« Je sais que les nombres sont beaux.
S'ils ne le sont pas, rien ne l'est. »
Paul Erdös

Pourquoi les nombres premiers ?

À l'image des atomes pour les molécules, les nombres premiers sont les briques élémentaires des nombres entiers. Quantité de problèmes sur les premiers sont aussi simples à énoncer que difficiles à attaquer. Un éminent mathématicien de Harvard a fait le pari de les présenter en ne faisant appel qu'à des notions élémentaires de mathématiques.

Barry Mazur
est professeur de mathématiques à Harvard.
mazur@math.harvard.edu

À en croire Aristote, les premiers pythagoriciens pensaient que les principes gouvernant le Nombre sont *« le principe de toutes choses »* ; les éléments du nombre étant plus fondamentaux encore que les quatre éléments physiques d'Empédocle : terre, air, feu et eau. Réfléchir sur le Nombre, c'est se rapprocher de l'architecture de *« ce qui est »*. Depuis cette époque, qu'est devenue la pensée sur les nombres ?
Il y a près de quatre siècles, René Descartes exprimait l'espoir qu'il n'y aurait bientôt *« plus rien à découvrir en géométrie »*. Les physiciens d'aujourd'hui rêvent d'une *« théorie unifiée »*. Mais, toute vénérable, belle et puissante qu'elle soit, la mathématique des nombres en est peut-être encore à ses débuts. Elle pourrait receler autant de profondeurs à explorer que l'âme humaine, sans que l'on attende ou même que l'on espère une théorie ultime.

ARISTOTE portait un grand intérêt à la distinction entre le « composé » et l'« incomposé ». ©DANIEL ARNAUDET/RMN

Dans les écrits d'un prédécesseur de Platon, Philolaos, les nombres premiers sont cités comme une classe particulière de nombres. Platon, lui, n'en fait pas spécifiquement mention dans ses dialogues — ce qui m'étonne, connaissant le grand intérêt que le philosophe portait aux développements mathématiques. Ils apparaissent incidemment dans les écrits d'Aristote, et ce n'est pas surprenant au regard de l'intérêt qu'il portait à la distinction entre le composé et l'incomposé : *« L'incomposé vient avant le composé »*, écrit-il dans le livre 13 de sa *Métaphysique* (faisant donc, entre autres, un usage intemporel fort intéressant du mot « avant »).
Bref, les nombres premiers, malgré la position essentielle qu'ils occupent dans la compréhension moderne du nombre, n'ont pas fait l'objet d'un intérêt particulier dans la littérature antique pré-euclidienne — du moins dans celle qui est parvenue jusqu'à nous. Ils ne paraissent pas avoir été reconnus comme la notion mathématique extraordinaire, au centre de toute compréhension profonde des phénomènes numériques, qu'ils représentent aujourd'hui.
Il existe une extraordinaire abondance de vérités établies sur les nombres. Ces vérités suscitent une profonde admiration pour la merveilleuse complexité des nombres premiers. Mais chaque découverte donne naissance à toute une nouvelle série de questions, d'hypothèses, d'heuristiques, de prévisions et de problèmes non résolus.

ILLUSTRATION GIANPAOLO PAGNI

Arbre de factorisation

Au cœur du mystère des nombres premiers se trouve l'un des grands problèmes mathématiques non résolus, la conjecture de Riemann. Elle vaudra un million de dollars offerts par l'Institut Clay à la personne qui saura la résoudre et sa solution — argent ou pas — est cruciale pour notre compréhension de la nature des nombres. Dans ce numéro (p. 26), Gilles Lachaud explique de quoi il s'agit et pourquoi la résolution de cette conjecture nous donnera une vision nouvelle de la *« structure intime »* des premiers.
Par définition, un « nombre premier » (on dit aussi simplement un « premier ») est un entier supérieur à 1 qui ne peut pas s'écrire sous la forme d'un produit de deux entiers plus petits. Les deux premiers de la série sont donc 2 et 3. L'entier suivant, 4, n'est pas premier car $4 = 2 \times 2$; le suivant, 5, l'est. En disposant de la multiplication pour outil, les premiers sont les briques qui permettent de fabriquer tous les nombres.
Selon un théorème fondamental d'arithmétique, tout nombre (supérieur à 1) peut être décomposé sous la forme d'un produit de facteurs premiers, et cette factorisation est unique (sauf à changer l'ordre des facteurs).
Par exemple, si l'on essaye de factoriser le nombre 300, il y a diverses façons de commencer :

$$300 = 30 \times 10$$

ou

$$300 = 6 \times 50$$

et plusieurs autres encore. Continuons à factoriser (à « descendre » le long chacun de ces possibles « arbres de factorisation ») jusqu'à la fin.
Par exemple :

$$300$$
$$30 \times 10$$
$$3 \times 10 \times 2 \times 5$$
$$3 \times 2 \times 5 \times 2 \times 5$$

On finit toujours avec le même jeu de ▷

nombres premiers :

$$300 = 2^2 \times 3 \times 5^2$$

Quels que soient les choix qui peuvent se présenter au cours du cheminement dans l'arbre de factorisation, l'unicité de ce jeu ultime de facteurs premiers — les atomes, de tout nombre N — est un authentique théorème. C'est Carl Friedrich Gauss, au début du XIXe siècle, qui en a donné la démonstration explicite (mais l'unicité a été utilisée par d'autres mathématiciens avant lui). La conjecture de Riemann nous amène à cette question : avec quelle profondeur peut-on connaître les nombres premiers, ces atomes de la multiplication ?

LES NOMBRES QUI S'ÉCRIVENT SOUS CETTE FORME S'APPELLENT LES « NOMBRES DE MERSENNE ». Ils ne peuvent être premiers que si *n* est premier. Le plus grand premier connu à ce jour est de cette forme. Il compte près de huit millions de chiffres dont quelques-uns sont indiqués dans cette représentation.

Il existe une infinité de nombres premiers. Dans ses *Éléments*, Euclide montre de manière très ingénieuse que, quel que soit un nombre premier p, la suite finie des premiers jusqu'à p,

$$2, 3, 5, 7, 11, \ldots, p,$$

ne contient pas la totalité des nombres premiers. En effet, en multipliant entre eux tous ces nombres et en ajoutant 1 au résultat, on obtient un nombre

$$N = 2 \times 3 \times 5 \times 7 \times 11 \times \cdots \times p + 1$$

et, comme tous les nombres supérieurs à 1, le nombre N ainsi construit est soit premier soit divisible par un nombre premier. Mais il n'est certainement pas divisible par l'un quelconque des premiers jusqu'à p puisque, par construction, le reste de la division de N par tout premier de la suite est égal à 1. Ainsi, tout diviseur premier de N doit être un nouveau nombre premier. En un mot, aucune liste finie de nombres premiers n'est exhaustive ! La clarté de ce raisonnement ne doit néanmoins pas nous faire croire que nous avons, avec ce calcul, une recette utilisable pour trouver concrètement des nombres premiers toujours plus grands.

Pourtant, les choses commencent bien : par exemple, avec les deux premiers nombres premiers, 2 et 3, le calcul d'Euclide permet de construire le nombre $N = 2 \times 3 + 1$ qui est justement le nombre premier 7.

En partant des trois premiers, 2, 3 et 5, on obtient $N = 2 \times 3 \times 5 + 1$, c'est-à-dire le nombre premier 31.

Cependant, après avoir fabriqué les quelque 200 premiers nombres premiers, le nombre colossal donné par le calcul d'Euclide (le produit de tous ces premiers, plus 1), dont les facteurs premiers doivent être nouveaux, est tellement grand que ni vous ni votre ordinateur ne pourrez le factoriser de manière à obtenir ces nouveaux premiers.

Nombre record

Dès lors, il n'est pas surprenant que certains aient travaillé dur pour découvrir — sous forme explicite — des nombres premiers très grands. À l'heure actuelle, le record est détenu par le nombre

$$P = 2^{25\,964\,951} - 1$$

qui compte 7 816 230 chiffres et dont la primalité a été démontrée en février 2005. Si vous recherchez ce nombre sur Google, vous apprendrez l'histoire de la découverte de sa primalité, une aventure menée par des passionnés des nombres à travers le monde. Vous apprendrez par exemple que, pour aborder efficacement la question du caractère premier d'un tel nombre (de près de huit millions de chiffres), il faut une théorie adaptée, spécialement conçue pour le manipuler : il est tellement grand qu'il lui faut une théorie pour lui tout seul !

Vous vous posez peut-être des questions sur la forme particulière sous laquelle se présente notre nombre record :

$$2^{25\,964\,951} - 1$$

Pour manipuler des nombres aussi grands, il vaut mieux avoir de bons indices sur la manière dont on peut les calculer. Une notation commode pour un nombre de grande taille devrait en effet aussi nous indiquer une façon de conduire des calculs avec ce nombre. C'est le cas pour celui-ci, qui nous souffle : multipliez 2 par lui-même un certain nombre de fois, puis soustrayez 1. Même notre notation décimale classique présente un mode de calcul du nombre écrit : quand on écrit par exemple « 389 », cette écriture nous dit d'ajouter trois centaines à huit dizaines et à neuf unités pour obtenir le nombre en question.

Les nombres de la forme précédente, $2^n - 1$, sont appelés nombres de Mersenne, du nom de Marin Mersenne, un moine de l'ordre des Minimes qui vivait au début du XVIIe siècle.

Pour qu'un tel nombre, $2^n - 1$, ait une chance d'être premier, il faut que l'exposant lui-même soit premier et, de fait,

$$n = 25\,964\,951$$

est premier.

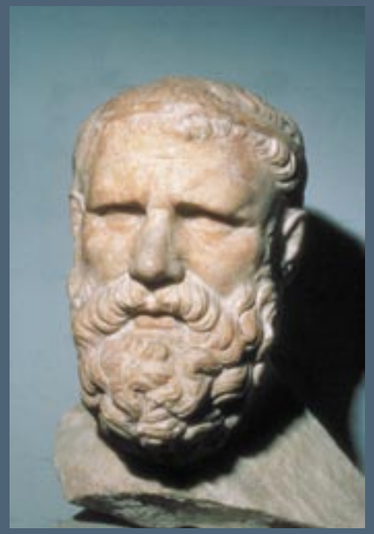
Précisons ce que l'on entend lorsque l'on affirme que le nombre premier

$$P = 2^{25\,964\,951} - 1$$

est « *donné sous forme explicite* ». Soit Q le plus petit nombre premier supérieur à P, qui existe d'après le théorème d'Euclide rappelé plus haut, et qui est un nombre parfaitement défini. Quelles sont les différences qualitatives entre les manières dont nous sont présentés les premiers P et Q ? Ce dernier n'est-il pas lui aussi « *donné de manière explicite* » ?

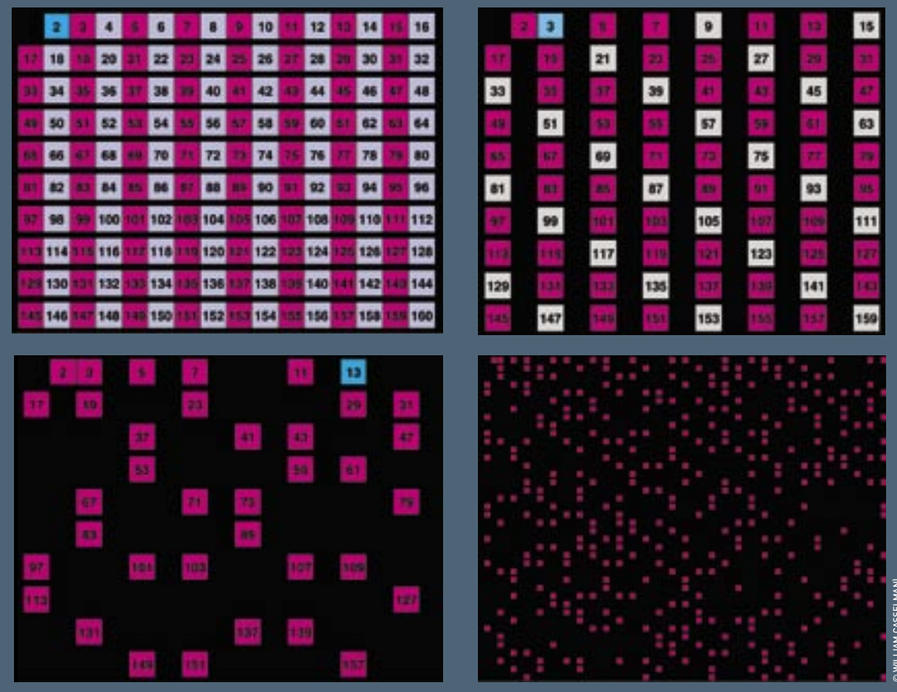
LES PREMIERS AU CRIBLE D'ÉRATOSTHÈNE

Appliquons la méthode d'Ératosthène aux 160 premiers entiers :
- 1 n'est pas premier, on le grise et on le supprime de la liste.
- 2 est premier, mais, de fait, aucun des multiples de 2 ne l'est.
- On conserve donc 2 et on supprime tous ses multiples.
- On procède de même pour 3, qui est aussi premier.
Si l'on continue au delà de 160, on obtient une figure qui peut paraître complètement désordonnée au premier abord, mais sur laquelle les mathématiciens cherchent des éléments de régularité.



ÉRATOSTHÈNE, ASTRONOME, MATHÉMATICIEN ET GÉOGRAPHE GREC, a laissé son nom à sa méthode pour trouver les nombres premiers. On lui doit aussi la première mesure relativement exacte de la circonférence de la Terre.

Le mathématicien Don Zagier témoigne ainsi de la fascination qu'exercent sur les mathématiciens l'élégance et la complexité des nombres premiers : *« Il y a deux faits concernant la distribution des nombres premiers qui, je l'espère, vous convaincront avec une force telle qu'ils resteront pour toujours gravés dans votre cœur. Le premier, c'est que ce sont des objets à l'intérêt purement décoratif et qui sont de surcroît les plus arbitraires étudiés par les mathématiciens. Ils poussent parmi les entiers naturels comme des mauvaises herbes, paraissant n'obéir à aucune autre loi que celle du hasard. Personne ne peut prévoir où se trouvera le suivant. Le deuxième fait est encore plus étonnant, parce qu'il dit exactement le contraire : les nombres premiers font preuve d'une régularité ahurissante, leur comportement répond à des lois, et ils obéissent à ces lois avec une précision quasi militaire. »*



Voici une petite indication de la raison pour laquelle je pense, moi au moins, qu'il y a une sérieuse différence entre les manières dont P et Q sont donnés. Si vous me le demandez, je peux répondre à des quantités de questions précises sur P, alors que j'en suis incapable pour Q ; par exemple, un calcul simple me permet de voir que le dernier chiffre de l'écriture décimale de P est 7, alors que je suis bien prêt à parier que personne de mon vivant ne pourra jamais me donner le dernier chiffre de Q.

Comment procéder maintenant pour dresser une liste de tous les nombres premiers dans une série de nombres entiers ? Ératosthène, le grand mathématicien de Cyrène (qui était aussi bibliothécaire à Alexandrie et correspondant d'Archimède), a expliqué comment procéder pour trouver de façon systématique tous les nombres premiers jusqu'à un nombre donné. Voici comment il nous dirait de procéder pour trouver tous les premiers jusqu'à 29. D'abord, dresser la liste des nombres jusqu'à 29 :

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

Maintenant, commencer par entourer le 2 puis rayer tous les multiples de 2 plus grands que 2. Ensuite, revenir au début de la suite et entourer le premier nombre qui n'est ni cerclé ni rayé (c'est évidemment le 3), puis rayer tous les multiples de 3 plus grands que 3.

On a compris le principe : revenir au début de la suite, entourer le premier nombre non cerclé ni rayé puis rayer tous ses multiples. Répéter l'opération jusqu'à ce que tous les nombres de la suite soient cerclés ou rayés : les nombres cerclés sont les nombres premiers.

Si vous n'avez aucune expérience des mathématiques, je vous conseille de suivre la méthode d'Ératosthène en entourant et rayant les différents nombres, pour voir émerger les nombres premiers, curieusement disséminés parmi tous les nombres de la séquence :

2 3 • 5 • 7 • • • 11 • 13 • • • 17 • 19 • • • 23 • • • • • 29, . . .

(voir l'encadré p. 23)

Rien de bien difficile en somme. Pourtant, des questions très simples sur les écarts entre les éléments de la suite infinie des nombres premiers aboutissent très vite à un blocage.

Par exemple : existe-t-il une infinité de paires de premiers dont la différence soit 2 ? La séquence précédente paraît riche en paires de ce type :

5 – 3 = 2
7 – 5 = 2
13 – 11 = 2
19 – 17 = 2

On sait qu'il y a 1 177 209 242 304 paires de ce type parmi les nombres inférieurs à 1 000 000 000 000 000.

Mais la réponse à notre question *« en existe-t-il une infinité ? »* n'est pas connue.

Autres questions :

– Existe-t-il une infinité de paires de premiers dont la différence soit égale à 4 ? Réponse tout aussi inconnue.

–Tout nombre pair supérieur à 2 est-il la somme de deux premiers ?

Réponse : inconnue.

– Existe-t-il une infinité de nombres premiers qui soient supérieurs de 1 à un carré parfait (c'est-à-dire à un carré d'un nombre entier) ?

Réponse : inconnue.

– Existe-t-il une formule claire donnant le prochain premier ? Plus précisément, si je vous donne un nombre N, par exemple N = 1 000 000 et si je vous demande de trouver le premier nombre premier après N, y a-t-il une méthode permettant de répondre sans, d'une manière ou d'une autre, parcourir toute la suite des nombres suivant N, en rejetant successivement les non-premiers jusqu'à découvrir le premier premier ?

Réponse : inconnue.

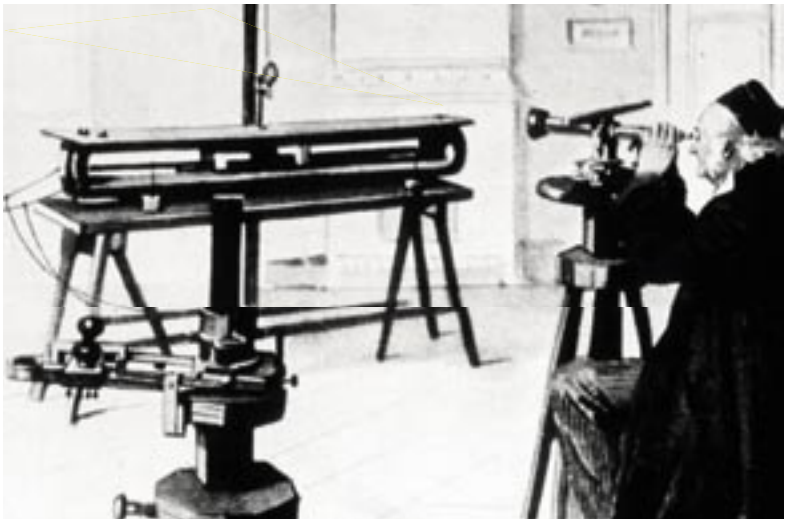
Les questions de ce type (il y en a des quantités d'autres), formulables en termes simples, abondent. Tout le monde pourrait se les poser et elles ont aussi été posées par les mathématiciens.

La conjecture de Riemann et beaucoup d'autres questions non résolues abordées dans ce numéro sont des questions d'une tonalité assez différente. Elles sont soigneusement formulées à la lumière d'une connaissance approfondie des mathématiques contemporaines, et visent à expliquer des structures fondamentales.

Il y a donc beaucoup à faire : élucider l'architecture encore cachée des nombres, et progresser dans la réponse aux innombrables questions simples qui viennent immédiatement à l'esprit chaque fois qu'on a affaire aux nombres. Il y a plus de deux millénaires que l'on étudie les nombres, mais nous n'en sommes encore qu'à l'aube de leur compréhension. ■

B. M.

Il existe une quantité de questions formulables en termes simples qui n'ont pas de réponse.



CARL FRIEDRICH GAUSS fut le premier à démontrer qu'il n'existe qu'une seule manière de factoriser un nombre en un produit de nombres premiers. Également astronome, il appliqua notamment des techniques mathématiques pour calculer des trajectoires planétaires. ©AKG IMAGES

Ce texte, traduit par Philippe Brenier, est extrait d'une conférence donnée le 3 mai 2005 au Massachusetts Institute of Technology et qui fera prochainement l'objet d'un livre illustré par William Stein, également mathématicien à Harvard.