Descartes, Newton et Bombelli considéraient que l'apparition de ces nombres comme solutions d'équations signifiait que le problème était en réalité impossible.

Mais, en terre de mathématiques, l'interdiction peut être contournée sans contrevenir aux règles de la logique. À la suite de Wallis et Gauss, les mathématiciens ont trouvé un espace nouveau dans lequel les nombres réels et imaginaires pouvaient cohabiter paisiblement : il suffisait de penser à introduire une dimension supplémentaire



René Descartes
(1596–1650)

pour l'univers des nombres — une révolution. À la droite numérique, où les nombres réels sont rangés à la queue-leu-leu, on a substitué un pré carré où la longueur était mesurée à l'aune du nombre réel 1, et la largeur à celle du nombre imaginaire i. Dans ce nouveau monde, un nombre est une combinaison du type

$$a + ib$$

où a et b sont réels. Sous cette forme, aucune simplification n'est possible, mais le calcul suit les règles ordinaires, compte tenu de la loi $i^2 = -1$: par exemple

$$(a + ib)^2 = a^2 - b^2 + 2iab.$$

L'univers des combinaisons $a+ib$ de nombres réels et imaginaires est désigné comme le champ des *nombres complexes*, habituellement noté par la lettre $\mathbb{C}$. Dans $\mathbb{C}$, on peut additionner, soustraire, diviser, multiplier selon les lois usuelles. On dit que $\mathbb{C}$ est un *corps*.[1]

Le corps $\mathbb{C}$ des nombres complexes offre une surprise de taille : non seulement *toutes* les équations polynomiales à coefficients réels y ont des solutions, mais il en va de même des équations à coefficients complexes. Ainsi, l'équation $x^3 + 2i = 0$ a pour solutions

$$i\sqrt[3]{2}, \quad -\tfrac{1}{2}\sqrt[3]{2}\sqrt{3} - i\tfrac{1}{2}\sqrt[3]{2}, \quad \tfrac{1}{2}\sqrt[3]{2}\sqrt{3} - i\tfrac{1}{2}\sqrt[3]{2}.$$

Riemann (1859) exploite l'idée géniale de prolonger la fonction zêta

$$\zeta(s) = \sum_{n \geqslant 1} n^{-s}$$

en une fonction de la variable complexe. Cela permet de donner un sens à $\zeta(s)$ même hors du domaine de convergence de la série et, comme le démontre Riemann, l'étude du prolongement se prête remarquablement bien à la déduction de renseignements asymptotiques concernant $\pi(x)$.

1. Si $z = a + ib$ est un nombre complexe, on dit que a est sa *partie réelle*, et que b est sa *partie imaginaire*. On écrit alors $\Re e\, z = a$, $\Im m\, z = b$.