Les Nombres premiers

Les Nombres premiers

Un long chemin vers l'infini

Enrique Gracián

Le monde est mathématique

Une édition réalisée avec le soutien de l'IHP

Institut Henri Poincaré

Créé en 1928, l'Institut Henri-Poincaré (IHP) est l'une des plus anciennes et des plus dynamiques structures internationales dédiées aux mathématiques et à la physique théorique. Il perpétue la tradition de mixité et d'universalisme, dont Henri Poincaré, mathématicien, physicien et philosophe, était l'emblème.

S'intéressant aux aspects théoriques comme aux applications, l'IHP a joué, depuis sa création, un rôle pionnier dans l'utilisation des mathématiques en statistique, biologie et informatique ; une politique aujourd'hui plus que jamais d'actualité.

Lieu d'échanges scientifiques nationaux et internationaux, l'IHP accueille chaque année chercheurs invités et visiteurs, et abrite des programmes thématiques, des cours doctoraux, ainsi que de nombreux colloques et séminaires. Cette véritable ambassade des mathématiques françaises entretient aussi un partenariat étroit avec les associations et sociétés de promotion des mathématiques. Aujourd'hui, l'IHP est dirigé par Cédric Villani.

Préface

Les nombres premiers sont les briques élémentaires permettant de construire tous les autres nombres entiers par multiplications successives. Ainsi, 2 et 3 sont des nombres premiers ; multipliés entre eux, ils donnent 6, qui n'est pas un nombre premier, mais un nombre composé. Le nombre premier suivant est 5 car 4, égal à 2 fois 2, est composé. Puis viennent 7, 11, 13, etc. Il paraît aisé de poursuivre cette énumération. 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

constituent la liste complète des nombres premiers inférieurs à 100.

Le lecteur apprendra dans cet ouvrage qu'il existe une infinité de nombres premiers, mais que ces nombres deviennent plus rares à mesure que le nombre de chiffres nécessaires pour les écrire augmente. Noyés dans une mer de nombres composés, ils sont donc, en quelque sorte, de plus en plus isolés et difficiles à localiser. C'est cette propriété que Paolo Giordano a popularisée en intitulant l'un de ses romans *La Solitude des nombres premiers* (2009).

Comment peut-on poursuivre en pratique l'énumération systématique des nombres premiers ? Existe-t-il un algorithme efficace permettant de décider si un nombre donné, très grand, est premier ou composé ? Et à quoi pourrait bien servir un tel algorithme ? Ces interrogations forment le cœur de cet ouvrage. Elles servent aussi de prétexte à des promenades à la fois historiques et scientifiques qui, en des lieux mythiques et en compagnie de quelques héros célèbres des mathématiques, mènent le lecteur à la rencontre de problèmes qui défient encore de nos jours la sagacité des mathématiciens.

Au sein de la bibliothèque d'Alexandrie, accompagné de Ptolémée I^{er} et Démétrios, on pourra réfléchir à la construction des centres de la connaissance, question encore d'actualité à l'heure où encyclopédies et bases de données se développent sur le réseau Internet. Le lecteur rencontrera dans ce haut lieu de l'Antiquité Eratosthène de Cyrène étudiant la famille des nombres premiers (son « crible » est encore enseigné aujourd'hui !).

On croisera aussi John Napier, mathématicien du XVI^{e} siècle, avec ses machines de calculs et ses « logarithmes », puis, en sautant quelques siècles, on découvrira l'un des problèmes théoriques actuels les plus importants pour l'informatique

théorique, c'est-à-dire la science des algorithmes. Il s'agit, précisément, du problème P = NP, l'une des sept questions mathématiques du millénaire posées par l'Institut Clay qui offre un million de dollars pour sa résolution.

Apparaît encore Leonhard Euler, auquel Christian Goldbach soumet sa conjecture que l'on peut décrire ainsi: puisque 2 et 2 font 4, 3 et 3 font 6, 3 et 5 font 8, 3 et 7 font 10, 7 et 5 font 12 et ainsi de suite, on voit que les petits nombres pairs sont tous somme de deux nombres premiers. La question de Goldbach demande si c'est toujours le cas et si tout nombre pair, aussi grand soit-il, est somme de deux nombres premiers. Elle est encore ouverte aujourd'hui ! Puis vient Carl Friedrich Gauss, qui, encore jeune homme, propose une estimation de la quantité de nombres premiers inférieurs à un nombre donné. Bernhard Riemann, Johann Dirichlet, Jacques Hadamard, Charles-Jean de la Vallée Poussin, Godfrey Harold Hardy et Srinivasa Ramanujan suivent tour à tour. Petit à petit, ces mathématiciens ont su dompter une partie du mystère de la répartition des nombres premiers au sein de la famille de tous les nombres entiers, mesurer leur éparpillement et émettre de nouvelles hypothèses décrivant leur structure.

Cette liste d'hommes remarquables mériterait d'être allongée en mentionnant les noms de Pafnouti Tchebychev, d'Ivan Vinogradov, d'Atle Selberg, de Paul Erdös, ou encore, tout récemment, de Ben Green et de Terence Tao. Elle montre que l'attraction des mathématiciens pour ce sujet demeure vive, et à raison.

On l'aura compris, l'auteur du livre nous présente un panorama personnel agréable de quelques étapes marquantes de l'histoire des nombres premiers. Des nombres que l'on rencontre dés le collège, mais qui préservent encore une grande partie de leurs secrets. Des nombres qui fascinent mathématiciens professionnels et amateurs.

Serge Cantat
Directeur de recherches au CNRS

Sommaire

Introduction

La majorité des nombres ont ce que nous pourrions appeler un « bon comportement » arithmétique : les pairs alternent toujours avec les impairs, les multiples de 3 apparaissent toujours tous les trois nombres et les carrés parfaits suivent une loi de formation facile à déterminer. Nous pourrions ainsi établir une longue liste de nombres qui font sagement ce que l'on attend d'eux, quels que soient leur grandeur et l'endroit où ils se situent. À l'inverse, les nombres premiers constituent un véritable casse-tête : ils apparaissent où bon leur semble, sans prévenir, de manière apparemment chaotique, et sans suivre une quelconque règle. Et le pire de tout, c'est qu'il est impossible de les ignorer : ils sont l'essence même de l'arithmétique, pour ne pas dire des mathématiques dans leur ensemble.

En réalité, il ne s'agit pas d'un concept compliqué qui nécessiterait des années d'études en mathématiques ; de fait, les nombres premiers sont enseignés dans les collèges, dès les premiers cours de mathématiques. Pour comprendre ce qu'est un nombre premier, il suffit de connaître un système de numérotation et les quatre opérations fondamentales. Cependant, les nombres premiers ont constitué et constituent toujours l'un des plus fabuleux défis de l'histoire de la science. Si quelqu'un souhaite se consacrer aux mathématiques et ne parvient pas à faire bon ménage avec lesdits nombres, alors il perd son temps : car il sont toujours là, omniprésents, tapis dans un coin et prêts à réapparaître lorsque l'on s'y attend le moins. Et quand ils surgissent, impossible de les éviter. Ils s'imposent de manière implacable, marquant leur territoire et affirmant leur force de décision.

Leur influence s'étend au-delà des limites de l'univers des mathématiques. Bien que nous n'en soyons pas nécessairement conscients, les nombres premiers jouent un rôle décisif dans notre vie quotidienne : dans le système de protection de notre ordinateur personnel, dans les transactions bancaires, ou encore dans la confidentialité de nos conversations sur un téléphone portable. Ils sont les pierres angulaires de la sécurité informatique.

Pour user d'une métaphore, les nombres premiers sont comme un virus maléfique qui, quand il attaque le cerveau d'un mathématicien, est très difficile à éradiquer. Euclide, Fermat, Euler, Gauss, Riemann, Ramanujan et bien d'autres encore : la liste est longue de ceux qui sont tombés dans ses filets. Certains réussirent avec plus ou moins de succès à s'en libérer, mais tous succombèrent à l'obsession de trouver la « formule magique », une règle de formation qui déter-

minerait quel nombre premier suit un nombre quelconque. Cependant, aucun d'eux n'y parvint.

Tout au long de l'histoire des mathématiques, les nombres premiers ont laissé dans leur sillage une longue série de conjectures. D'une certaine manière, on pourrait dire que l'histoire des nombres premiers est l'histoire d'un grand échec ; mais un échec merveilleux qui a permis de donner naissance à de nouvelles théories, à de nouveaux paradigmes, et de fixer de nouvelles bornes qui délimitent un avant et un après. En ce qui concerne la créativité mathématique, les nombres premiers ont été une véritable source de richesse : bien que cette affirmation puisse paraître paradoxale, c'est une chance qu'ils ne se soient pas encore laissé dominer. Et tout laisse à penser que cette situation n'est pas près de changer.

Au fil de ce livre, nous avons essayé de maintenir un « haut » niveau de vulgarisation, ce qui signifie que le bagage des connaissances mathématiques requises pour cette lecture est « bas » - l'usage des guillemets s'imposant dès lors qu'il s'agit de concepts relatifs, en particulier dans le cas qui nous occupe. Quoi qu'il en soit, ce livre peut être abordé par n'importe quel lecteur qui connaît les nombres et les opérations de base. L'objectif est que cette lecture lui donne une idée concise de ce qu'est l'univers des nombres premiers.

En contrepartie, en pensant aux lecteurs qui possèdent des connaissances mathématiques plus avancées, nous avons souhaité inclure aussi des informations concernant certains processus historiques bien précis. Ceux-ci sont, en effet, essentiels pour qui veut comprendre les chemins sinueux qu'ont empruntés les grands mathématiciens tout au long de l'histoire, dans leurs investigations sur les problèmes posés par les nombres premiers.

Pour conclure, et comme cela apparaît clairement dès le premier chapitre, le concept de nombre premier et les défis que ces nombres ont lancés sont très simples à expliquer. En revanche, les solutions proposées appartiennent, quant à elles, dans leur majorité, aux sphères les plus élevées des mathématiques professionnelles.

Chapitre 1

À l'aube de l'arithmétique

Les nombres premiers ont, comme toute chose, une origine, qu'il faut chercher au tout début des systèmes de numérotations eux-mêmes. Ils ont vu le jour avec les nombres naturels, mais très tôt ils s'en démarquèrent, en tant que « nombres spéciaux ».

Il n'y a rien de plus naturel qu'un nombre naturel

« Dieu fit les dix premiers nombres ; le reste est l'œuvre de l'Homme. » Cette affirmation est attribuée à Leopold Kronecker (1823-1891), mathématicien allemand, qui se réfère aux nombres naturels, ceux que nous utilisons pour compter : 1, 2, 3, 4, 5… Kronecker affirmait ainsi qu'une grande partie de l'édifice mathématique se construit à partir de l'arithmétique élémentaire. Mais affirmer que Dieu nous donna les dix premiers nombres équivaut à dire, hors de tout contexte religieux, qu'il n'y a rien de plus naturel qu'un nombre naturel. C'est-à-dire que ces nombres ont toujours été présents, formant partie intégrante de la nature qui nous entoure.

On peut raisonnablement admettre que l'être humain commença à compter lorsqu'il abandonna l'état de chasseur-cueilleur pour entamer sa longue marche en tant qu'agriculteur-éleveur. À ce moment là, de nombreux biens, comme les grains de blé ou les têtes de bétail, cessèrent d'avoir un usage immédiat et devinrent des produits, ce qui nécessitait la mise en œuvre de processus d'inventaires. Imaginons un berger qui mène son troupeau au pâturage. Il doit s'assurer qu'à son retour à l'étable il y a autant d'animaux qu'à la sortie. La façon la plus naturelle de le faire, s'il ne dispose pas d'un système de numération, est de rassembler un grand nombre de petites pierres et de déposer dans un sac une pierre par tête de bétail qui sort. Au retour, il n'aura plus qu'à retirer une pierre par tête de bétail et vérifier ainsi qu'à la fin il ne reste plus aucune pierre au fond du sac. Il s'agit là d'un processus de calcul primitif (rappelons que le mot calcul provient du latin *calculis*, « pierre ») qui ne requiert pas le concept de nombre. En termes mathématiques actuels, nous dirions que le pasteur établit une application bijective et biunivoque entre l'ensemble des animaux et l'ensemble des pierres. Or, si nous pensons qu'en mathématiques le concept

PERCEPTION NUMÉRIQUE

Quand les Chinois parlaient des dix mille étoiles qu'il y a dans le ciel, ils ne prétendaient pas les avoir toutes comptées. Il s'agissait simplement d'une manière d'exprimer un grand nombre. On peut penser qu'un milliard serait un meilleur nombre pour exprimer une très grande quantité. D'emblée, il faut tenir compte du fait que notre perception directe d'un nombre ne va pas au-delà de cinq unités. Quand quelqu'un tend les cinq doigts d'une main et trois de l'autre, nous pouvons tout de suite dire qu'il y a un total de huit doigts, mais il s'agit là quasiment d'un code. Si nous alignons huit objets sur une table nous devrons les compter ou les grouper en sous-ensembles pour savoir combien il y en a. Inutile de dire qu'au-delà de ces quantités notre perception sensorielle numérique disparaît complètement. Pour cette raison, il est très difficile de se faire ne serait-ce qu'une vague idée de ce qu'est un million d'unités si nous n'avons pas une référence immédiate. Nous savons ce que veut dire « gagner un million d'euros au Loto » car nous connaissons la valeur de l'argent et nous faisons un calcul rapide de ce que nous pourrions acheter. Mais de là à avoir une perception claire de ce que représenterait l'alignement de 1 million de pièces de 1 euro, il y a une grande différence (cela équivaut à une distance de 23,25 km de long).

D'un seul coup d'œil, notre cerveau est capable de reconnaître au maximum cinq objets. Au-delà, il faut qu'il trouve une stratégie pour les compter.

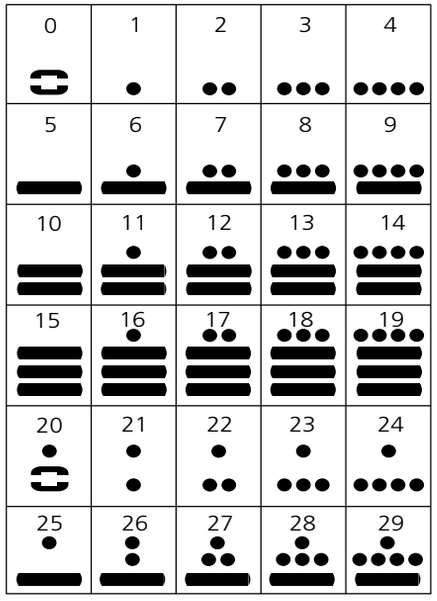
d'application biunivoque n'a été établi de manière précise qu'à partir du XIX^e^ siècle, il peut sembler paradoxal de considérer le fait de compter comme naturel. Quand nous affirmons que quelque chose est « naturel », nous devons, au moins dans ce cas, apporter quelques précisions.

Nous pourrions entendre par naturel un processus mental qui surgit de façon immédiate, sans besoin de réflexion préalable. Mais il n'est pas du tout certain que le système de décompte au moyen du sac de pierres ne requière dans l'absolu aucune réflexion préalable. Ce qui le caractériserait serait plutôt son immédiateté sur le plan de l'usage, de la finalité pratique recherchée dans le processus. Se représenter le degré de réflexion qu'implique un processus mental pour le qualifier de naturel ou non peut s'avérer une tâche bien trop complexe. Dans ce contexte, il nous sera plus utile de parler de niveaux d'abstraction.

L'assimilation d'un système de numération implique un fort processus d'abstraction, au point que de nombreux spécialistes considèrent qu'avec l'apprentissage du langage, c'est l'un des plus importants efforts mentaux que réalise un être humain dans sa vie. Quand nous disons « trois », nous pouvons nous référer aussi bien à trois moutons qu'à trois pierres, trois maisons, trois arbres ou trois objets quelconques. Si nous avions dû employer des mots différents pour dénombrer chacun des objets auxquels nous faisons référence, la société d'agriculteurs-éleveurs se serait peut-être effondrée à ses débuts. Trois est un concept abstrait, une pure image mentale qui pour circuler telle quelle dans un groupe social, requiert seulement un mot ou un signe comme moyen de communication.

Rappelons que le langage quotidien implique, lui aussi, des processus d'abstraction. Quand un enfant apprend pour la première fois le mot « chaise », il se réfère habituellement au seul objet qu'il utilise lui-même pour s'asseoir, mais il se rend compte petit à petit que le même mot peut se référer non seulement à son siège, mais aussi à bien d'autres objets dans la maison dont la fonction est toujours la même. Le processus d'abstraction continue et un jour apparaît le mot « siège », à un niveau d'abstraction qui n'inclut pas seulement les chaises, mais aussi les bancs, les gradins et tout objet qui sert à s'asseoir. Ainsi, personne ne peut douter que le processus d'évolution, s'agissant des espèces « intelligentes », est inexorablement lié à leur capacité toujours plus grande d'abstraction.

Beaucoup de gens ont une aversion pour les mathématiques, une aversion qu'ils justifient en alléguant qu'elles sont trop abstraites, comme si le processus d'abstraction était quelque chose d'artificiel, peu naturel. Mais c'est tout le contraire. Sans faire appel à notre capacité d'abstraction, nous ne serions même pas capables d'établir un langage commun. Parfois, la pensée abstraite est qualifiée de peu pratique, ce qui n'est pas non plus certain. Plus on souhaite qu'une méthode soit pratique, et plus nous devons la concevoir de manière élaborée et abstraite. Un bon exemple de cela est le système de numération positionnel que nous utilisons tous les jours (de la façon la plus « naturelle »). Dans un système de numération non positionnel, le symbole qui représente un nombre a la même valeur quelle que soit sa position. Par exemple, dans le système de numération romain, le nombre 5, représenté par la lettre V, a la même valeur dans les expressions XV, XVI ou VII. En revanche, si le système romain avait été un système de numération positionnel comme le nôtre, le V équivaudrait à 5 unités dans le premier cas, 50 dans le deuxième et 500 dans le troisième.



La culture maya fut l'une des rares du monde antique qui développa un système de numération positionnel. Les Mayas utilisaient trois symboles : une coquille pour représenter le zéro, un point pour l'unité et un tiret pour exprimer cinq unités.

Créer un système de numération positionnel ne fut précisément pas une tâche facile : il fallut près de mille ans pour y parvenir. L'histoire des nombres est longue et passionnante, mais ce n'est pas le sujet qui nous occupe ici. Nous considérons, dans cet ouvrage, que les nombres sont déjà là et qu'en outre nous connaissons les opérations élémentaires : l'addition, la soustraction, la multiplication et la division.

Qu'est-ce qu'un nombre premier ?

Prenons un exemple quelconque : le nombre 12. Nous savons que nous pouvons exprimer ce nombre de différentes manières comme le produit d'autres nombres :

$$12 = 2 \cdot 6 ;$$
$$12 = 3 \cdot 4 ;$$
$$12 = 2 \cdot 2 \cdot 3.$$

À partir de maintenant, nous appellerons ces nombres des « facteurs » ou « diviseurs ». Nous dirons ainsi que 3 est un facteur de 12, de la même manière que nous pouvons dire que 3 est un diviseur de 12. *Diviseur* signifie qu'il divise ; ainsi 3 divise 12. De la même manière, nous disons que 5 est un diviseur de 20, car 5 divise 20. Dire que 5 divise 20 veut dire que si nous faisons la division de 20 par 5, nous obtenons un nombre naturel – dans ce cas 4 – et que le reste de la division est 0.

Le mot facteur a lui aussi une définition précise. Il vient du latin *facere*, « faire » ou « fabriquer ». Dans l'expression $12 = 3 \cdot 4$, le nombre 3 est un facteur car c'est un nombre qui permet de « fabriquer » le nombre 12.

Selon cette définition, à la question « Quels sont les diviseurs de 12 ? », nous pouvons répondre que 2, 3, 4, 6 sont diviseurs de 12. En effet, 12 divisé par n'importe lequel de ces nombres donne un résultat exact. Parmi tous les diviseurs d'un nombre nous devons aussi compter 1, car tout nombre est divisible par l'unité et par lui-même. Par exemple, à la question « Quels sont les diviseurs de 18 ? », nous pouvons répondre que 18 est divisible par 1, 2, 3, 6, 9 et 18.

Supposons que se pose la même question, mais avec le chiffre 7. Si nous cherchons des diviseurs possibles, nous trouverons que les seuls chiffres qui divisent 7

SIGNES DU DIABLE

Durant les époques les plus sombres de la culture européenne, les chiffres étaient considérés comme les signes mystérieux d'une « écriture secrète ». D'ailleurs, encore aujourd'hui, on appelle les messages codés « messages chiffrés ». De manière rigoureuse, nous devrions appeler « chiffrés » les messages dans lesquels les lettres ont été remplacées par des nombres.

Quand furent introduits les premiers chiffres arabes en Europe, dans les colonnes des abaques, les « abacistes » purs les remplacèrent par des nombres romains. Ils ne pouvaient permettre la présence de ces « signes diaboliques avec lesquels Satan avait perverti les Arabes ». Six siècles après la mort du pape Sylvestre II, l'Église demanda à ouvrir sa tombe pour vérifier si les démons qui avaient inspiré la science sarrasine des nombres étaient encore présents.

Gerbert d'Aurillac était Sylvestre II, le pape mathématicien.

sont 1 et lui-même, 7. Il en est de même pour 2, 3, 5, 11 ou 13. Ce sont tous des nombres « premiers ».

Nous sommes maintenant en position de donner une définition précise de ce qu'est un nombre premier : un nombre est dit premier quand il est divisible seulement par lui-même et par 1.

Dans cette réflexion sur les nombres naturels sont intervenues les opérations de multiplication et de division. Nous sommes arrivés à la conclusion qu'il existe des nombres spéciaux, et en les caractérisant tous au moyen d'une définition, nous avons réalisé un processus d'abstraction. En leur attribuant un nom et une propriété qui les définissent, nous en avons fait un objet d'étude.

Le théorème fondamental de l'arithmétique

Il est fréquent de se référer aux nombres premiers comme aux « briques » des mathématiques, aux atomes de l'arithmétique ou au code génétique des nombres. Les maisons sont construites avec des briques ; tous les éléments de la nature avec les atomes ; tous les êtres vivants avec le code génétique. Toutes ces expressions ont une signification commune : elles désignent des éléments primitifs à partir desquels se construit autre chose – dans ce cas, les nombres. Nous verrons comment les nombres premiers ont rempli ce rôle.

Nous avons vu qu'un nombre pouvait se décomposer en diviseurs ou facteurs. Ainsi, le nombre 12 peut se décomposer en $3 \cdot 4$. Rappelons-nous que lorsque nous parlons de facteurs, nous voulons dire que les nombres 3 et 4 peuvent fabriquer 12. Nous savons aussi que nous pourrions le fabriquer au moyen d'autres nombres, par exemple :

$$12 = 2 \cdot 6 = 3 \cdot 4 = 2 \cdot 2 \cdot 3.$$

Ces nombres sont tous des facteurs du nombre 12. Ce processus s'appelle « décomposer un nombre en produit de facteurs ». Rappelons que c'était là le critère qui nous avait permis de donner une définition précise de ce qu'est un nombre premier : celui dont les uniques facteurs sont lui-même et 1. Ainsi, les seuls facteurs d'un nombre premier, comme 13, sont :

$$13 = 1 \cdot 13.$$

Lorsque, dans un produit, l'un des facteurs se répète, nous écrivons le nombre avec un exposant qui indique le nombre de fois qu'il se répète ; par exemple,

$$2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^5 ;$$
$$3 \cdot 3 \cdot 3 \cdot 3 = 3^4.$$

Il s'agit là de ce qu'on appelle en mathématiques « puissance » : 2^5 se lit « deux puissance 5 », et 3^4 « trois puissance 4 ».

Dans l'exemple précédent, nous avons décomposé le nombre 12 en trois produits de facteurs différents : 2 et 6 ; 3 et 4 ; 2, 2 et 3. De tous ces produits, seul le dernier est formé uniquement de nombres premiers.

Voyons un autre exemple avec le nombre 20 :

$$20 = 2 \cdot 10 = 2 \cdot 2 \cdot 5 = 4 \cdot 5.$$

Seule la décomposition $20 = 2 \cdot 2 \cdot 5 = 2^2 \cdot 5$ contient uniquement des facteurs premiers.

La question que nous posons maintenant est la suivante : soit un nombre quelconque, est-il toujours possible de trouver une décomposition de ce dernier en facteurs premiers ? C'est-à-dire, peut-il s'exprimer comme un produit de nombres qui soient tous premiers ? La réponse est oui. Mais en outre, il n'existe qu'une seule façon de le faire. Quand nous écrivons le nombre 20 comme produit de facteurs premiers, $20 = 2^2 \cdot 5$, nous le faisons de la seule façon possible (étant donné que l'ordre dans lequel les facteurs interviennent ne compte pas, il n'y a en effet aucune différence entre $2 \cdot 5 \cdot 2$ et $5 \cdot 2 \cdot 2$). Ceci est le théorème, attribué à Euclide, connu comme le « théorème fondamental de l'arithmétique » et qui énonce que « tout nombre naturel peut se décomposer d'une façon unique comme le produit de facteurs premiers ».

COMMENT DÉCOUVRIR LES NOMBRES PREMIERS

120	2
60	2
30	2
15	3
5	5
1	

Pour faire une décomposition en facteurs premiers, la méthode est la suivante : on place le nombre en question à la gauche d'une ligne verticale. On voit ensuite s'il est divisible par 2, 3, 5, etc., c'est-à-dire par des nombres premiers, en commençant par le plus petit. Dans le cas où il est divisible, on place le résultat de la division dans la partie à gauche et on recommence avec ce nouveau nombre. On poursuit le processus jusqu'à ce que le nombre à gauche soit 1. Dans la colonne de droite apparaissent les nombres premiers qui factorisent le nombre donné.

De telle sorte que, quand nous écrivons $24 = 2^3 \cdot 3$, nous affirmons qu'il s'agit là de l'unique manière possible de le décomposer avec des facteurs premiers. Dans ce cas, le titre de « théorème fondamental » est tout à fait justifié. C'est en effet littéralement l'un des grands piliers sur lesquels s'appuie l'arithmétique. De plus, de ce point de vue-là, les nombres premiers acquièrent une dimension transcendantale. En revenant à nos comparaisons antérieures, nous pourrions dire que $2^3 \cdot 3$ est l'ADN du nombre 24, une chaîne formée par les gènes 2^3 et 3, ou que 2 et 3 sont les atomes avec lesquels se forme l'élément 24.

Par conséquent, les nombres premiers sont les éléments primordiaux avec lesquels se construisent tous les nombres. Le mot « premier », qui vient du latin *primus*, veut dire « le premier » et fait référence au concept de « primaire », « primitif », dans le sens d'« originel », c'est-à-dire que tous les nombres peuvent s'obtenir à partir d'eux. De la même manière que les atomes s'unissent pour former des molécules, les nombres premiers forment des nombres naturels. Tous les éléments chimiques connus sont formés par des atomes qui se combinent entre eux sous des formes particulières. Dmitri Ivanovitch Mendeleïev (1834-1907) fut le chimiste russe qui créa la table périodique des éléments. Celle-ci permet d'ordonner les éléments chimiques naturels mais aussi ceux qui ont été créés artificiellement. Il n'existe cependant pas de table analogue pour les nombres premiers, une table qui permettrait de les grouper suivant un critère, une loi de formation à laquelle ils répondraient sans ambiguïté. Les nombres premiers apparaissent comme un ensemble chaotique, sans ordre ni lois, et surgissent de manière apparemment aléatoire dans la série des nombres naturels.

Les nombres premiers, invention ou découverte ?

Une fois établi le système de numération, il paraît logique que la première propriété qui se détecte dans un nombre soit le fait qu'il est pair ou impair, un concept intuitif et immédiat. L'étape suivante fut la factorisation des nombres, amenant l'établissement des critères de divisibilité qui s'enseignent dès le collège. De cette manière, une culture ayant établi son système de numération possédait une collection de nombres contrôlés par un petit nombre de propriétés faciles à établir. Tous exceptés les nombres premiers. La seule certitude concernant ces nombres était qu'aucun d'entre eux ne pouvait être pair, excepté le premier d'entre eux (2 est le seul nombre premier pair). On ne pouvait pas non plus les traiter comme une rareté difficile à découvrir, puisque Euclide avait démontré qu'ils étaient en quantité

infinie (nous verrons plus loin de quelle élégante manière il le démontra). Il n'était pas non plus possible de sous-estimer leur importance, le théorème fondamental de l'arithmétique les ayant inscrits au tableau d'honneur des mathématiques. Par conséquent, et comme nous l'avons déjà dit, ils s'étaient constitués en objet d'étude.

Quand on parle d'objet d'étude dans les sciences expérimentales, il paraît clair qu'il s'agit d'un objet extérieur, qui existe quelque part. Nous pouvons l'avoir découvert ou non et, par la suite, décider de l'étudier ou de l'ignorer, mais dans un cas comme dans l'autre, il reste présent, indépendamment de ce que nous pensons ou faisons de lui. À partir d'un certain moment, les bactéries devinrent un objet d'étude pour les biologistes. Personne ne met en doute le fait qu'elles étaient déjà présentes dans les organismes vivants avant que n'apparaissent les biologistes, et bien avant d'ailleurs que ne surgisse l'espèce humaine. C'est une question que personne ne se pose dans le milieu scientifique. Cependant, en mathématiques, la question se pose différemment. Les nombres premiers sont-ils une invention ou une découverte ? Auraient-ils existé sans les êtres humains ? Cette discussion a provoqué et provoque encore la polémique parmi les plus passionnés. Le plus probable est qu'il s'agit d'une question sans réponse, face à laquelle nous devons nous contenter de prendre une position.

L'universalité des mathématiques pose la question de savoir si ces dernières ont une existence propre, en marge de l'être humain. Cette réflexion ne fut pas étrangère au physicien allemand Heinrich Rudolf Hertz.

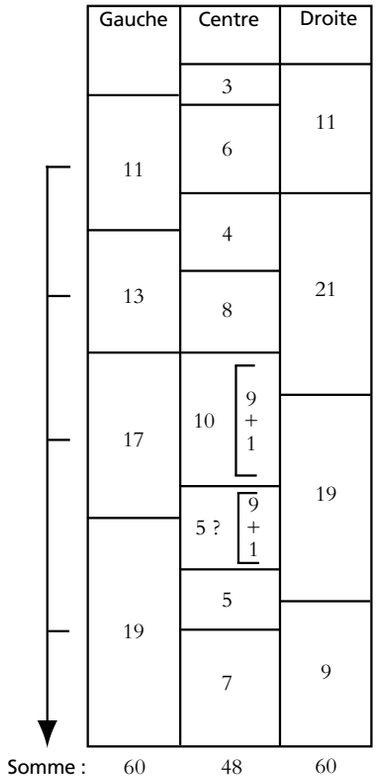
Le plus important en ce qui concerne la nature du raisonnement mathématique, c'est que le chercheur agisse comme s'il était un explorateur qui s'engage dans des contrées inconnues, comme si les mathématiques lui étaient réellement étrangères. Ce sentiment d'aventure fait partie de l'essence même de l'investigation mathématique, et c'est ce qui lui imprime son caractère artistique. Le physicien allemand Heinrich Rudolf Hertz (1857-1894) se demandait : « Peut-on éviter de ressentir le fait que ces formules mathématiques ont une existence indépendante et une intelligence propre, qu'elles sont plus savantes que nous ne le sommes nous-mêmes, plus savantes que leur propre inventeur, et que nous obtenons d'elles plus que ce que nous avons initialement mis en elles ? »

Le courant philosophique, ou mieux, épistémologique, qui accepte le fait que les objets (y compris les

L'OS D'ISHANGO

Cet os est probablement un péroné de babouin, avec une forme apparente d'outil : c'est comme un manche qui peut se saisir facilement et qui possède à son extrémité un cristal de quartz affûté. Il fut découvert non loin des sources du Nil, entre les frontières de l'Ouganda et de la République Démocratique du Congo, et appartient à une société tribale qui fut ensevelie à cause d'une éruption volcanique. L'os est daté de près de 20 000 ans.

L'os d'Ishango est exposé au Muséum des sciences naturelles de Bruxelles, en Belgique.



Le schéma montre la distribution des entailles, réparties en trois colonnes, sur l'os d'Ishango, un outil qui aurait pu servir pour faire des calculs simples.

vérités mathématiques) ont leur existence propre porte l'étiquette de « platonisme ». Il repose sur l'idée qu'on ne peut maintenir une posture objective que dans la mesure où l'on est en présence d'objets. Les historiens des mathématiques ont l'habitude de faire pencher la balance en faveur du platonisme en se fondant sur le fait incontestable de l'universalité de leur discipline. En effet, dans des cultures très éloignées les unes des autres dans le temps et dans l'espace, les réflexions mathématiques aboutissent aux mêmes conclusions, aux mêmes vérités objectives. Dans le cas des nombres premiers, par exemple, on a une donnée intéressante, que nous pourrions qualifier de « vestige mathématique » : l'os d'Ishango.

Nous pouvons voir dans l'os des petites entailles sous la forme de petits segments rectilignes. Leur examen détaillé a permis de conclure qu'il ne s'agissait pas d'un outil quelconque, mais d'un système de numération qui permettait de compter. Dans ce cas, il est probable que la pointe de quartz servait pour noter, d'une façon ou d'une autre, l'état des

comptes. En d'autres termes, le manche en os pouvait avoir la fonction d'une table primitive de calculs. La répartition des entailles dans cette colonne suggère des opérations d'addition et de multiplication dans un système de numération en base 12. Les nombres à droite sont tous impairs, mais le plus incroyable est que tous les nombres de gauche sont premiers, concrètement ceux compris entre 10 et 20. Il serait très imprudent d'attribuer la répartition de ces entailles au simple hasard ou à une quelconque autre fonction qui n'impliquerait pas un calcul numérique avancé. Rappelons que le concept de nombre premier requiert un processus d'abstraction qui va bien au-delà des seules techniques de décompte.

À la question de savoir si les vérités mathématiques existent indépendamment de l'être humain, il y aurait une troisième réponse, qui constitue une sorte de solution de conciliation : on peut en effet admettre que, certes, ces objets mathématiques susceptibles d'être découverts existent, mais qu'il s'agit d'« objets mentaux » dont nous héritons avec le paquet génétique. Dans ce cas, il devrait exister dans la nature une forme primitive de ces configurations. En ce qui concerne la capacité à compter, on rencontre dans le règne animal de nombreux exemples d'espèces qui peuvent le faire avec une certaine précision. Les guêpes solitaires, par exemple, sont capables de compter le nombre de chenilles vivantes qu'elles laissent comme aliment pour leurs larves dans les loges dans lesquelles elles ont entreposé les œufs : toujours exactement 5, 12 ou 24. Parmi les espèces qui appartiennent à la classe *Eumenes*, nous rencontrons un cas encore plus incroyable : la guêpe sait si un mâle ou une femelle sortira de l'œuf. Nous n'avons pas de connaissances en ce qui concerne le mécanisme qu'elle utilise pour vérifier le sexe de sa descendance, d'autant plus que les cellules dans lesquelles elle pond et dépose l'aliment ne présentent aucun signe distinctif apparent. La guêpe laisse 5 chenilles pour chaque œuf mâle et 10 s'il s'agit d'une femelle. La raison de cette disparité est que les guêpes femelles sont plus grandes que les mâles.

Les femelles des guêpes solitaires posent les œufs dans des petites cellules dans lesquelles elles laissent aussi des chenilles anesthésiées au préalable afin que, après l'éclosion, leurs larves puissent s'en nourrir. Le plus surprenant est que ces guêpes laissent toujours le même nombre de chenilles, et elles prennent en compte le sexe futur de l'œuf, mâle ou femelle, ce qui détermine le nombre de « victimes » dont disposera la descendance.

Même en ce qui concerne un concept plus élaboré, comme celui de nombre premier, il existe un curieux exemple : les espèces de cigales dénommées *Magicicada septendecim* et *M. tredecim*. Les noms spéciaux *septendecim* et *tredecim* signifient, respectivement, 17 et 13, et font référence aux cycles vitaux des deux cigales. Les deux sont des nombres premiers et les zoologues ont élaboré différentes théories qui expliquent le choix d'un nombre premier d'années pour le cycle de vie de ces insectes.

Prenons comme exemple *Magicicada septendecim*. Cette cigale vit sous terre à l'état de nymphe et s'alimente de sève en suçant les racines des arbres. Elle passe 17 ans dans cet état et remonte ensuite à la surface pour se transformer en insecte adulte, étape qui dure seulement quelques jours, durant lesquels elle se reproduit puis meurt. La théorie qui explique un tel comportement est la suivante : parmi les ennemis de la cigale adulte existe un parasite dont le cycle de vie est de deux ans. Si le cycle de vie de la cigale était un multiple de 2, les deux espèces finiraient par coïncider tous les 2, 4, 8… ans. La même chose arriverait avec les autres multiples quelconques. Mais si le cycle de vie était un nombre premier d'années assez grand, comme 17 dans notre cas, alors le parasite et la cigale ne pourraient coïncider que tous les 34 ans, puisque 34 est le premier multiple de 17. Dans le cas hypothétique où le cycle de vie du parasite serait de 16 ans, la probabilité de se rencontrer aurait lieu tous les $16 \cdot 17 = 272$ ans.

Il est tout à fait possible qu'avec le temps l'étude du comportement animal nous donne davantage d'exemples d'espèces qui « savent compter ». De tels raisonnements peuvent paraître banals, mais le plus important dans cette affaire, c'est que, bien que les objets mathématiques, comme les nombres premiers, soient une création mathématique, l'explorateur puisse les vivre et les sentir comme s'ils avaient une existence propre.

Le crible d'Ératosthène

La recherche des nombres premiers a toujours constitué un sujet épineux. L'une des premières méthodes connues est attribuée à Ératosthène de Cyrène (273-194 av. J.-C.), mathématicien, astronome et géographe grec, qui fut directeur de la Bibliothèque d'Alexandrie. Cette méthode est connue sous le nom de « crible d'Ératosthène ». Nous allons voir comment elle s'applique aux cent premiers nombres naturels.

En premier lieu, il faut construire une table avec tous les nombres naturels, disons ceux entre 1 et 100, pour fixer les idées. On commence ensuite à éliminer tous ceux qui sont multiples de deux : 4, 6, 8, 10… ; puis ceux qui sont multiples de trois : 6 (déjà éliminé), 9, 12, 15… ; puis ensuite les multiples de cinq et de sept.

~~1~~	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

Les nombres non éliminés sont tous premiers.

On observe que le crible se termine quand on arrive au nombre 10, soit la racine carrée de 100. En général, pour trouver tous les nombres premiers inférieurs à un nombre N donné, il suffit de réaliser le crible pour tous les nombres inférieurs ou égaux à $\sqrt{N}$. Il s'agit là d'une méthode pour trouver les nombres premiers inférieurs à un autre donné. Cette méthode est toujours utilisée actuellement, plus de deux mille ans après sa création, pour trouver des nombres premiers petits, inférieurs à dix mille millions.

LES DIMENSIONS DE LA TERRE

Le nom d'Ératosthène est lié au crible des nombres premiers qui porte d'ailleurs son nom. Cependant, ce ne sont pas là ses travaux les plus importants. De fait, Ératosthène est entré dans l'histoire de la science pour avoir été le premier à calculer les dimensions de la Terre. Avec les moyens techniques disponibles au IIIe siècle av. J.-C., il calcula la circonférence polaire avec une marge d'erreur inférieure à 1 %.

Planisphère qui montre le monde connu selon Ératosthène. Le savant grec fut le premier à utiliser une division en parallèles réguliers, alors que les méridiens étaient séparés de manière irrégulière.

Combien y a-t-il de nombres premiers ?

Si nous voulons commencer à réfléchir sur la nature des nombres premiers pour chercher une relation entre eux ou une règle quelconque qui nous permette de prédire à quel moment apparaîtra le suivant, il nous faut d'abord disposer d'une liste de ces nombres. Le tableau suivant, obtenu à partir du crible d'Ératosthène, montre les nombres premiers qui sont compris parmi les mille premiers nombres entiers naturels.

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	103	107	109	113	127	131
137	139	149	151	157	163	167	173
179	181	191	193	197	199	211	223
227	229	233	239	241	251	257	263
269	271	277	281	283	293	307	311
313	317	331	337	347	349	353	359
367	373	379	383	389	397	401	409
419	421	431	433	439	443	449	457
461	463	467	479	487	491	499	503
509	521	523	541	547	557	563	569
571	577	587	593	599	601	607	613
617	619	631	641	643	647	653	659
661	673	677	683	691	701	709	719
727	733	739	743	751	757	761	769
773	787	797	809	811	821	823	827
829	839	853	857	859	863	877	881
883	887	907	911	919	929	937	941
947	953	967	971	977	983	991	997

Un examen préliminaire nous permet de constater que les nombres premiers sont tout à fait imprévisibles. Il y a, par exemple, plus de nombres premiers entre 1 et 100 qu'entre 101 et 200. Entre les nombres 1 et 1.000, il y a 168 nombres premiers. Nous pouvons penser que si notre table était bien plus grande encore, nous verrions comment la quantité de nombres premiers augmente à mesure que nous avançons de mille unités en mille unités. Mais non. Il existe actuellement des tables

immensément grandes et l'on sait que, par exemple, entre les mille unités qui vont de 10^{100} à $10^{100} + 1.000$, il y a seulement 2 nombres premiers. Et il s'agit là de nombres de plus de cent chiffres !

Il est clair que pour pouvoir trouver une règle, le mieux serait de disposer d'une table exhaustive avec tous les nombres premiers. Tous ? Et s'ils étaient nombreux ? Peu importe : avec les moyens dont nous disposons actuellement, il est possible de les soumettre à tous les types de cribles et de tests permettant de trouver la règle. Car lorsqu'il s'agit d'ensembles finis, aussi grands soient-ils, il est toujours possible de trouver une règle, ou tout du moins d'en inventer une qui corresponde. Mais tout change radicalement quand il s'agit d'ensembles infinis. Par conséquent, il est très important de savoir s'il existe une infinité de nombres premiers. Cette question fut aussi posée par Euclide. Sa manière d'y répondre est si ingénieuse et mathématiquement intuitive que cela vaut la peine de l'étudier en détail.

Partons d'une petite liste de nombres premiers consécutifs, par exemple :

$$2, 3, 5.$$

À présent, faisons le produit de ces nombres entre eux :

$$2 \cdot 3 \cdot 5 = 30.$$

Ajoutons une unité au résultat :

$$2 \cdot 3 \cdot 5 + 1 = 30 + 1 = 31.$$

Il est clair que la division de 31 par n'importe lequel des trois nombres premiers de la liste initiale 2, 3, 5 aura pour reste 1 :

$$31/2 = 15 \text{ reste } 1 \,;\, 2 \cdot 15 + 1 = 31$$
$$31/3 = 10 \text{ reste } 1 \,;\, 3 \cdot 10 + 1 = 31$$
$$31/5 = 6 \text{ reste } 1 \,;\, 5 \cdot 6 + 1 = 31.$$

Cela garantit qu'il n'est divisible par aucun d'eux. Cela arrive tout le temps : si nous partons d'une liste de nombres premiers consécutifs, quand nous les multiplions entre eux et ajoutons une unité au résultat, le nombre obtenu n'est divisible par aucun de ceux de la liste. Ce petit détail *a priori* tout simple est le cœur même de la démonstration d'Euclide.

Le nombre 31 est un nombre premier qui ne se trouve pas dans la liste initiale ; en effet, elle n'était pas complète. Prenons par exemple la liste suivante :

$$\{2, 3, 5, 7, 11, 13\}.$$

Faisons le produit de tous les nombres entre eux et ajoutons une unité :

$$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30.030 + 1 = 30.031.$$

Ce dernier n'est pas un nombre premier car il peut s'exprimer comme le produit de deux nombres :

$$30.031 = 59 \cdot 509.$$

Euclide avait déjà démontré que tout nombre naturel pouvait se décomposer de manière unique comme un produit de facteurs premiers. Si nous appliquons ce résultat au nombre 30.031, qui est un nombre composé, il est clair qu'avec les nombres premiers de la liste $\{2, 3, 5, 7\}$ nous n'avons pas ce qu'il nous faut pour effectuer la décomposition en facteurs. Il manque donc dans cette liste des nombres premiers.

La conclusion est la suivante : aussi longue que soit la liste initiale de nombres premiers, en effectuant l'opération de multiplication entre eux et l'addition d'une unité, le résultat est un nouveau nombre qui correspond à l'une des deux situations suivantes :

1) Il s'agit d'un nombre premier qui n'était pas dans la liste.
2) Il s'agit d'un nombre composé et dans sa décomposition figurent des nombres premiers qui n'étaient pas dans la liste.

De telle sorte que la liste, à moins d'être infinie, est toujours incomplète.

Malheureusement, cette méthode n'est pas une méthode pour obtenir des nombres premiers, bien qu'elle constitue un point de départ très important car elle délimite une dimension du problème et une perspective sans laquelle il serait impossible d'envisager la moindre stratégie. Nous pourrions penser qu'il n'est pas si important de démontrer qu'il existe une infinité de nombres premiers, car c'est une donnée intuitive. Mais il faut rester très prudent avec les nombres premiers : ils sont si « étranges » qu'il pourrait bien arriver un moment où ils disparaissent ! Le théorème d'Euclide nous garantit cependant que cela n'arrivera pas.

Chapitre 2

La règle inaccessible des nombres premiers

Comme nous l'avons déjà vu, la question des nombres premiers est l'une des questions majeures dont l'étude nous renvoie aux commencements mêmes des mathématiques et nous conduit, à travers un parcours d'une complexité croissante, jusqu'aux sommets de la science contemporaine. Cette étude s'avère donc très précieuse pour comprendre la fascinante et intrigante histoire de la discipline, et en particulier la façon dont elle s'est construite sur un ensemble de vérités acceptées. Dans le présent chapitre, nous verrons de quelle manière les générations successives de mathématiciens ont fouillé l'univers des nombres à la recherche d'une règle expliquant l'apparition des nombres premiers (une règle qui, au fil du temps, ne cessait de se dérober). Nous examinerons aussi de manière plus détaillée les questions relatives au contexte historique dans lequel ils ont travaillé, ainsi que la façon dont ce travail se confondait avec des pratiques mystiques et quasi religieuses, dans une curieuse synthèse située aux antipodes de l'idéal scientifique contemporain. Ce n'est que petit à petit que ce terrain fut déserté, au profit de nouveaux paradigmes, comme ceux auxquels Fermat et Euler donnèrent naissance aux XVII^e^ et XVIII^e^ siècles et que nous traiterons en détail dans le prochain chapitre.

Le génie en contexte

Comme dans toute histoire de la science, dans celle des nombres premiers apparaissent des noms propres associés à de grandes découvertes. Mais ces personnages n'existeraient pas sans le tissu culturel qui leur servait d'appui. Les « génies » ne surgissent pas du néant, mais au contraire d'un bouillon de culture adéquat. D'où la nécessité d'examiner aussi bien les paradigmes qu'engendre le tissu culturel que les organisations sociales qui ont servi de moteur pour que la science puisse continuer à avancer.

Dans la décennie des années 1930, commencèrent à apparaître dans les librairies spécialisées une série de livres de mathématiques qui étaient signés Nicolas Bour-

LE GÉNÉRAL MATHÉMATICIEN

Le général Charles Denis Bourbaki a inspiré des patriotes et des mathématiciens.

D'où vient le nom de Bourbaki ? Selon la version de l'un de ses membres les plus éminents, André Weil, l'idée vient d'un canular de leur passé d'étudiants. Apparemment, Cartan et Weil, entre autres, assistèrent à un séminaire animé par un étrange mathématicien, au nom à consonance nordique, à l'accent indéfinissable et à l'aspect saugrenu, durant lequel il énonça le théorème de Bourbaki, au contenu aussi stupéfiant qu'incroyable : un théorème que l'on était supposé devoir au général français Charles Denis Bourbaki (1816-1897), une figure célèbre de la guerre franco-prussienne. Le séminaire tout entier était une farce monumentale orchestrée par un étudiant, Raoul Husson, mais Cartan et Weil trouvèrent dans la figure de ce général, de surcroît mathématicien, et dans son nom d'origine grecque le pseudonyme parfait sous lequel présenter leur « reconstruction euclidienne » des mathématiques.

baki, un auteur jusqu'alors inconnu. Cette série connut au sein de la communauté mathématique un certain succès, dû, entre autres choses, à ce qu'elle permettait aux étudiants de disposer d'un bon traité d'analyse mathématique, qui n'existait pas jusqu'alors. Mais son objectif n'était pas seulement d'approvisionner le marché des manuels scolaires. Il s'agissait aussi de réussir à unifier les connaissances dans certains secteurs des mathématiques, comme l'algèbre ou l'analyse, des secteurs dans lesquels régnait un désordre dû à l'énorme quantité de nouveaux résultats obtenus dans les années précédentes. Ce fut une surprise pour beaucoup de découvrir qu'en réalité il n'existait pas d'individu portant le nom de Nicolas Bourbaki. C'était le nom choisi par un groupe de mathématiciens, parmi lesquels Henri Cartan (1904-2008) et André Weil (1906-1998), pour mener à bien une reconstruction des mathématiques, dans un esprit purement philanthropique. Le groupe Bourbaki est bien connu, car il s'agit d'un fait récent. Mais de tels regroupements sous un nom commun ont pu se produire dans l'Antiquité, sans que nous ayons les moyens de le savoir.

Les « centres d'information »

Ce qui est remarquable, c'est le fait que la connaissance scientifique en général et mathématique en particulier ne soit jamais le fait d'une seule personne. Il est certain que nous devons de grandes découvertes à certains individus, mais toujours au sein d'une communauté mathématique. Cela suppose l'existence d'écrits, d'écoles, de lieux de réunion et de centres avec la capacité de regrouper l'information et d'établir des réseaux de communication entre les scientifiques. Actuellement, les possibilités de communication ont atteint les niveaux les plus hauts de l'histoire de l'humanité. La communication *on line* permet de partager immédiatement une découverte ou une avancée scientifique avec n'importe quelle personne intéressée. Cependant, la nécessité de stocker l'information afin que d'autres puissent y avoir accès est un fait commun à toutes les époques de l'Histoire ; c'est ce qui constitue le legs culturel d'une société. De ce point de vue, les nombres premiers constituent un objet d'investigation singulier. On les retrouve partout et à toutes les époques. Ils sont les protagonistes d'une œuvre qui remonte à la nuit des temps et qui n'est pas encore terminée. Suivre leurs traces ne nous permet pas seulement de recueillir des informations sur leur nature mathématique, mais aussi d'assister à l'évolution de ces espaces de rencontre que nous pourrions qualifier, en employant une terminologie moderne, de « centres d'information ». Le cas de la Bibliothèque d'Alexandrie est, en ce sens, un exemple paradigmatique.

Alexandrie

Ptolémée I^{er}, ou Sôter, établit sa capitale à Alexandrie. Entouré des meilleurs architectes du monde, il fit de la ville une merveille architecturale. Il construisit un long pont jusqu'à l'île de Pharos et y fit bâtir une tour qui durant mille ans servit de guide aux navigateurs de la Méditerranée. Il fonda ensuite une bibliothèque dont la renommée a traversé l'Histoire. Un phare et une bibliothèque étaient les deux éléments nécessaires pour qu'Alexandrie devienne le centre d'information le plus important du monde antique, un objectif que Ptolémée était disposé à atteindre coûte que coûte. Il commença par sauver de l'exil Démétrios, un tyran qui avait été nommé gouverneur d'Athènes par Cassandre, l'un des trois héritiers d'Alexandre. Démétrios était celui qui avait continué à faire vivre la fondation du Lycée créée par Aristote. Même s'il s'était pris au jeu des intrigues du pouvoir, sa véritable vocation était la transmission du savoir. C'est donc avec grand plaisir qu'il reçut

l'invitation de Ptolémée à venir fonder à Alexandrie une bibliothèque capable de rassembler et de classifier dans un centre unique tout le savoir du monde civilisé.

Le port d'Alexandrie était formé de petites îles protégées par des digues, avec une unique sortie vers la mer, qui était le grand canal par lequel entraient et sortaient les navires. La protection face aux intrus était quasi totale. L'un des quartiers les plus importants auxquels il était possible d'accéder était le Brucheïon, situé en plein cœur de la ville, qui abritait les principaux palais. Parmi eux, le « Musée » (*Mouseïon*), dédié aux Muses, était consacré à la musique et aux sciences, c'est-à-dire aux mélodies, aux rythmes et aux nombres. Quand Démétrios prit conscience du fait que ce centre du savoir était soutenu par l'un des rois les plus puissants du monde connu, il n'hésita pas un instant à en prendre la direction. La première chose qu'il fit fut de solliciter de la part d'Athènes le prêt des textes de penseurs et d'écrivains les plus importants qu'avait pu produire la culture hellénique. Il en fit des copies qu'il renvoya à Athènes et conserva les originaux avec les autres textes que Ptolémée avait réussi à obtenir comme butins de guerre au cours de ses campagnes. Bien que peu orthodoxe, cette méthode s'avéra très efficace pour accroître le volume des ouvrages. Tout navire qui faisait escale au port d'Alexandrie était sommé de fournir tous les textes originaux disponibles à bord pour en faire des copies ; les originaux étaient destinés à la Bibliothèque et les copies étaient remises aux navires. C'est ainsi que naquit la « bibliothèque des bateaux ». Mais ceux qui détenaient le pouvoir et les richesses en Méditerranée comprirent rapidement ce qui se passait et commencèrent à se méfier. Démétrios proposa alors une incitation aux marchands : s'ils souhaitaient profiter des énormes richesses que pouvait leur offrir le port d'Alexandrie, ils devaient apporter, en guise de sauf-conduit, des manuscrits provenant de leurs ports d'origine. Peu importait qu'il s'agisse de traités d'ingénierie, de philosophie, d'art, de mathématiques ou de musique, ils constituaient tous un apport supplémentaire de connaissances. Le marché était que des copies seraient alors effectuées et rendues aux marchands alors que les originaux resteraient dans la Bibliothèque. Les copies étaient conservées dans les étuis d'origine et la majorité des propriétaires n'y virent que du feu, et quand bien même ils remarquaient la différence, cela ne semblait guère leur importer. Le fait est historiquement avéré : Alexandrie fit travailler le plus grand nombre de copistes qu'on eût jamais rassemblés jusque-là.

Mais Alexandrie n'était pas seulement un centre où se stockaient les « archives de l'information » : elle constituait aussi un centre où ces données étaient « gérées ». Ce centre attira très vite de nombreux maîtres de toutes les disciplines qui donnaient des cours et partageaient leur savoir avec leurs condisciples. Des salles furent

LA RÈGLE INACCESSIBLE DES NOMBRES PREMIERS

Alexandrie fut le centre d'information le plus important de l'Antiquité. Ci-dessus, la gravure représente une scène à l'intérieur de la fameuse Bibliothèque. À gauche, des pièces de monnaie romaines frappées de l'image du Phare, l'autre merveille de la ville.

construites pour atteindre un tel objectif, mais aussi des petits logements, des portiques et des promenades aménagées dans les jardins.

On peut raisonnablement penser qu'au cours du temps se formèrent différentes écoles. Parmi elles – pourquoi pas – l'école d'Euclide, qui, à l'instar du groupe Bourbaki, put réunir les connaissances mathématiques alors disponibles pour les convertir en une école de pensée, c'est-à-dire en une façon de penser et de faire en mathématiques, dont notre époque actuelle recueille encore les fruits. Souvenons-nous que, deux mille ans plus tard, on continue d'enseigner à l'école la même géométrie que celle qui naquit dans les salles et les jardins d'Alexandrie.

Intervalles

La première chose qui retint l'attention des mathématiciens de l'Antiquité qui étudiaient les nombres premiers fut l'absence de règles quant à leur apparition dans la succession des nombres entiers naturels. En outre, les choses ne sont pas plus claires en ce qui concerne leur absence, c'est-à-dire la manière dont ils cessent d'apparaître. Par conséquent, ils peuvent être relativement proches, ou, au contraire, très éloignés les uns des autres. Par exemple, si nous prenons en compte les nombres premiers qui se situent parmi les cent premiers nombres entiers naturels :

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,

nous observons que les huit premiers apparaissent quasiment à la suite. Il y en a huit parmi les vingt premiers et, au contraire, il n'y en a aucun entre 89 et 97.

Si nous considérons maintenant les nombres premiers compris entre 100 et 200 :

101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167,
173, 179, 181, 191, 193, 197, 199,

nous observons des intervalles importants, comme celui qui sépare 181 de 191, composé de neuf nombres consécutifs.

La question que nous pouvons nous poser est donc : est-il possible qu'il existe des intervalles extraordinairement grands, qu'il puisse y avoir, par exemple, cinquante mille nombres consécutifs sans l'apparition du moindre nombre premier ? L'univers des nombres premiers est suffisamment vaste pour qu'on trouve de tels intervalles, c'est-à-dire de très longues séries de nombres dans lesquelles ne se trouve aucun nombre premier. Il ne s'agit pas là d'une simple hypothèse, mais d'un résultat simple à démontrer.

Considérons le produit des quatre premiers nombres entiers naturels :

$$1 \cdot 2 \cdot 3 \cdot 4.$$

Nous pouvons être certains que le nombre $1 \cdot 2 \cdot 3 \cdot 4 + 2$ ne peut être premier car il est divisible par 2. La vérification est très rapide : $1 \cdot 2 \cdot 3 \cdot 4 + 2 = 24 + 2 = 26$, et divisé par 2 cela donne 13.

Il n'était d'ailleurs pas nécessaire de faire la moindre opération pour savoir que le résultat était divisible par 2 car les deux termes de l'opération contenaient le chiffre 2.

De la même manière :

$1 \cdot 2 \cdot 3 \cdot 4 + 3$ ne peut être premier car il est divisible par 3 ;
$1 \cdot 2 \cdot 3 \cdot 4 + 4$ ne peut être premier car il est divisible par 4.

De cette façon, nous avons obtenu trois nombres consécutifs : 26, 27, 28, qui ne sont pas premiers. Si nous voulons maintenant obtenir quatre nombres consécutifs qui ne soient pas premiers, nous faisons :

$1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 + 2 = 122$;
$1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 + 3 = 123$;
$1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 + 4 = 124$;
$1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 + 5 = 125$.

Pour faciliter la lecture, nous représentons le produit de nombres consécutifs par un point d'exclamation :

$1 \cdot 2 \cdot 3 \cdot 4 = 4!$;
$1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 = 5!$

En mathématiques, ce type d'expression a reçu le nom de « factorielle ». Par exemple, la factorielle de 6 est

$$6! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 = 720.$$

Par conséquent, il est plus commode d'écrire les expressions antérieures sous la forme suivante :

$5! + 2$;
$5! + 3$;
$5! + 4$;
$5! + 5$.

De cette manière, nous pouvons écrire des séries de nombres consécutifs qui ne contiennent aucun nombre premier. Par exemple, si nous voulons écrire cent nombres consécutifs de manière à ce qu'aucun d'eux ne soit premier, il faut tout simplement faire comme indiqué ci-après :

101! + 2 ;
101! + 3 ;
101! + 4,
et ainsi de suite jusqu'à 101! + 101.

Cela veut donc dire qu'il existe de très grands intervalles dans lesquels n'apparaît aucun nombre premier. Grâce à la même méthode, nous pourrions construire une série de cinq milliards de nombres consécutifs dans laquelle n'apparaîtrait aucun nombre premier. Cela laisse à penser que les nombres premiers sont de moins en moins nombreux à mesure que nous avançons dans la succession des nombres naturels. Par conséquent, à mesure que nous nous éloignons vers l'infini, il arrivera un moment où il n'y en aura plus.

Cette idée pour le moins tentante répond à une fausse intuition, car nous savons déjà que le théorème d'Euclide garantit qu'il y a une infinité de nombres premiers et que, aussi longue que soit une série de nombres composés, un nombre premier apparaîtra à un moment ou à un autre.

L'USAGE DE LA CALCULATRICE

Il est tentant de créer des programmes qui facilitent le calcul des grands intervalles entre les nombres premiers. De fait, un algorithme serait assez pratique. Mais on doit prendre en compte le fait que, en maniant des factoriels, on effectue un calcul trop rudimentaire pour être efficace, car les factoriels ont une vitesse de croissance vertigineuse. On peut le vérifier avec n'importe quelle calculatrice domestique qui dispose de cette fonction (rappelons que le symbole est le point d'exclamation : !). Rien qu'avec les premiers nombres nous obtenons les résultats suivants :

1! = 1 ; 2! = 2 ; 3! = 6 ; 4! = 24 ; 5! = 120 ; 6! = 720 ;
7! = 5.040 ; 8! = 40.320 ; 9! = 362.880 ;
10! = 3.628.800.

Un bon nombre de calculatrices ne peuvent plus réaliser cette fonction à partir de 70.

Le sens du rythme

Il existe une situation qui se produit souvent dans certains concerts, lorsque le public s'anime et applaudit au rythme de la musique. Au début, tout semble bien fonctionner, mais petit à petit on remarque qu'apparaît un manque de synchronisation entre le rythme du public et le rythme que tente d'insuffler le percussionniste. La synchronisation peut se maintenir plus ou moins dans le cas de rythmes simples, mais il est rare que ce soit le cas lorsqu'il s'agit de rythmes compliqués. Nous pouvons transposer cette analogie pour comprendre l'effort des mathématiciens à l'heure d'imposer un rythme à la série des nombres premiers : quelque chose comme « Un, deux, trois… OK ! » Cela ne fonctionne pas : les nombres premiers n'apparaissent pas une fois sur quatre. Essayons autre chose : « Un, deux, trois, vingt, cent… OK ! » Cela ne fonctionne pas non plus. Et nous pourrions essayer ainsi à l'infini. À ce jour, personne ne sait si ce « groupe » de nombres suit un rythme diablement compliqué ou si, au contraire, il n'est animé par aucun rythme d'aucune sorte.

Comment faire pour déterminer la rythmique, la logique interne, d'une suite de nombres ? Il existe plusieurs manières de procéder. L'important est que, lorsqu'on réussit, on doit être capable de prédire quel est le nombre qui suit un nombre donné. Par exemple, dans le cas de la suite

2, 4, 6, 8...

cela ne pose guère de problème de savoir que le nombre suivant est 10.
Dans le cas de la suite

1, 3, 5, 7...

il est aussi très facile d'affirmer que le nombre suivant est 9. La première est la suite des nombres pairs et la seconde la suite des nombres impairs. Un autre exemple :

2, 3, 5, 9, 17…

Ici, le nombre suivant est obtenu en multipliant le précédent par 2 et en retranchant 1 au résultat.

Ce type de suites s'utilise très fréquemment comme passe-temps et elles font souvent partie également des exercices de certains tests d'intelligence.

En mathématiques, le sujet est considéré comme clos lorsqu'on obtient ce qui s'appelle « l'expression du terme général » a_n, une expression qui nous donne la va-

leur de chaque terme suivant la valeur de n. Par exemple, dans la suite des nombres pairs, nous aurions :

$$a_n = 2n$$

Si $n = 1$ $\quad a_1 = 2 \cdot 1 = 2.$
Si $n = 2$ $\quad a_2 = 2 \cdot 2 = 4.$
Si $n = 3$ $\quad a_3 = 2 \cdot 3 = 6.$

Dans le cas de la suite des nombres impairs, nous aurions comme expression du terme général de la suite :

$$a_n = 2n + 1.$$

Avec cette expression, nous pouvons connaître la valeur d'un terme quelconque. Si nous souhaitons savoir combien vaut le terme qui occupe le rang 27, nous devons simplement appliquer cette expression pour $n = 27$:

$$a_{27} = 2 \cdot 27 + 1 = 55.$$

Connaître la formule du terme général revient à avoir découvert la loi de formation de la suite. De ce fait, si nous connaissons l'expression du terme général, nous connaissons la loi de formation, et trouver la valeur d'un terme quelconque de la suite n'est donc plus un problème. Cependant, lorsque la question est posée en sens inverse, le problème peut devenir infiniment plus compliqué. Par exemple, considérons la suite de nombres suivante :

$$\frac{2}{4}, \frac{5}{7}, \frac{10}{12} \ldots$$

L'expression du terme général n'est pas aisée à trouver. La voici ci-après :

$$a_n = \frac{n^2 + 1}{n^2 + 3}.$$

Pour trouver les trois premiers termes, il suffit tout simplement de remplacer n par les nombres :

$$a_1 = \frac{1^2 + 1}{1^2 + 3} = \frac{2}{4};$$
$$a_2 = \frac{2^2 + 1}{2^2 + 3} = \frac{5}{7};$$
$$a_3 = \frac{3^2 + 1}{3^2 + 3} = \frac{10}{12}.$$

Il s'agit là d'un des plus grands efforts que les mathématiciens aient effectué au long de l'Histoire dans l'étude des nombres premiers : des essais répétés pour vérifier si les nombres premiers répondent à une quelconque règle, avec leur lot de frustrations et d'échecs en tout genre. Comment est-il possible que cette chaotique collection de nombres n'obéisse qu'à la loi du hasard ? Cela étant, il faut tout de même nuancer le propos lorsqu'on parle d'échec en mathématiques. Si les spécialistes échouent, c'est qu'ils n'ont pas réussi à atteindre leurs objectifs initiaux, mais dans leurs démonstrations ils tracent bien souvent des chemins nouveaux, inventent d'autres façons de raisonner en mathématiques et ouvrent des portes qui mènent à d'autres paradigmes. Bien souvent, l'objectif de départ fonctionne comme un prétexte pour se poser de nouveaux problèmes. En ce sens, les nombres premiers ont été et restent l'une des sources les plus intarissables en paradoxes et conjectures de toutes sortes.

Nombres premiers jumeaux

S'il n'est pas possible d'établir une loi de formation générale, on peut au moins essayer d'étudier le comportement de certains nombres premiers qui possèdent des caractéristiques spéciales. Imaginons que nous sommes assis devant une fenêtre. Nous voyons défiler un nombre infini de personnes différentes. Nous savons qu'il y a des femmes et des hommes, mais nous n'arrivons pas à établir une quelconque règle qui nous permette de prédire le moment où passera l'une ou l'autre. Mais soudain, un jour, nous notons un élément caractéristique : nous remarquons que, de temps à autre, passent des hommes avec des chapeaux, des personnes avec des lunettes et d'autres avec des parapluies. Nous essayons alors de trouver une règle qui définisse l'apparition de groupes précis, d'observer, par exemple, si les hommes qui portent un chapeau apparaissent après que sont passées 100 femmes ou si, chaque fois que passe un homme portant un chapeau, lui succède une femme. N'importe quel détail dont nous puissions déduire une règle est bon à prendre. Or, il est possible que nous trouvions une règle et qu'elle fonctionne, puis que tout d'un coup, après le passage de trois millions de personnes, elle ne fonctionne plus. Nous nous exclamerons alors : « Oh ! presque ! » Ce « presque » nous amènera à dire que « les choses fonctionnent comme si… », une expression très fréquente dans l'histoire des nombres premiers.

Il a cependant été possible de caractériser certaines familles de nombres premiers (de fait, il en existe une douzaine), qui ont permis des avancées tout au long

LA SOLITUDE DES NOMBRES PREMIERS

Les nombres premiers peuvent être séparés par des millions et des millions de nombres ou bien par un seul. Ils ne peuvent cependant être plus proches : en aucun cas ils ne peuvent être consécutifs, à l'exception de 2 et 3. Cette donnée a fourni la métaphore qu'utilise le titre d'un classique de la littérature contemporaine : *La solitude des nombres premiers*, de Paolo Giordano. Dans l'un des paragraphes du roman, cette métaphore est explicite : « Assez tôt dans l'enseignement secondaire, Mattia avait étudié le fait que, parmi les nombres premiers, certains étaient encore plus spéciaux que d'autres. Les mathématiciens les appellent « nombres premiers jumeaux » : il s'agit de couples de nombres premiers qui sont ensemble ou, pour mieux dire, presque ensemble car entre eux se trouve toujours un nombre qui les empêche de se toucher pour de vrai. Des nombres comme 11 et 13, 17 et 19, ou 41 et 43. Mattia pensait qu'Alice et lui étaient ainsi, deux premiers jumeaux, seuls et perdus, ensemble mais pas assez ensemble pour se toucher pour de vrai. »

de l'Histoire. Pour le moment, nous allons nous attarder sur quelques couples singuliers de nombres premiers, dont les caractéristiques nous aideront à comprendre un peu mieux les problèmes mathématiques que posent ces nombres erratiques.

Les nombres premiers 2 et 3 se suivent, mais à partir du nombre 3, il n'existe plus de nombres premiers consécutifs. En effet, tout nombre premier supérieur à 2 est impair ; le nombre qui suit est forcément pair, et n'est donc pas premier. En vertu de quoi, la plus grande proximité entre deux nombres premiers plus grands que 2, c'est la séparation par un seul chiffre.

Parmi les cent premiers nombres entiers naturels, on trouve les couples suivants, tous séparés par deux unités :

(3, 5) (5, 7) (11, 13) (17, 19) (29, 31) (41, 43) (59, 61) et (71, 73).

On appelle ces couples « premiers jumeaux » ou simplement « jumeaux ».

Les jumeaux répondent à la structure $(p, p + 2)$, où p est un nombre premier.

Ci-dessous la liste de tous les nombres premiers jumeaux qui existent parmi les mille premiers nombres entiers naturels :

(3, 5),	(5, 7),	(11, 13),	(17, 19),	(29, 31),
(41, 43),	(59, 61),	(71, 73),	(101, 103),	(107, 109),
(137, 139),	(149, 151),	(179, 181),	(191, 193),	(197, 199),
(227, 229),	(239, 241),	(269, 271),	(281, 283),	(311, 313),

(347, 349),	(419, 421),	(431, 433),	(461, 463),	(521, 523),
(569, 571),	(599, 601),	(617, 619),	(641, 643),	(659, 661),
(809, 811),	(821, 823),	(827, 829),	(857, 859),	(881, 883).

Nous savons que les nombres premiers jumeaux commencent à se raréfier à mesure que l'on avance dans la suite des nombres entiers naturels. Cependant, il existe une certaine constance. Des méthodes de calcul sophistiquées permettent d'exhiber des nombres premiers jumeaux extraordinairement grands. « Les plus grands nombres premiers jumeaux connus (à la date d'août 2009) sont ceux formés par les nombres $65516468355 \cdot 2^{333333} - 1$ et $65516468355 \cdot 2^{333333} + 1$; chacun est composé de cent mille trois cent cinquante-cinq chiffres. Ce type de découverte amène les mathématiciens à supposer qu'il existe une infinité de nombres premiers jumeaux, une hypothèse que personne n'a encore réussi à démontrer.

Lorsqu'on observe la liste de tous les nombres premiers parmi les cent premiers nombres entiers naturels, un autre groupe de nombres premiers retient l'attention : c'est le groupe 3, 5, 7. Soit p un nombre premier, ces trois nombres répondent à la structure $(p, p + 2, p + 4)$. C'est un groupe qui pourrait s'appeler « les triplés », mais que l'on nomme « triplet ». En réalité, il n'était même pas nécessaire de lui donner une quelconque appellation : ce triplet est en effet unique. Heureusement qu'il s'agit là d'un sujet clos, sinon les triplets auraient donné lieu eux aussi à d'autres conjectures qui ne seraient certainement pas résolues. »

SÉPARATIONS INFINIES

Les nombres premiers jumeaux ont donné lieu à de multiples hypothèses, en plus de celle qui affirme qu'ils sont infinis. L'une d'entre elles, plus générale, fut établie en 1849 par le mathématicien français Alphonse de Polignac (1817-1890). Une hypothèse selon laquelle il existe pour tout C une infinité de couples de nombres premiers qui sont séparés par $2 \cdot C$ nombres composés. C'est-à-dire qu'il existe une infinité de nombres premiers séparés par quatre nombres composés, par six nombres composés, par huit nombres composés, et ainsi de suite. Dans le cas de $C = 1$, il s'agit des nombres premiers jumeaux.

Magie et mathématiques

Nous avons souligné l'importance qu'eurent et ont toujours les centres d'information tout au long de l'Histoire. Nous devons maintenant mettre l'accent sur un second élément qui revêt une certaine importance quand nous parcourons l'histoire des mathématiques, en particulier quand il s'agit des nombres. Il s'agit de la possible relation qui aurait existé entre la magie et les mathématiques. En parlant de magie, nous nous référons à une partie de la tradition historique des mathématiques qui est communément appelée « arithmologie ». Il existe une relation entre les mathématiques et l'arithmologie similaire à celle qui a existé entre l'astronomie et l'astrologie ou entre la chimie et l'alchimie. De nos jours, ces couples sont dissociés. Ce ne fut pas le cas tout au long de l'Histoire. Ils ont parfois formé des mariages de convenance qu'on ne peut négliger si l'on veut adopter un point de vue historique sur ce que supposait une certaine « vision du monde » à chaque étape du développement de la science.

Les nombres, et par conséquent les nombres premiers, ont fait l'objet de recherches non seulement mathématiques, mais aussi philosophiques et surtout religieuses. Lorsqu'ils s'insèrent dans le tissu culturel, ils le font sous des formes très distinctes : nous les rencontrons dans la Bible, dans les carrés magiques, les sommes magiques, et tout particulièrement dans la conception philosophique de l'école pythagoricienne. Une école pour laquelle les figures géométriques et les nombres sont à l'origine de toute chose.

Nous allons donc à présent rencontrer les mystères et les légendes qui entourent de célèbres mathématiciens, comme Mersenne ou Fermat, dont on dit qu'ils connaissaient des méthodes mathématiques très simples qui leur permirent d'atteindre des objectifs inaccessibles à d'autres. L'historien Libri affirmait que « Fermat savait des choses que nous ignorons, et, pour le rejoindre, il faut des méthodes plus parfaites que les inventions postérieures ». Il ne faut pas oublier que Fermat, à la différence de bien d'autres mathématiciens de son époque, n'était pas le genre de scientifique qui dissimulait systématiquement ses connaissances, mais il aurait pu dissimuler la manière dont il avait obtenu ses résultats.

Nous allons nous plonger dans des époques dans lesquelles la rigueur mathématique, telle qu'elle commence à être conçue au XVIII^e^ siècle, n'avait pas autant d'importance qu'aujourd'hui. Il s'agissait de créer un édifice mathématique à caractère plus pratique que théorique. De ce point de vue, l'enseignement traditionnel, avec tout ce qu'il pouvait comporter de symbolisme mystique, n'était pas un obstacle. Bien au contraire, il offrait un espace dans lequel l'imagination avait libre cours.

En ce sens, nous avons une idée assez erronée de ce que sont les mathématiques, car nous avons aussi une idée erronée des mathématiciens et de la nature de leurs travaux. Non seulement la méconnaissance du travail mathématique génère une méconnaissance de la nature du raisonnement mathématique, mais elle est aussi à bien des égards la source de son impopularité. Le résultat final d'une recherche, qui prend communément la forme d'un théorème, a été ordonné, révisé et peaufiné de telle manière qu'il pâtit bien souvent d'un certain hermétisme pour celui ou celle qui manque de préparation préalable. Ainsi, il est difficile de faire comprendre la beauté que renferment des énoncés certes très techniques et d'une extrême logique. Cependant, ce n'est pas dans ce cadre ordonné que se déroule le travail du chercheur en mathématiques : il se meut, au contraire, à travers une jungle où les sentiers sont à peine visibles et où, de surcroît, il fait nuit noire.

LES NOMBRES ET LE PENTATEUQUE

Les Nombres est le quatrième livre de la Bible, qui forme une partie du Pentateuque et est attribué à Moïse. De manière un peu superficielle, les Nombres est un ouvrage de comptabilité et en ce sens il a une grande valeur historique : il donne le juste compte de toutes les quantités présentes, depuis les chefs de tribu jusqu'aux têtes de bétail qui formaient le cadre historique auquel cet ouvrage fait référence. Mais c'est aussi un livre contenant des clés secrètes pour les initiés qui savent déchiffrer ses messages. En effet, les nombres ne représentent pas seulement des quantités, mais revêtent aussi une signification. Par exemple, 1 symbolise Dieu, 2 l'homme, 3 la totalité des choses, etc. Il est curieux que le chiffre 5 représente une quantité indéfinie, « quelques ». Par exemple, dans le passage de la multiplication des pains, il est dit que Jésus prit cinq pains, c'est-à-dire « quelques » pains. La curiosité réside dans le fait que 5 est le premier nombre d'objets que nous ne pouvons pas comptabiliser d'un seul coup d'œil. On sait que nous pouvons compter, sans faire aucune opération, des groupes jusqu'à quatre objets ; à partir de cinq, nous sommes obligés de les répartir en groupes et de les additionner.

Le Pentateuque est l'un des cinq premiers livres de la Bible.

Le fait que le raisonnement mathématique emprunte les chemins les plus reculés de l'esprit a même réussi à inquiéter les gardiens de l'ordre moral. En sont la preuve ces paroles de saint Augustin : « Le bon chrétien doit être sur ses gardes vis-à-vis des mathématiciens et de tous ceux qui font de vaines prophéties. Le danger n'est pas exclu que les mathématiciens aient conclu un pacte avec le Démon avec pour mission de troubler l'esprit de l'homme pour l'enfermer dans les limites de l'enfer. »

Il existe un troisième point qu'il faut prendre en considération, avec ce que nous avons appelé les centres d'information et les aspects magiques des nombres, si l'on veut comprendre la longue marche des nombres premiers à travers l'Histoire. Il s'agit des qualités exceptionnelles dont disposent certaines personnes à l'égard des nombres. Des qualités qui vont bien souvent de pair avec un goût pour les lettres. La majorité des illustres mathématiciens que nous verrons « rôder » autour des nombres premiers possédaient aussi des qualités extraordinaires pour les langues, ce qui au fond n'a rien de surprenant. Comme nous l'avons expliqué au début de cet ouvrage, les nombres et les lettres sont intimement liés par leur nature abstraite. À l'époque où les outils de calcul étaient pratiquement inexistants, la capacité de calcul mental était indispensable. Il ne s'agit pas seulement de la capacité de calcul numérique, plus exploitée finalement dans le monde du spectacle que dans celui des mathématiques (*cf.* encadré). Des hommes de la stature de Fermat, Mersenne, Euler ou encore Ramanujan possédaient le don magique de « voir » dans l'univers des nombres. Cette capacité leur permettait de découvrir des relations qui leur apparaissaient à eux et à personne d'autre. Ces relations requéraient des démonstrations qui restaient bien souvent hors de leur portée, et dans certains cas, étrangères à leurs intérêts personnels.

LES CALCULISTES

Les calculistes professionnels apparurent au XIX^e^ siècle. Ils devinrent « à la mode » et commencèrent à offrir des spectacles dans les théâtres d'Europe et d'Amérique, auxquels assistait ponctuellement un public adepte de ces prodigieuses prouesses mentales. Zerah Colburn, le premier calculiste professionnel sur lequel nous disposons d'une ample documentation, naquit à Cabot, dans le Vermont (USA), en 1804. Un jour, on lui demanda de calculer le produit de 21.734 par 543. Il répondit quasi instantanément 11801562. Une personne présente lui demanda alors comment il avait fait et il répondit tout naturellement : « J'ai vu que 543 était égal à trois fois 181. J'ai donc multiplié en premier 21.734 par 3 puis le résultat par 181. » Il n'avait besoin que de quelques secondes pour les nombres à cinq chiffres. Tout ceci se passait en 1812 : Zerah Colburn n'avait alors que 8 ans.

Chapitre 3

Les nouveaux paradigmes

Vers le milieu du XVII^e siècle, un important mouvement scientifique fit son apparition en marge des institutions académiques. À cette époque, les premières universités européennes existaient déjà. Elles constituaient des lieux d'accumulation des savoirs, mais la rigidité de leur organisation interne les rendait imperméables aux nouveaux paradigmes. Cela posait un sérieux problème pour tous ceux qui désiraient poursuivre le cours de leurs recherches en marge du cercle académique, puisqu'en dehors de celui-ci ils ne pouvaient recevoir aucun financement. C'est ainsi que débuta l'époque des grands mécènes : les nobles et les puissants propriétaires terriens étaient fiers d'accueillir de grands esprits qui commençaient à ouvrir les portes d'une nouvelle conception du monde. Dans la plupart des biographies apparaissent, aux côtés des noms des célèbres grands scientifiques, ceux de leurs mécènes. Mais cette situation posait, une fois de plus, un problème de communication.

C'est alors que vit le jour un centre qui mérite l'attention du fait du rôle essentiel qu'il joua dans la communication scientifique de l'époque. Ce centre singulier, qui allait donner naissance à la future Académie des sciences (fondée par Colbert en 1666), se trouvait dans une antichambre d'un couvent de Paris. Il fut créé et maintenu en vie par le père Mersenne.

Marin Mersenne

Mersenne naquit le 8 septembre 1588 à Oizé, dans l'actuel département de la Sarthe (France). Nous ne disposons que de peu d'éléments et de dates concernant les premières années de sa vie. Nous savons qu'en 1604 il fut admis en tant qu'interne à La Flèche, un collège fondé en 1603 par des jésuites, où il resta un an. Durant cette période, il se lia d'une profonde amitié avec Descartes, son condisciple, avec qui il maintint une relation amicale toute sa vie.

Marin Mersenne (1588-1648).

L'ORDRE DES MINIMES

Le nom de cet ordre répond au fait que tous ses membres devaient obéir à un minimum de principes religieux. Son objectif était de fuir tout corps doctrinal qui, à partir d'un ensemble de vérités révélées, aboutissait à l'imposition de règles de conduite excessivement restrictives. De fait, l'unique chose que les minimes combattaient sans ambiguïté était l'athéisme. Ils se consacraient fondamentalement à la prière, à l'étude et à l'enseignement, et essayaient par tous les moyens de faire en sorte que leurs convictions religieuses n'interfèrent ni dans l'éducation ni dans le développement scientifique. Preuve en est, le combat acharné que Mersenne mena en faveur de Galilée, tant de sa personne que de sa pensée.

En 1609, il commença ses études de théologie à la Sorbonne, où il obtint son diplôme deux ans plus tard, pour intégrer l'ordre des Minimes. En 1612, il fut nommé prêtre du couvent de l'Annonciation, à Paris. De 1614 à 1618, il donna des cours de philosophie au couvent de Nevers. Il revint ensuite à sa cellule de Paris, où il resta jusqu'à sa mort, le 1er septembre 1648. Animé jusqu'au bout par sa volonté de servir les objectifs de la science, Mersenne fait état dans son testament de sa volonté posthume de donner son corps à la faculté de médecine pour des études anatomiques.

Parmi les premières œuvres de Mersenne à caractère purement théologique, figurent *Quaestiones celeberrimae in Genesim* (1623), *La Vérité des sciences contre les sceptiques ou pyrrhoniens* (1625) et *Questions théologiques, physiques, morales et mathématiques* (1634). Parmi ses œuvres scientifiques, il faut citer *Harmonie universelle* (1636), dans laquelle il établit une formule qui met en relation la longueur d'une corde et la fréquence du son émis par celle-ci.

Cette formule lui permit de créer une échelle dans laquelle tous les intervalles sont égaux, qui rendait inutile le fameux comma pythagoricien, et établissait les bases théoriques de ce qui serait l'une des révolutions majeures de l'histoire de la musique : l'échelle chromatique tempérée.

Les nombres de Mersenne

La grande œuvre scientifique de nature purement mathématique de Mersenne fut *Cogitata physico-mathematica* (1644), dans laquelle apparaît sa célèbre étude sur les nombres premiers.

Dans le prologue de cette œuvre, Mersenne affirme que, d'entre tous les nombres premiers p compris entre 2 et 257, le nombre $2^p - 1$ est premier uniquement si la valeur de p est l'un des nombres suivants :

$$2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257.$$

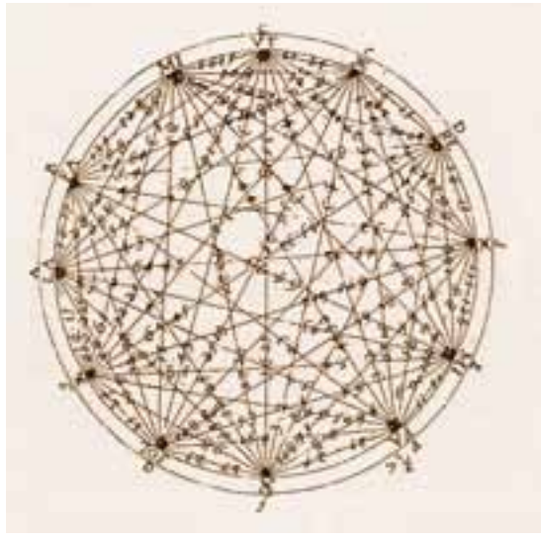
Quand nous prenons 2 et que nous l'élevons au dernier nombre de la liste, le résultat est un nombre de soixante-dix-sept chiffres. Comment Mersenne a-t-il réussi avec les moyens de calcul de l'époque à analyser les nombres pour décider qu'un nombre est premier ? Cela constitue un vrai mystère que personne n'est encore parvenu à résoudre.

Il est facile de démontrer que si $2^p - 1$ est premier, alors p doit être premier (et autrement dit, si p n'est pas premier, alors $2^p - 1$ ne l'est pas non plus). Ce résultat, qui était déjà connu à l'époque de Mersenne, amène à chercher ce qui se passe quand, dans cette expression, on introduit un nombre p, premier. On sait également que $2^p - 1$ est premier pour les valeurs de $p = 2, 3, 5, 7, 13, 17$ et 19, mais non pour $p = 11$.

Il a fallu attendre cent ans pour qu'Euler réussisse à démontrer que $2^{31} - 1$ était premier. En 1947, la liste fut complètement résolue, comme il suit :

$$p = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107 \text{ et } 127,$$

par rapport à la liste initiale, deux nombres manquent à l'appel et trois ont été ajoutés. Malgré tout, ces nombres sont toujours appelés « nombres de Mersenne ». Ils jouent actuellement un rôle important dans les tests dits « de primalité », un ensemble d'algorithmes permettant de décider si un nombre est ou non premier.



Mersenne étudia les vibrations des cordes et créa une échelle divisée en 12 intervalles égaux.

CENTRE NÉVRALGIQUE

La petite cellule dans laquelle Mersenne passa les trente dernières années de sa vie, dans le couvent des Minimes, près de la place Royale, finit par se transformer en un centre névralgique de la science européenne de son temps. On pourrait dire qu'informer Mersenne d'une découverte équivalait à diffuser une publication à travers toute l'Europe. Après sa mort, on retrouva dans sa chambre des documents qui attestent que Mersenne, parmi ses multiples activités de recherche, entretenait soixante-dix-huit correspondances distinctes, dont certaines avec des personnalités du monde scientifique de l'époque aussi célèbres que Torricelli, Descartes, Pascal, Gassendi, Roberval, Beaugrand ou Fermat.

Pierre de Fermat

Fermat (1601-1665) est devenu une authentique légende dans le monde des mathématiques. Ses découvertes, particulièrement dans le domaine de la théorie des nombres, une branche des mathématiques dont on peut le considérer comme le fondateur, l'ont fait entrer dans l'Histoire comme le « prince des amateurs ». De plus, il possédait une maîtrise absolue des langues classiques, le latin et le grec, ainsi que de la majorité des langues européennes qui se parlaient en son temps.

Fermat jouissait d'une position privilégiée qui lui permettait de se consacrer pleinement à sa passion pour les nombres. Il était né dans une famille aisée et ses études de droit législatif lui permirent d'occuper un poste de fonctionnaire à la conciergerie royale du parlement local de Toulouse. L'une des exigences de cette fonction publique était qu'il devait se tenir éloigné de tout type d'activité sociale afin d'éviter la moindre tentation de corruption. Il se maria avec Louise de Long, une cousine de sa mère, avec laquelle il eut trois enfants : l'aîné, Clément-Samuel, est celui qui se chargea de publier son œuvre, tandis que ses deux filles devinrent religieuses dans un couvent.

Fermat ne voyagea presque pas. Son unique déplacement notable l'amena à Paris, où, par l'intermédiaire de Pierre de Carvaci (1600-1684), un influent mathématicien français, il entra en contact avec le père Mersenne au couvent des Minimes.

Il y a des amateurs de fleurs qui consacrent beaucoup de temps à essayer de faire germer de nouvelles espèces, provenant de graines apportées de pays lointains ou de croisements, qui en certaines occasions peuvent produire d'agréables surprises. Fermat, cultivait les nombres. Un matin, il passa dans son jardin mental et y trouva

une nouvelle espèce qui, pour le reste des mortels, fit son apparition de façon quasi miraculeuse. Il ne faisait pas partie de ces mathématiciens qui cachaient leurs résultats, car il les dévoilait à tout le monde, mais il n'expliquait pratiquement jamais comment il les avait obtenus. La propriété « Tout nombre premier de la forme $4n + 1$ est une somme de deux carrés » fut, par exemple, l'un des nombreux résultats qu'il ne démontra jamais et qui fut prouvé par Euler en 1749 après six ans de travail sur la démonstration. Gauss considérait ce résultat comme « une des plus belles fleurs que Fermat eût découverte dans son jardin de nombres ».

Le petit théorème de Fermat

En 1995, Fermat se retrouva en première page des journaux, grâce à Andrew Wiles, après que celui-ci eut réussi à démontrer l'une des plus célèbres conjectures de l'Histoire : « Si n est un nombre entier supérieur à 2 (autrement dit, $n > 2$), alors il n'existe pas d'entiers x, y, z distincts de 0 qui résolvent l'égalité suivante :

$$x^n + y^n = z^n \text{ »},$$

conjecture qui est connue comme « le dernier théorème de Fermat ».

Le « dernier théorème de Fermat » fut résolu en 1995 par le Britannique Andrew John Wiles. Deux ans plus tôt, le mathématicien britannique avait présenté une première démonstration, dans laquelle apparut cependant une erreur qu'il fut capable de corriger par la suite.

Mais il existe un autre théorème, beaucoup moins populaire, connu comme le « petit théorème de Fermat », qui a eu une grande importance dans la théorie des nombres premiers. Son énoncé apparaît pour la première fois dans une carte que Fermat envoya le 18 octobre 1640 à Bernard Frénicle de Bessy (1605-1675), l'un de ses amis, également mathématicien amateur, avec lequel il partagea certains de ses résultats (ils font tous les deux partie du cercle très fermé de Mersenne). La missive énonçait ceci :

> « Tout nombre premier vaut une des puissances moins un de quelque progression que ce soit, et l'exposant de ladite puissance est un sous-multiple du nombre premier donné moins un. […] Et cette proposition est généralement vraie pour toutes progressions et tous nombres premiers ; de quoi je vous aurais envoyé la démonstration, si je n'appréhendais pas d'être trop long. »

Comme à son habitude, Fermat omet la démonstration, prétextant, comme ce fut le cas pour son célèbre dernier théorème, son importante longueur. Il est très probable – et la majorité des historiens actuels converge vers cette hypothèse – qu'il ne connaissait pas réellement la démonstration de celui-ci ni d'autres hypothèses auxquelles il est arrivé. En tout cas, Fermat se considérait lui-même comme un « amateur », ce qui lui permit de prendre certaines libertés.

L'énoncé qui figure sur la carte envoyée à Bessy apparaît comme assez énigmatique, du fait de l'utilisation d'une terminologie d'époque dans la formulation.

Le théorème affirme que, si p est un nombre premier et a est un nombre naturel quelconque, alors $a^p - a$ est divisible par p.

Prenons, par exemple, le nombre premier 3 et le nombre 8 : nous obtenons alors $8^3 - 8 = 512 - 8 = 504$, qui est divisible par 3. En effet, nous vérifions que $504/3 = 168$.

On peut affirmer que le « petit » théorème de Fermat (l'adjectif *petit* fut utilisé pour la première fois en 1913 par le mathématicien allemand Kurt Hensel) est « petit, mais costaud », puisque c'est l'un des théorèmes auquel on a le plus recours quand il faut implémenter un test de primalité pour pouvoir dire si un nombre très grand est premier ou non.

De fait, Fermat eut à l'utiliser comme outil mathématique, pour décomposer certains grands nombres premiers en produits de facteurs. On sait, par

LA VERSION CHINOISE

Il existe des sources documentées (J. Needham) qui prétendent que les mathématiques chinoises avaient déjà mis en lumière, deux mille ans avant Fermat, une hypothèse, connue comme « l'hypothèse chinoise », avec un résultat très similaire à celui que l'on obtient grâce au petit théorème de Fermat. Cette hypothèse affirme que p est un nombre premier si et seulement si $2^p - 2$ est divisible par p. Dans un sens l'hypothèse chinoise peut être considérée comme un cas particulier du petit théorème de Fermat. Cependant, la réciproque, qui assure que si la condition est réalisée alors p est premier, n'est pas certaine : elle s'avère fausse dans certains cas.

exemple, qu'il fut capable de décomposer 100.895.598.169 comme le produit des nombres 898.423 et 112.303, tous deux premiers, en réponse à une demande de Mersenne, qui voulait savoir si ce nombre était ou non premier. Même ainsi, il est difficile de savoir comment Fermat pouvait travailler avec de si grands nombres.

Le théorème fut démontré pour la première fois par Euler en 1736 (Leibniz avait fait une démonstration similaire, mais n'est pas arrivé à la publier). Gauss en fit une autre démonstration dans son célèbre livre *Disquisitiones arithmeticae*, publié en 1801. Euler, lui-même, fit plus tard deux démonstrations de plus. De toutes ces démonstrations, la plus simple est la première d'Euler. Il suffit d'avoir des connaissances basiques en mathématiques pour la comprendre (cf. annexes).

Il faut souligner que le petit théorème de Fermat est une méthode permettant de déterminer si un nombre est premier sans nécessairement trouver ses facteurs. Voyons un exemple simple :

Prenons $p = 9$ et $a = 2$; nous avons $2^9 - 2 = 510$, qui n'est pas divisible par 9. Nous pouvons en conclure que 9 n'est pas premier, chose que nous savions déjà. Cette méthode peut être appliquée à des nombres très grands.

Il faut noter que le petit théorème de Fermat impose une condition nécessaire, mais non suffisante. Cela signifie que si p est premier, la condition est nécessairement respectée. Cependant, le fait que la condition soit remplie ne signifie pas forcément que p est premier. Par exemple, considérons le nombre $p = 91$; c'est un nombre composé car $p = 7 \times 13$. Mais en prenant $a = 3$ on peut montrer assez facilement que 91 divise $3^{91} - 3$. Ainsi, bien que 91 soit composé, la paire ($p = 91$, $a = 3$) vérifie le petit théorème de Fermat. La paire ($p = 341$, $a = 2$) fournit un contre-exemple similaire.

Les nombres de Fermat

Un « nombre de Fermat » est un nombre naturel qui a l'aspect suivant :

$$2^{2^n}+1\,.$$

On le symbolise habituellement par la lettre F (comme Fermat) avec un indice (n) qui indique le nombre dont on parle, de façon à ce que F_0 soit le premier nombre de Fermat, F_1 le deuxième et ainsi de suite. Nous allons calculer la valeur des cinq premiers nombres de Fermat. Rappelons-nous que n'importe quel nombre élevé à la puissance 0 vaut 1. Ainsi

$$2^0 = 1\,;\, 2^1 = 2\,;\, 2^2 = 4\,;\, 2^3 = 8.$$

En opérant une substitution dans la formule précédente, nous obtenons :

$$F_0 = 2^{2^0}+1 = 2^1+1 = 3$$
$$F_1 = 2^{2^1}+1 = 2^2+1 = 4+1 = 5$$
$$F_2 = 2^{2^2}+1 = 2^4+1 = 16+1 = 17$$
$$F_3 = 2^{2^3}+1 = 2^8+1 = 256+1 = 257$$
$$F_4 = 2^{2^4}+1 = 2^{16}+1 = 65.536+1 = 65.537.$$

Fermat émit l'hypothèse que tous les nombres qui s'obtenaient de cette façon étaient premiers. Les cinq nombres 3, 5, 17, 257, et 65.537 le sont.

Quand n vaut 5, le nombre qui s'obtient est :

$$F_5 = 2^{2^5}+1 = 2^{32}+1 = 4.294.967.296+1 = 4.294.967.297.$$

Fermat n'avait pas à ce moment-là les ressources nécessaires pour savoir si un nombre supérieur à quatre mille millions était ou non premier. Mais, apparemment, Euler si. En 1732, il trouva une factorisation de ce nombre (voir ci-après), qui est le produit de deux autres :

$$4.294.967.297 = 641 \cdot 6.700.417.$$

Fermat avait orienté Euler vers une fausse hypothèse. C'était la première fois que quelque chose de similaire se produisait. Bien que la conjecture soit fausse, les nombres de Fermat n'en sont pas moins importants. Ils ont généré à leur tour de nouvelles questions et hypothèses et se sont avérés très utiles au moment de créer un test de primalité, c'est-à-dire un test pour déterminer si un nombre donné est un nombre premier ou non.

Pour le moment, on sait que seuls les cinq premiers nombres de Fermat sont premiers, ce qui ne veut pas dire qu'il n'y en ait pas d'autres, y compris une infinité.

La factorisation complète n'est connue que jusqu'à $n = 11$. En effet, réduire un nombre à un produit de nombres premiers n'est pas une tâche facile. Comme nous allons le voir un peu plus tard, c'est sur cette difficulté que se base l'un des systèmes de cryptage les plus connus parmi ceux que l'on utilise actuellement.

Leonhard Euler

Il n'existe pas de branche des mathématiques, qu'il s'agisse du calcul, des équations différentielles, de la géométrie analytique et différentielle, de la théorie des nombres ou des séries, ou encore du calcul des variations, dans laquelle le nom du mathématicien et physicien suisse Leonhard Euler (1707-1783) n'apparaisse pas. Il s'agit d'un des mathématiciens les plus prolifiques de tous les temps. Après sa mort, à Saint-Pétersbourg, ses écrits ont continué à être découverts, publiés année après année par l'Académie des sciences de Saint-Pétersbourg. Aujourd'hui encore viennent d'être publiées, sous les auspices de l'Académie des sciences de Suisse, ses œuvres complètes, estimées à près de quatre-vingt-dix grands volumes.

Euler a toujours manifesté un intérêt particulier pour les nombres premiers. Il construisit des tableaux pour tous les nombres premiers compris entre 1 et 100.000,

Billet de banque suisse de dix francs datant de l'année 1997. Sur le recto est reproduit un portrait d'Euler, tandis que sur le verso on peut observer une turbine hydraulique, le système solaire et la propagation de la lumière à travers diverses lunettes. Tout ceci fait allusion à la contribution d'Euler à la physique mathématique.

et créa des formules qui lui permirent d'en obtenir une quantité surprenante. L'une des plus intéressantes fut

$$x^2 + x + q,$$

une formule qui produit des nombres premiers pour certaines valeurs de x, par exemple pour x compris entre 0 et $q - 2$ lorsque $q = 2, 3, 5, 7, 11$ ou 17. Il s'agit de mathématiques expérimentales, dont l'objectif est d'obtenir des résultats pratiques, mais ceux-ci ne sont pas toujours accompagnés de démonstrations rigoureuses. Cependant, Euler, à la différence de Fermat, ne conserve aucune démonstration pour lui : lorsqu'il la connaît, il la publie, et s'il ne le fait pas, c'est simplement qu'il ne l'a pas trouvée.

Euler provoqua un changement dans le panorama des mathématiques, un scénario qui était la conséquence d'une lente mais continuelle évolution du paradigme. Trois de ses nombreux apports apparaissent comme ayant eu une importance décisive dans les recherches postérieures autour des nombres premiers : le concept de fonction, les sommes infinies et l'utilisation de quantités imaginaires (nous allons revenir sur cette dernière un peu plus tard).

Les fonctions

Euler établit de manière claire les fondements de ce qui, bien des siècles plus tard, sera appelé « l'analyse mathématique ». C'est à lui que nous devons la notation utilisée actuellement pour symboliser une fonction $f(x)$. Une fonction agit comme une machine qui transforme les nombres en d'autres nombres, selon une règle établie (nous faisons référence exclusivement aux fonctions réelles de nombres réels). Par exemple, si la règle impose d'ajouter au nombre en question une quantité fixe, par exemple 3, la fonction s'écrira alors de la manière suivante :

$$f(x) = x + 3.$$

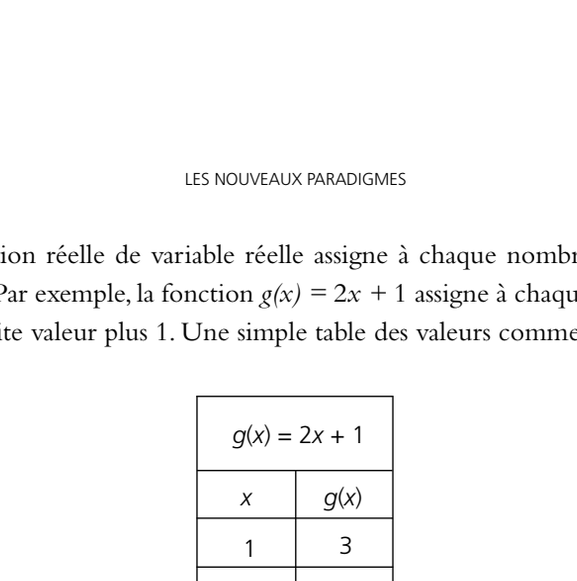
À partir de ce moment-là, la règle peut déjà être utilisée :

$$f(1) = 1 + 3 = 4 ;$$
$$f(2) = 2 + 3 = 5 ;$$
$$f(24) = 24 + 3 = 27 ;$$
$$f(0{,}32) = 0{,}32 + 3 = 3{,}32.$$

Une fonction réelle de variable réelle assigne à chaque nombre réel un autre nombre réel. Par exemple, la fonction $g(x) = 2x + 1$ assigne à chaque valeur de x le double de ladite valeur plus 1. Une simple table des valeurs comme celle-ci :

$g(x) = 2x + 1$	
x	$g(x)$
1	3
2	5
3	7
–1	–1
– 2	–3
– 3	–5

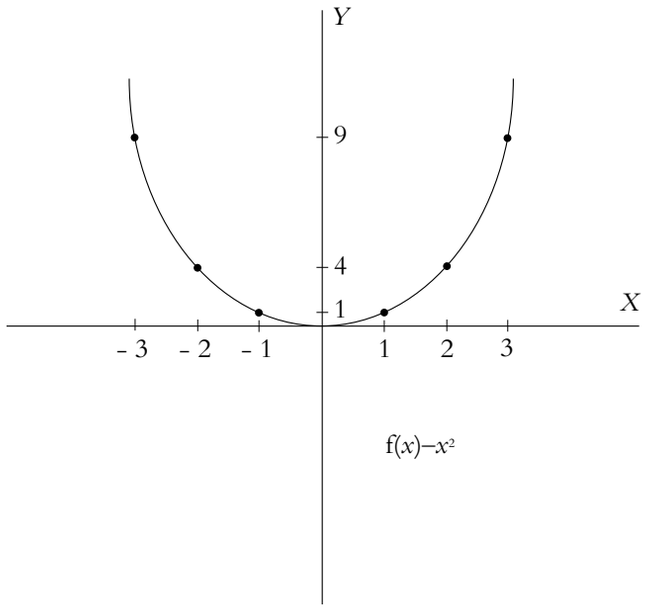
… nous permet de dessiner le graphique de la fonction à partir des points suivants :



Dans ce cas, la représentation est très simple parce qu'il s'agit d'une droite. Pour la dessiner, deux points suffisent. Cependant, une fonction comme $f(x) = x^2$, pour laquelle on obtient le tableau suivant :

$f(x) = x^2$	
x	x^2
1	1
2	4
3	9
4	16
…	…

… n'est pas si simple à dessiner :



Il est certain que plus nous disposons de points, plus le graphique gagne en précision. Mais quand l'expression n'est plus linéaire, c'est-à-dire au moment où la variable *x* est élevée à un exposant supérieur à 1, on obtient alors une courbe, qui, dans certains cas, peut être prévisible et, dans d'autres, s'avère capricieuse et impossible à dessiner, si l'on ne dispose pas de la technique adaptée. L'un des plus grands mérites d'Euler réside dans le fait qu'il a été capable de représenter certaines fonctions compliquées sans avoir les outils analytiques adéquats.

Sommes infinies

Euler introduisit un signe spécial, qui est encore utilisé de nos jours, pour symboliser une somme. Il s'agit de la lettre sigma de l'alphabet grec (Σ), qui est la première du mot somme.

Une somme est une expression du type

$$\sum_{i=1}^{i=5}$$

dans laquelle sont fixés une variable, qui dans ce cas est *i*, et plusieurs indices qui nous indiquent la façon dont varie la variable en question. Dans l'exemple, les indices nous indiquent que *i* varie entre 1 et 5. C'est-à-dire :

$$\sum_{i=1}^{i=5} i = 1+2+3+4+5\ ;$$

$$\sum_{n=1}^{n=3} (n+1) = (1+1)+(2+1)+(3+1)\ ;$$

$$\sum_{n=1}^{n=4} n^2 = 1^2+2^2+3^2+4^2.$$

Il est fréquent, pour économiser de la place, de mentionner en indice supérieur seulement la valeur finale de la suite, comme suit :

$$\sum_{i=1}^{5} i = 1+2+3+4+5.$$

On indique ainsi que *i* varie de 1 à 5.

Si l'indice supérieur n'est pas un nombre donné, mais le signe de l'infini, cela veut dire que la somme possède une infinité de termes. Par exemple :

$$\sum_{i=1}^{\infty} i = 1+2+3+4+5+\ldots$$

Même si cela peut en principe paraître étrange, il existe des sommes infinies dont le résultat final est un nombre fini (les séries de ce type sont appelées « convergentes »). Par exemple, la série

$$\sum_{i=1}^{\infty} \frac{i}{2^i} = \frac{1}{2}+\frac{2}{4}+\frac{3}{8}+\frac{4}{16}+\ldots$$

a une somme finie dont la valeur est égale à 2. Intuitivement on peut penser que, comme les termes sont à chaque fois plus petits, il va arriver un moment où ils seront si proches de zéro que le résultat de la somme sera un nombre fini. C'est certes une manière de voir, mais qui manque évidemment de précision mathématique. Un tel raisonnement pourrait nous conduire à penser que la série

$$\sum_{n=1}^{\infty} \frac{1}{n} = 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \ldots$$

a également une somme finie, alors que ce n'est pas le cas. Cette série, à laquelle Euler s'intéressait particulièrement, reçut le nom d'« harmonique ». Grâce à elle, il obtint une démonstration différente de celle qu'avait donnée Euclide pour prouver l'existence d'une infinité de nombres premiers.

LE PROBLÈME DE BASILEA

Jacob Bernoulli (1654-1705) et son frère Johann (1667-1748) se consacrèrent à l'étude de la série harmonique, spécialement entre les années 1689 et 1704. Ce sont eux qui démontrèrent leur divergence. Encouragés par ces résultats, ils étudièrent la série formée par les inverses des carrés :

$$1 + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \ldots = \sum_{n=1}^{\infty} \frac{1}{n^2}.$$

Jacob démontra que la série convergeait et il est également arrivé à prouver que la somme devait être inférieure ou égale à deux. Cependant il ne parvint pas, de quelque manière que ce soit, à trouver la valeur exacte de la somme. Son acharnement fut tel qu'il en arriva à dire : « Grande sera notre gratitude si quelqu'un trouve et nous communique ce qui, jusqu'à aujourd'hui, a échappé à nos efforts. » Cette question fut alors connue sous le nom de « problème de Basilea », car Basilea était la ville suisse où se trouvait l'université dans laquelle Johann avait une chaire de mathématiques, et d'où fut lancée la fameuse proposition.

Avant que ce défi ne soit lancé, les frères Bernoulli n'étaient pas les seuls à s'être heurtés à d'insurmontables difficultés : des mathématiciens de la stature de Mengoli et de Leibniz avaient aussi échoué. La solution ne fut trouvée que trente ans plus tard par Euler, le « magicien ». Le résultat fut réellement spectaculaire :

$$1 + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \ldots = \frac{\pi^2}{6}.$$

La série harmonique diverge, ce qui signifie que la somme de ses termes vaut l'infini. Mais elle diverge d'une façon extraordinairement lente, par rapport à une série du type

$$\sum_{n=1}^{\infty} n^2 = 1^2 + 2^2 + 3^2 + 4^2 + \ldots$$

En se basant sur la série harmonique, Euler définit une fonction qui sera une des plus importantes de toute l'histoire des mathématiques, la « fonction zêta d'Euler » (même si aujourd'hui, chose injuste, elle reçoit le nom de « fonction zêta de Riemann »). Pour la définir, Euler utilisa la lettre grecque ζ (zêta) :

$$\zeta(x) = \frac{1}{1^x} + \frac{1}{2^x} + \frac{1}{3^x} + \frac{1}{4^x} + \ldots + \frac{1}{n^x} + \ldots$$

Euler écrivit à ce sujet :

« Cependant, j'ai découvert aujourd'hui, et contre toute attente, une expression élégante pour la somme de la suite 1+1/4+1/9+1/16+…, qui dépend de la quadrature du cercle… Je me suis aperçu que six fois la somme de cette suite est égale au carré de la circonférence du cercle dont le diamètre est l'unité. »

Par malheur, Jacob était déjà mort quand Euler publia ce résultat. « Si seulement mon frère était vivant ! » se lamenta Johann.

Le qualificatif de « magicien » attribué à Euler répond à l'authentique jeu de magie mathématique que suppose la démonstration. En réalité, il n'y a rien de compliqué, mais cela requiert certaines connaissances de mathématiques supérieures, en plus de l'audace dont Euler fit preuve en traitant la suite en question comme s'il s'agissait d'une fonction polynomiale, pour ensuite la mettre en relation avec le développement en série de la fonction sinus : d'où l'apparition du nombre π, qui est l'un des zéros de ladite fonction.

Johann Bernoulli fut le maître d'Euler et l'un des meilleurs mathématiciens de son époque.

Si nous prenons $x = 1$, nous obtenons la suite harmonique $\sum_{n=1}^{\infty} \frac{1}{n}$ que nous avons vue précédemment, et dont la somme des termes est égale à l'infini. Cependant, Euler soupçonnait qu'en prenant $x = 2$, la suite résultante,

$$\frac{1}{1^2}+\frac{1}{2^2}+\frac{1}{3^2}+\frac{1}{4^2}+\ldots = 1+\frac{1}{4}+\frac{1}{9}+\frac{1}{16}+\ldots,$$

ne tendrait pas vers l'infini, sachant qu'il avait pris uniquement les fractions de la suite harmonique dans lesquelles apparaissaient des carrés. Calculer la valeur de cette dernière suite était pratiquement impossible avec les connaissances de l'époque. Euler, dans l'une de ses trouvailles les plus extraordinaires, réussit à démontrer l'égalité suivante :

$$1+\frac{1}{4}+\frac{1}{9}+\frac{1}{16}+\ldots = \frac{\pi^2}{6}$$

Euler réalisa cette découverte à 28 ans, même s'il ne perfectionna sa démonstration que six ans plus tard. L'apparition soudaine du nombre π, avec lequel se mesure la circonférence, dans le résultat de cette somme, provoqua la stupéfaction dans toute la communauté mathématique de l'époque. Avec cette découverte, Euler put résoudre l'un des problèmes les plus intrigants du moment : le fameux « problème de Basilea ».

En jouant avec la fonction zêta, Euler obtint différents résultats. On sait avec certitude que, quand x prend des valeurs inférieures ou égales à 1, la valeur de la somme est infinie. C'est pourquoi la suite converge uniquement pour les valeurs de x supérieures à 1.

EULER ET LE SON

Euler introduisit dans la fonction appelée exponentielle, définie par $f(x) = 2^x$, une variable imaginaire. Sa surprise fut énorme quand il se rendit compte que dans la courbe de la fonction étaient apparues des ondes. Ces ondes sont une série de lignes sinueuses, similaires à celles que l'on rencontre lorsque l'on tente de représenter les sons musicaux. En fonction des valeurs que prennent les nombres imaginaires, les sons correspondent à des notes plus aiguës ou plus graves.

Quelques années plus tard, le mathématicien français Jean-Baptiste-Joseph Fourier (1768-1830) élabora, en se basant sur le résultat obtenu par Euler, un système d'analyse des fonctions périodiques mettant en étroite relation les méthodes analytiques avec le monde sonore.

Euler pensa alors à la possibilité de faire intervenir dans la fonction les nombres premiers. Il savait que le théorème fondamental de l'arithmétique d'Euclide garantit que tout nombre naturel peut s'exprimer sous forme unique comme le produit de nombres premiers. Cela signifie que chacune des fractions qui intervient dans la fonction zêta peut s'exprimer de manière à ce que, au dénominateur, n'interviennent que des nombres premiers. Par exemple, supposons que nous donnions à la fonction la valeur $x = 2$:

$$\zeta(2) = \frac{1}{1^2}+\frac{1}{2^2}+\frac{1}{3^2}+\frac{1}{4^2}+\ldots+\frac{1}{n^2}+\ldots$$

Et prenons $n = 360$; il s'agit donc de calculer l'inverse de 360^2.

Procédons à la décomposition de 360 en facteurs premiers : $360 = 2^3 \cdot 3^2 \cdot 5$, de manière à ce que

$$\frac{1}{360} = \frac{1}{2^3}\cdot\frac{1}{3^2}\cdot\frac{1}{5^1}.$$

En élevant au carré les différents termes, nous obtenons :

$$\left(\frac{1}{360}\right)^2 = \left(\frac{1}{2^3}\right)^2 \cdot \left(\frac{1}{3^2}\right)^2 \cdot \left(\frac{1}{5^1}\right)^2.$$

En généralisant cette opération à chacun des dénominateurs de la fonction zêta, Euler parvint à l'expression

$$\zeta(x) = \frac{1}{1^x}+\frac{1}{2^x}+\frac{1}{3^x}+\frac{1}{4^x}+\ldots+\frac{1}{n^x}+\ldots =$$
$$= \left(1+\frac{1}{2^x}+\frac{1}{4^x}+\frac{1}{8^x}\ldots\right)\cdot\left(1+\frac{1}{3^x}+\frac{1}{9^x}+\frac{1}{27^x}\ldots\right)\cdot\left(1+\frac{1}{p^x}+\frac{1}{(p^2)^x}+\frac{1}{(p^3)^x}\ldots\right)\ldots,$$

dans laquelle n'interviennent que des nombres premiers. Il s'agit d'une équation dans laquelle le terme de gauche apparaît comme une somme de nombres infinis et celui de droite comme un produit, également de nombres infinis. Cette équation peut être considérée comme la première pierre de ce qui deviendra l'édifice de la théorie analytique des nombres, qui se développera durant les siècles suivants. Cette expression, connue sous le nom de « produit eulérien », constitua le point de départ à partir duquel Riemann réussit, pour la première fois, à imposer un rythme à la troupe disparate et désordonnée des nombres premiers, comme nous le verrons au chapitre 6.

La conjecture de Goldbach

Christian Goldbach (1690-1764) fut un mathématicien prussien qui entretint une intense correspondance avec Euler. Le 18 novembre 1752, il lui envoya une carte dans laquelle il affirmait la proposition suivante : que tout nombre naturel pair supérieur ou égal à 4 peut s'écrire comme la somme de deux nombres premiers. Dans cette phrase, l'expression « somme de deux premiers » inclut le cas où il s'agirait d'un nombre premier répété deux fois. Par exemple :

$$4 = 2 + 2$$
$$6 = 3 + 3$$
$$8 = 3 + 5$$
$$10 = 3 + 7$$
$$12 = 5 + 7$$
$$14 = 3 + 11.$$

Le 16 décembre de la même année, Euler lui répondit qu'il avait vérifié la conjecture jusqu'au nombre 1.000 et, dans une autre lettre datée du 3 avril 1753, il répondit que le résultat était certain jusqu'au nombre 2.500. Actuellement, la conjecture a été vérifiée par des méthodes informatiques pour tous les nombres pairs inférieurs à deux mille milliards, mais elle n'a pas encore été démontrée. Elle est considérée par la communauté mathématique comme l'un des problèmes les plus difficiles de l'histoire de la science.

Chen Jingrun (1933-1996), l'un des mathématiciens les plus remarquables du xx^e siècle, offrit en 1996 le meilleur résultat de la conjecture de Goldbach. Il démontra que tout nombre pair suffisamment grand peut s'écrire comme la somme d'un premier et d'un semi-premier (nombre qui est le produit, comme beaucoup, de deux facteurs premiers). La République populaire de Chine rendit hommage à Chen en imprimant un timbre à son honneur en 1999. Sur ce timbre à l'effigie du mathématicien, apparaît aussi son inéquation.

ONCLE PETROS ET LA CONJECTURE DE GOLDBACH

Ceci est le titre d'une fameuse nouvelle d'Apostolos Doxiadis, dans laquelle un mathématicien reclus propose à son neveu de résoudre un problème mathématique. Le protagoniste souhaite que son neveu renonce à étudier les mathématiques si, durant ses vacances, il ne réussit pas à résoudre le problème. Après tout un été d'efforts acharnés, le neveu renonce et s'inscrit en droit. Le problème posé était la conjecture de Goldbach. Avec l'intention de faire de la publicité pour le livre, l'éditeur britannique Tony Faber promit en l'an 2000 d'offrir une récompense de 1 million de dollars au premier anglophone qui démontrerait la conjecture avant avril 2002. Évidemment, personne ne vint réclamer le prix.

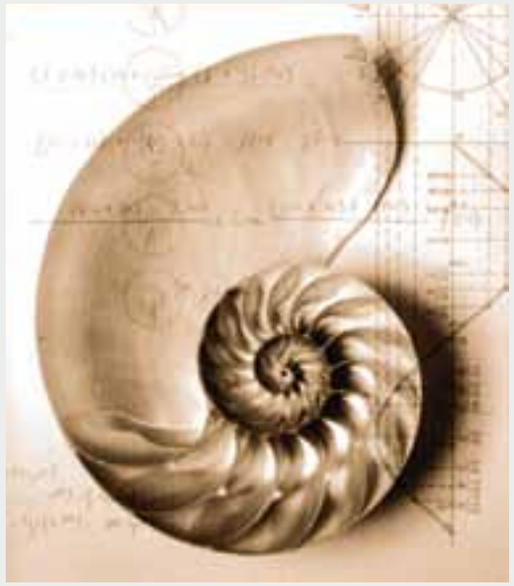


Illustration de la couverture de certaines éditions du livre d'Apostolos Doxiadis, dominée par une coquille de nautile, incarnation dans le monde naturel d'une spirale logarithmique.

Chapitre 4

Logarithmes et nombres premiers

Dans les recherches menées sur un objet, les dispositifs utilisés pour son observation jouent souvent un rôle décisif. Le développement de l'astronomie est lié à l'évolution technologique des télescopes, tout comme les progrès de la microbiologie sont liés aux microscopes. Les appareils d'observation, de mesure ou de détection sont les clés qui ont permis d'ouvrir les portes donnant sur des contrées inconnues. En ce sens, les mathématiques ne sont pas une exception : ses objets de recherche n'existent que dans le champ de la pensée, et c'est pourquoi ce ne sont pas des dispositifs matériels, mais malgré tout, ils peuvent être représentés de façon concrète. Parmi les dispositifs mathématiques les plus puissants qui aient été inventés, on trouve les logarithmes, qui sont nés comme instruments de calcul, mais qui, à travers Gauss, ont fini par jouer un rôle décisif, en tant qu'instruments d'observation, dans la recherche des nombres premiers.

John Napier

Dans de nombreux textes apparaissent des références aux logarithmes népériens ou logarithmes de Neper, tandis que d'autres font référence aux logarithmes de Napier. Très peu de noms, dans l'histoire des mathématiques, ont connu tant de versions différentes : Napeir, Nepair, Nepeir, Neper, Napare, Naper, Naipper… Cependant, le seul nom que le créateur des logarithmes n'utilisa jamais durant sa vie fut celui de Napier, qui était en réalité son vrai nom.

Le mathématicien et théologien écossais John Napier est entré dans l'Histoire pour sa contribution décisive à la simplification du calcul moderne.

John Napier naquit en 1550 dans le château de Merchiston, près d'Édimbourg, en Écosse. Il était le fils d'un noble, Archibald Napier, qui jouissait d'une excellente situation économique. John fit des études de théologie à l'université de Saint-Andrews. Son intérêt pour les mathématiques surgit au cours d'un long voyage qu'il effectua à travers toute l'Europe. Nous savons qu'il passa un moment à l'université de Paris et également quelque temps en Italie et en Hollande. À son retour en Écosse, en 1572, il se maria avec Élisabeth Stirling. Durant les deux années suivantes, il se consacra à la construction d'un château à Gartness. Napier passa de nombreuses heures enfermé dans ce château, et c'est à cette époque qu'il se consacra à ses mystérieux travaux mathématiques. « Mystérieux » parce que Napier, dans les rares occasions où il apparaissait en public, était toujours vêtu de noir et portait avec lui un coq, également noir, perché sur son épaule. Toute cette scénographie lui valut une réputation de sorcier, qui ne fit que croître lorsqu'il fit étalage d'une série de connaissances pratiques que personne ne possédait. En plus d'être un remarquable amateur de mathématiques, il passait une grande partie de son temps à faire des recherches sur les Évangiles, et particulièrement sur l'Apocalypse de saint Jean. Il publia ses conclusions dans une œuvre intitulée *Plaine Discovery of the Whole Revelation of St John* (*Ouverture de tous les secrets de l'Apocalypse ou révélation de saint Jean*), qui fut traduite en plusieurs langues et qui prétendait démontrer que le pape de Rome était l'antéchrist.

L'un des premiers modèles de l'abaque népérien, inventé par John Napier pour le calcul de produits et quotients.

ÉTRANGES DÉCIMALES

Que l'on exprime une fraction comme 19/8 sous la forme du nombre décimal 2,375 nous paraît on ne peut plus normal : il suffit de faire la division de 19 par 8. Mais, au XVI^e^ siècle, les expressions décimales étaient réellement exotiques. Napier, dans son *Descriptio* de 1614, se prononçait déjà en faveur des fractions décimales. Dans son œuvre *Constructio* (1619, publication posthume), il défendit avec énergie l'utilisation de la virgule comme signe de séparation décimale en Angleterre. Mais cette proposition, ainsi que celle de l'ingénieur flamand Stevin (1548-1620) d'utiliser le système décimal pour les poids et les mesures, ne parvint pas à s'imposer, ni en Angleterre ni aux États-Unis.

Napier était intéressé par l'arithmétique et l'astrologie. Cette dernière discipline l'amena à rechercher les propriétés des figures géométriques sur une surface sphérique. Il obtint d'importants résultats dans la résolution de triangles sphériques. N'importe quel étudiant ayant suivi des études de trigonométrie sphérique a forcément rencontré plus d'une formule portant son nom.

Cependant, pour Napier, une question demeurait prioritaire. À cette époque, les calculs numériques étaient extrêmement ennuyeux. Napier considérait qu'il pouvait consacrer son temps à faire des choses plus intéressantes que remplir des feuilles et des feuilles avec d'interminables calculs, qui n'était en réalité rien d'autre qu'un travail répétitif.

Il parvint donc à inventer un dispositif, fabriqué à partir de baguettes de sections carrées, qui s'encastrent sur des tables de multiplication et qui permettent de réaliser des sommes et des produits avec plus de facilité. En 1617, il publia un manuel intitulé *Rabdologiae*, dans lequel il expliquait comment l'utiliser. Cet outil, véritable ancêtre de la règle à calcul, fut utilisé en Écosse durant plus de cent ans. Plus tard, il le perfectionna en remplaçant les baguettes par des planches perforées – ce qui permettait de faire des multiplications de nombres beaucoup plus grands. De fait, on pourrait dire que ces planches sont les ancêtres des fameuses cartes perforées qui apparurent quatre siècles plus tard avec les premiers ordinateurs IBM.

Cependant, la plus grande invention de Napier, celle qui a marqué l'histoire des mathématiques, fut celle des logarithmes. Il s'agit d'une ingénieuse méthode de calcul qu'il publia en 1614 sous le titre de *Mirifici logarithmorum canonis descriptio*.

Pour évaluer l'importance du rôle que les logarithmes ont joué dans l'étude des nombres premiers, il est intéressant de rappeler certains concepts de base les concernant.

Logarithmes

Les logarithmes partent de l'idée suivante : nous savons que $1.000 = 10 \cdot 10 \cdot 10$, c'est-à-dire dix élevé à la puissance trois, que nous représentons sous forme de puissance, soit 10^3, de sorte que

$$1.000 = 10^3 ;$$
$$10.000 = 10^4 ;$$
$$1.000.000 = 10^6.$$

Supposons que nous voulions multiplier ces trois nombres entre eux :

$$1.000 \cdot 10.000 \cdot 1.000.000 = 10.000.000.000.000.$$
$$\text{Mais, } 10.000.000.000.000 = 10^{13}.$$

Nous aurions pu effectuer la multiplication en faisant $10^{3+4+6} = 10^{13}$. Il est certain qu'il est plus facile d'additionner que de multiplier. Pour nous en convaincre, il suffit de faire la multiplication $10^{38}.10^{52} = 10^{90}$ en écrivant les zéros.

Passons maintenant au langage des logarithmes. Avec l'égalité $1.000 = 10^3$, nous pouvons nous demander à quel nombre nous devons élever 10 pour obtenir 1.000. La réponse est 3. Nous pouvons écrire ceci de la façon suivante : $\log(1.000) = 3$. De sorte que, par exemple,

$$\log 100 = 2,$$
$$\log 1.000 = 3,$$
$$\log 1.000.000 = 6.$$

L'idée sous-jacente dans ce schéma est qu'il est beaucoup plus simple d'effectuer des sommes plutôt que des produits. Par exemple :

$$\log (100 \cdot 1.000) = \log 100 + \log 1.000 = 2 + 3 = 5.$$

Par conséquent, il suffit d'effectuer le processus inverse, l'antilogarithme, pour obtenir le résultat final : $10^5 = 100.000$.

Nous pouvons faire un tableau de toutes ces opérations, ainsi que l'on peut le voir ci-dessous :

1	10	100	1.000	10.000	100.000	1.000.000	10.000.000	100.000.000	1.000.000.000
0	1	2	3	4	5	6	7	8	9

La première ligne de ce tableau a été construite en commençant par le nombre 1, et chaque nouvelle cellule est égale à la précédente multipliée par 10 ; c'est ce que l'on appelle une progression géométrique de raison 10. En revanche, les cellules correspondant à la seconde ligne s'obtiennent en ajoutant une unité au nombre de la cellule précédente. Le plus remarquable est que dans la ligne du haut, nous parlons de produits, et dans celle du bas nous nous référons à des sommes. Selon ce principe, la multiplication

$$1.000 \cdot 100.000 = 100.000.000$$

est équivalente à la somme

$$3 + 5 = 8.$$

Nous pouvons créer un tableau comme celui-ci en mettant dans la première ligne la progression géométrique que nous désirons. Par exemple :

1	2	4	8	16	32	64	128	256
0	1	2	3	4	5	6	7	8

Pour calculer le produit $4 \cdot 16$, nous devons additionner dans la ligne du bas $2 + 4$. Nous pouvons faire, de la même manière, des divisions. Mais dans ce cas, il faut prendre en compte le fait que le résultat équivaut à la soustraction des nombres correspondant à la ligne inférieure. Par exemple, pour calculer 256 divisé par 8, nous n'avons qu'à faire la soustraction $8 - 3 = 5$. Le résultat est donc 32. Cela correspond au nombre inscrit dans la case au-dessus du 5. Dans cette relation qui existe entre les nombres de la ligne inférieure et ceux de la ligne supérieure, nous trouvons, comme nous l'avons dit précédemment, la clé du concept des logarithmes.

Nous pouvons maintenant établir une définition rigoureuse du logarithme. Quand nous disons qu'au nombre 5 correspond le nombre 32, nous exprimons l'égalité :

$$2^5 = 32.$$

Rappelons-nous que « 2 élevé à la puissance 5 » signifie « 2 multiplié par lui-même cinq fois ». Nous pourrions faire une lecture des deux lignes du dernier tableau, de la façon suivante : « 3 est le nombre auquel il faut élever 2 pour obtenir 8 » et « 7 est le nombre auquel il faut élever 2 pour obtenir 128 », ce qui peut s'exprimer plus simplement ainsi :

$$\log_2 8 = 3 ;$$
$$\log_2 128 = 7.$$

Ces expressions se lisent, respectivement, « le logarithme en base 2 de 8 est 3 » et « le logarithme en base 2 de 128 est 7 ». Si nous prenons maintenant comme exemple le premier tableau, nous avons $10^4 = 10.000$, c'est-à-dire que 4 est le nombre auquel il faut élever 10 pour avoir 10.000. Exprimé sous forme de logarithme, nous obtenons $\log_{10} 10.000 = 4$, qui se lit « le logarithme en base 10 de 10.000 est 4 ».

Cela nous permet d'établir une définition générale des logarithmes : le logarithme en base a d'un nombre b est un nombre c qui est la puissance à laquelle il faut élever la base a pour obtenir b ($a^c = b$). Il s'écrit sous la forme

$$\log_a b = c.$$

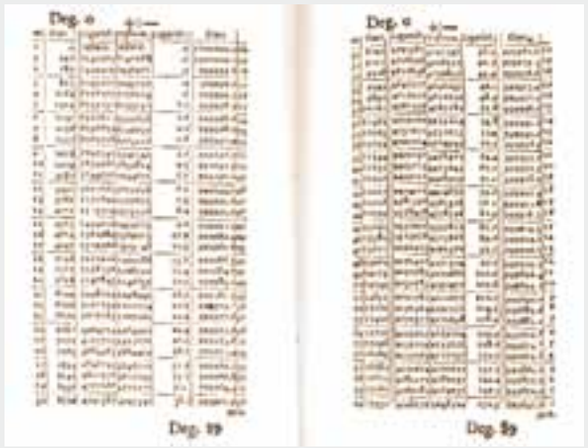
Napier était intéressé par l'accélération des calculs en trigonométrie sphérique et son idée des logarithmes s'appliquait initialement aux fonctions trigonométriques. Son approche d'origine était différente de la nôtre, qui peut être qualifiée d'arithmétique : elle était de type cinématique, car elle envisageait deux segments de droites qui étaient parcourus à différentes vitesse. Le terme « logarithme » fut employé pour la première fois par Napier et signifie « nombre de la raison » : le mot *raison* se réfère ici à la relation qui existe entre les différents segments des droites utilisées par Napier (et dans notre cas, à la relation qui existe entre les nombres de la première et de la seconde ligne du tableau). Napier travailla avec des logarithmes en base 10, ce qui n'était pas très pratique. De plus, il traînait comme un handicap le fait que le logarithme de 1 était 0, ce qui revenait à admettre que $10^0 = 1$. Henry Briggs (1561-1630), titulaire de la chaire de géométrie d'Oxford, lui écrivit une lettre pour lui faire part de l'intérêt qu'avait éveillé en lui la question des logarithmes et lui proposer une rencontre. Durant l'été 1616, Briggs rencontra Napier dans son château de Merchiston, et ils discutèrent de la possibilité d'utiliser le nombre 10 comme base et du fait que $\log 1 = 0$. Napier, qui à ce moment-là était déjà malade, refusa d'entreprendre une nouvelle version de ses tables de logarithmes. Il devait mourir peu après et Briggs proposa alors une définition du logarithme très similaire à celle qui est exprimée dans ce livre, donnant naissance à ce que l'on appelle « les logarithmes de Briggs ».

Mais un fait apparemment accidentel dans la création des tables de logarithmes allait devenir un événement important dans l'histoire des mathématiques. De la même façon que dans les cahiers scolaires on a coutume de mettre sur la quatrième de couverture les tables de multiplication, dans la majorité des tables de logarithmes est jointe, à la fin, une liste de nombres premiers. Cet usage peut s'expliquer de la façon suivante : si nous prenons en compte le fait que n'importe quel nombre peut

s'exprimer comme un produit de facteurs premiers, le plus logique est de calculer d'abord le logarithme des nombres premiers et d'obtenir ensuite les logarithmes des autres nombres grâce à de simples sommes. Le fait est que dans les tables de logarithmes que Gauss utilisa à l'école, il y avait au final une liste des mille premiers nombres premiers. Un esprit prodigieux se trouvait ainsi confronté à deux concepts apparemment déconnectés l'un de l'autre, et c'est de leur alchimie qu'allait naître l'un des théorèmes les plus intéressants de l'algèbre.

TABLES LOGARITHMIQUES

Actuellement, le calcul d'un logarithme se réduit à appuyer sur la touche d'une simple calculatrice de poche, mais au XVII[e] siècle cela nécessitait d'être en possession de grands volumes qui contenaient les logarithmes de la plus grande quantité de nombres possible. En 1617, Briggs publia les premières tables dans lesquelles on pouvait trouver les logarithmes des nombres compris entre 1 et 1.000 avec une précision de quatorze décimales. Sept ans plus tard apparurent plusieurs nouvelles tables, tout d'abord avec des valeurs comprises entre 1 et 20.000 et entre 90.000 et 100.000, également avec une précision de quatorze chiffres. En très peu de temps, des éditions de ces tables furent réalisées dans divers pays, car l'utilisation des logarithmes dans le calcul était d'un grand intérêt pratique : en effet, la navigation maritime nécessitait l'usage de cartes astronomiques toujours plus précises ; or, la complexité des calculs trigonométriques que cela supposait pour les astronomes les occupait pendant des heures, des jours et même des années. Laplace aurait dit : « Grâce à ses travaux [ceux de Napier] la vie des astronomes est deux fois plus longue. »



Les premières tables de logarithmes, publiées à Édimbourg en 1614.

Johann Carl Friedrich Gauss

Gauss naquit à Brunswick, en Allemagne, le 30 avril 1777. Il était d'origine modeste et son avenir, si rien ni personne n'y avait remédié, était destiné aux travaux des champs. Mais déjà à l'école primaire, Gauss se fit remarquer alors qu'il n'avait que 9 ans. Il s'agissait d'une école rurale dotée de peu de moyens dans laquelle le maître, appelé Büttner, se voyait contraint de s'occuper d'une centaine d'écoliers. Une manière facile de le faire était d'obliger les enfants à effectuer de lourds calculs répétitifs. Un jour, il leur fit calculer la somme des cent premiers nombres. Au bout d'un moment, Gauss laissa son cahier sur la table et s'exclama : « Ça y est ! » Gauss non seulement avait effectué la somme

$$1 + 2 + 3 + 4 + \ldots + 100 = (1 + 100) + (2 + 99) + (3 + 98) + \ldots + (50 + 51)$$
$$= 101 + 101 + \ldots + 101 = 101 \cdot 50 = 5.050,$$

en un temps record, mais il avait également résolu le problème de la somme des termes d'une progression arithmétique. Büttner se rendit compte aussitôt qu'il avait affaire à un élève particulièrement doué et décida de le présenter à Johann Martin Bartels (1769-1836), un élève passionné par les mathématiques, de huit ans l'aîné de Gauss. C'est en compagnie de Bartels que Gauss fit ses premiers pas dans l'univers des nombres, et il maintint avec lui une profonde amitié durant toute sa vie. La mère de Gauss, Dorothea Benz, consciente qu'elle devait faire quelque chose pour que les extraordinaires aptitudes de son fils reçoivent l'aide que ses parents ne pouvaient lui donner, prit contact avec celui qui allait devenir leur protecteur : le duc de Brunswick. Celui-ci obtint les bourses nécessaires pour les études de Gauss au lycée et, plus tard, à l'université de Göttingen. De cette façon, le jeune Gauss réussit à sortir de son milieu social pour devenir le « prince des mathématiques ». Sa carrière professionnelle atteignit son sommet quand on lui attribua les

Portrait de jeunesse de Gauss.

Œuvre lithographique d'Eduard Ritmüller dans laquelle Gauss apparaît sur la terrasse de l'observatoire de l'université de Göttingen.

titres de professeur d'astronomie à l'Université et de directeur de l'observatoire astronomique de l'université de Göttingen.

Gauss mena une vie relativement paisible. Il adopta, par respect pour le duc, son protecteur, une position conservatrice en une époque marquée par une certaine agitation politique. Il était fils unique et ne se maria qu'à 32 ans, avec Johanna Osthoff, avec laquelle il eut trois enfants, dont le troisième mourut quelques mois après sa mère. Gauss se remaria en 1810 avec Wilhelmine Waldeck, fille d'un professeur de droit. De ce mariage naquirent trois autres enfants. Le 23 février 1855, Gauss mourut dans la ville de Göttingen. À cette époque, sa renommée en tant que scientifique avait déjà fait le tour du monde.

La première conjecture

Dans le cahier de notes que Gauss utilisait à l'âge de 14 ans, on peut lire la note suivante :

« Nombres premiers plus petits que a (= ∞) a / 1a ».

Gauss s'était concentré sur l'étude de la longue liste de nombres premiers qui figurait à la fin de sa table de logarithmes, et il était dès lors inévitable qu'il succombe à son tour au sortilège de la chaotique série. Mais il avait déjà décidé qu'il

ne s'orienterait pas vers la recherche d'une formule permettant de savoir comment était et où serait « le nombre premier suivant ». Il pressentait clairement que cette voie ne pouvait mener qu'à un échec. Au lieu de cela, il décida de calculer combien de nombres naturels il y avait entre deux nombres premiers donnés, ou plus exactement, combien de nombres premiers il y avait parmi les dix, les cent, les mille et les dix mille premiers nombres naturels. De cette manière, on peut déjà estimer la fréquence d'apparition des nombres premiers dans la série des nombres naturels.

Nous savons que parmi les dix premiers nombres naturels, nous trouvons seulement quatre nombres premiers (2, 3, 5 et 7). Entre dix et cent en apparaissent vingt et un. Pour exprimer cela, Gauss établit une fonction qu'il appela π (x) et la définit de la façon suivante :

π (x) = la quantité de nombres premiers qui sont plus petits que x.

UN SCIENTIFIQUE COMPLET

Gauss mena également à bien divers travaux en dehors du cadre des mathématiques. Les résultats qu'il obtint sur le magnétisme terrestre, l'électromagnétisme, la capillarité, l'attraction des ellipsoïdes et la dioptrique sont remarquables. Dans le cadre de ses travaux sur la géodésie, on doit à Gauss, entre autres choses, l'invention de l'héliotrope (un appareil qui transmet des signaux grâce à la lumière réfléchie). Un événement curieux se produisit en 1833, alors que Gauss menait conjointement avec Wilhelm Weber (1804-1891) des recherches en électromagnétisme. Pour pouvoir envoyer des messages avec rapidité, Gauss construisit, de ses propres mains, un appareil électrique capable de transporter des messages à la vitesse de la lumière. Il avait inventé, ni plus ni moins, le télégraphe électrique.

Monument en hommage à Gauss et Weber à Göttingen.

Selon cette fonction, π (10) = 4.

Par exemple, pour calculer π (15), nous devons compter les nombres premiers inférieurs à 15, qui sont

2, 3, 5, 7, 11, 13,

si bien que π (15) = 6.

Le symbole π qui apparaît dans la formule est le fameux nombre *pi*, mais dans ce contexte il est dépourvu de signification mathématique, puisque la fonction se définirait de la même façon si nous mettions n'importe quel autre symbole, comme C(x). La vérité est que le choix de π ne fut pas très pertinent de la part de Gauss, et il est probable qu'il prit le premier symbole qui lui vint à l'esprit. Ce choix n'est pas pertinent parce que la vision de π évoque immédiatement toutes sortes de relations mathématiques mettant en jeu la circonférence, relations qui sont complètement étrangères, dans ce contexte, à la question des nombres premiers. Quoi qu'il en soit, nous continuerons ici à utiliser la notation de Gauss.

Le mathématicien allemand construisit alors un premier tableau de deux colonnes, de manière à ce que la première colonne contienne les puissances de 10 et la seconde, la valeur que prend π (x).

Le tableau suivant est prévu pour les dix mille premiers millions. Évidemment, à l'époque de Gauss, les outils de calcul étaient beaucoup plus précaires et Gauss ne disposait pas de rangs d'une telle valeur.

x	$\pi(x)$
10	4
100	25
1.000	168
10.000	1.229
100.000	9.592
1.000.000	78.498
10.000.000	664.579
100.000.000	5.761.455
1.000.000.000	50.847.534
10.000.000.000	455.052.512

Logiquement, $\pi(x)$ est un nombre qui va en augmentant, mais la façon dont il le fait ne nous apprend pas grand-chose. Nous allons ajouter une autre colonne qui nous renseigne sur la proportion de nombres premiers inférieurs à un nombre donné. Pour cela, nous calculons le quotient

$$\frac{\pi(x)}{x}.$$

Nous savons qu'il existe 168 nombres premiers inférieurs à 1.000 :

$$\frac{\pi(x)}{x} = \frac{\pi(1.000)}{1.000} = \frac{168}{1.000} = 0,168.$$

Ce nombre nous indique que 16,8 % des nombres qu'il y a entre 1 et 1.000 sont premiers. Les 83,2 % restants sont des nombres composés. En ajoutant cette troisième colonne au tableau, on obtient :

x	*π(x)*	*π(x) / x*
10	4	0,40000000
100	25	0,25000000
1.000	168	0,16800000
10.000	1.229	0,12290000
100.000	9.592	0,09592000
1.000.000	78.498	0,07849800
10.000.000	664.579	0,06645790
100.000.000	5.761.455	0,05761455
1.000.000.000	50.847.534	0,05084753
10.000.000.000	455.052.512	0,04550525

Nous pouvons observer que la proportion de nombres premiers va en diminuant au fur et à mesure que nous avançons vers les plus grands nombres. Ceci commence déjà à constituer une donnée, mais c'était une donnée prévisible. Pour qu'un nombre soit premier, il ne peut être divisible par aucun des nombres qui le précèdent. Par exemple, pour que 13 soit premier, il ne doit pas être divisible par 2, 3, 4, 5, 6, 7, 8, 9, 10, 11 et 12. Plus le nombre est grand et plus l'exigence de ne pas

être divisible est difficile à satisfaire. Par conséquent, il est logique que les nombres premiers soient de plus en plus rares.

Mais Gauss savait que cela ne signifiait pas qu'il arriverait un moment où il ne trouverait plus de nombre premier disponible, puisqu'il connaissait parfaitement l'existence du théorème fondamental de l'arithmétique avec lequel Euclide avait démontré l'infinité des nombres premiers.

La troisième colonne qu'inclut Gauss dans le tableau ne fut pas celle qui s'obtient en effectuant le quotient $\frac{\pi(x)}{x}$, mais l'inverse, $\frac{x}{\pi(x)}$.

x	*π(x)*	*x / π(x)*
10	4	2,5
100	25	4
1.000	168	6
10.000	1.229	8,1
100.000	9.592	10,4
1.000.000	78.498	12,7
10.000.000	664.579	15
100.000.000	5.761.455	17,4
1.000.000.000	50.847.534	19,7
10.000.000.000	455.052.512	22

Ce tableau nous indique, par exemple, que parmi les cent premiers nombres, un nombre sur quatre est premier ; que parmi les mille premiers nombres, un nombre sur six est premier, et ainsi de suite. Il s'agit simplement d'une estimation. Le tableau n'affirme pas que parmi les cent premiers nombres apparaît un nombre premier tous les quatre nombres, chose que nous pouvons vérifier de manière rapide en consultant le crible d'Ératosthène pour les cent premiers nombres. Ainsi, ce tableau doit plutôt être interprété comme indiquant une distance probable entre les nombres premiers.

Gauss observa que les nombres de la dernière colonne croissaient approximativement de deux unités chaque fois qu'on avançait d'une ligne. De telle manière que la situation était la suivante : si on multipliait par dix dans la première ligne, on devait additionner deux dans la seconde. Cette relation entre produit et somme résidait implicitement dans la nature propre des logarithmes. Gauss avait dans les

mains une table de logarithmes et une autre de nombres premiers dans un même volume. Cela lui donna l'idée de créer, avec un outil différent, un nouveau dispositif d'observation. Les logarithmes devinrent la nouvelle lentille que Gauss adapta à son télescope. Comme nous l'avons vu, quand la base des logarithmes est 10, chaque fois que l'on multiplie par 10, les logarithmes décimaux augmentent de un en un. C'est pourquoi cette base ne convenait pas bien au schéma de Gauss, qui décida de prendre des logarithmes en base *e,* un nombre aux caractéristiques similaires à celles du nombre π. Sa valeur approximative est

$$e = 2{,}7182818284590452354\ldots$$

Il s'agit d'une expression décimale infinie, qui apparaît en mathématiques avec autant, voire plus de fréquence que le nombre π. En effet, quand on prend un logarithme en base *e*, on dit qu'il s'agit d'un « logarithme naturel ». Comme il a déjà été expliqué, nous devrions écrire log_e pour symboliser les logarithmes naturels ; cependant, ils s'écrivent sous la forme abrégée « ln ». Dans les calculatrices scientifiques, il existe une touche pour « log », logarithme décimal, et une autre pour « ln », logarithme en base *e*.

La conjecture élaborée par Gauss à partir de ce point fut la suivante :

Pour les grandes valeurs de *x*, la valeur de $\frac{\pi(x)}{x}$ s'approche de $\frac{1}{ln\,x}$, ce qui peut s'exprimer sous la forme

$$\frac{\pi(x)}{x} \approx \frac{1}{ln\,x} \text{ (pour les grandes valeurs de } x\text{)}.$$

Ce résultat donne une estimation de la fréquence avec laquelle apparaissent les nombres premiers dans la succession des nombres naturels. Supposons que $P(N)$ soit le nombre de premiers inférieurs à N ; la formule affirme qu'à mesure que N augmente, le quotient $N/P(N)$ se rapproche chaque fois plus du logarithme naturel de N. Il existe une manière simple de mettre en pratique la formule de Gauss quand nous voulons savoir combien il y a de nombres premiers inférieurs à un nombre donné. Par exemple, supposons que quelqu'un nous pose la question suivante : « Combien de nombres premiers croyez-vous qu'il y ait parmi les mille premiers nombres ? » Prenons une calculatrice de poche et procédons comme suit :

1) introduisons le nombre 1.000 ;
2) appuyons sur la touche « ln » ;
3) puis la touche « 1/*x* » ;
4) multiplions le résultat par 1.000 : alors apparaît le nombre 144,764827301083942550376306305 54.

Cette démarche permet d'estimer la quantité de nombres premiers compris entre 1 et 1 000 : d'après l'estimation prévue par Gauss, il y en a environ 145. L'approximation n'est pas fabuleuse parce qu'en réalité il y en a 168. Mais n'oublions pas que le théorème se précise au fur et à mesure que le nombre N s'accroît et nous permet d'affirmer avec une certaine tranquillité, par exemple, que seulement 3,6 % du premier billion de nombres sont premiers.

Maintenant nous pouvons déjà déchiffrer ce que Gauss voulait dire quand il écrivit « Nombres premiers plus petits que *a* (= ∞) *a*/l*a* » dans son cahier de notes :

« Nombres premiers plus petits que *a* » signifie la même chose que $\pi(a)$.

« 1*a* » est ce que nous utilisons comme ln*a*.

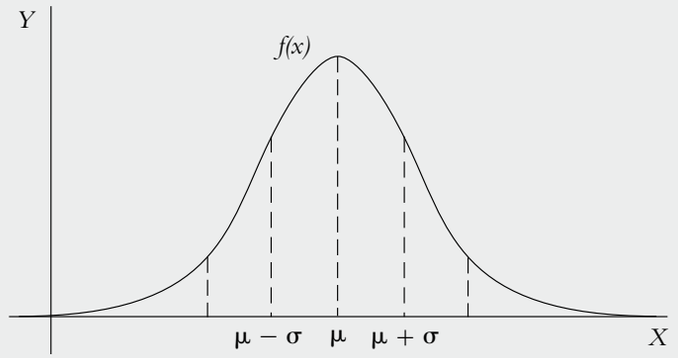
« = ∞ » signifie que l'égalité est validée pour des valeurs très grandes de *a* (quand *a* tend vers l'infini).

Aujourd'hui, ce résultat est connu sous le nom de « théorème des nombres premiers » et il est l'un des plus importants de l'histoire des mathématiques.

LA COURBE DE GAUSS

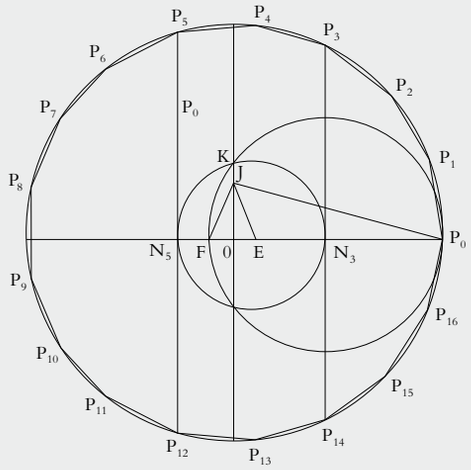
À ses 18 ans, Gauss découvrit la méthode des moindres carrés, qui éveilla en lui un intérêt particulier pour la théorie des erreurs. Il créa alors une méthode d'observation statistique dans laquelle la distribution normale des erreurs suit une courbe en forme de cloche. C'est sans doute la plus populaire des courbes qui existe en mathématiques : elle a reçu le nom de « courbe en cloche de Gauss ».

Cette méthode d'observation finit par produire des résultats très rentables, puisque Gauss commença une étude systématique des mouvements boursiers internationaux figurant dans la presse étrangère qui arrivait régulièrement à la salle de lecture de l'Université. La cloche de Gauss sonna et les bénéfices qu'il obtint grâce à cette recherche ont largement surpassé son salaire de professeur.



LE POLYGONE DE GAUSS

La construction de polygones réguliers avec règle et compas était demeurée un problème sans solution depuis le temps des géomètres grecs. On savait comment construire ceux de trois, quatre, cinq et quinze côtés, ainsi que les duplications de ceux-ci. Le 30 mars 1796, Gauss découvrit la façon dont il fallait construire le polygone de dix-sept côtés. Cela constitue une date importante dans sa biographie, puisque ce même jour il commença son journal scientifique, qui couvre la période 1796-1814 et qui est considéré comme un authentique joyau des mathématiques. En effet, toutes ses découvertes scientifiques y sont notées. Mais le fait le plus important est peut-être qu'à cette même date, Gauss décida de se consacrer aux mathématiques plutôt qu'à la philologie, branche dans laquelle il avait donné des preuves de son génie.



La bande indisciplinée des nombres premiers avait trouvé à qui parler. Dans leur étude, s'était introduite une « fonction », ce qui revenait à l'orienter vers une autoroute dont, avec le temps, les normes de circulation ne cesseraient de s'améliorer.

Gauss ne fit pas connaître ce résultat. Ses motifs ne relevaient pas d'une attitude de dissimulation mesquine, ni d'une posture à la Fermat, qui aurait allégué la longueur excessive de la démonstration pour ne pas la publier. Gauss disposait assurément d'assez de papier pour inclure n'importe quelle démonstration, quelle que fût sa longueur. C'est parce qu'il n'avait aucun moyen de le démontrer que Gauss ne fit pas connaître ce théorème. Les mathématiques avaient pris un tournant qui s'amorçait déjà avec Euler. La théorie mathématique devait à présent être articulée de façon indiscutable dans un scénario logique, qui commençait à se frayer un chemin entre des techniques ambiguës et des pragmatismes douteux. L'intuition, axe central de n'importe quelle découverte, devait s'appuyer sur de solides bases théoriques. La démonstration d'un théorème s'était transformée en une argumentation objective qui, grâce à un langage commun, accédait au statut de vérité.

La conjecture de Gauss ne se transforma en un théorème que cent ans plus tard : en 1896, Jacques Hadamard (1865-1963) et C.-J de La Vallée Poussin (1866-1962) démontrèrent le théorème simultanément, mais de façon indépendante ; c'est pourquoi le mérite doit être attribué aux deux. Parmi les nombreux théorèmes qui ont été créés autour des nombres premiers, celui auquel Gauss donna naissance avec sa conjecture occupe une place privilégiée dans l'histoire des mathématiques, non seulement pour sa beauté, mais également pour l'énorme importance qu'il eut dans le développement postérieur de la recherche sur les nombres premiers.

Sur le recto du billet de dix marks, Gauss apparaît à côté de la courbe connue comme « cloche de Gauss ». Sur le verso est reproduit un sextant, instrument employé pour établir l'un des premiers réseaux géodésiques du monde, dans la région de Hambourg, comme on peut le voir dans le coin inférieur droit. La notion de « géodésique », ou chemin le plus court entre deux points d'une surface donnée, est un concept clé de géométrie et fut un autre des apports scientifiques du stupéfiant génie allemand.

Chapitre 5

Les pierres angulaires

L'étude moderne des nombres premiers prend appui sur trois champs théoriques qui en constituent les principaux piliers : l'arithmétique, les nombres complexes et la théorie des fonctions analytiques. Cette dernière théorie est celle qui nécessite les connaissances mathématiques les plus pointues pour pouvoir être abordée. Cependant, l'un de ses aspects, à savoir l'effort effectué pour tenter de visualiser une fonction dont la représentation requiert un espace quadridimensionnel, peut se comprendre facilement et aide ensuite à appréhender la manière dont la fonction zêta de Riemann réussit finalement à imposer un rythme à la suite chaotique des nombres premiers.

Sommes magiques

Comme nous le savons, les nombres ont une signification symbolique, plus ou moins précise, qui varie selon le courant mystique qui la détermine. La majorité de ces symboles, au moins dans le monde occidental, ont une base commune dans la Bible mais aussi dans les écoles pythagoriciennes. « Tout ce qui est connu a un nombre, car sans nombre il n'est pas possible que quelque chose soit conçu ou connu », affirmait un disciple de Pythagore, Philolaos (Crotone, né en 480 av. J.-C.), mathématicien et philosophe grec.

Les temps obscurs du Moyen Âge entravèrent la transmission de cette « culture numérique ». L'Église catholique fit une distinction claire entre les différentes conceptions philosophiques du monde et les principes inamovibles de sa doctrine. L'un des éléments qui réussit, jusqu'à un certain point, à passer à travers le filet de l'intolérance, fut le jeu du tarot. Bien que l'Église ait fini par le condamner, son arithmologie fut préservée dans de nombreux textes au caractère ambigu dans lesquels on ne savait pas très bien s'il s'agissait de rites divinatoires ou d'arithmétique.

Basé sur un système de numération décimale, le tarot assigne une signification particulière à chaque nombre parmi les neuf premiers. Le chiffre 1 correspond à l'unité comme principe unique, le chiffre 2 est le symbole de la polarité, et donc aussi de la génération, la reproduction. Le 3 est la direction que prend le 2 au moyen

de la somme 2 + 1. Le 7, pour prendre un autre exemple, représente l'action du 1, qui développe la puissance contenue dans le 6 : 7 = 6 + 1. Et ainsi de suite...

De cette manière, en partant de l'unité, on attribue des principes élémentaires aux neuf premiers nombres, et n'importe quel autre doit pouvoir être réduit à l'un d'entre eux. C'est ainsi que se définit alors ce que l'on nomme la « somme magique ». L'idée de base consiste à additionner tous les chiffres qui composent un nombre donné pour le réduire à un seul chiffre. Prenons par exemple le nombre 47 ; il se réduit de la manière suivante : 4 + 7 = 11 = 1 + 1 = 2. De cette manière, le nombre 47 est héritier de la symbolique du chiffre 2 mais situé à un niveau supérieur. D'autres réductions seraient, par exemple,

$$157 = 1 + 5 + 7 = 13 = 1 + 3 = 4.$$

Les opérations basiques de somme et de produit se feraient aussi par réduction. Par conséquent, pour faire la somme de deux nombres comme 248 et 396, nous pouvons tout d'abord faire les réductions

$$248 = 2 + 4 + 8 = 14 = 1 + 4 = 5 \text{ et}$$
$$396 = 3 + 9 + 6 = 18 = 1 + 8 = 9,$$

de manière à ce que les sommes de ces deux nombres soient

$$9 + 5 = 14 = 1 + 4 = 5.$$

Si, au lieu de cela, nous commençons par additionner puis ensuite réduire le résultat , nous obtenons

$$248 + 396 = 644 = 6 + 4 + 4 = 14 = 1 + 4 = 5.$$

NOMBRES ET LETTRES

Dans les cultures grecque et hébraïque, les lettres étaient associées à des nombres, de manière à ce que les mots puissent acquérir différentes significations mystiques. L'opération basique consiste en la somme des nombres qui étaient associés à chaque lettre. Pour comparer deux mots, on comparait les nombres correspondants, et celui qui était supérieur à l'autre était considéré comme plus important. La légende raconte que la supériorité d'Achille face à Hector vient du calcul suivant : la somme du mot Achille faisait 1.276, alors que celle d'Hector donnait un résultat inférieur, seulement 1.125.

On vérifie ainsi que cette opération de réduction maintient les résultats de la somme. De manière analogue, pour un produit de deux nombres, nous observons qu'il se passe la même chose :

$$45 \cdot 27 = 1.215 = 1 + 2 + 1 + 5 = 9.$$
$$45 = 4 + 5 = 9.$$
$$27 = 2 + 7 = 9.$$
$$9 \cdot 9 = 81 = 8 + 1 = 9.$$

Si, selon ce critère, nous disposons maintenant tous les nombres entiers naturels en colonnes, de manière à ce que dans chaque colonne figurent tous ceux qui sont équivalents selon la somme magique, nous aurons :

1	2	3	4	5	6	7	8	9
10	11	12	13	14	15	16	17	18
19	20	21	22	23	24	25	26	27
28	29	30	31	32	33	34	35	36
37	38	39	40	41	42	43	44	45
46	47	48	49	50	51	52	53	54
55	56	57	58	59	60	61	62	63
64	65	66	67	68	69	70	71	72
73	74	75	76	77	78	79	80	81
82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99
100	…	…	…	…	…	…	…	…

Nous pouvons maintenant dire que 78 se trouve dans le groupe du 6, ou bien que 93 est dans celui du 3. Dans le langage mathématique actuel, ces groupes sont appelés des « classes d'équivalence ». On parle par exemple, de la « classe du 3 », la « classe du 5 », etc.

Ce type de classification, qui était déjà connu par les mathématiciens, amena Gauss à construire un nouvel outil de calcul qui se révéla être très utile au moment de déterminer certaines des caractéristiques des nombres premiers.

LE CARRÉ MAGIQUE

On a aussi coutume d'appeler « somme magique » l'opération de somme qui est réalisée dans les carrés magiques (une disposition de nombres dans un carré telle que la somme des lignes, des colonnes et des diagonales donne toujours le même résultat). La majorité des cultures ont développé des carrés magiques. De nombreux mathématiciens de renom, comme Stifel, Fermat, Pascal, Leibniz et même Euler, se sont intéressés à ce type de dispositions numériques. De nos jours, on connaît des algorithmes permettant de construire la majorité des carrés magiques.

Carré magique représenté dans le tableau Melencolia I*, œuvre du peintre de la Renaissance Albrecht Dürer.*

L'horloge de Gauss

Le cadran d'une horloge contient douze nombres répartis sur le périmètre d'un cercle. Après le nombre 12 devrait venir le nombre 13, mais nous revenons au début, à 1. Le schéma est quasiment le même que celui que nous avons expliqué pour introduire la méthode des sommes magiques, avec la différence que, au lieu de recommencer à compter à partir de 9, nous le faisons à partir de 12. Nous pourrions construire un tableau similaire au précédent, avec douze colonnes au lieu de neuf. Nous allons seulement remplir les deux premières lignes de ce tableau :

1	2	3	4	5	6	7	8	9	10	11	12
13	14	15	16	17	18	19	20	21	22	23	24
…	…	…	…	…	…	…	…	…	…	…	…

Nous effectuons cette opération lorsque nous regardons notre montre, puisque pour distinguer les heures qui précèdent midi de celles qui suivent, nous continuons à compter à partir du nombre 12. Par exemple, quand nous disons « 17 heures » nous savons que cela correspond à « 5 heures de l'après-midi », car en réalité nous savons que le nombre 17 appartient à la même « classe » que 5. À partir de là, Gauss conçoit différents types d'horloge, ou plus exactement, différents cadrans. Par exemple, une horloge qui aurait simplement cinq heures donnerait un tableau du type :

1	2	3	4	5
6	7	8	9	10
11	12	13	14	15
16	17	18	19	20
…	…	…	…	…

De sorte que, selon le critère que nous avons établi auparavant, nous pouvons dire que le nombre 17 est du groupe du 2 ou, pour le dire de façon plus précise, qu'il appartient à la « classe » de 2.

Il est facile de savoir à quelle classe appartient un nombre quelconque. Par exemple 18 : nous devrions faire 3 tours avec l'aiguille de notre horloge de 5 heures pour atteindre 15 et ensuite recommencer depuis le début pour atteindre le chiffre 3 ; ainsi, 18 appartient à la classe de 3. Cela revient au même que de diviser 18 par 5 et garder le reste de la division, 3. Cette opération est très pratique lorsqu'il s'agit de grands nombres. Si nous souhaitons savoir à quelle classe appartient le nombre 40.248, nous le divisons par 5, ce qui donne un quotient de 8.049 et un reste de 3 ; ainsi, il appartient lui aussi à la classe de 3. Comme les multiples de 5 donnent tous un reste de 0 quand on les divise par 5, l'usage est d'appeler 0 la classe de 5, ce qui donne la forme suivante au tableau.

0	1	2	3	4
10	6	7	8	9
15	11	12	13	14
20	16	17	18	19
…	…	…	…	…

Nous pourrions dire que 17 est équivalent à 2, mais une égalité sous la forme 17 = 2 pourrait prêter à confusion, donc nous avons l'habitude de l'écrire sous la forme 17 ≡ 2.

Nous pouvons donc convenir que cette expression est correcte, mais il paraît évident qu'il faut ajouter un élément : il est primordial de savoir de quel type d'horloge il s'agit. Dans ce cas précis, il s'agit d'une horloge dont le cadran est composé de seulement cinq chiffres, ce que nous indiquons en écrivant *mod 5* à droite. L'expression précédente s'écrirait donc de la façon suivante :

$$17 \equiv 2 \ (mod\ 5).$$

Cette expression équivaut à dire que 17 et 2 sont équivalents modulo 5.

Comme c'était l'habitude à cette époque, Gauss utilisait le latin pour ses écrits scientifiques, raison pour laquelle il adopta le vocable modulo (diminutif de *modulus*). C'est à ce moment-là que naquit ce qui est aujourd'hui connu comme l'arithmétique modulaire, l'un des outils les plus puissants de la théorie des nombres.

Congruences

En arithmétique modulaire, on parle de congruences à la place d'égalités, de sorte que la formulation correcte pour se référer à l'expression précédente est « 17 est congru à 2 modulo 5 ». Pour savoir si deux nombres quelconques sont congrus modulo 5, il suffit de faire la différence et de vérifier que le résultat est un multiple de 5. Dans l'exemple précédent, nous avons $17 - 2 = 15$, qui est un multiple de 5.

$82 \equiv 58 \ (mod\ 4)$ parce que $82 - 58 = 24$, qui est un multiple de 4.

Une fois établi un modulo (un cadran dans l'horloge de Gauss), nous pouvons parler de groupes ou classes pour nous référer à l'un de ses représentants. Supposons que nous choisissions un cadran à quatre chiffres, c'est-à-dire que nous travaillions modulo 4. Nous aurions seulement quatre groupes ou classes de nombres et nous pouvons prendre en guise de représentants les plus simples, qui seraient 0, 1, 2 et 3. Cela signifie qu'au lieu de prendre 382 nous écrirons 2 (car 382 divisé par 4 donne un reste de 2). Ceci nous permet d'établir le tableau des sommes suivant :

0	1	2	3
1	2	3	0
2	3	0	1
3	0	1	2

Rappelons-nous que, par exemple, $2 + 3 = 5$, mais que dans l'horloge de quatre chiffres le chiffre 5 est équivalent à 1 ou, en d'autres termes, $5 \equiv 1 \ (mod\ 4)$.

En suivant les mêmes critères, la table de multiplication est ainsi :

1	2	3
2	0	2
3	2	1

Dans cette table, la curiosité réside dans le fait que deux nombres différents de zéro multipliés entre eux donnent zéro ($2 \cdot 2 = 0$). Il se passerait la même chose si nous construisions la table de multiplication modulo 6 avec les nombres 2 et 3, puisqu'en les multipliant le produit donnerait 6, qui est la même chose que 0 car $6 \equiv 0 \ (mod\ 6)$. Ceci ne se produit pas si le nombre choisi comme modulo est un nombre premier, car ce dernier ne peut se décomposer en produit de facteurs.

Et ici les nombres premiers ont déjà fait acte de présence. Les congruences s'étudient dans l'enseignement secondaire et représentent, d'une certaine manière, une promenade agréable. Mais si nous nous dirigeons vers les contrées éloignées de l'arithmétique modulaire, nous nous trouverons avec « un caillou dans la chaussure », car les nombres premiers sont en effet d'incontournables compagnons de route.

La « calculatrice-horloge » qu'avait créée Gauss est en réalité extrêmement puissante. Il pouvait par exemple savoir que le résultat de la division de 8^{514} par 7 donnait comme reste 1 sans avoir besoin de poser des opérations compliquées, car $8 \equiv 1 \ (mod\ 7)$ ou, ce qui revient au même, 8 divisé par 7 donne comme reste 1. Ce qui veut dire que dans la table de multiplication 8 multiplié par 8 revient au même que de multiplier 1 par 1 :

$8 \cdot 8 = 64$, qui divisé par 7 donne comme reste 1.

Par conséquent, multiplier 8 par lui-même 514 fois revient à multiplier 1 par lui même autant de fois ; en d'autres termes,

$$8^{514} \equiv 1 \ (mod\ 7).$$

Gauss observa dans sa calculatrice-horloge que lorsque le cadran avait un nombre premier p d'heures, ces dernières se répétaient toutes les p fois, c'est-à-dire qu'elles formaient des cycles répétés de p nombres. Gauss reformula donc le petit théorème de Fermat selon sa calculatrice-horloge de la façon suivante :

« Si p est un nombre premier, pour tout nombre entier naturel a on aura donc $a^p = a \ (mod\ p)$. »

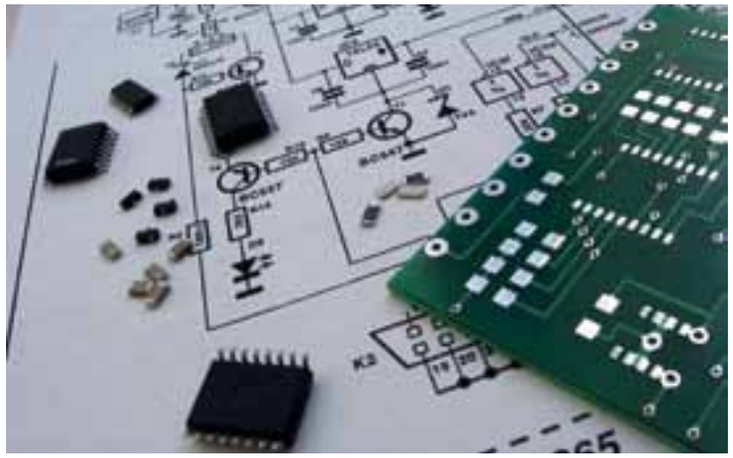
Ou bien, $a^p - a$ est un multiple de p. Par exemple, $3^5 - 3 = 240$ est un multiple de 5. Dans les termes de l'horloge de Gauss, le théorème peut être interprété de la manière suivante. Supposons que nous voulions savoir si p est un nombre premier. Nous construisons une horloge avec un cadran de p heures, nous prenons des nombres différents et nous vérifions si en élevant certains de ces nombres à la puissance p, les aiguilles marquent à nouveau le même nombre. Si tel n'est pas le cas, c'est que d'une manière certaine il ne s'agit pas d'un nombre premier. Supposons

que le nombre que nous souhaitons vérifier est 6. Construisons une horloge avec 6 heures. Prenons maintenant une heure quelconque, par exemple 4 heures. Faisons l'opération $4^6 = 4.096$, qui divisé par 6 nous donne comme reste 4. En d'autres termes, les aiguilles feront des tours successifs autour du cadran jusqu'à ce qu'elles s'arrêtent au chiffre 4. Nous savons de manière certaine que, selon le petit théorème de Fermat, le chiffre 6 n'est pas un nombre premier. Nous pouvons faire la vérification avec un nombre premier, par exemple 7, et nous vérifierons que lorsque nous l'élevons à une heure quelconque, les aiguilles reviennent toujours à la même heure. Il faut se rappeler que le théorème nous montre une condition nécessaire mais non suffisante : si quand nous vérifions avec *a* les aiguilles reviennent au nombre *a*, nous savons que nous avons de bonnes chances pour que le nombre *p* soit premier ; cependant la preuve n'est pas concluante. Plus nous répéterons l'expérience, et plus nous pourrons affirmer avec certitude que le nombre en question est premier, mais nous ne pourrons pas tirer de conclusion définitive. Comme nous le verrons dans le chapitre 7, il s'agit là d'un des systèmes les plus utilisés par l'informatique de nos jours pour obtenir des garanties certaines qu'un grand nombre est premier.

Nombres imaginaires

À entendre cette expression, « nombres imaginaires », le profane peut penser qu'il s'agit de l'une des nombreuses extravagances des mathématiciens. Cette méfiance n'est pas illégitime, puisque cette opinion fut en effet partagée durant très longtemps par de nombreux professionnels de la communauté mathématique qui souhaitaient repousser hors de leur domaine ces nombres si exotiques, qui furent littéralement traités de « fantasmes ». Mais ces fantasmes apparaissaient constamment dans la solution d'équations et il était très difficile de les ignorer. Ils commencèrent alors à être introduits dans les calculs, jusqu'au jour où ils furent acceptés comme solutions des équations et acquirent une identité propre, devenant ainsi un concept fondamental des mathématiques. Il serait faux de croire que leur présence se limite au monde de la pure théorie mathématique ; de fait, les nombres imaginaires constituent un outil de base de la physique actuelle et ont une infinité d'applications pratiques.

Si les logarithmes ont joué un rôle décisif dans le tournant que Gauss imprima à l'histoire des nombres premiers, les nombres imaginaires allaient fermer un cycle avec les théories postérieures de Riemann, ce qui rend donc indispensable un petit voyage à travers le territoire de l'« imaginaire » pour mieux comprendre la révolution que supposèrent ces théories.



Les nombres imaginaires ont une application pratique dans l'ingénierie électronique, dans laquelle on utilise des nombres réels pour mesurer la résistance (opposition que permet un corps lorsqu'un courant électrique le traverse), des nombres imaginaires pour l'inductance (dans une bobine, la relation entre le flux magnétique et l'intensité du courant électrique) et la capacité (différence de tension électrique entre les plaques d'un condensateur et la charge électrique stockée dans ce dernier).

Leibniz dit un jour : « L'esprit divin trouva une sublime expression dans cette merveille qu'est l'analyse, ce prodige du monde idéal, cet amphibie entre l'être et le non-être que nous appelons racine imaginaire de l'unité négative. » Nous allons voir à quoi il faisait référence lorsqu'il parlait de la racine imaginaire de l'unité négative.

La racine carrée d'un nombre *a*, qui est symbolisée par $\sqrt{a}$, est, par définition, un autre nombre *b* tel que en l'élevant au carré nous obtenons *a* ; c'est-à-dire que $\sqrt{a} = b$ signifie que $b^2 = a$. Par exemple :

$$\sqrt{4} = 2 \text{ parce que } 2^2 = 4 ;$$
$$\sqrt{9} = 3 \text{ parce que } 3^2 = 9.$$

D'un autre côté, il existe une règle de signes pour la multiplication et la division qui se traduit par « plus par plus fait plus, plus par moins (ou moins par plus) fait moins » et « moins par moins fait plus », qui, écrit de manière mathématique, donnerait :

$$+ \cdot + = +$$
$$+ \cdot - = - \cdot + = -$$
$$- \cdot - = +$$

Ceci se traduit littéralement dans les opérations entre les nombres :

$$5 \cdot 2 = 10$$
$$(-5) \cdot 2 = -10$$
$$(-5) \cdot (-5) = 25.$$

Selon ce qui précède, le carré d'un nombre, qui est le résultat de ce nombre multiplié par lui-même, ne peut jamais donner un résultat négatif : lorsque le nombre est positif, « plus par plus » donne un résultat positif, et si le nombre est négatif, « moins par moins » donnera aussi un résultat positif. C'est la raison pour laquelle, en principe, il n'est pas possible d'extraire la racine carrée d'un nombre négatif. Par exemple, $\sqrt{-4}$ ne peut être égal à 2, puisque $2 \cdot 2 = 4$, ni d'ailleurs -2, car $(-2) \cdot (-2) = 4$.

Nous pouvons donc affirmer que $\sqrt{1} = 1$, mais $\sqrt{-1}$ n'existe pas. Elle n'existe pas comme nombre réel, mais rien ne nous empêche de la définir comme un nouveau nombre « imaginaire », que nous appellerons i.

$$\sqrt{-1} = i.$$

Voyons ce qu'il advient avec ce nouveau nombre que nous avons obtenu en l'élevant à différentes puissances :

$$\sqrt{-1} = i ;$$
$$i^2 = \left(\sqrt{-1}\right)^2 = -1 ;$$
$$i^3 = i^2 \cdot i = (-1) \cdot i = -i ;$$
$$i^4 = i \cdot i^3 = i \cdot (-i) = -i^2 = -(-1) = 1.$$

Et à partir de là, la même cadence se répète :

$$i^5 = i ;$$
$$i^6 = -1 ;$$
$$i^7 = -i ;$$
$$i^8 = 1 ;$$
$$\ldots$$

La nécessité de trouver la valeur des racines carrées des nombres négatifs est apparue quand on essaya de résoudre certaines équations du second degré. On savait qu'une équation du type $ax^2 + bx + c = 0$ en 2 solutions données par la formule :

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

Mais la solution du problème s'effondrait quand la quantité qui figurait à l'intérieur de la racine était négative.

Dans l'œuvre *Ars magna* de Gerolamo Cardano (1501-1576), publiée en 1545, apparaît le problème suivant : « Diviser 10 en deux parties dont le produit est 40 ». Soit x et y ces deux parties, on a :

$$x + y = 10 ;$$
$$x \cdot y = 40.$$

En isolant $y = 10 - x$ et en remplaçant y dans la seconde équation on obtient : $x(10 - x) = 10x - x^2 = 40$, et en passant tout au second membre, nous obtenons l'équation du second degré $x^2 - 10x + 40 = 0$, dont les solutions seraient :

$$x = \frac{10 \pm \sqrt{100 - 160}}{20} = \frac{10 \pm \sqrt{-60}}{20} = 5 \pm \sqrt{-15}.$$

Cardano étudia les deux nombres qu'il avait obtenus comme solution,

$$5 + \sqrt{-15} \text{ et } 5 - \sqrt{-15}.$$

Conscient du fait qu'il s'agissait là de nombres « complexes », il observe que la somme est 10 et le produit 40 et qu'ils sont donc, en dépit « des tortures mentales qu'ils impliquent », solutions de l'équation proposée.

Ces racines « complexes » apparaissaient souvent comme solutions dans une multitude de problèmes (rappelons que lorsque l'on parle des racines d'une équation, on désigne les possibles solutions de cette dernière). Elles étaient là et incommodaient les mathématiciens, qui ne les considéraient pas comme des nombres. Descartes affirmait, en parlant d'elles : « Ni les vraies racines ni les fausses ne sont toujours réelles, elles sont parfois imaginaires. » C'est ainsi qu'il intronisa l'un des termes qui allait servir pour se référer à ce type de racines : « imaginaires ».

Un nombre imaginaire comme $\sqrt{-4}$ peut s'écrire aussi sous la forme $\sqrt{4} \cdot \sqrt{-1} = 2 \cdot \sqrt{-1}$, et comme nous avons appelé i la racine carrée de -1, nous pouvons poser :

$$\sqrt{-4} = 2i.$$

De sorte que tout nombre complexe peut s'écrire sous la forme $a + bi$, appelée *forme cartésienne* des nombres complexes, dans laquelle « a » est la partie réelle et « b » la partie imaginaire. Par exemple, le nombre $2+\sqrt{-9}$ peut s'écrire sous la forme $2 + 3i$ dans laquelle 2 est la partie réelle et 3 la partie imaginaire. Quand un nombre complexe n'a pas de partie réelle, comme $2i$, on dit alors qu'il est *imaginaire pur*.

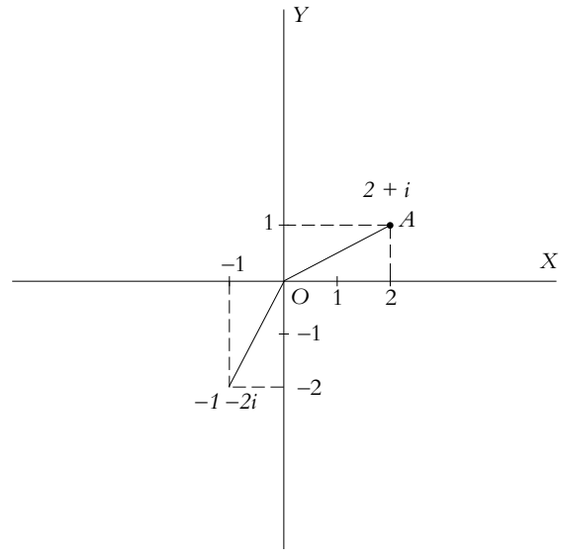
La somme et la soustraction de nombres complexes s'effectuent très facilement de la manière suivante : « La somme de deux nombres complexes est un autre nombre complexe dont la partie réelle est la somme des parties réelles de chacun des nombres et dont la partie imaginaire est la somme correspondante des parties imaginaires. » Par exemple :

$$(3 + 2i) + (8 - 3i) = (3 + 8) + (2 - 3)i = 11 - i.$$

Pour la soustraction, on suit une règle analogue. Pour la multiplication, on peut mettre les nombres l'un en dessous de l'autre et effectuer une multiplication normale et courante, comme nous le ferions avec des nombres quelconques.

En termes algébriques, les nombres complexes pouvaient se manier sans problème, mais il n'était pas possible d'en avoir une image claire, comme celle des nombres réels, qu'il est possible de représenter le long d'une droite, en fixant un point de référence que nous appelons « zéro », puis en situant à la droite de ce dernier les nombres positifs et à sa gauche, les négatifs. Les nombres complexes sont représentés par un couple de nombres, ce qui, d'une manière ou d'une autre, supposait un changement de dimension dans l'espace géométrique. La représentation géométrique des nombres complexes a eu une longue trajectoire historique. Plusieurs mathématiciens, parmi lesquels Euler, Abraham de Moivre ou Alexandre-Théophile Vandermonde, avaient déjà conçu la possibilité d'imaginer un nombre complexe $x + yi$ comme un point du plan de coordonnées (x, y). Mais ce fut grâce au travail de Jean Robert Argand (1768-1822), un comptable passionné de mathématiques dont l'unique apport fut une brève étude sur la représentation géométrique des nombres complexes, ainsi qu'aux exposés de Gauss, qui détermina leur nature géométrique, que les nombres complexes acquirent leur forme définitive telle que nous la connaissons aujourd'hui. De fait, Gauss fut celui qui introduisit le symbole i pour représenter $\sqrt{-1}$, et son avis était que 1, -1, $\sqrt{-1}$, ne devaient pas s'appeler des unités positive, négative et imaginaire mais directe, inverse et latérale. De cette manière, la compréhension des nombres imaginaires aurait été plus rapide, les dépouillant de leur halo de mystère. Il fut aussi celui qui, suivant le même critère, introduisit le terme « nombre complexe » pour le substituer à celui de « nombre imaginaire ».

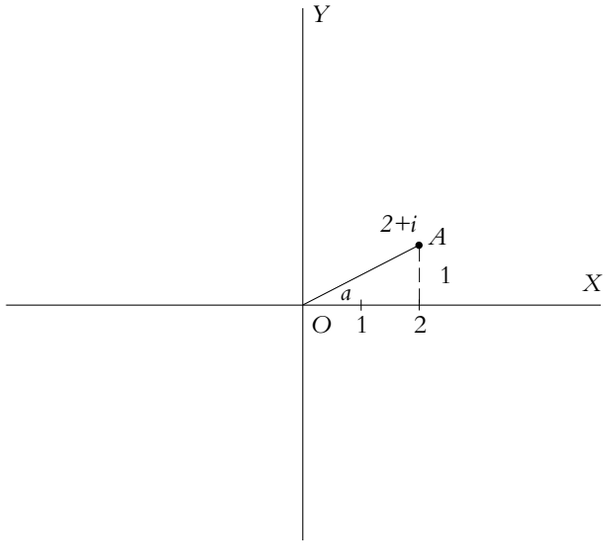
La représentation des nombres complexes est simple et s'effectue de la manière suivante : prenons dans un plan des axes de coordonnées rectangulaires. Nous appellerons l'axe OX axe réel, et nous y situerons la partie réelle du nombre complexe, à sa droite s'il est positif et à sa gauche s'il est négatif. Nous appellerons l'axe OY axe imaginaire, et nous y situerons la partie imaginaire du nombre complexe, dans sa partie supérieure s'il est positif et dans sa partie inférieure s'il est négatif. Ainsi, pour représenter le nombre complexe $2 + i$, nous aurons :



FONCTIONS AVEC DES NOMBRES COMPLEXES

Des premiers calculs effectués par Cardano avec les nombres imaginaires jusqu'au début du XVIII^e^ siècle, les mathématiciens essayèrent d'éviter toute rencontre avec des nombres dont ils mettaient fortement en doute l'existence. Des mathématiciens de la renommée d'Euler, de Wallis ou de d'Alembert se sont attaqués à eux avec plus ou moins de succès. Les nombres complexes commencèrent à se montrer utiles dans des contextes bien spécifiques, en particulier dans les étapes intermédiaires de certaines démonstrations. Gauss fut l'un des premiers à traiter avec eux « en tête à tête » et établit même une façon de les représenter. Mais il faudra attendre le XIX^e^ siècle pour qu'ils s'implantent de façon définitive grâce à l'apparition, du fait de Riemann, des fonctions complexes, fonctions *f(x)* dans lesquelles la variable *x* est un nombre complexe.

Nous prendrons deux unités dans la partie positive de l'axe OX et une unité dans la partie supérieure de l'axe OY. Nous pouvons calculer la distance OA en appliquant le théorème de Pythagore, soit $(OA)^2 = 1^2 + 2^2 = 1 + 4 = 5$, ce qui donne $OA = \sqrt{5}$, quantité qui reçoit le nom de *module* du nombre complexe.



Le fait de pouvoir représenter de façon graphique les nombres complexes représentait un grand pas en avant, car cela signifiait qu'ils allaient pouvoir être utilisés dans l'analyse mathématique des fonctions : la variable pourrait y être représentée par un nombre complexe.

Une dimension supplémentaire

L'observation de la représentation graphique d'une fonction par un œil aguerri peut donner accès à des niveaux d'information insoupçonnés. En ce sens, mis à part son degré excessif de condensation, elle pourrait être considérée comme une œuvre d'art. Comme l'affirmait Lord Kelvin : « Une simple courbe, tracée à la manière de la courbe des prix du coton, décrit tout ce que l'ouïe peut entendre comme résultat des compositions musicales les plus compliquées. À mon avis, ceci est une merveilleuse preuve de la puissance des mathématiques. »

Nous avons déjà vu, dans le chapitre 3, qu'il était possible de représenter des fonctions dans lesquelles était assigné à chaque nombre réel un autre nombre réel.

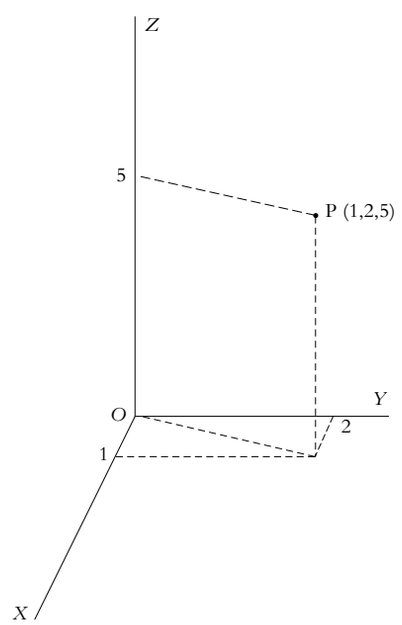
Au moyen d'un mécanisme similaire, il est possible de représenter des fonctions qui assignent un nombre réel à chaque paire de nombres réels. Par exemple :

$$(x, y) \rightarrow x^2 + y^2,$$

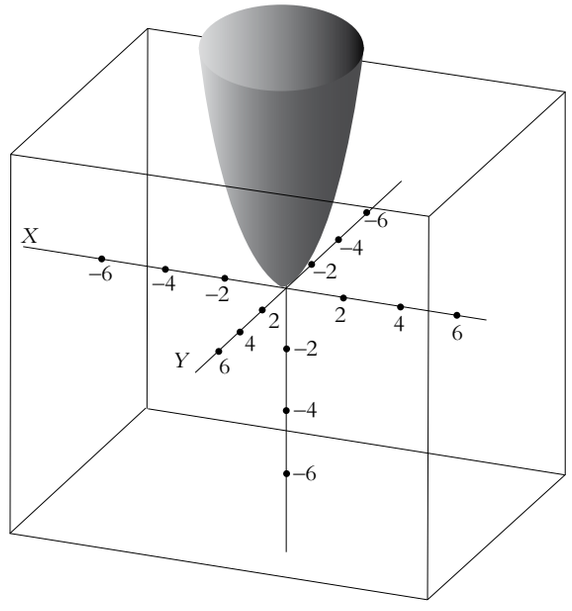
pour laquelle le tableau correspondant serait :

(x, y)	$x^2 + y^2$
(1, 1)	2
(1, 2)	5
(3, 5)	34
(2, 3)	13
…	…

Pour la représentation d'une fonction comme celle-là, il est nécessaire de faire appel à un espace tridimensionnel où, par exemple, l'image du point P (1, 2, 5), qui se trouve dans l'espace est située à une hauteur de 5 dans la direction de l'axe perpendiculaire à ce plan.



Et une représentation de la fonction $f(x, y) = x^2 + y^2$ serait :

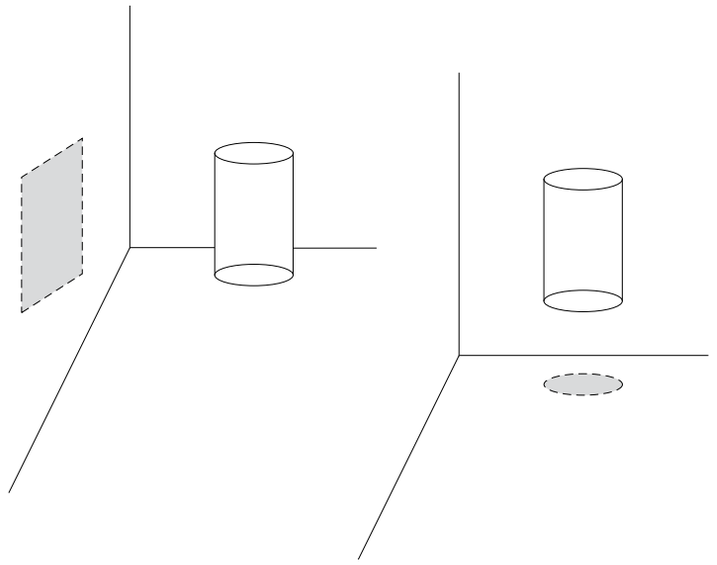


Au XIXe siècle, la théorie des fonctions s'était suffisamment développée pour pouvoir aborder ce type de graphiques de manière relativement satisfaisante. Cependant, le nouveau problème qui allait apparaître à l'horizon était la possibilité d'introduire dans les variables les nombres complexes, un pas qui serait alors décisif dans la recherche sur les nombres premiers.

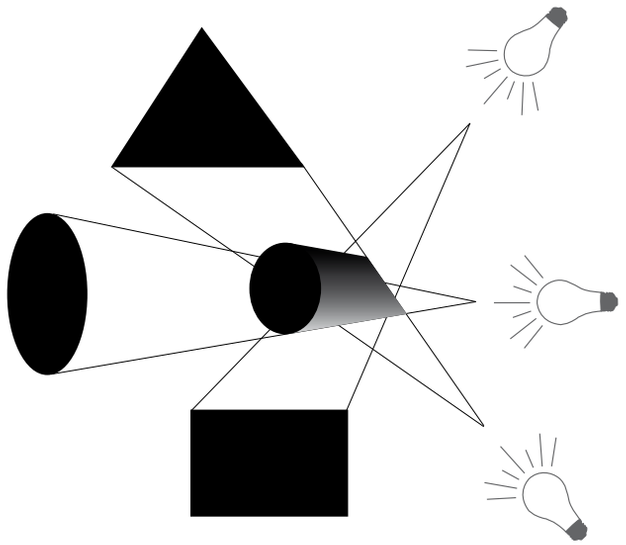
Gauss avait déjà introduit les fonctions de variable complexe en concevant un espace tridimensionnel où il pouvait les représenter. Comme nous le verrons dans le prochain chapitre, Riemann fit un pas supplémentaire et définit ce que devaient être les fonctions d'une variable complexe et à valeurs complexes. Dans les représentations spatiales que nous avons vues jusqu'à présent, l'image de deux nombres donnait comme résultat un autre nombre. Nous partions d'une position dans le plan et nous calculions l'image dans un troisième axe, ce qui implique de travailler dans un espace à trois dimensions. Mais il s'agit maintenant d'obtenir que, partant d'un point avec deux coordonnées, l'image soit aussi un point avec deux coordonnées. En d'autres termes, il nous manque une dimension pour pouvoir effectuer la représentation graphique car une fonction de ce type ne peut se représenter que dans un espace à quatre dimensions. Visualiser un graphique à quatre dimensions

est une possibilité qui demeure réservée au domaine de la science-fiction. Par conséquent, il ne nous reste plus qu'à utiliser certaines astuces pour nous donner une idée de la forme que pourrait avoir l'objet en question.

Une possibilité est d'étudier ses projections sur l'espace à trois dimensions, comme si nous examinions ses ombres. Pour le comprendre, il est très utile d'imaginer que nous nous déplaçons dans un espace à deux dimensions, que nous sommes des êtres complètement plats et que nous essayons de vérifier la forme que peut avoir un objet qui occupe un espace à trois dimensions. Une ombre est la projection sur un plan d'un objet illuminé par un projecteur. Il est possible que l'ombre projetée sur un plan soit insuffisante et que nous ayons besoin de deux ou trois autres projections supplémentaires. Par exemple, un cylindre qui se trouve suspendu dans l'air au milieu d'une maison pourrait projeter sur l'un des murs la figure d'un rectangle, ce qui pourrait nous induire en erreur quant à la figure que nous sommes en train d'étudier. Nous pourrions penser qu'il s'agit d'un parallélépipède, qui projetterait le même type d'ombre. Mais si nous observions l'ombre qu'il projette sur le sol, nous nous rendrions compte qu'il s'agit d'un cercle, ce qui changerait immédiatement notre première idée et nous permettrait une meilleure approximation de la réalité du cylindre. Le problème est que, étant des êtres bidimensionnels, nous n'aurions jamais vu un cylindre en trois dimensions.



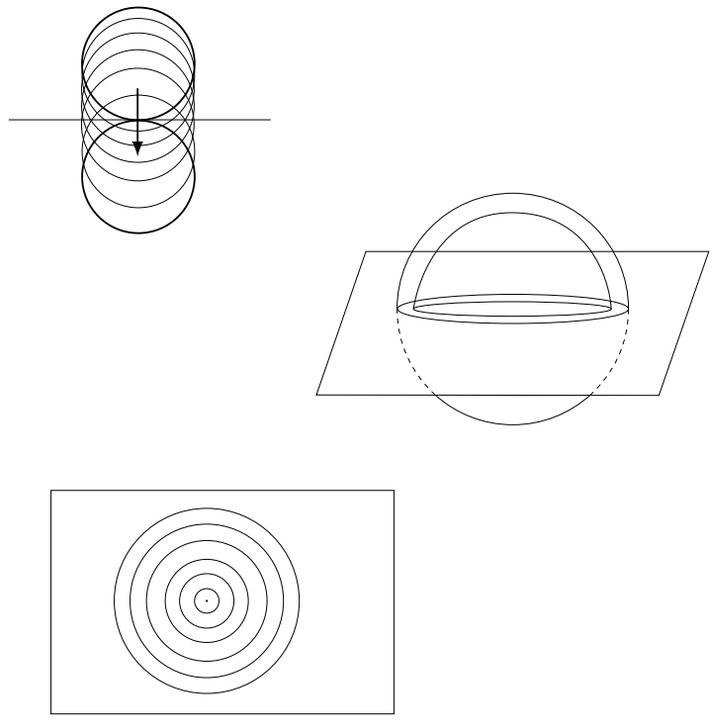
D'un autre côté, les ombres peuvent être plus trompeuses ou très difficiles à interpréter. Pensons par exemple à un objet qui éclairé sur le côté droit donne l'ombre d'un cercle sur le mur. En revanche, quand il est éclairé par en dessous, l'ombre est un triangle, et en éclairant par en haut, cela donne un carré. Existe-t-il un objet tridimensionnel avec ces caractéristiques ? S'il existait, il pourrait s'agir d'un bouchon très particulier qui servirait pour reboucher les bouteilles dont le goulot serait circulaire, triangulaire ou carré.



La question qui se pose désormais est de savoir s'il existe une relation entre les différentes ombres d'un même objet qui puisse nous permettre de définir la forme tridimensionnelle de l'objet. La réponse à cette question difficile fut obtenue en 1986 par un professeur de mathématiques à l'université de St. Andrews, Ken Falconer, comme la conséquence d'un théorème. Et la réponse est non ; en général, il n'existe aucune relation de ce type.

Comment faire alors pour connaître la forme d'une figure située dans un espace à quatre dimensions ? Nous ne pourrons jamais savoir la forme exacte qu'elle a, entre autres parce que même si nous avions la possibilité de la représenter, nous n'aurions ni la faculté ni les sens nécessaires pour la voir. En revanche, il existe des techniques analytiques qui nous permettent de connaître certaines caractéristiques géométriques de la figure en question.

Pour reprendre notre image précédente, ces techniques s'apparentent à celles que nous utiliserions pour connaître la forme d'une sphère si nous étions des êtres bidimensionnels. L'astuce consisterait à obtenir des coupes transversales de la sphère dans son intersection avec le plan dans lequel nous nous trouverions et à observer attentivement les figures obtenues. Quand la sphère serait tangente au plan, la première chose que nous verrions serait un point. Ensuite apparaîtrait une série de cercles concentriques dont la taille augmenterait petit à petit, pour ensuite commencer à diminuer jusqu'à se transformer à nouveau en un point, quand la sphère aurait terminé de couper totalement le plan.

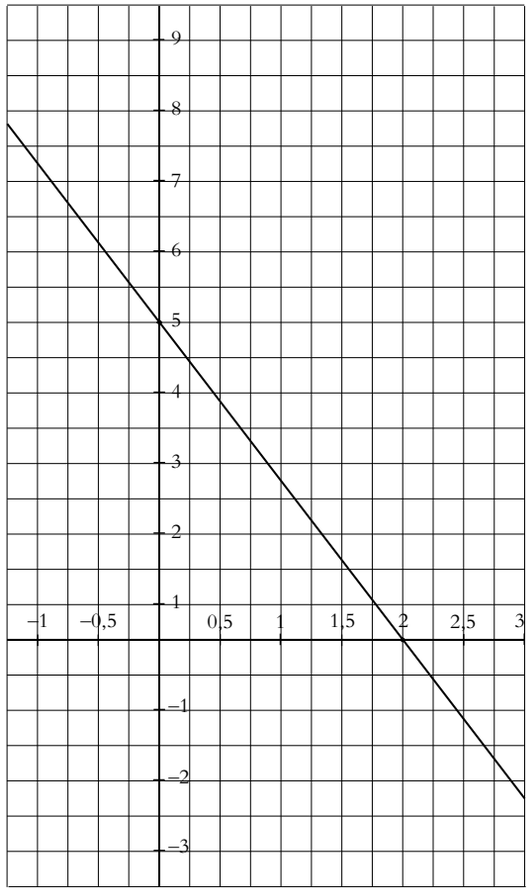


Dans cet exemple, nous pouvons avoir une perspective claire de la situation car nous avons le privilège de pouvoir adopter un point de vue en trois dimensions, ce qui n'est pas le cas quand il s'agit d'un espace quadridimensionnel. Mais le plus important est que nous pouvons savoir ce qui se passe dans l'espace de l'intersection, dans la coupe de la figure par le plan ; or, cela est en étroite relation avec ce qu'on appelle les zéros de la fonction.

Une équation comme $-\frac{5x}{2}+5=0$ peut facilement se convertir en une fonction de la façon suivante :

$$y=-\frac{5x}{2}+5.$$

Si nous la représentons, nous aurons une droite. L'intersection de cette droite avec l'axe horizontal $x = 2$ est précisément la solution de cette équation ; ici, on obtient $x = 2$.

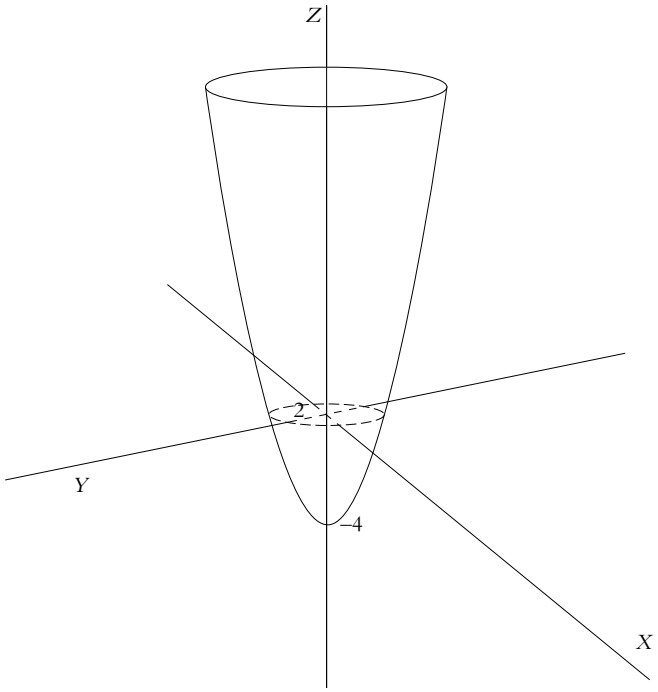


De façon analogue, si nous avons la fonction du second degré $x^2 + x - 2 = 0$ et que nous représentons la fonction $f(x) = x^2 + x - 2$, nous observons que l'intersection de cette fonction avec l'axe OX nous donne deux points qui sont précisément les solutions $x = 1$ et $x = -2$ de l'équation.

Si nous élevons le problème à trois dimensions, l'équation $x^2 + y^2 - 4 = 0$ peut se représenter par une fonction comme $f(x,y) = x^2 + y^2 - 4$, qui est un paraboloïde dont l'intersection avec le plan XY nous donne un cercle de rayon 2, comme on peut l'observer dans la figure suivante. Tous les points de ce cercle sont solutions de l'équation proposée.

LEGS CULTUREL

Si nous disions qu'« une fonction est une quantité composée d'une quelconque manière à partir d'une variable et de constantes arbitraires », cette définition ne serait pas acceptée à un examen élémentaire de mathématiques, car elle indiquerait que le concept de fonction n'est pas encore clair pour l'auteur de ces mots. L'auteur de ces mots est pourtant Jean Bernoulli, l'un des plus importants mathématiciens du XVIIIe siècle. Il ne fut pas facile d'établir le concept de fonction, auquel a aujourd'hui accès n'importe quel élève de l'enseignement secondaire ; ce fait démontre l'extraordinaire solidité des mathématiques comme legs culturel.



De sorte que lorsque nous employons l'astuce illustrée auparavant pour « voir » comment est une figure à quatre dimensions, ce qui est intéressant est en réalité d'avoir une idée précise de l'intersection de cette figure quadridimensionnelle dans l'espace à trois dimensions. Ceci ne nous donnera pas une idée précise de la forme de la figure, que d'un autre côté nous savons que jamais nous ne pourrons avoir, mais une idée des solutions que propose l'équation correspondante. Et cela était, comme nous le verrons dans le prochain chapitre, l'objectif de Riemann quand il analysa la fameuse fonction zêta, qui allait essayer d'imposer un rythme à l'ensemble des nombres premiers.

Chapitre 6

Les deux faces d'une pièce

L'Allemand Bernhard Riemann (1826-1866) et l'Indien Srinivasa Ramanujan (1887-1920) représentent, pour le premier, le paradigme de la rigueur mathématique, et pour le second, l'imagination à l'état pur. Tous deux eurent affaire aux nombres premiers et connurent des succès et des échecs. Dans les deux cas, par leur vie et leur travail, ils sont des représentants extraordinaires de la pensée mathématique.

Bernhard Riemann

Riemann est le moteur qui arrive à imposer un rythme afin que tout le public (les nombres premiers) se mette à applaudir à l'unisson. Il s'agit en réalité d'un rythme très compliqué. La vulgarisation scientifique, particulièrement en mathématiques, devient relativement difficile quand on aborde certains domaines. Le vulgarisateur devient en quelque sorte un guide de montagne. Lorsqu'il s'agit d'une simple randonnée, il suffit juste de ne pas se tromper de route, mais lorsqu'il s'agit de gravir une falaise, les choses changent. Il y a certaines excursions qui demandent un effort particulier, et il faut alors progresser lentement afin que l'ascension ne soit pas trop éprouvante. Puis, à partir d'une certaine altitude, les randonneurs doivent avoir reçu une certaine préparation et être équipés du matériel adéquat. Ce n'est pas la même chose de gravir un pic de 2 000 m ou un de 4 000. Avec Riemann, c'est le second que nous abordons.

Georg Friedrich Bernhard Riemann naquit à Breselenz, dans le royaume de Hanovre. Sans doute à cause de sa grande timidité et de sa peur quasi pathologique de s'exprimer en public, il n'a pas suivi la voie tracée par son père, pasteur luthérien. Friedrich Constantin Schmalfuss, directeur de l'école dans laquelle étudia le jeune Riemann, lui permit de rapporter chez lui l'un de ses livres personnels, la *Théorie des nombres* de Legendre, un traité de mathématiques d'une grande complexité. Riemann le dévora en à peine une semaine et le lui rendit en lui disant qu'il l'avait trouvé très intéressant. Ce n'était pas du bluff : de ce traité, il allait en effet tirer des années plus tard les éléments nécessaires pour élaborer sa théorie sur les nombres premiers, donnant naissance à l'une des conjectures les plus célèbres de l'histoire des mathématiques.

À 19 ans, Riemann assista, à l'université de Göttingen, aux conférences mathématiques de Moritz Stern ; c'est à ce moment-là qu'il eut son premier contact avec les travaux de Gauss. Une année plus tard, il s'inscrivit en mathématiques à l'université de Berlin, où il eut comme professeurs Peter Gustav Lejeune Dirichlet, Carl Jacobi, Jakob Steiner et Ferdinand Eisenstein. Grâce à l'intense relation qu'il entretint avec ce dernier naquit l'une des plus importantes théories mathématiques du XIXe siècle, la « théorie des fonctions d'une variable complexe », un outil fondamental qui allait lui permettre d'établir son hypothèse en relation avec les nombres premiers.

Bernhard Riemann.

THÈSE DOCTORALE

« Je pense que j'ai amélioré mes perspectives avec ma dissertation. J'espère aussi apprendre à écrire plus rapidement et avec une plus grande fluidité, surtout si je fréquente la société et que j'ai l'opportunité de donner des conférences ; c'est pourquoi j'ai du cœur à l'ouvrage ». Dans ces lignes d'une lettre à son père, Riemann se réfère à la soutenance de sa thèse doctorale qu'il présenta à l'université de Göttingen à l'âge de 25 ans, et dont le titre était *Fondements pour une théorie générale des fonctions d'une variable complexe*. Sa soutenance éveilla l'enthousiasme de Gauss, l'une des figures mythiques des mathématiques de l'époque.

La fonction zêta

Comme nous l'avons vu dans le chapitre 3, Euler a défini une fonction basée sur une suite harmonique et dont l'expression est

$$\zeta(x) = \frac{1}{1^x} + \frac{1}{2^x} + \frac{1}{3^x} + \frac{1}{4^x} + \ldots + \frac{1}{n^x} + \ldots = \sum_{n=1}^{\infty} \frac{1}{n^x}.$$

Le mathématicien suisse avait déjà vérifié que la suite était infinie si x prenait des valeurs inférieures ou égales à 1. Il réussit à calculer certaines valeurs, pour $x = 2$ et $x = 4$.

$$\zeta(2) = \frac{\pi^2}{6} \; ; \; \zeta(4) = \frac{\pi^2}{90}.$$

Nous avons vu aussi que le même Euler avait établi une relation entre cette fonction et les nombres premiers (le « produit d'Euler »), relation qui lui servit ensuite ainsi qu'à d'autres mathématiciens pour démontrer l'infinité des nombres premiers. En son temps et au moyen de techniques élémentaires, Euclide avait déjà démontré l'infinité des nombres premiers.

D'un autre côté, Gauss avait trouvé, mais pas démontré, que pour des grandes valeurs de x,

$$\pi(x) \approx \frac{x}{\ln x}.$$

Rappelons que $\pi(x)$ est le nombre de premiers inférieurs à x.

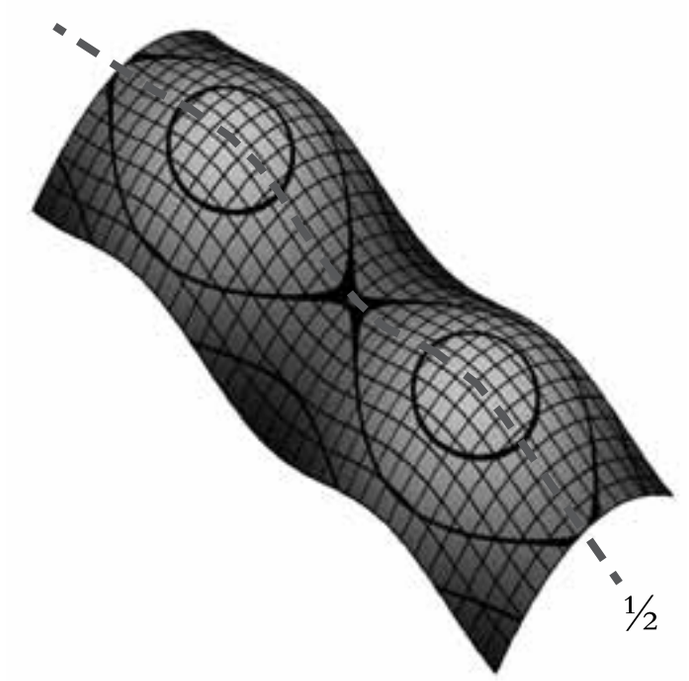
Riemann proposa d'étudier l'hypothèse de Gauss en se servant de la fonction zêta d'Euler et pensa que la meilleure façon de faire était d'élargir cette fonction au domaine des nombres complexes. Pour cela, il imagina un système appelé « prolongation analytique » (en toute rigueur, nous devrions nous référer à ce système quand nous parlons de la fonction zêta de Riemann) :

$$\zeta(x) = \sum_{n=1}^{\infty} \frac{1}{n^x} = \prod_{p} \frac{1}{1 - p^{-x}}.$$

La seconde partie de cette égalité, un produit infini étendu à tous les nombres premiers p, fait référence au produit d'Euler et met en relation la fonction zêta avec les nombres premiers (rappelons que ce produit était obtenu comme la conséquence directe du théorème fondamental de l'arithmétique d'Euclide).

Nous avons vu que Gauss avait introduit les fonctions d'une variable complexe en concevant un espace tridimensionnel dans lequel elles pouvaient être représentées. Riemann fit un pas supplémentaire et définit ce que doivent être les fonctions complexes d'une variable complexe. Le problème était dorénavant de pouvoir visualiser ces fonctions, ce qui aurait nécessité un espace à quatre dimensions.

En utilisant des techniques sophistiquées, similaires à celles évoquées dans le chapitre précédent, Riemann a obtenu une image tridimensionnelle des zéros de la fonction zêta, un paysage dans lequel apparaissent des vallées et des montagnes réparties avec une certaine régularité.



Dans cette fonction, il y a deux classes de zéros, c'est-à-dire deux classes de valeurs qui, en remplaçant x dans la fonction, donnent comme résultat zéro. Il y a tout d'abord les entiers naturels pairs négatifs $x = -2$, $x = -4$, $x = -6$,… qui sont appelés « solutions triviales ». Les autres zéros n'ont rien de trivial, et leur calcul est extrêmement difficile : il en existe une infinité et ils se trouvent tous dans ce que l'on appelle la « bande critique », où les valeurs réelles se situent entre 0 et 1 ($0 \leq Re(x) \leq 1$), une partie du paysage qui est intimement liée aux nombres premiers. C'est dans ce contexte que deux mathématiciens, Jacques Hadamard et Charles de La Vallée Poussin, démontrèrent en 1896, indépendamment l'un de l'autre, le « théorème des nombres premiers » qui avait été énoncé par Gauss.

Dans une note informelle et sans aucune démonstration, Riemann avança que tous les zéros non triviaux de la fonction zêta étaient de la forme $½ + iy$, et que cela

revenait à dire qu'ils se trouvaient sur la droite $x = ½$. Cette affirmation constitue ce qui est connu comme étant la conjecture ou l'hypothèse de Riemann, qui dit :

« La partie réelle de tout zéro non trivial de la fonction zêta est ½. »

Si l'hypothèse est vraie, cela signifie que tous les nombres premiers se distribuent de manière régulière, ou, pour être plus exact, de la manière la plus régulière possible. Ceci peut s'interpréter, au moyen d'une analogie, de la façon suivante : imaginons une fonction qui représente l'analyse d'un son, une série de courbes sinusoïdales qui traduisent un concert de violon. Pour l'expliquer plus clairement, supposons qu'il s'agit d'un seul violon. À côté d'une série de crêtes et de vallées bien définies, peuvent apparaître d'autres figures moins bien définies et qui, d'une certaine manière, « rompent l'harmonie » de la courbe. C'est ce qu'on appelle en langage technique le « bruit aléatoire », qui est dû à différentes

VOUS POUVEZ L'ESSAYER

Si vous décidez d'accroître vos connaissances sur les fonctions d'une variable complexe et les séries, sujets sur lesquels il existe une abondante bibliographie, vous pouvez essayer de démontrer l'hypothèse de Riemann. Si vous réussissez, le Clay Mathematics Institute vous gratifiera de la belle somme d'un million de dollars comptant, sans distinction d'âge, de sexe ou de profession. Il est juste probable que l'attribution du prix tardera un peu, car il faut en effet vérifier que la démonstration est correcte. En juin 2004, Louis de Branges de Bourcia, mathématicien de l'université Purdue West Lafayette, dans l'Indiana, affirma l'avoir démontrée, mais sa démonstration ne fut pas acceptée. La même chose se produisit en 2008.

Louis de Branges de Bourcia

causes (sons électrostatiques, bruit ambiant sporadique). L'hypothèse de Riemann vient affirmer que les possibles irrégularités qui apparaissent dans la répartition des nombres premiers proviennent du bruit aléatoire, ce qui voudrait dire que les nombres premiers suivent une règle de distribution et que cette distribution n'est pas due au hasard. C'est pourquoi nous avons affirmé précédemment que Riemann avait réussi à imposer un rythme à cette folle répartition.

En 1914, les mathématiciens britanniques Godfrey Harold Hardy (1877-1947) et John Edensor Littlewood (1885-1977) démontrèrent qu'il existait une infinité de zéros sur la droite, ce qui ne démontre pas l'hypothèse de Riemann, mais en tout cas accrédite l'opinion, très répandue dans la communauté mathématique, selon laquelle cette hypothèse est vraie. On pourrait penser que s'il y a une infinité de zéros sur la droite critique, ils doivent tous y être, mais il s'agit là d'une opinion qui indique une certaine méconnaissance à l'égard du concept d'infini (un monde rempli de paradoxes). En outre, il est possible qu'il y ait une infinité de zéros qui ne soient pas présents sur cette droite. Actuellement ont été calculés quelque dix millions de zéros non triviaux qui se trouvent sur la droite critique.

On a demandé au mathématicien allemand David Hilbert quelle serait la première question qu'il poserait s'il pouvait assister à un congrès de mathématiciens cent ans après sa mort. Sa réponse fut : « Je demanderais si la conjecture de Riemann a été démontrée ». À ce jour, ce n'est pas le cas.

À propos de Ramanujan : sur la pensée mathématique

Henri Poincaré (1854-1912) affirmait que le travail du mathématicien s'effectuait en trois étapes.

La première consiste en une analyse minutieuse qui met en évidence les difficultés d'un problème, les différentes approches nécessaires pour l'aborder, et les outils dont on dispose, ce qui suppose une complète révision de ses connaissances.

La suivante est définie comme une étape d'abandon apparent. Il faut arrêter de penser au problème, ou tout du moins, arrêter d'y penser de manière déterminée, afin que l'esprit s'engouffre dans ce mystérieux territoire de l'inconscient, dans lequel l'activité créatrice suit ses propres règles. C'est le territoire de l'imprécision, de l'inexactitude et de l'errance intellectuelle. Le résultat de ce processus inconscient peut apparaître à tout moment, par surprise et en fonction d'événements qui n'ont apparemment rien à voir avec l'objet de la recherche. C'est un tel moment

qu'évoque le mathématicien irlandais Sir William Hamilton (1805-1865) quand il raconte que, le 6 octobre 1843, comme il se promenait avec sa femme aux alentours de Dublin, il s'arrêta brusquement comme s'il avait été frappé par la foudre. Selon ses propres mots : « …C'est ici que j'ai refermé le circuit galvanique de mes pensées et les étincelles qui en jaillirent furent les équations fondamentales entre i, j, k… » Ce qu'Hamilton venait de découvrir, c'était qu'il fallait non pas trois,

LES PARADOXES DE L'INFINI : L'HÔTEL D'HILBERT

L'hôtel d'Hilbert est un hôtel imaginaire qui dispose d'une infinité de chambres. Son gérant s'enorgueillit du fait qu'il ne laisse jamais tomber un client. Une nuit, toutes les chambres de l'hôtel étant occupées, un nouveau client se présente. Le concierge demande de l'aide au gérant et lui signale l'impossibilité de loger le nouveau client. Le gérant lui répond qu'il faut qu'il demande aux autres clients qui sont déjà logés de bien vouloir changer de chambre et se décaler à la suivante, de manière à ce que celui ou celle qui occupe la n° 1 passe dans la 2, celui de la 2 dans la 3, etc. Une fois cette opération réalisée, la chambre 1 sera libre et le nouveau client pourra s'y installer. Mais à minuit, le concierge fait de nouveau appel au gérant, cette fois-ci vraiment désespéré. En effet, vient de se présenter à l'accueil un groupe infini de mathématiciens qui viennent assister à un congrès. « Cette fois-ci, il sera absolument impossible de tous vous loger ! » Après mûre réflexion, le gérant propose la solution suivante : « Nous devons demander une faveur à nos clients. Chacun d'eux devra multiplier par 2 son numéro de chambre et déménager dans la chambre dont le numéro sera le résultat de cette petite opération. » C'est-à-dire que celui qui était dans la 8 passe dans la 16, celui de la 23 dans la 46, celui de la 352 dans la 704, et ainsi de suite. Une fois cette opération réalisée, toutes les chambres dont le numéro est impair seront libres, et comme il y a une infinité de chambres, il sera donc possible de loger tous les membres du congrès.

Portrait de David Hilbert réalisé en 1912.

mais quatre nombres pour décrire le comportement spatial d'un nombre hypercomplexe. C'est le moment magique au cours duquel le chercheur a l'impression qu'une lumière s'est tout à coup allumée dans une chambre dans laquelle il n'avait jamais mis les pieds. Poincaré analyse donc le processus de sélection qu'effectue l'inconscient pour amener au conscient certaines idées et en refuser d'autres, et en arrive à la conclusion que, dans la mesure où l'inconscient n'a pas la capacité de vérifier si ces idées sont justes ou fausses, son unique critère de sélection est la beauté mathématique.

Henri Poincaré fut un homme de science reconnu dans tous les domaines des mathématiques.

À partir de ce point, la troisième étape est celle de la pleine conscience : le mathématicien soumet alors les idées à un jugement sévère, en acceptant certaines et en refusant d'autres. Il peut y avoir un ou plusieurs retours à la deuxième étape jusqu'à ce que finalement, si le problème est résolu, il se soumette aux règles du jeu qu'impose le formalisme mathématique. Alors, enfin, est donnée à la solution sa forme définitive.

Toutes les étapes sont importantes dans une découverte mathématique, mais, pour beaucoup, la deuxième est la plus fascinante car c'est celle du « vol libre » de l'esprit qui n'est pas soumis à la rigueur de la pensée consciente. Jacques Hadamard dédia une de ses œuvres, *Essai sur la psychologie de l'invention dans le domaine mathématique* (1945), à l'étude du rôle joué par l'inconscient dans l'activité créatrice, en se centrant particulièrement sur l'esprit mathématique. Dans cette œuvre, il décrit la création mathématique comme un processus qui débute avec un choix délibéré des aspects les plus importants du problème, ne permettant pas d'obtenir, dans la majorité des cas, des résultats concluants. Hadamard pensait que cette période devait être suivie d'un « repos », d'une autre période où le chercheur devait se tenir éloigné du problème, et au cours de laquelle apparaissaient pour lui de manière inattendue des moments d'inspiration, des illuminations, dus à des processus non conscients.

Alors enfin arrivait l'état dit « de précision », dans lequel le formalisme reprenait ses droits pour ordonner les résultats de façon séquentielle. Hadamard considérait que l'intervention de l'inconscient tout au long du processus créatif était cruciale, particulièrement pendant la période de repos.

Les conclusions d'Hadamard coïncident avec celles de Poincaré. La seule différence est que Poincaré accordait un rôle plus important aux périodes de repos. Il faut comprendre ici « repos » y compris au sens littéral, puisque ces périodes comprennent aussi les phases de sommeil. Divers témoignages dans l'histoire de la science, et de la créativité mathématique en particulier, attestent que de nombreuses « idées clés » dans le processus de recherche apparaissent pendant le sommeil. Il est notable que, dans la majorité des cas, il n'est pas question d'un sommeil concret durant lequel l'auteur aurait travaillé à sa recherche, mais du fait qu'il ait trouvé au réveil la solution à un problème auquel il avait travaillé intensément la veille. Dirichlet disait qu'il dormait avec les *Disquisitiones arithmeticae* de Gauss sous son oreiller parce qu'il savait que durant son sommeil avait lieu un processus mystérieux, qu'il ne contrôlait pas, et grâce auquel le jour suivant il réussissait à percer les parties obscures du texte qu'il n'avait pas réussi à déchiffrer la veille.

Tout ceci fait aussi partie du monde magique auquel nous avons déjà fait référence. Il ne s'agit pas là de magie au sens commun du terme. Dans l'acception traditionnelle, les rituels et les cérémonies magiques avaient pour objet que « quelqu'un » ou « quelque chose » nous révèle des vérités occultées. Dans la signification que nous voulons lui donner ici, il s'agit du fait qu'un rituel, une croyance, ou mieux encore, l'activité onirique elle-même laisse l'esprit dans un état particulier dans lequel, étant libéré de certaines sujétions, il peut exercer un autre type de pensée. C'est comme si les paramètres d'un récepteur étaient changés afin que, dans une bande de fréquence déterminée, il puisse entendre des choses différentes alors que l'émetteur n'a pas changé. Nous stockons l'information dans notre cerveau, mais il peut y avoir plusieurs manières différentes de la gérer. Dans ce schéma mental que nous sommes en train d'exposer, il y a un mathématicien qui pourrait être considéré comme paradigmatique. En effet, on peut affirmer que Ramanujan se déplaçait à son aise dans la deuxième des trois étapes créatrices que définissaient Poincaré et Hadamard, et qu'il éprouvait de sérieuses difficultés dans la troisième. Du fait des conditions dans lesquelles il s'était formé aux mathématiques, il manquait des ressources qu'offre une formation académique sur le plan du formalisme que requiert toute démonstration. En d'autres termes, Ramanujan pouvait « voir » des résultats, mais il éprouvait de sérieuses difficultés à les démontrer, tout du moins à

les démontrer dans le cadre que la communauté mathématique considérait comme adéquat. Ramanujan ne serait pas une légende si l'on ne disposait pas d'une documentation précise sur son histoire et ses travaux mathématiques. Sans éducation ni ressources économiques, il devint l'un des plus importants mathématiciens de son époque et le plus grand de toute l'histoire de l'Inde.

Srinivasa Ramanujan

Ramanujan naquit le 22 décembre 1887 à Erode, une petite ville située à 400 km de Madras, au sein d'une famille très modeste. À sept ans, il réussit à obtenir une bourse qui lui permit d'assister aux cours dans un collège de Kumbakonam. Ses dons extraordinaires dans le domaine des nombres, sur le plan de la mémoire comme du calcul, se manifestèrent dès sa plus tendre enfance. Il était capable de réciter de mémoire des centaines de décimales de π et de la racine carrée de 2. Le premier texte de mathématiques qui tomba entre ses mains fut *Synopsis of Elementary Results in Pure Mathematics*, de G. S. Carr. Il avait alors 15 ans et l'on peut considérer que c'est avec cet ouvrage qu'il réalisa son premier travail de recherche. Il s'agissait d'un texte synthétique, dans lequel figuraient peu de démonstrations, et qui, étant donnée la situation de précocité mathématique dans laquelle il se trouvait, était pratiquement incompréhensible.

À 16 ans, il réussit à avoir une bourse pour intégrer le collège du gouvernement de Kumbakonam. Mais la passion que Ramanujan éprouvait pour les mathématiques fit qu'il y consacra tout son temps et, par conséquent, laissa de côté les autres matières, ce qui lui valut de perdre la bourse. À partir de ce moment-là, il ne valida aucune autre matière à part les mathématiques.

En 1909, il se maria et fut donc obligé de trouver un travail qui lui permette de faire vivre sa famille. Grâce à un ami, il réussit à obtenir une lettre de recommandation pour collaborer avec un passionné de mathématiques, Diwan Behadur R. Ramachandra Rao, qui était percepteur des impôts de Nelore, à 130 km au nord de Madras. Voici comment ce dernier décrit le premier entretien avec Ramanujan :

Timbre indien émis en 1962 en commémoration du 75e anniversaire de la naissance de Srinivasa Ramanujan.

« Il y a quelques années, un de mes neveux, qui ne connaissait rien aux mathématiques, me dit : "Mon oncle, j'ai un visiteur qui parle de mathématiques mais je ne comprends rien. Pourrais-tu voir s'il y a un intérêt quelconque à ses paroles ?" Et dans la plénitude de mes connaissances mathématiques, je consentis à recevoir Ramanujan. Une petite figure rustique, vigoureuse, pas rasée, négligée, avec des traits caractéristiques, des yeux brillants, entra avec un livre de notes usé sous le bras. Il était extrêmement pauvre. Il avait fui Kumbakonam pour Madras dans le but de réussir à trouver des financements pour continuer ses études. Il ne demanda jamais aucune distinction. Il cherchait juste un soulagement. En d'autres termes, qu'on lui fournisse le minimum vital sans efforts de sa part pour lui permettre de rêver. Il ouvrit le livre et commença à expliquer certaines de ses découvertes. Je vis tout de suite qu'il ne s'agissait pas là de quelque chose de courant, mais mes connaissances ne me permettaient pas de juger si ses paroles avaient un sens. Je lui demandai alors de reprendre tout depuis le début, ce qu'il fit. Il apprécia dûment mon ignorance et me démontra quelques-unes de ses trouvailles les plus simples. Elles allaient bien plus loin que les livres existants et je ne doutais plus qu'il s'agissait là d'un homme remarquable. Ensuite, petit à petit, il m'initia aux intégrales elliptiques et aux séries hypergéométriques et, finalement, sa théorie des séries divergentes, non encore divulguée, me convainquit. Je lui demandai alors ce qu'il souhaitait. Il me dit qu'il souhaitait une petite pension pour vivre et pouvoir ainsi continuer ses recherches. »

Ramanujan, qui refusait de vivre d'une quelconque charité, accepta finalement un travail de comptable dans la Compagnie du port de Madras. Même si, par sens des responsabilités, il honorait ses engagements envers la Compagnie, son esprit et son âme n'avaient qu'un seul objectif : avoir des moyens suffisants pour subvenir à ses besoins et à ceux de sa famille et pouvoir se consacrer aux mathématiques.

Maison de Ramanujan à Kumbakonam, ville dans laquelle le mathématicien indien mourut le 26 avril 1920.

Ramanujan possédait aussi le « don des nombres » auquel nous avons fait référence dans les chapitres précédents. Il y a quelques anecdotes qui témoignent de ce don. La première d'entre elles est racontée par P. C. Mahalanobis (1892-1972), un de ses collègues indiens à Cambridge. Ce dernier était en train de s'entraîner à résoudre un problème de logique mathématique figurant dans un quotidien. Il trouva la solution après plusieurs minutes, une solution qui consistait en un couple de nombres. Il la proposa à Ramanujan, qui était à ce moment-là en train de se préparer à manger (il était végétarien) : « Voici un problème pour toi… » et il le lui lut. Ramanujan, instantanément et sans pour autant laisser de côté ce qu'il avait sur le feu, lui répondit : « Note la solution… », et il lui donna une formule générale pour obtenir une infinité de couples de nombres, qui constituaient autant de solutions du problème. Le premier couple était la solution qu'avait trouvée Mahalanobis.

La seconde anecdote eut lieu à l'été 1917. Ramanujan était hospitalisé pour des symptômes de tuberculose à Putney, une clinique de Cambridge. Son ami et mentor, le mathématicien britannique Hardy, lui rendit visite un matin. « Je me rappelle être allé le voir quand il était hospitalisé à Putney, raconte Hardy. J'avais voyagé dans le taxi numéro 1.729, et fis observer que ce nombre me paraissait bien insipide et que j'espérais que cela n'était pas un mauvais présage."Non, me répondit-il, c'est un nombre très intéressant. C'est le plus petit nombre qui peut s'exprimer comme la somme de deux cubes, de deux manières différentes." » En effet,

$$1.729 = 1^3 + 12^3 = 9^3 + 10^3.$$

« Je lui demandai tout naturellement s'il connaissait la réponse au problème équivalent pour la puissance 4. Il me répondit, après un moment de réflexion, que l'exemple n'était pas évident et que le premier parmi de tels nombres devait être très grand. »

Ramanujan s'était laissé tenter par la branche des mathématiques que Hardy considérait comme la plus difficile, la théorie des nombres. Et très vite il tomba dans le « piège » que, depuis près de deux mille ans, les nombres premiers avaient tendu à tous les mathématiciens qui s'étaient aventurés sur leurs sentiers obscurs. Ramanujan s'était proposé de trouver la « formule magique » au moyen de laquelle il serait possible de découvrir tous les nombres premiers. Cet acharnement allait inévitablement le conduire à affronter des problèmes de grande envergure, comme l'étude des séries divergentes.

Mais il arriva à un point où sa situation économique et sociale ne lui permettait pas de continuer d'avancer. Les amis qui l'entouraient ne pouvaient pas l'aider. Certains d'entre eux rédigèrent une lettre en anglais qu'ils envoyèrent à plusieurs ma-

GODFREY HAROLD HARDY (1877-1947)

Selon les dires de Hardy lui-même, sa plus grande contribution aux mathématiques fut la découverte de Ramanujan.

Hardy était un personnage pittoresque, avec un sens de l'humour typiquement britannique et un cercle d'amis très restreint. Un jour, il décida d'établir une évaluation personnelle des mathématiciens : il notait leur talent sur une échelle de 0 à 100. N'hésitant pas à rendre cette évaluation publique, il s'y attribua une note de 25, donna un 30 à Littlewood et un 80 à Hilbert (il est vrai que c'était son meilleur ami et le mathématicien avec lequel il collabora le plus). Il attribua la note maximale à Ramanujan.

thématiciens européens et dans laquelle Ramanujan exposait ses connaissances et son désir de pouvoir les développer. La lettre était ainsi rédigée :

« Cher Monsieur,

Je me permets de me présenter à vous comme un employé de bureau du département de comptabilité du Port Trust Office de Madras, avec un salaire de 20 livres annuelles seulement. J'ai bientôt 23 ans. Je n'ai suivi aucune formation universitaire, j'ai simplement suivi les cours de l'école ordinaire. Une fois l'école terminée, j'ai consacré le temps libre dont je disposais à étudier les mathématiques. Je ne suis pas passé par la formation régulière conventionnelle d'un cursus universitaire, mais j'ai suivi ma propre trajectoire. J'ai réalisé une étude détaillée des séries divergentes en général et les résultats auxquels je suis arrivé sont qualifiés de "surprenants" par les mathématiciens locaux…

Je vous demande de bien vouloir revoir les travaux ci-joints. Si vous pensez que certains éléments ont une quelconque valeur, j'aimerais pouvoir publier mes théorèmes, mais je suis pauvre. Je n'ai pas présenté les calculs réels ni les expressions que j'ai adoptées, mais j'ai indiqué le processus que j'ai suivi. Étant donné mon peu d'expérience, je vous serais infiniment reconnaissant pour les éventuels conseils que vous me donnerez. Je vous prie de bien vouloir m'excuser de vous avoir importuné.

Je reste, Cher Monsieur, à votre entière disposition,

S. Ramanujan. »

Parmi tous les mathématiciens qui reçurent la lettre de Ramanujan, seul Hardy comprit la valeur de ses travaux. Le jeune homme lui avait envoyé près de 120 théorèmes qui contenaient une multitude de formules. Hardy fit ce commentaire : « Je n'avais jamais rien vu de pareil, ni de près ni de loin. Un simple coup d'œil suffisait pour comprendre qu'elles ne pouvaient avoir été écrites que par un mathématicien du plus haut niveau. Elles ne pouvaient qu'être vraies, parce que, si elles ne l'étaient pas, personne n'aurait pu avoir l'imagination suffisante pour les inventer. »

En mai 1913, Hardy réussit à obtenir une bourse afin que Ramanujan vienne à Cambridge, mais ce dernier refusa car sa mère ne l'autorisa pas à aller en Angleterre. Elle lui donna finalement cette autorisation quelque temps après. Selon Hardy, la raison de ce revirement était qu' « un jour, sa mère déclara que la nuit précédente elle avait vu son fils, dans une grande salle, entouré d'un groupe d'Européens, et que la déesse Namagiri avait ordonné qu'elle ne s'interpose pas sur le chemin de son fils et qu'elle l'aide à atteindre le but de sa vie ».

Enfin, et grâce aux efforts de Hardy, Ramanujan put partir à Cambridge avec une bourse financée pour moitié par Madras et pour l'autre moitié par le Trinity College. À partir de ce moment, la tâche du mathématicien anglais, qui allait être son maître, fut aussi ardue que difficile. Quelle méthode suivre pour lui enseigner les mathématiques modernes ? « Les limites de son savoir étaient aussi stupéfiantes que sa profondeur », se lamentait Hardy. La difficulté était accrue par l'extraordinaire variété de thèmes que Ramanujan avait abordés, dans lesquels se mélangeaient des

NOMBRES TAXICAB

Depuis cette rencontre à la clinique entre Ramanujan et Hardy, les nombres qui ont la propriété de pouvoir s'exprimer comme la somme de *n* cubes de deux manières différentes sont appelés taxicab et se définissent de la manière suivante : « Un nombre taxicab *n*-ième est le nombre entier naturel le plus petit possible qui peut s'exprimer de *n* façons distinctes comme la somme de deux cubes positifs. » Actuellement, les nombres taxicab connus sont :

Ta(1) = 2 ;

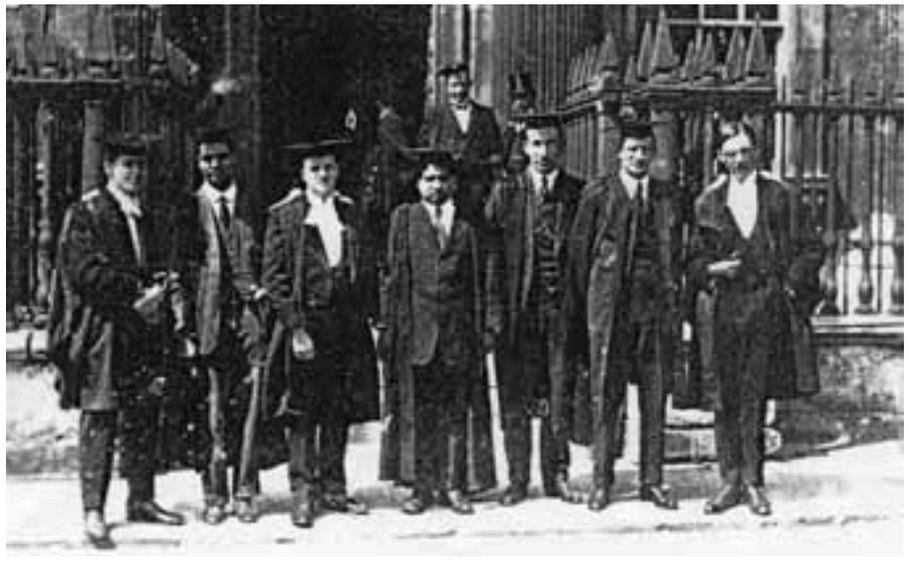
Ta(2) = 1 729 ;

Ta(3) = 87 539 319 ;

Ta(4) = 6 963 472 309 248 ;

Ta(5) = 48 988 659 276 962 496.

Le sixième taxicab, Ta(6), n'est pas encore connu.



Ramanujan (au centre) et Hardy (à droite), sur une photographie de groupe devant les portes du Trinity College de Cambridge.

résultats nouveaux avec d'autres qui avaient déjà été démontrés. Dans une large mesure, Ramanujan devait être rééduqué, mais Hardy essaya de ne pas rompre, par un formalisme excessif, ce qu'il appelait « le charme de son inspiration ».

Ramanujan vécut cinq ans à Cambridge, durant lesquels il publia vingt et un articles, dont cinq en collaboration avec Hardy, qui finit par avouer : « J'appris bien plus de lui que lui de moi. »

Durant le printemps de 1917 apparurent les premiers symptômes de la tuberculose qui eut raison de Ramanujan. L'été de la même année, il fut hospitalisé à la clinique de Cambridge. Il allait passer alité la majeure partie du temps qui lui restait à vivre. À l'automne 1918 arriva l'élection tant attendue pour une Trinity Fellowship, qui coïncida avec une amélioration de son état de santé, ce qui lui donna de l'énergie pour reprendre ses travaux et fit de cette période l'une des plus productives de sa vie. Au début de l'année 1919, il retourna en Inde, où il mourut l'année suivante.

La majeure partie de son œuvre se trouve dans ses lettres et dans trois cahiers personnels, dont l'un a été perdu puis retrouvé en 1976. La révision totale de son travail n'est pas encore terminée, puisque, bien que décédé à 33 ans, il a légué près de 4.000 énoncés à l'univers des mathématiques.

Les travaux de Ramanujan sur les nombres premiers, à savoir la découverte d'une formule exacte pour les trouver, sont entourés d'un petit halo de mystère, bien que d'une certaine manière ils puissent être considérés comme un échec. Hardy déclara : « En dépit du fait que Ramanujan eut de nombreux et brillants succès, ses travaux sur les nombres premiers et surtout sur tous les problèmes en relation avec cette théorie étaient certainement faux. On peut dire que ceci fut son unique grand échec. Mais je ne suis pas encore convaincu que, d'une certaine façon, son échec ne fut pas plus merveilleux qu'un quelconque de ses triomphes… »

Ramanujan ne connaissait ni l'œuvre de Riemann ni celle de Gauss, mais il était décidé à trouver une formule qui donne la liste des nombres premiers. Il disait en avoir une pour connaître avec une parfaite précision la quantité de nombres premiers inférieurs à un nombre quelconque. Parmi les résultats qu'il envoya à Hardy, il n'y avait aucune démonstration de ses affirmations. En revanche, il y avait une formule qui était sur le point de détruire toutes les ambitions de Ramanujan :

$$1+2+3+4+\ldots+\infty=\frac{1}{-12}.$$

L'absurdité de cette égalité aurait pu laisser croire que l'auteur n'avait aucune idée de ce que pouvait être une série convergente. Mais la perspicacité de Hardy lui laissa penser, par le reste des résultats mathématiques qui accompagnaient la lettre, qu'il devait y avoir là anguille sous roche. L'erreur d'interprétation fut résolue quand ils se rendirent compte qu'il y avait une confusion dans le système de notation et que ce que Ramanujan avait mis entre ses mains n'était ni plus ni moins qu'un des zéros de la fonction zêta de Riemann, concrètement la solution pour $x = -1$. La méthode que Ramanujan disait posséder lui donnait une formule pour obtenir le nombre de premiers compris entre 1 et cent millions avec une marge d'erreur incroyablement faible. Littlewood démontra que Ramanujan s'était

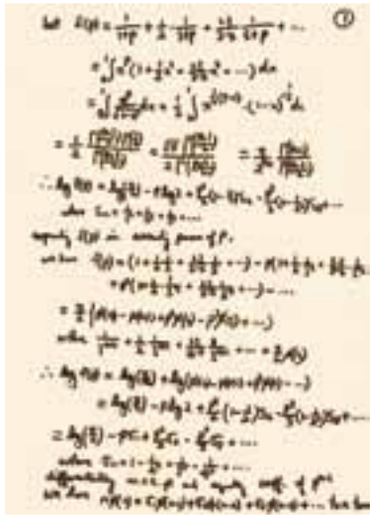
VIE ORDONNÉE

Ramanujan suivait une vie de brahmane, la caste hindoue la plus élevée au plan spirituel, marquée par un strict contrôle de soi et une frugalité ascétique, qui excluait du régime alimentaire tout produit d'origine animale et de nombreux végétaux, comme l'ail ou l'oignon. Il est curieux de noter que c'est surtout le matin au réveil qu'il écrivait précipitamment ses découvertes, desquelles il n'arrivait pas à proposer de démonstrations rigoureuses.

trompé. La recherche de la formule magique l'amena, comme bien d'autres avant lui, à s'aventurer le long de chemins extrêmement fructueux et qui, comme ce fut souvent le cas, avaient une relation directe avec les séries convergentes.

Le mathématicien américain Bruce Berndt, professeur au département de mathématiques de l'université de l'Illinois, qui consacra une grande partie de son temps à l'étude des œuvres de Ramanujan, découvrit que ce dernier avait établi une table, différente de la première qu'il avait envoyée à Hardy, dans laquelle il étudiait avec plus de détails et de précision l'apparition des nombres premiers parmi les cent premiers millions de nombres naturels. Berndt affirma que la précision était encore plus grande que celle que permettait la formule de Riemann, ce qui l'amena à envisager la possibilité que Ramanujan possédait réellement une formule que, pour une raison ou pour une autre, il ne fit connaître à personne. Il est fort probable que dans les cahiers personnels de Ramanujan demeurent encore de nombreuses vérités à révéler.

Il est certain que l'esprit mathématique très original de Ramanujan a produit quelques résultats apparemment faux, mais en majorité il donna des démonstrations justes et d'une grande beauté mathématique. En tout cas, ses travaux occupent actuellement des dizaines de mathématiciens dans les universités du monde entier, et ses résultats s'appliquent dans des domaines aussi divers que la chimie des polymères, la construction des ordinateurs ou encore la recherche contre le cancer.



Page manuscrite d'un cahier de Ramanujan.

Chapitre 7

À quoi servent les nombres premiers ?

Trouver des nombres premiers, surtout de grands nombres premiers, n'est pas une tâche facile, puisque, comme nous l'avons vu, personne n'a encore été capable de trouver la formule, l'algorithme qui permette de construire des nombres premiers à volonté. Face à cette situation, on peut tout simplement se poser la question : « Pourquoi vouloir trouver des nombres premiers ? ». Il y a deux réponses. La première raison est d'ordre théorique. En effet, les tentatives d'élaboration d'un tel algorithme sont à l'origine de la naissance d'outils de calcul très intéressants, en particulier dans le domaine informatique. Par ailleurs, disposer de listes interminables de nombres premiers sert aussi à vérifier des théorèmes qui n'ont toujours pas été démontrés. Si quelqu'un lance une hypothèse sur les nombres premiers et que l'on peut prouver qu'il en existe ne serait-ce qu'un, même s'il est composé de millions de chiffres, qui ne la vérifie pas, la question est réglée. Ainsi s'est déclenchée une recherche de nombres premiers de toutes les sortes, de Mersenne, jumeaux, etc., qui, dans certains cas, a pris l'aspect de ce que nous pourrions appeler une compétition, inscrite dans l'univers des records et des grands prix. Mais il y a aussi une autre raison, d'ordre pratique, qui est liée à ce que l'on appelle les clés cryptographiques : le courrier électronique, les transactions bancaires, les cartes de crédit et les communications par téléphone portable sont protégés au moyen de clés secrètes qui sont basées directement sur les propriétés des nombres premiers.

Les nombres premiers dans la cryptographie

En 1975, W. Diffie et M. Hellman, de l'université de Stanford, développèrent l'idée de codes asymétriques ou de « clé publique », un système basé sur des fonctions mathématiques précises, appelées « à sens unique » ou « fonctions avec piège », qui rendent possible le code, mais théoriquement impossible le déchiffrage si l'on ne connaît pas la clé. L'idée est que chaque utilisateur possède deux clés, l'une publique et l'autre privée. Si je veux envoyer un message à une personne, je code le message selon sa clé publique, que n'importe qui peut connaître, mais qu'elle seule, avec sa clé privée, peut déchiffrer. L'un des avantages de cette méthode est que la clé privée

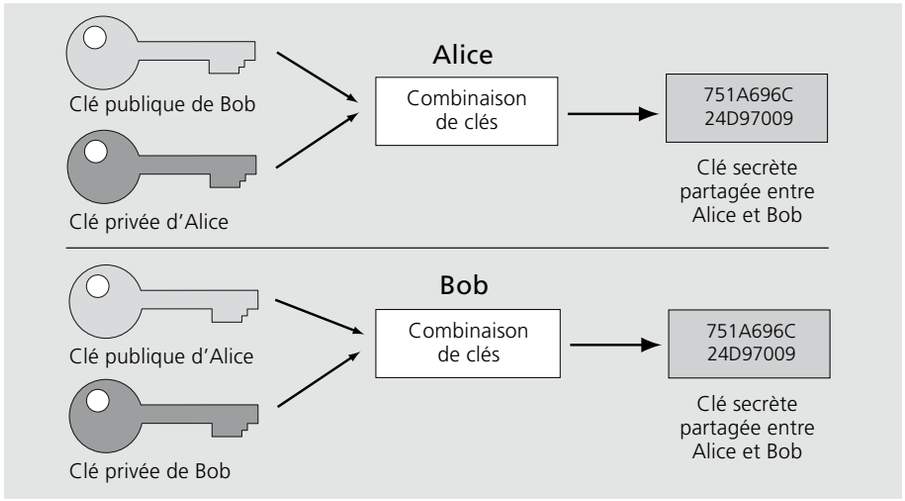


Schéma du principe théorique sous-jacent aux codes du type Diffie-Hellman. Supposons deux émetteurs/récepteurs, Alice et Bob. Tous deux s'accordent publiquement sur deux paramètres (un nombre premier p *et un autre* g*, avec certaines propriétés). L'un comme l'autre effectuent une opération sur ces paramètres au moyen d'un nombre entier, qui demeure privé, et ils s'envoient publiquement le résultat. Ils font ensuite une opération sur cette seconde expression et obtiennent la même valeur, qui peut alors servir de clé secrète partagée. Un espion potentiel qui aurait intercepté les communications publiques d'Alice et de Bob ne pourrait, à partir de cette information, trouver la clé secrète.*

ne circule jamais par les moyens de communication. Nul besoin donc de la changer constamment. Il ne s'agit pas là d'une question simple, mais essayons de comprendre le principe au moyen d'une analogie. Imaginons un grand magasin de peinture dans lequel nous disposons de centaines de milliers de pots de couleurs différentes. Prenons deux pots quelconques et mélangeons différentes quantités de peinture de chaque pot. Jusque-là, rien de bien compliqué. Mais si nous montrons maintenant le résultat à quelqu'un et lui demandons de « déchiffrer » la dose de chaque couleur qui est intervenue dans le mélange final, nous lui posons un problème difficile à résoudre.

Tel est le mécanisme des fonctions mathématiques avec piège ou à sens unique, dans lesquelles il est très facile d'« aller » mais quasiment impossible de « revenir ». Supposons maintenant que dans le magasin, à la place des pots de peinture, nous ayons des nombres premiers. Prenons-en deux au hasard, par exemple 7 et 13, et multiplions-les l'un par l'autre, comme nous avons mélangé les peintures. Le résultat est $7 \cdot 13 = 91$.

La question qui se pose maintenant est la suivante : « Est-il possible de savoir que deux nombres premiers multipliés entre eux donnent 91 comme résultat ? » Il s'agit d'avoir une liste de nombres premiers et de faire des essais. Cela paraît simple, comme cela pourrait l'être de vérifier les couleurs qui forment le mélange de peinture si dans le magasin il n'y avait qu'une douzaine de couleurs basiques. Mais les choses ne se passent pas ainsi et encore moins avec les nombres premiers.

Vérifier par exemple que le nombre 1.409.305.684.859 est le résultat de la multiplication des deux nombres premiers 705.967 et 1.996.277 peut venir à bout de la patience de quiconque. D'autant plus que ces deux nombres premiers sont extraits d'une liste dans laquelle figurent tous les nombres premiers existants entre 1 et 2.000.000, pas moins de 148.933 nombres. Mais comme nous l'avons souligné à plusieurs reprises jusqu'à maintenant, nous vivons à l'heure de l'informatique, et en principe, ce problème peut très vite être résolu au moyen d'un bon programme inséré dans un puissant ordinateur… Du moins jusqu'à un certain point, car tout dépend de la taille du magasin de peinture, et il faut insister sur le fait que celui des nombres premiers n'est pas seulement grand, il est infini.

Le couple de nombres premiers de l'exemple précédent n'avait pas beaucoup de chiffres. Si l'on prend des nombres premiers composés de centaines de chiffres chacun, le temps d'attente de ce programme informatique, qui est tout compte fait en train de chercher « bêtement » les nombres les uns après les autres – on dirait, dans le jargon cryptographique, au moyen d'une attaque de « force brute » -, peut arriver à dépasser notre espérance de vie sur Terre.

LE RSA 129

La « déchiffrage » du RSA 129, qui se produisit en avril 1994, est célèbre. Il s'agissait d'un nombre composé de 129 chiffres que les auteurs du système avaient rendu public, en le proposant comme un défi. Un groupe de 600 mathématiciens, avec l'aide de 1.600 volontaires recrutés sur Internet, réussirent à factoriser ce nombre. Cependant, on a calculé que si tous les ordinateurs du monde se connectaient en parallèle et se mettaient à travailler, il faudrait un temps équivalent à l'âge de l'univers (13.700 millions d'années) pour briser une clé de 1.024 chiffres. Notons que dans la cryptographie de clé publique, des nombres de 128, 1.024 et jusqu'à 2.048 bits sont utilisés. Plus le système comprend de chiffres et plus résistant il sera en cas d'attaque, mais l'inconvénient est que du coup le processus de décryptage est plus lent.

S'il est certain que les nombres premiers sont présents dans notre vie quotidienne, via la carte de crédit ou l'ordinateur personnel, il doit nécessairement exister une demande de nombres premiers : en effet, il en faut quelques-uns pour construire une clé secrète. Il existe un « marché » de nombres premiers qui assure une production à grande échelle de grands nombres premiers, mais dans cette activité le contrôle de qualité est aussi important que la production. Pour qu'un nombre très grand acquière la qualité de premier, il doit être testé par un quelconque organisme officiel.

Le système RSA existe depuis 1978, mais son usage généralisé comme clé de cryptage n'intervint qu'à la fin des années 1990, avec l'arrivée d'Internet. Obtenir des grands nombres premiers était difficile : il fallait en effet pour cela un logiciel très précis. Ce qui se faisait était de les acheter à des entreprises spécialisées ou à certains départements universitaires qui les obtenaient comme résultat de leurs propres recherches. Mais la croissance exponentielle de la capacité de calcul des ordinateurs, couplée à l'apparition régulière d'algorithmes d'implémentation plus sophistiqués, a transformé le marché des nombres premiers : en peu de temps, trouver des nombres premiers devint plus facile.

Les temps de l'ordinateur

L'apparition des logarithmes a permis d'économiser une bonne partie du temps et de l'énergie qui étaient employés jusque-là à d'ennuyeux calculs sans grande valeur mathématique. Un peu plus tard apparurent la règle de calcul et les premières calculatrices mécaniques, des machines pour lesquelles il fallait faire tourner une série de rouleaux pour obtenir les résultats des sommes et des produits.

Les ordinateurs furent les premiers à faire des calculs qui allaient bien au-delà de la capacité mentale de l'esprit humain. Arriva le moment où les machines furent capables de réaliser la simulation d'un raisonnement déductif, pourtant propre à un esprit mathématique. À ce moment-là, certains scientifiques eurent la sensation qu'une frontière allait être franchie, une frontière que jusqu'alors aucune machine n'avait réussi à dépasser. Avaient-ils raison ou tort ? Avec sa croissance exponentielle, le développement de l'informatique était en train de changer des paradigmes vieux de plusieurs siècles. C'est alors que firent leur apparition les premiers algorithmes de calcul capables de démontrer des théorèmes.

Les détracteurs des démonstrations d'origine informatique exposent en général deux raisons pour mettre en question cette procédure. La première est que ces démonstrations ne sont pas vérifiables, car il y a des étapes dans le programme qui ne pourront jamais être vérifiées par aucun mathématicien. La seconde est que le processus est sujet à des erreurs, aussi bien de *software* que de *hardware*. Dans la majorité des cas, il s'agit d'erreurs aléatoires. Une manière de pallier ces défauts consiste à insérer différents programmes dans d'autres machines pour voir s'ils conduisent au même résultat.

Il a été calculé que le super-ordinateur Cray ne commet qu'une seule erreur toutes les mille heures de fonctionnement.

Mais les ordinateurs sont limités par le fait qu'ils ne peuvent travailler qu'avec des zéros et des uns : quand il s'agit de nombres qui ne sont pas exprimés en base 2, ils doivent faire des approximations, ce qui les soumet à de possibles erreurs. En 1991, David R. Stoutemyer réalisa 18 expériences de calcul avec des programmes d'ordinateurs qui donnèrent des résultats incorrects.

Cela explique pourquoi nombreux sont ceux qui considèrent que cette nouvelle façon de faire des mathématiques appartient plutôt au champ des sciences empiriques ou expérimentales. Mais personne n'a décrété que le travail mathématique avait été conçu d'une seule manière pour toujours. Si l'on reprend le cours de son histoire, le raisonnement mathématique « traditionnel » n'a pas non plus été exempt d'erreurs. Plus d'un résultat faux a été considéré comme juste durant des années. De plus, les mathématiques ont aujourd'hui atteint un tel niveau de diversité et de complexité que la vérification d'un théorème peut durer des années ou, dans le meilleur des cas,

SÉCURITÉ MAXIMALE

Le gouvernement des États-Unis n'autorise l'utilisation de certaines clés de cryptage que sur son territoire et au Canada ; au-delà de ces frontières, la vente n'est pas autorisée, sauf s'il s'agit d'un établissement financier. L'exportation non autorisée de standards de cryptage est considérée comme un trafic d'armes. Les entreprises qui se consacrent à la fabrication de programmes de cryptage stockent les clés secrètes sur des sortes de « pastilles » dotées de dispositifs de sécurité sophistiqués. Quand elles s'ouvrent et qu'elles entrent en contact avec l'oxygène, elles se solidifient en une masse informe. Si on essaie de les voir aux rayons X, tout ce qui est écrit se transforme en zéros.

rester entre les mains de quelques spécialistes. En définitive, de nombreux experts pensent aujourd'hui que l'utilisation de l'ordinateur comme outil d'investigation et aussi de vérification de théorèmes a donné naissance à une manière différente de concevoir les mathématiques. Il ne serait pas insensé d'imaginer qu'un jour ou l'autre un ordinateur réalise la démonstration de la conjecture de Riemann.

En tout cas, personne ne peut remettre en cause la validité des méthodes de calcul pour trouver des nombres premiers, et pour vérifier si un nombre est premier ou non. Lorsque nous entrons plus en détail dans le monde de l'algèbre de calcul, des termes comme « polynomial », « polynomial déterministe » ou « probabiliste » font leur apparition. Leur emploi est courant mais ils demeurent inaccessibles au profane. Bien qu'il s'agisse d'une simple appellation, il est préférable d'avoir une idée approximative des concepts que recouvrent ces termes.

Quand il s'agit de temps polynomial, il est fait référence au temps que prend la machine pour résoudre un algorithme précis. Supposons que nous ayons une variable d'entrée que nous appellerons n. Cette variable d'entrée a une certaine taille : ainsi, la taille d'un entier peut-être résumée au nombre k de chiffres de son écriture décimale, ou au nombre de 0 et de 1 nécessaires pour l'écrire en base 2 (ceci donne deux notions de taille comparables). À partir de cette variable d'entrée, l'algorithme va effectuer une suite d'opérations élémentaires afin d'arriver à une conclusion. Le nombre d'opérations dépend de la taille de la variable d'entrée et, typiquement, plus cette taille est grande plus il y aura d'opérations à effectuer. Si le nombre d'opérations nécessaires à l'algorithme ne croît pas plus vite qu'un polynôme en k, par exemple si ce nombre d'opération est inférieur à $k^3 + 2k + 1$, nous dirons qu'il s'agit d'un algorithme en temps polynomial. Dans le cas contraire, par exemple

si 5^k opérations sont nécessaires à l'algorithme pour que le programme termine, nous parlerons d'un algorithme non polynomial. L'idée de base est qu'en termes très généraux, les algorithmes polynomiaux ont un temps d'exécution raisonnable, contrairement aux exponentiels.

P versus NP

Comme nous venons de l'expliquer, certains calculs peuvent être conduits de manière déterministe par des algorithmes qui fonctionnent en temps polynomial, c'est-à-dire des algorithmes utilisant assez peu d'opérations élémentaires. On peut ainsi effectuer des sommes d'entiers naturels, ou résoudre certaines équations simples. Dans de nombreux cas, avec des algorithmes adéquats, le temps de résolution est compris dans des intervalles acceptables. Les problèmes qui peuvent être traités de cette manière sont appelés problèmes de type P. Les problèmes de type NP sont d'une nature a priori différente. On dit qu'un problème est NP s'il existe un algorithme qui teste si une solution proposée est solution du problème, et ceci en temps polynomial par rapport à la taille des variables d'entrée. Il ne s'agit plus de trouver une solution de manière déterministe, mais de tester si un candidat est bien solution. Il est donc plus simple d'écrire des programmes de type NP que des programmes de type P, et ces programmes sont souvent très rapides : tester est plus simple que trouver. Ainsi, un problème de catégorie P est automatiquement NP, tandis que l'inverse paraît à première vue improbable. À ce point d'avancement, il convient d'éclaircir le concept d'algorithme.

Un algorithme est comme une recette de cuisine, c'est-à-dire qu'il est constitué d'une série d'instructions qui ne doivent laisser aucune place au doute. Par exemple, pour résoudre une équation comme $x - 2 = 8$, l'algorithme de résolution dirait quelque chose comme :

1. Isoler x (passer tous les autres nombres de l'autre côté de l'équation en changeant de signe) : $x = 8 + 2$.
2. Faire l'opération correspondante dans le second membre : $8 + 2 = 10$.
3. Écrire la solution : $x = 10$.

Ceci serait un problème de type P auquel correspondrait son temps polynomial de résolution. Cet exemple est bien entendu un cas trivial dont la solution est très rapide à trouver.

LES SEPT PROBLÈMES DU MILLÉNAIRE

Le Clay Mathematics Institute (CMI) est une fondation privée à but non lucratif créée par Landon T. Clay, un entrepreneur multimillionnaire de Boston. Ses objectifs sont le développement et la vulgarisation du savoir mathématique.

Le 25 mai 2000, l'Institut a annoncé la création des « Millennium Prize Problems », un prix financé par un total de sept millions de dollars destinés à la résolution des sept problèmes que les membres de l'Institut considèrent comme les plus décisifs pour les mathématiques du XX^e siècle. Les problèmes peuvent être résolus un par un, c'est-à-dire qu'un prix d'un million de dollars (une somme supérieure à celle du Prix Nobel) serait attribué à chaque problème résolu.

Il n'y a aucune limite d'âge ni de temps pour participer ; aucune formation universitaire n'est par ailleurs exigée. Les sept problèmes sélectionnés sont :

1. Le problème ouvert P versus NP.
2. L'hypothèse de Riemann.
3. Les équations de Yang-Mills.
4. Les équations de Navier-Stokes.
5. La conjecture de Birch et Swinnerton-Dyer.
6. La conjecture de Hodge.
7. La conjecture de Poincaré.

Étant donné la difficulté et l'importance des problèmes proposés, les conseillers financiers de M. Clay doutaient sérieusement que l'Institut ait à verser un jour l'argent des prix. Cependant, en 2006, le Russe Grigori Perelman surprit tout le monde en trouvant la solution du septième et dernier problème : la conjecture de Poincaré. Pour des raisons personnelles, il refusa la médaille Fields qui lui fut pourtant accordée lors du XXV^e congrès international des Mathématiques célébré à Madrid.

Nous pourrions, par exemple, essayer les solutions $x = 3$, $x = -2$, etc., et le temps de calcul serait bien plus rapide. En effet, la seule chose que doit faire le programme est de remplacer x par une valeur et de vérifier si la solution est juste.

La question inverse serait la suivante : si nous avons un algorithme de vérification, pouvons-nous garantir qu'il existe un algorithme polynomial qui nous permette de résoudre de manière déterministe le problème (ce qui revient encore à se demander si nous pouvons être certains qu'il existerait un quelconque type d'algorithme pour trouver la solution en temps polynomial) ?

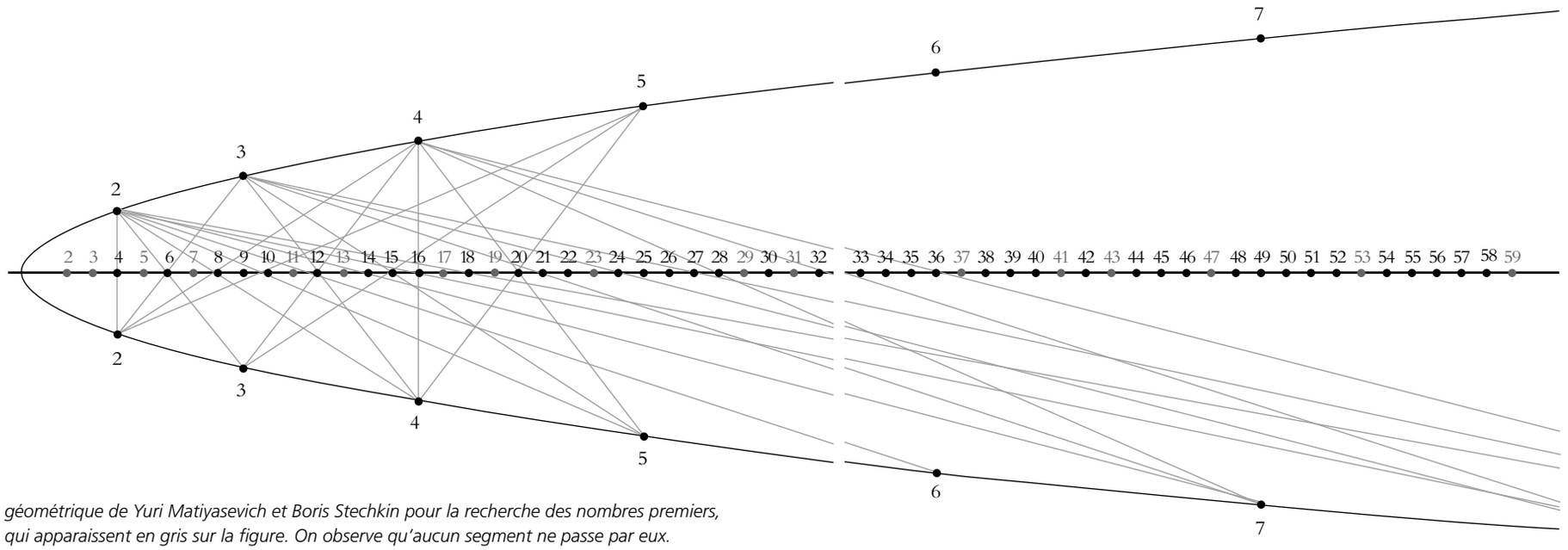
C'est le problème que se posèrent indépendamment l'un de l'autre Stephen Cook et Leonid Levin en 1971 : « Si tout problème P est NP, existe-t-il des problèmes NP qui ne soient pas P ? » Ce problème est considéré comme le plus grand défi lancé à l'informatique théorique et fait partie de l'un des sept problèmes du mil-lénaire selon l'Institut Clay. Cette institution garantit à quiconque résoudrait l'un de ces problèmes d'empocher la belle somme d'un million de dollars.

Fabriquer des nombres premiers

Il est fréquent qu'une personne sans véritable culture mathématique soit fière d'avoir trouvé, presque toujours sur Internet, un système ou une formule pour vérifier quel est le nombre premier qui suit un nombre naturel n quelconque. Il faut simplement préciser qu'une information de cet acabit ne devrait même pas se chercher. Quiconque l'aurait trouvée se serait, en effet, certainement empressé de prévenir tous les journaux et magazines du monde entier pour qu'ils en fassent leurs gros titres.

Il existe de nombreux modèles géométriques pour trouver des nombres premiers. Ils peuvent cependant parfois piéger les imprudents, car ils se présentent en effet comme des formules qui permettent de trouver tous les nombres premiers, alors qu'en réalité ils ne sont rien de plus que des variantes du crible d'Ératosthène ou d'autres façons de réaliser le crible par des méthodes géométriques. Et de fait, certains d'entre eux sont vraiment ingénieux.

L'un des plus intéressants est celui que créèrent les mathématiciens russes Yuri Matiyasevich (né en 1947) et Boris Stechkin (1920-1995) en se servant d'une parabole. Elle se représente avec ses deux branches, et dans son axe s'écrit la suite des nombres naturels. Il faut ensuite tracer une perpendiculaire qui corresponde au carré de chaque nombre, c'est-à-dire qu'à l'endroit où se situe le 4, il faut tracer une perpendiculaire correspondante, sur chacune des deux branches, avec le chiffre 2. La signification géométrique de la perpendiculaire est que le produit de 2 par



Crible géométrique de Yuri Matiyasevich et Boris Stechkin pour la recherche des nombres premiers, qui apparaissent en gris sur la figure. On observe qu'aucun segment ne passe par eux.

lui-même est réalisé. De la même manière, nous aurions une autre perpendiculaire pour symboliser le produit de 3 par lui-même et nous la tracerions au point 9 de l'axe, et ainsi de suite.

Lorsque tous ces nombres sont représentés par des points sur la parabole, il faut joindre chaque point d'une branche avec tous ceux de l'autre. Ainsi, nous joignons le point 2 de la branche supérieure avec les points 2, 3, 4, 5… de la branche inférieure. Chacun de ces segments coupe l'axe sur le produit correspondant. Si nous réalisons toutes les intersections possibles, les seuls points de la parabole par lesquels ne passe aucun segment sont précisément les nombres premiers. Ceci est un exemple d'un crible de type géométrique.

Les cribles de type algébrique sont plus adéquats pour obtenir des algorithmes rapides. L'un d'entre eux est le crible d'Atkin, conçu par A.O.L. Atkin et Daniel J. Bernstein, qui permet de trouver tous les nombres premiers inférieurs ou égaux à un nombre naturel donné. Par certains aspects, il s'agit là d'une version améliorée du crible d'Ératosthène, ou plus exactement, d'une version actualisée, car le crible d'Atkin, en termes arithmétiques, présente certaines déficiences par rapport à celui d'Ératosthène : il requiert une préparation préalable et n'élimine pas les multiples des nombres premiers mais seulement les multiples des carrés des nombres premiers.

Nous savons déjà que l'idéal serait de pouvoir trouver une formule qui associerait à chaque nombre naturel n le n-ième nombre premier. Nous avons vu que les mathématiciens recherchent une telle formule depuis trois mille ans. Ce qui existe en revanche, ce sont les procédures qui permettent de calculer de façon pratique les nombres premiers. Par exemple, on peut démontrer (théorème de Wilson) que p est un nombre premier si et seulement si $(p–1)! \equiv -1 (mod\ p)$, mais comme nous l'avons expliqué précédemment, aucune fonction qui inclut des factorielles n'est viable lorsqu'il s'agit de programmer un algorithme dans une calculatrice, à cause de la rapidité de croissance de la fonction qui rend les temps de calcul excessivement longs.

Il existe aussi des polynômes qui « fabriquent » des nombres premiers, comme celui qu'utilisa Euler pour calculer une liste de quarante nombres premiers au moyen de la fonction $f(x) = x^2 + x + 41$, qui permet de trouver des nombres premiers suivant les valeurs de x. Par exemple :

$$x = 0 \quad f(0) = 0 + 0 + 41 = 41 ;$$
$$x = 1 \quad f(1) = 1 + 1 + 41 = 43 ;$$
$$x = 2 \quad f(2) = 4 + 2 + 41 = 47.$$

Cependant, la fonction ne fonctionne pas pour 41 et 42, qui donnent comme résultat des nombres composés :

$$x = 41 \quad f(41) = 1.681 + 41 + 41 = 1.763.$$
$$x = 42 \quad f(42) = 1.764 + 42 + 41 = 1.847.$$

Euler poursuivit ses investigations sur les polynômes et constata que la formule $x^2 - x + q$ fournissait souvent des nombres premiers lorsque q était lui même un nombre premier et x un entier naturel compris entre 0 et q - 2.

À ce jour, la majeure partie des nombres premiers connus (nous parlons ici des grands nombres premiers) sont les nombres premiers de Mersenne. Cela est dû au fait qu'il existe un test de primalité, le test de Lucas-Lehmer, qui fonctionne très bien avec ce type de nombres. Rappelons qu'un nombre de Mersenne est un nombre de la forme $2^n - 1$. Lorsqu'un tel nombre est premier, on parle alors de « premier de Mersenne ». Au 10 juin 2009, seulement quarante-sept nombres premiers de Mersenne étaient connus. Le plus grand d'entre eux est $2^{43.112.609} - 1$, qui compte près de treize millions de chiffres.

LE PROJET GIMPS

La Great Internet Mersenne Prime Search, « grande recherche des nombres premiers de Mersenne par Internet », est un projet créé par George Woltman qui consiste en un réseau de collaboration dans lequel les ordinateurs personnels des personnes qui participent au projet (tout le monde peut s'inscrire) agissent en parallèle, créant ainsi des capacités largement supérieures à celles que pourrait avoir n'importe quel super-ordinateur. L'idée est que chaque utilisateur qui souhaite participer installe le *software* adéquat et que son ordinateur travaille durant les temps morts, agissant ainsi comme un écran de veille. Le projet commença à fonctionner en 1997 et entre cette date et août 2009, 12 nombres premiers de Mersenne ont été trouvés. L'Electronic Frontier Foundation (EFF), Fondation Frontières Électroniques, offrit un prix de 150.000 dollars à la première personne qui découvrirait un nombre premier de Mersenne avec un minimum de dix millions de chiffres. Le prix fut attribué le 23 août 2008 à Edson Smith, du Département de Mathématiques de l'UCLA, pour la découverte du nombre $2^{43.112.609} - 1$.

Logo de l'Electronic Frontier Foundation.

Comment savoir si un nombre est premier ?

L'unique manière de le savoir avec certitude est de le diviser par tous les nombres qui lui sont inférieurs. S'il n'est divisible par aucun d'eux, il est premier. Nous savons (*cf.* chapitre précédent) que nous pouvons nous arrêter à la racine carrée du nombre en question. Pour des petits nombres et des calculs manuels, c'est une bonne méthode. Par exemple, vérifions si le nombre 101 est premier ou composé. Pour cela, le fait de connaître les critères de divisibilité peut nous éviter des calculs inutiles. Nous savons déjà que 101 n'est pas divisible par 2, il ne se termine ni par 0 ni par un chiffre pair. Il n'est pas non plus divisible par 3, car la somme de ses chiffres n'est pas divisible par 3 (1 + 0 + 1 = 2). De même, il n'est pas divisible par 5 car il devrait alors se terminer par 0 ou 5. Nous pouvons aussi passer le 4, le 6 et le 9 : ils sont tous multiples de 2 ou de 3. Si nous essayons avec 7, cela nous donne un quotient de 14 et un reste de 3 : il n'est donc pas divisible par 7. Le nombre suivant qu'il faut essayer est 11 (101 n'est évidemment pas un multiple de 10). La division par 11 donne comme quotient 9 et comme reste 2. Nous pouvons nous arrêter ici et affirmer que 101 est un nombre premier, puisque la racine carrée de 101 vaut approximativement 10, ce qui nous garantit avec certitude qu'il ne sera divisible par aucun des nombres qui restent jusqu'à 101.

Cette méthode est connue sous le nom de « test de divisibilité ». C'est la plus facile et la plus sûre de toutes. Le problème est qu'elle n'est pas viable pour des nombres plus grands, même pas au moyen de méthodes informatiques. Pensons qu'un nombre de cinquante chiffres requerrait un calcul allant au minimum jusqu'au vingt-cinquième chiffre, celui qui correspondrait plus ou moins à sa racine carrée. Un ordinateur ayant la capacité de réaliser des milliards de divisions à la seconde aurait besoin de plus de trois cents millions d'années pour terminer le calcul. Il est d'ailleurs fort probable que l'espèce humaine aurait déjà disparu. Cependant, il faut préciser que s'il s'agit d'un nombre composé et que si l'un de ses facteurs n'est pas excessivement grand, la méthode peut fonctionner. Il faut prendre en compte que pour un nombre n donné quelconque, la probabilité que le nombre 2 soit un facteur est de 50 % ; celle pour que 3 le soit, de 33 %, et ainsi de suite.

D'un autre côté, les ordinateurs modernes ont suffisamment gagné en rapidité et en capacité de mémoire pour que la recherche d'un nombre premier dans une longue liste puisse s'avérer dans certains cas plus efficace que le processus compliqué de vérification du fait qu'un nombre donné est premier.

Pseudopremiers

Le petit théorème de Fermat est l'un des plus utilisés dans les tests de primalité. Rappelons que ce théorème affirme : « Si p est premier, il n'existe aucune base a avec $a < p$ (avec a et p premiers entre eux), telle que $a^{p-1} - 1$ donne un reste différent de zéro quand on le divise par p. »

Le théorème a ses limites parce que, comme nous l'avons déjà vu, il donne une condition nécessaire mais pas suffisante. Par exemple, si nous prenons $p = 7$, nous obtenons que $3^6 - 1$ est divisible par 7. Ceci ne nous garantit pas que 7 soit un nombre premier (nous savons qu'il l'est car nous avons pris un petit nombre pour simplifier les choses mais nous devons imaginer que nous avons des grands nombres). En revanche, si nous prenons $p = 8$, nous aurons comme résultat de la division $3^7 - 1$ le nombre 273,25. Il n'est donc pas divisible, ce qui nous garantit que 8 n'est pas premier (sans nécessité de trouver aucun de ses facteurs).

Nous savons qu'un nombre est composé lorsque ce nombre ne passe pas le test pour une base a déterminée. Nous appelons donc cette base a le « témoin ».

Si en revanche le nombre passe le test et n'est pas premier, nous appelons cette base a « menteur ». Nous pouvons donc continuer à faire des essais. La probabilité de trouver des menteurs se réduit d'un facteur ½ à chaque essai, et ainsi la probabilité que le nombre soit premier augmente.

On dit d'un nombre p qui, n'étant pas premier, passe le test pour un nombre a qu'il est « pseudopremier » pour cette base. La définition plus générale d'un pseudopremier est la suivante : « Un nombre est dit pseudopremier quand il passe un test de primalité et que le résultat montre qu'il est composé. »

La question se complique lorsqu'il y a des nombres qui passent les tests pour n'importe quelle base a et qui ne sont pas premiers. Par exemple, le nombre 561 passe le test pour n'importe quelle base et est un nombre composé ($561 = 3 \cdot 11 \cdot 17$). Ces nombres-là sont appelés les « nombres de Carmichael », du nom du mathématicien américain Robert Daniel Carmichael (1879-1967) qui les a découverts. On connaît aujourd'hui seulement 2.163 nombres de Carmichael, qui se trouvent parmi les vingt-cinq mille premiers millions de nombres naturels. Tous ont au moins trois facteurs premiers.

Il y a seize nombres de Carmichael inférieurs à 100.000 :

561, 1.105, 1.729, 2.465, 2.821, 6.601, 8.911, 10.585, 15.841, 29.341, 41.041, 46.657, 52.633, 62.745, 63.973 et 75.361.

Les nombres de Carmichael sont aussi appelés « pseudopremiers absolus ».

Les méthodes

À ce jour, les algorithmes qui sont utilisés pour déterminer si un nombre quelconque est premier sont de deux types : polynomial déterministe ou polynomial probabiliste.

Le premier garantit de manière absolue qu'il s'agit d'un nombre premier, mais son temps de réalisation est élevé. Le second est plus rapide mais présente une relative incertitude quant à son résultat.

La méthode la plus utilisée est la « méthode de Miller-Rabin », une version du test de primalité de Fermat mais basée sur la conjecture de Riemann. Il s'agit d'une méthode du type polynomial probabiliste, mais la probabilité qu'elle contienne une erreur se situe entre $1/10^{50}$ et $1/10^{80}$, si bien qu'elle peut donc être utilisée dans la pratique avec des garanties.

Le 6 août 2002, trois chercheurs de l'Institut technologique de Kanpur (Inde), M. Agrawal, N. Kayal et N. Saxena, publièrent une méthode déterministe en temps d'exécution polynomial basée sur une généralisation du petit théorème de Fermat :

$$n \text{ est premier } \Leftrightarrow (x-a)^n = x^n - a \text{ dans l'intervalle } \frac{\mathbb{Z}_n[n]}{x^r - 1}.$$

En dépit de cela, la plus usitée continue d'être la polynomiale probabiliste, à cause de son temps de réalisation inférieur.

La majorité des navigateurs incluent un algorithme de cryptage qui est capable de trouver grâce à ce type de méthode des nombres premiers jusqu'à 2.048 bits, comme ceux utilisés, par exemple, pour l'avis d'imposition sur le revenu ou la carte d'identité.

Aujourd'hui, les trois systèmes utilisés en sécurité cryptographique sont le RSA, le logarithme de signature standardisé (DSA) et le logarithme de cryptographie sur courbe elliptique (ECDSA).

Aucun expert ne met en doute la sécurité qu'offre chacun de ces trois systèmes. La différence entre eux réside dans la capacité des clés qui sont utilisées : la sécurité que confèrent les clés de 2.048 bits dans les deux premiers est équivalente à celle que donnent des clés de 224 bits dans le troisième, ce qui fait que le temps de calcul se réduit considérablement. Alors que dans les deux premiers systèmes on connaît des algorithmes subexponentiels, dans le troisième ce que nous savons utiliser de mieux est de type exponentiel.

CURIOSITÉ NUMÉRIQUE

Le nombre 313 est le nombre que l'on retrouve sur la plaque d'immatriculation des voitures du canard Donald. Il a la curieuse propriété d'être un nombre palindrome (il peut se lire indifféremment de gauche à droite et de droite à gauche), aussi bien en base 10 qu'en base 2, et c'est l'unique nombre premier de trois chiffres qui possède cette propriété : 313 (base 10) = 100111001 (base 2). Par ailleurs, 100111001 en base 10 est premier.

Nombreux sont les nombres premiers qui font partie de la liste des curiosités numériques, comme par exemple les « repunit » (néologisme dérivé à partir de *repeated unit*) qui sont formés de longues séries de chiffres 1, comme 11111111111111111111111, qui est un nombre premier. Ce ne sont pour l'instant que de simples curiosités mathématiques, mais peut-être qu'un jour elles feront partie d'un théorème ou d'une hypothèse d'une certaine valeur mathématique. Une curieuse série de ce type est celle qui est formée à partir du nombre 91. Il s'agit d'un nombre composé, car $91 = 13 \cdot 7$, mais quand on lui ajoute à la fin une série de zéros terminés par 1, il devient alors premier puis composé, en alternance :

9901 premier
999001 composé
99990001 premier
9999900001 composé
999999000001 premier
99999990000001 composé
9999999900000001 premier
999999999000000001 composé

Mais malheureusement, le suivant, 99999999990000000001, est un nombre composé.

Et l'histoire continue…

Nous avons vu que des mathématiciens comme Mersenne, Fermat et même parfois Euler recherchaient des résultats pratiques. Souvent, c'était au détriment d'une certaine consolidation théorique. Ils contournaient les démonstrations mais continuaient d'utiliser les résultats. Gauss initia une nouvelle étape de l'histoire des mathématiques, pour laquelle la rigueur des démonstrations devait impérativement primer sur tout autre critère. Mais dans le cas des nombres premiers, il apparaît que nous avons repris la voie empirique. Nous utilisons des théorèmes non démontrés et donnons pour certain un résultat en pensant que la probabilité de commettre

une erreur est très basse. Nous faisons comme Fermat mais sans avoir besoin de cacher une hypothétique démonstration. Nous en sommes arrivés là, d'une part, du fait de l'énorme capacité des algorithmes de calcul, et, d'autre part, du fait de la nécessité actuelle de disposer de grands nombres premiers.

Sur un plan purement théorique, il est possible d'affirmer que les nombres premiers continuent de résister aux mathématiciens. Leur histoire est dans une certaine mesure l'histoire d'un échec. La plus grande réussite se trouve dans la fonction zêta de Riemann, mais il faut garder à l'esprit que ce succès n'est que partiel. Euler, qui fut l'un des grands visionnaires des mathématiques, n'était pas spécialement optimiste quant aux possibilités de succès dans la compréhension de ces nombres rebelles :

> « Depuis fort longtemps, les mathématiciens ont essayé en vain de découvrir une quelconque séquence dans l'ordre des nombres premiers, mais j'ai toutes les raisons de croire qu'il s'agit d'un mystère que jamais l'esprit humain ne pourra pénétrer. ».

Annexe

Démonstrations

1. Démonstration du théorème fondamental de l'arithmétique

Le théorème affirme que tout nombre naturel différent de 1 peut s'exprimer d'une façon unique comme le produit de facteurs premiers (à l'ordre près des facteurs). En premier lieu, il convient de préciser pourquoi le chiffre 1 est exclu de la liste des nombres premiers. Il y a diverses raisons, mais la plus évidente est que s'il en était autrement le théorème ne serait pas vérifié ; ainsi, on pourrait écrire

$$6 = 2 \cdot 3, \text{ conformément au théorème, mais aussi}$$

$$6 = 1 \cdot 2 \cdot 3 = 1 \cdot 1 \cdot 2 \cdot 3 = 1 \ldots 1 \cdot 2 \cdot 3$$

ce qui produirait plusieurs écritures distinctes comme un produit et contredirait l'unicité de la décomposition. On doit donc exclure 1 de la liste des nombres premiers, et donc aussi de l'énoncé du théorème car 1 ne peut pas s'écrire comme produit de nombres premiers qui lui sont tous supérieurs. Pour démontrer l'existence d'une décomposition en produit de facteurs premiers, on procède comme suit. Tout d'abord, la décomposition existe pour $n = 2$, tout simplement parce que dans ce cas n est un nombre premier. Supposons que l'on sache décomposer les entiers n en un tel produit jusqu'à l'entier N (non inclus). Pour décomposer l'entier N, deux cas se présentent. Ou bien N est premier, et alors la décomposition est immédiate. Ou bien N est composé, c'est-à-dire que N est produit de deux entiers a et b inférieurs à $N = a \cdot b$; puisque a et b sont plus petits que N, chacun peut être décomposé en un produit de facteurs premiers et le produit de ces deux décompositions donne une décomposition de N. Ainsi, de proche en proche, tout entier naturel est décomposable. Il s'agit ensuite de montrer l'unicité de la décomposition. Il s'agit d'établir que, dans deux décompositions de N en un produit de facteurs premiers, les facteurs premiers qui interviennent sont les mêmes, ainsi que le nombre d'occurrences de chacun d'entre eux ; seul l'ordre peut varier (par exemple $2 \cdot 3 = 3 \cdot 2$). Cette étape, bien plus délicate, est basée sur la propriété suivante, que nous admettrons : *si un nombre premier p divise un produit de deux entiers a . b, alors p divise a ou b*. Considérons

l'un des facteurs premiers p intervenant dans la première décomposition de N ; alors p divise N, et donc l'un des facteurs premiers q de la seconde décomposition. Mais q est lui-même premier, donc n'est divisible que par 1 et par lui-même, ce qui assure $p = q$. Retirant le facteur $p = q$ de chacune des décompositions, on obtient deux nouvelles décomposition de N / p, et l'on recommence le raisonnement avec l'un des facteurs premiers restant. Ceci permet de conclure en un nombre fini d'étapes. Bien sûr, il aurait fallu montré la propriété, cruciale, qui a été employée, mais cela nous mènerait légèrement trop loin.

2. Démonstration du petit théorème de Fermat

En l'exprimant au moyen des congruences, comme nous l'avons vu dans le chapitre 5, le théorème affirme que « si p est un nombre premier, alors $a^p = a \bmod (p)$ pour chaque nombre naturel a. » Le théorème équivaut à démontrer que p divise $a^p - a$. Démontrons le théorème par la méthode d'induction sur a, c'est-à-dire que nous supposerons que le théorème est vrai pour un nombre naturel a et nous démontrerons donc que c'est aussi le cas pour $a + 1$. Nous partons donc de l'hypothèse que p divise $a^p - a$. Selon le développement du binôme de Newton, nous avons

$$(a+1)^p = a^p + \binom{p}{1} a^{p-1} + \binom{p}{2} a^{p-2} + \ldots + \binom{p}{p-1} a + 1.$$

En passant les termes a^p et 1 dans le premier membre, il nous reste

$$(a+1)^p - a^p - 1 = \binom{p}{1} a^{p-1} + \binom{p}{2} a^{p-2} + \ldots + \binom{p}{p-1} a.$$

Le facteur p est dans tous les facteurs du second membre ; nous pouvons donc affirmer que p divise le membre de droite et, par voie de conséquence, également le membre de gauche $(a + 1)^p - a^p - 1$.

Or, par hypothèse d'induction, p divise $a^p - a$; nous pouvons donc affirmer qu'il divise aussi la somme

$$\left[(a+1)^p - a^p - 1\right] + a^p - a.$$

Une somme qui, en effectuant les opérations appropriées, peut s'exprimer sous la forme

$$\left[(a+1)^p - a^p - 1\right] + a^p - a = (a+1)^p - (a+1).$$

De cette manière, nous savons que le résultat est également vrai pour $a + 1$, ce qui établit le théorème.

Bibliographie

Bentley, P.J., *Livre des nombres. Leur histoire et leurs secrets, des origines à nos jours*, Paris, Eyrolles, 2009.

delahaye, J.-P., *Merveilleux Nombres Premiers,* Paris, Belin, « Pour la Science », 2000.

Derbyshire, J, *Dans la Jungle des nombres premiers,* Paris, Dunod, « Quai des sciences », 2007.

Durán, A.J., *Pasiones, piojos, dioses…y matemáticas,* Barcelona, Destino, 2009.

Hardy, G.H., *L'Apologie d'un mathématicien (autobiographie),* Paris, Belin, 1991.

Ifrah, G., *Les Chiffres ou l'histoire d'une grande invention*, Paris, Robert Laffont, 1985.

Kircher, P., *Aritmología,* Madrid, Breogán, 1984.

Kline, M., *Mathematical Thought from Ancient to Modern Times*, Oxford University Press, 1990.

Newman, J.R., *The World of Mathematics*, New York, Simon and Schuster, 1956.

Pickover, C.A., *Oh, les nombres !*, Paris, Dunod, 2001.

Sautoy, M. du, *La Symphonie des nombres premiers*, Paris, Points, 2007.

Stewart, I., *La nature et les nombres*, Paris, Hachette, 2000.

— : *Arpenter l'infini – Une histoire des mathématiques*, Paris, Dunod, 2010.

Szpiro, G., *The Secret Life of Numbers*, Washington, National Academies Press, 2006.

Tenenbaum, G., et Mendès-France, M., *Les Nombres premiers, entre l'ordre et le chaos*, Paris, Dunod, 2011.

Index analytique

Société éditrice :
RBA Coleccionables. S.A.
Avenida Diagonal, 189
08018 Barcelone - Espagne
RCS de Barcelone ESA 78898350

Graphisme couverture : Llorenç Martí
Version française : NordOok
Crédits photographiques : age fotostock, Corbis, iStockphoto
Traduit de l'espagnol par : Youssef Halaoua, Maguy Ly, Laurence Moinereau

Administration, marketing, adaptation éditoriale
Cobra SAS
18-22 rue des Poissonniers
92 200 Neuilly-sur-Seine

DIFFUSION EN KIOSQUE
Service des ventes France :
PROMÉVENTE
(réservé aux dépositaires de presse)
Pour la Belgique :
AMP - 1, rue de la Petite-Île - 1070 Bruxelles
Pour la Suisse :
Naville - 38-42, avenue Vibert - CH 1227 Carouge – GE
Tel : (022) 308 04 44

SERVICE CLIENTS (France)
Le Monde est mathématique
90, boulevard National
92258 La Garenne Colombes Cedex
Tél. : 01 75 43 30 66 (prix d'un appel national)
Pour en savoir plus sur votre collection, vous abonner, payer vos factures d'abonnement, contactez le service clients : www.mondemathematique.fr
L'éditeur se réserve le droit d'interrompre la publication en cas de mévente.

ISBN : 978-2-8152-0238-1
Dépôt légal : septembre 2011

Imprimé et relié par Rodesa
Villatuerta (Navarre) - Espagne
Achevé d'imprimer : septembre 2011.
Imprimé en Espagne - *Printed in Spain*