POUR LA SCIENCE
Édition française de Scientific American

HORS-SÉRIE

COMPLÉTEZ VOTRE COLLECTION DÈS MAINTENANT !

N° 91 (avr. 16)
réf. DO091

N° 92 (juil. 16)
réf. DO092

N° 93 (oct. 16)
réf. DO093

N° 94 (janv. 17)
réf. DO094

N° 95 (avr. 17)
réf. DO095

N° 96 (août 17)
réf. DO096

N° 97 (nov. 17)
réf. DO097

N° 98 (févr. 18)
réf. DO098

N° 99 (mai 18)
réf. DO099

N° 100 (août 18)
réf. DO100

N° 101 (nov. 18)
réf. DO101

N° 102 (fév. 19)
réf. DO102

RETROUVEZ L'ENSEMBLE DES ANCIENS NUMÉROS SUR **BOUTIQUE.POURLASCIENCE.FR/HORS-SERIE.HTML**

À retourner accompagné de votre règlement à :
Pour la Science – Service VPC – 19 rue de l'Industrie – BP 90053 – 67402 Illkirch Cedex – email : pourlascience@abopress.fr

☑ **OUI, je commande des numéros de Pour la Science Hors-série, au tarif unitaire de 10,90 €.**

1 / JE REPORTE CI-DESSOUS LES RÉFÉRENCES à 5 chiffres correspondant aux numéros commandés :

1re réf. ..... 0 1 x 10,90 € = 1 0 9 0 €
2e réf. ..... x 10,90 € = €
3e réf. ..... x 10,90 € = €
4e réf. ..... x 10,90 € = €
5e réf. ..... x 10,90 € = €
6e réf. ..... x 10,90 € = €

TOTAL À RÉGLER €

Offre valable jusqu'au 31/12/2019 en France Métropolitaine. Pour une livraison à l'étranger, merci de consulter **boutique.pourlascience.fr**

Les informations que nous collectons dans ce bon de commande nous aident à personnaliser et à améliorer les services que nous vous proposons. Nous les utiliserons pour gérer votre accès à l'intégralité de nos services, traiter vos commandes et paiements, et vous faire part notamment par newsletters de nos offres commerciales moyennant le respect de vos choix en la matière. Le responsable du traitement est la société *Pour La Science*. Vos données personnelles ne seront pas conservées au-delà de la durée nécessaire à la finalité de leur traitement. *Pour la Science* ne commercialise ni ne loue vos données à caractère personnel à des tiers. Les données collectées sont exclusivement destinées à *Pour la Science*. Nous vous invitons à prendre connaissance de notre charte de protection des données personnelles à l'adresse suivante : https://rebrand.ly/charte-donnees-pls Conformément à la réglementation applicable (et notamment au Règlement 2016/679/UE dit « RGPD ») vous disposez des droits d'accès, de rectification, d'opposition, d'effacement, à la portabilité et à la limitation de vos données personnelles. Pour exercer ces droits (ou nous poser toute question concernant le traitement de vos données personnelles), vous pouvez nous contacter par courriel à l'adresse protection-donnees@pourlascience.fr.

2 / J'INDIQUE MES COORDONNÉES

☐ M. ☐ Mme
Nom : .....
Prénom : .....
Adresse : .....
.....
Code postal ..... Ville : .....
Téléphone .....
J'accepte de recevoir les offres de Pour la Science ☐ OUI ☐ NON

3 / JE CHOISIS MON MODE DE RÈGLEMENT

☐ **Par chèque à l'ordre de** *Pour la Science*
☐ **Carte bancaire**
N° .....
Date d'expiration .....
Clé (les 3 chiffres au dos de votre CB) .....

Signature obligatoire :

Groupe Pour la Science – Siège social : 170 bis, boulevard du Montparnasse, CS20012, 75680 Paris Cedex 14 – Sarl au capital de 32000 € – RCS Paris B 311 797 393 – Siret : 311 797 393 000 23 – APE 5814 Z

PLUS SIMPLE, PLUS RAPIDE
ABONNEZ-VOUS SUR BOUTIQUE.POURLASCIENCE.FR

L'ESSENTIEL

- La répartition des nombres premiers est un défi pour les mathématiciens. La fonction *zêta* de Riemann apporte des informations sur cette répartition.
- Cette fonction *zêta*, au départ définie pour une variable complexe s de partie réelle $\mathrm{Re}(s)$ supérieure à 1, peut être prolongée à tout le plan complexe, à l'exception du point $s=1$.
- D'après la conjecture de Riemann, les zéros non triviaux (pour lesquels la fonction *zêta* s'annule) se trouvent tous sur la droite verticale $\mathrm{Re}(s)=1/2$. Cette conjecture semble vraie, mais reste indémontrée.
- Un million de dollars est promis à qui apportera la preuve de cette hypothèse.

LES AUTEURS

PETER MEIER est assistant à l'Institut de mathématiques de l'université de Würzburg, en Allemagne.

JÖRN STEUDING est professeur à l'Institut de mathématiques de l'université de Würzburg, en Allemagne.

L'hypothèse qui valait un million

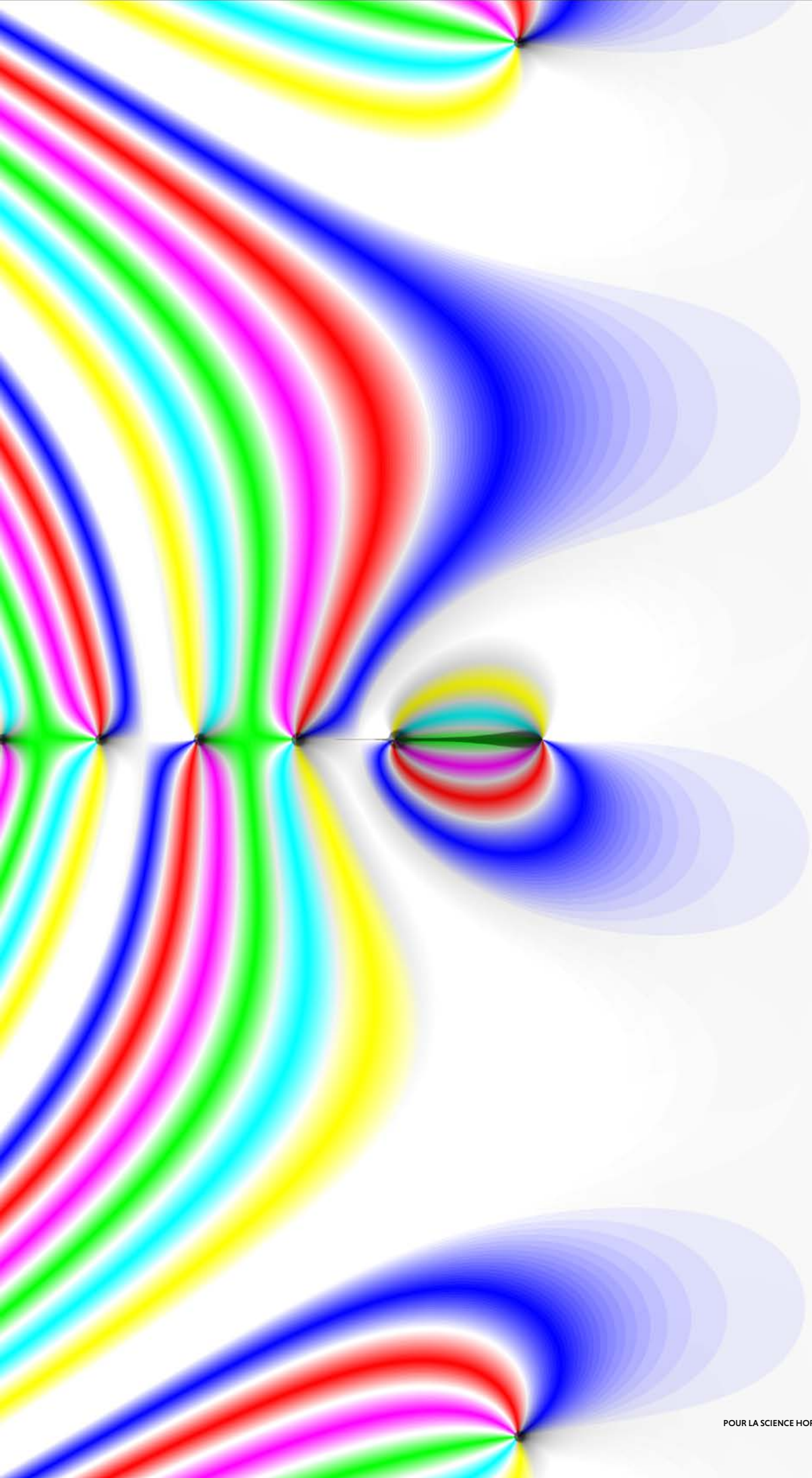
La fonction *zêta* de Riemann est la clé de nombreux résultats de la théorie des nombres, notamment sur la répartition des nombres premiers. Mais ces résultats dépendent d'une hypothèse qui, depuis 160 ans, résiste aux assauts des mathématiciens.

Lors du deuxième Congrès international des mathématiciens, à Paris, en août 1900, le mathématicien David Hilbert dresse une liste de vingt-trois problèmes alors irrésolus. Selon lui, ils montraient la voie vers le XX^{e} siècle. Où en est-on aujourd'hui? Quelques-uns, environ une dizaine, ont été résolus, parfois assez rapidement. D'autres ne le sont que partiellement. D'autres encore continuent de résister aux assauts des plus grands mathématiciens. Il en est ainsi du huitième problème qui rassemble trois conjectures portant sur les nombres premiers. L'une d'elles est l'hypothèse de Riemann, et elle semble si difficile qu'elle figure désormais parmi les sept défis mathématiques réputés insurmontables, posés par l'institut de mathématiques Clay en 2000 (un seul a été relevé depuis): chacun est doté d'un prix de un million de dollars pour qui en apportera la preuve... En quoi consiste cette hypothèse?

LE PRINCE IMPRESSIONNÉ

Le mathématicien allemand Bernhard Riemann (1826-1866) accomplit durant sa courte vie une multitude de prouesses. Il impressionna même le «prince des mathématiques», Carl Friedrich Gauss, par les nouvelles méthodes de nature topologique qu'il introduisit en analyse complexe et par la >

La fonction *zêta* de Riemann, ζ, est calculée pour les points du plan complexe $s=x+iy$. Dans le domaine présenté, x varie entre -10 et $+20$ et y entre -15 et $+15$. La valeur $\zeta(s)$ est aussi un nombre complexe de module ρ et d'argument τ: $\zeta(s)=\{\rho, \tau\}$. L'ensemble des valeurs calculées $\zeta(s)$ est représenté comme une surface vue de dessus, chaque point (x, y) ayant comme élévation le module ρ et comme couleur une fonction de l'argument τ. Les zéros (triviaux et non triviaux) sont les creux dans la surface ($\rho=0$) où «convergent» toutes les couleurs (τ est indéterminé).



D'UN PRODUIT INFINI À UNE SOMME INFINIE

Chaque facteur $1/(1-1/p^s)$ dans le produit eulérien infini peut lui-même s'écrire comme une somme infinie. En effet, d'après la formule donnant la somme d'une série géométrique de raison $0<r<1$, on a :

$$1 + p^{-s} + p^{-2s} + \ldots = \frac{1}{1-p^{-s}}$$

Le produit eulérien s'écrit donc comme un produit infini de sommes infinies :

$$(1 + 2^{-s} + 2^{-2s} + \ldots)\cdot(1 + 3^{-s} + 3^{-2s} + \ldots)\cdot(1 + 5^{-s} + \ldots)\cdot\ldots$$

En développant, on obtient la somme (infinie) de tous les produits possibles obtenus en prenant un terme dans chacune des parenthèses. C'est donc la somme de tous les produits possibles de puissances de nombres premiers (on inclut 1 parmi les puissances). Mais à cause de l'unicité de la décomposition d'un nombre entier en un produit de puissances de nombres premiers, c'est aussi exactement la somme des $1/n^s$ pour tous les entiers n, et l'on retrouve la fonction *zêta*. Comme pour tous les calculs avec une infinité de termes, on doit s'assurer que les manipulations indiquées sont permises, ce qui est le cas ici.

> géométrie aujourd'hui nommée riemannienne. À cela s'ajoutent des travaux remarquables de géométrie différentielle et sur les équations différentielles, au rôle si important dans les sciences de la nature, des mémoires de physique mathématique, une fondation théorique de la notion d'intégration et bien d'autres choses.

Un seul article de la plume de Riemann concerne la théorie des nombres : « Sur le nombre des nombres premiers inférieurs à une quantité donnée ». Ce texte aussi témoigne du génie de son auteur. Il contient de nombreuses conjectures qui n'ont été prouvées que plusieurs décennies plus tard. Ainsi qu'une autre que Riemann commente de façon lapidaire : « Il serait à désirer sans doute que l'on eût une démonstration rigoureuse de cette proposition ; néanmoins, j'ai laissé cette recherche de côté pour le moment après quelques rapides essais infructueux, car elle paraît superflue pour le but immédiat de mon étude. »

« CAR ELLE PARAÎT SUPERFLUE »

Dommage… La démonstration que Riemann avait « laissée de côté pour le moment » continue de faire défaut. Et ce qu'il voulait prouver est devenu célèbre sous le nom de conjecture ou hypothèse de Riemann.

En fait, la conjecture de Riemann revêt une importance considérable en théorie des nombres. Sa démonstration donnerait un fondement plus solide à des centaines de travaux mathématiques qui supposent vraie l'assertion de Riemann. Ces résultats concernent en particulier l'ensemble des nombres premiers.

D'un côté, ils constituent les « atomes » indispensables du royaume des nombres : chaque entier peut être décomposé de façon unique, à l'ordre près des facteurs, en un produit de puissances de nombres premiers. De l'autre côté, ils incarnent en quelque sorte l'irrégularité, ce qui reste lorsqu'on a éliminé tout ce qui est régulier, c'est-à-dire les multiples de 2, de 3… bref, les nombres composés. Précisément en raison de cette irrégularité, les nombres premiers sont très difficiles à saisir.

De nombreuses questions élémentaires sur les nombres premiers restent aujourd'hui sans réponse, ou du moins sans réponse satisfaisante. En voici trois parmi les plus saillantes :

Comment les nombres premiers sont-ils répartis parmi les nombres entiers ? Existe-t-il une infinité de nombres premiers jumeaux (*voir Des jumeaux, des cousins et… des nombres sexy, par B. Martin, page 60*) ? Tout entier pair supérieur ou égal à 4 est-il la somme de deux nombres premiers ?

La dernière question est nommée conjecture de Goldbach et fait aussi partie du huitième problème de Hilbert. On sait que les exceptions à cette conjecture, si elles existent, doivent être des nombres gigantesques, mais une réponse définitive semble inaccessible par les méthodes actuelles. Il en est de même pour la conjecture des nombres premiers jumeaux.

Quant à la première question, qui porte sur la répartition des nombres premiers, nous disposons de certains résultats. Nous les devons pour l'essentiel à une idée introduite par le Suisse Leonhard Euler (1707-1783) : on construit un nouvel objet mathématique où chacun des nombres premiers (qui sont en nombre infini) contribue, puis on essaie de l'analyser le plus complètement possible. L'objet porte aujourd'hui le nom de fonction *zêta* (*zêta* étant la lettre grecque ζ) et est défini par :

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

Autrement dit, on prend tous les nombres entiers n élevés à la puissance s, où s est pour l'instant un nombre réel quelconque, on en prend les inverses et on additionne (comme on le verra, on peut exprimer cette fonction à partir des seuls nombres premiers). Le signe Σ (la lettre grecque *sigma* majuscule) est l'abréviation usuelle pour une somme.

La somme ainsi définie comporte une infinité de termes, ce qui ne donne pas toujours une valeur finie. On doit plus rigoureusement définir la somme comme une limite, et celle-ci n'existe pas toujours. Si on prend par exemple $s=1$, on obtient la série dite harmonique :

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

qui tend vers l'infini. Si l'on choisit $s<1$, chaque terme de la somme est plus grand que pour $s=1$, la somme est donc *a fortiori* infinie. Mais si $s>1$, la série prend une valeur finie, et on dit qu'elle converge.

La propriété cruciale de la fonction $\zeta(s)$ est qu'on peut l'exprimer, du moins pour $s>1$, comme un produit infini de termes correspondant chacun à un nombre premier. En effet, on a:

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

Le *pi* majuscule, Π, symbolise le produit des termes successifs. Il porte ici sur tous les nombres premiers p, et s'appelle dans ce cas un produit eulérien (*voir l'encadré page ci-contre*).

Il est en fait possible de prolonger la fonction *zêta* en une fonction qui associe à tout nombre réel s différent de 1 une valeur unique bien déterminée. Le calcul de cette valeur dans des cas particuliers donne d'ailleurs lieu à des résultats intéressants; par exemple, un autre exploit d'Euler est l'étonnante formule (*voir l'encadré page suivante*):

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

Mais ce ne sont pas ces valeurs particulières qui nous intéressent ici. Il s'agit plutôt de traduire des assertions sur les nombres premiers en propriétés de la fonction *zêta*, parce qu'avec cette fonction une vaste boîte à outils devient disponible. Parmi les nombreuses méthodes ainsi accessibles, figurent la dérivation et l'intégration, mais aussi et surtout l'arsenal de l'analyse complexe.

L'IDÉE CLÉ DE RIEMANN

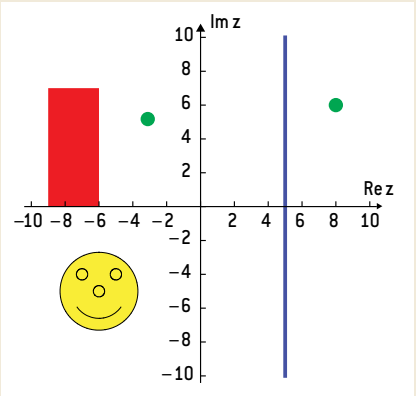
L'idée clé de Riemann a été de ne plus étudier $\zeta(s)$ seulement comme une fonction réelle de la variable réelle s, mais comme une fonction d'une variable complexe (*voir l'encadré ci-dessous*). La définition initiale de la fonction reste la même, mais la variable s peut désormais prendre des valeurs complexes. Un terme tel que n^s avec un exposant complexe sera défini comme $\exp(s \ln n)$, les fonctions exponentielle (exp) et logarithme (ln) étant définies dans le domaine complexe par des séries de puissances entières; par exemple, on a pour tout nombre complexe z: $\exp(z)=e^z=1+z/1!+z^2/2!+z^3/3!+\ldots$

Certaines choses changent peu dans cette extension aux nombres complexes. La série d'Euler converge pour s réel supérieur à 1; cette condition devient maintenant que la partie réelle de s, notée $\mathrm{Re}(s)$, soit supérieure à 1. Sur la droite réelle, le point 1 est la barrière qui bloque la convergence de la série; dans le plan complexe, cette barrière est la droite de tous les nombres dont la partie réelle est 1.

Mais les nombres complexes offrent aussi la possibilité de regarder la fonction définie par la série d'Euler sous un autre angle. Le procédé, nommé « prolongement >

NOMBRES COMPLEXES ET FONCTIONS COMPLEXES

Un nombre complexe est un nombre de la forme $a+ib$, où a et b sont deux nombres réels et i un nombre imaginaire vérifiant, par définition, $i2=-1$. Les nombres complexes sont ainsi une extension des nombres réels – motivée, entre autres, par le désir que toute équation algébrique ait une solution. On peut représenter les nombres complexes par des points dans le plan (on parle de plan complexe, ou de plan de Gauss-Argand). Le nombre $z=a+ib$ est ainsi représenté par le point de coordonnées (a, b), où a est la « partie réelle » $\mathrm{Re}(z)$ de z et b sa « partie imaginaire » $\mathrm{Im}(z)$.
Les nombres réels sont les nombres complexes dont la partie imaginaire est nulle. Les opérations élémentaires, mais aussi la notion de limite, fonctionnent comme pour les nombres réels. On peut donc définir des séries de puissances entières, fonctions de la forme:
$f(z)=a_0+a_1(z-z_0)+a_2(z-z_0)^2+\ldots$
La valeur de f en chaque point z (complexe) est donc définie par une somme infinie. Les coefficients a_j peuvent aussi être des nombres complexes.
Les fonctions de ce genre sont dites analytiques. Les fonctions analytiques, qui ont de nombreuses propriétés intéressantes et fécondes, font l'objet de tout un domaine des mathématiques, l'analyse complexe. Des propriétés remarquables ou mystérieuses que présente une fonction analytique réelle apparaissent souvent sous un autre jour et bien plus clairement lorsque l'on examine la fonction complexe correspondante. L'une des propriétés les plus intéressantes des fonctions complexes est le « prolongement analytique »:
les séries de puissances entières comme précédemment convergent seulement dans un disque autour du point central z_0.
Ce disque ne peut s'étendre que jusqu'à la première singularité rencontrée. Mais rien n'empêche d'évaluer la série autour d'un autre point. Elle a alors un nouveau disque de convergence et celui-ci peut en partie empiéter sur l'ancien. On peut ainsi étendre de proche en proche le domaine de définition d'une fonction analytique.



Dans ce plan de Gauss-Argand ont été figurés les deux points *(en vert)* $8+6i$ et $-3+5i$, la droite de tous les nombres complexes de partie réelle 5 *(en bleu)*, le domaine de tous les nombres complexes de partie réelle comprise entre -9 et -6 et de partie imaginaire comprise entre 0 et 7 *(en rouge)*, ainsi que quelques cercles et arcs de cercle *(en jaune)*.

analytique », est d'usage fréquent en analyse complexe. À l'instar d'Euler avec sa représentation de la série sous forme d'un produit, Riemann trouva une autre expression de la fonction *zêta* qui fournit les mêmes valeurs là où cette fonction était définie auparavant, mais qui de plus attribue des valeurs finies pour toutes les autres valeurs complexes de s – à l'exception de $s=1$.

La valeur $s=1$ est pour la fonction *zêta* ce que le mathématicien nomme une singularité. La fonction prend ici inévitablement une valeur infinie. Lorsqu'on se restreint à la droite réelle, la singularité constitue une barrière infranchissable ; mais dans le plan, on peut simplement la contourner.

RELIER ZÊTA ET GAMMA

Pour mieux appréhender la fonction *zêta*, Riemann appela à la rescousse une autre fonction, initialement définie elle aussi sur une partie du plan complexe et qui peut également être étendue à presque tout le plan par prolongement analytique : la fonction *gamma* (Γ). Celle-ci généralise la fonction factorielle, c'est-à-dire que pour tout entier positif n, elle vérifie : $\Gamma(n)=n!=n(n-1)(n-2)\ldots 2\,.\,1$.

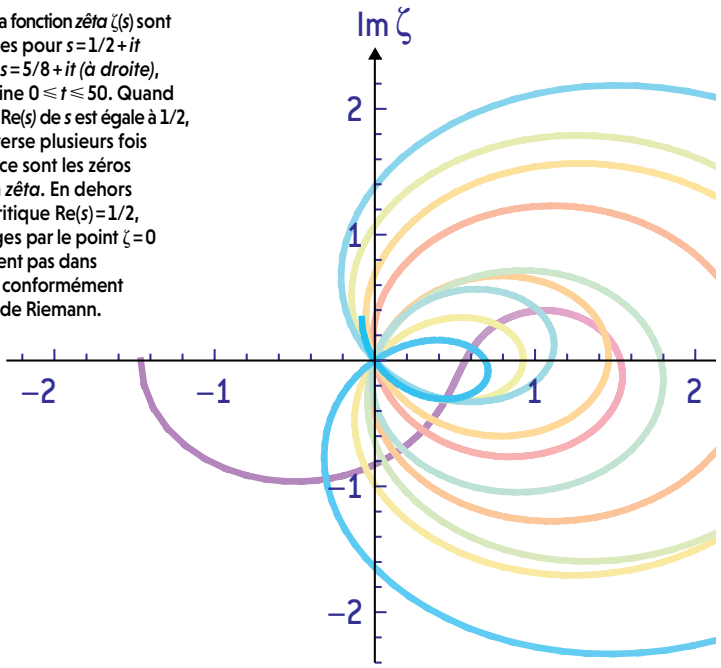
Pour tous les nombres complexes distincts de 0, −1, −2, −3, etc., la fonction *gamma* prend des valeurs finies. Grâce aux techniques de la théorie des fonctions, Riemann obtint la relation suivante entre les fonctions *zêta* et *gamma* :

$$\pi^{-\frac{s}{2}}\,\Gamma\left(\frac{s}{2}\right)\zeta(s)=\pi^{-\frac{1-s}{2}}\,\Gamma\left(\frac{1-s}{2}\right)\zeta(1-s)$$

Une telle équation, qui relie les valeurs de fonctions en différents points, est qualifiée de fonctionnelle. L'équation fonctionnelle ci-dessus a une propriété particulière : elle est invariante si on y remplace s par $1-s$ et réciproquement. Autrement dit, elle est symétrique par rapport au point $s=1/2$. Comme, en outre, les fonctions concernées restent inchangées lors d'une réflexion par rapport à l'axe réel (à une « conjugaison complexe » près, c'est-à-dire au changement de i en $-i$ près), on a une symétrie par rapport à la droite des nombres complexes de partie réelle égale à 1/2. On nomme droite critique cet axe de symétrie.

La symétrie mentionnée a d'intéressantes conséquences. Là où la partie réelle de s est supérieure à 1, on connaît directement la fonction *zêta*, comme expliqué plus haut. On sait ainsi que $\zeta(s)$ n'a là aucun « zéro », c'est-à-dire aucune valeur de s pour laquelle la fonction s'annule, car aucun des facteurs du produit eulérien n'est égal à zéro. Grâce à l'équation fonctionnelle, on peut transposer cette connaissance sur le côté gauche du plan complexe.

Prenons un exemple. Le facteur $\Gamma(s/2)$, qui apparaît dans le membre de gauche de l'équation fonctionnelle, prend aux points $s=0$, −2, −4… une valeur infinie. Mais si l'on choisit pour s l'une de ces valeurs ($s=-2n$ pour un entier naturel n), le membre de droite de l'équation



Les valeurs de la fonction *zêta* $\zeta(s)$ sont ici représentées pour $s=1/2+it$ *(à gauche)* et $s=5/8+it$ *(à droite)*, dans le domaine $0\leqslant t\leqslant 50$. Quand la partie réelle Re(s) de s est égale à 1/2, la courbe traverse plusieurs fois le point $\zeta=0$; ce sont les zéros de la fonction *zêta*. En dehors de la droite critique Re(s)=1/2, de tels passages par le point $\zeta=0$ ne se produisent pas dans ce domaine – conformément à l'hypothèse de Riemann.

UNE FORMULE REMARQUABLE

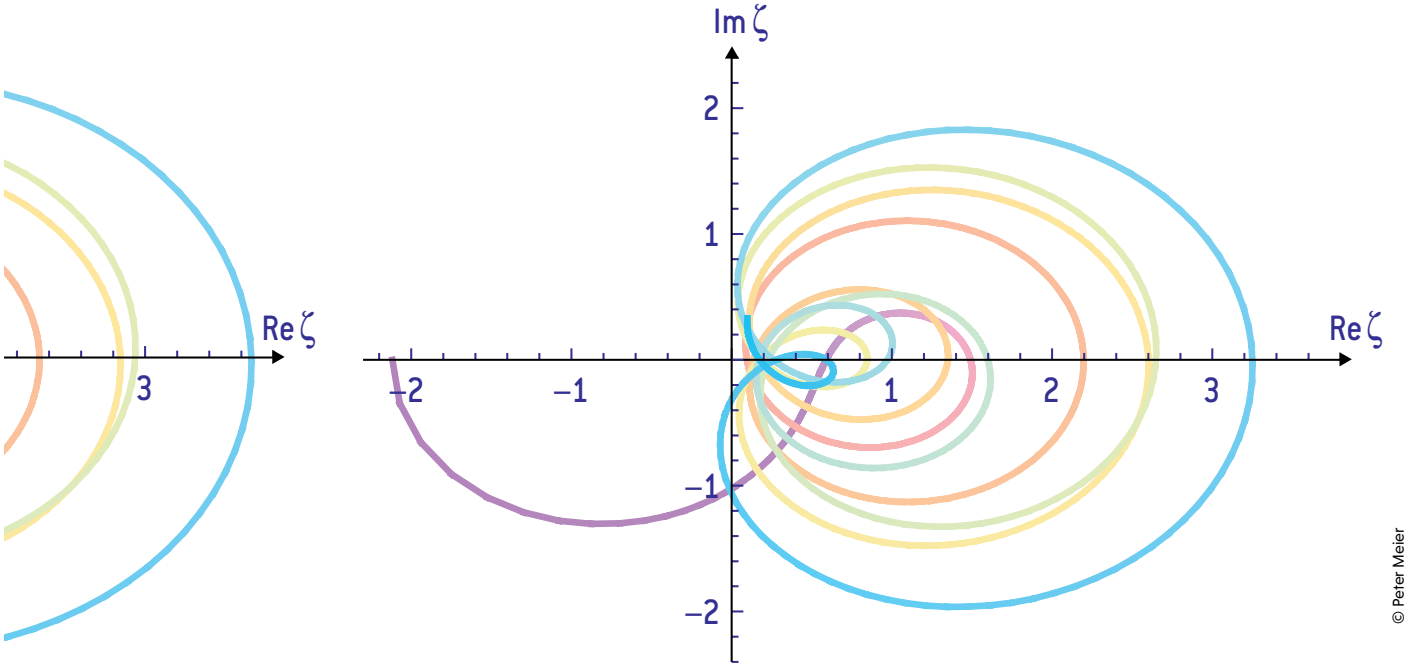
Leonhard Euler a obtenu la formule $1+1/2^2+1/3^2+1/4^2+1/5^2\ldots=\pi^2/6$ en représentant non pas la fonction *zêta* $\zeta(s)$, mais la fonction $(\sin x)/x$, de deux façons : d'une part comme une somme infinie, d'autre part comme un produit infini. Des multiplications et transformations habiles le conduisirent ensuite au résultat. Plus généralement, Euler trouva la formule :

$$\zeta(2k)=\sum_{n=1}^{\infty}\frac{1}{n^{2k}}=(-1)^{k+1}\,\frac{(2\pi)^{2k}B_{2k}}{2(2k)\,!}$$

Le nombre B_j est le j-ème « nombre de Bernoulli ». Ces nombres peuvent être introduits par exemple par des suites définies par récurrence ou par des séries infinies (voir http://bit.ly/Bern-Nu). Les premiers sont $B_0=1$, $B_1=-1/2$, $B_2=1/6$, $B_4=-1/30$, $B_6=1/42$; pour les nombres impairs $j\geq 3$, on a $B_j=0$.
Une formule simple analogue pour les valeurs de la fonction (s) quand la variable est un entier positif impair n'est pas connue ; on sait toutefois que la valeur de $\zeta(3)$ est irrationnelle (un remarquable résultat de Roger Apéry datant de 1978). Autres exemples, Tanguy Rivoal a montré en 2000 qu'il existe une infinité de nombres irrationnels parmi les valeurs prises par $\zeta(s)$ pour les entiers impairs, et Wadim Zudilin a prouvé en 2001 que parmi les quatre nombres $\zeta(5)$, $\zeta(7)$, $\zeta(9)$ et $\zeta(11)$, l'un au moins est irrationnel.
Par ailleurs, on peut écrire aussi $\zeta(2)$ sous la forme d'un produit :

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

Comme π^2 est irrationnel, le nombre de facteurs dans le produit ne peut être fini (sinon, le résultat serait rationnel). C'est l'une des nombreuses preuves de l'infinité des nombres premiers.



© Peter Meier

fonctionnelle donne une expression finie et non nulle. Comment est-ce possible? La seule possibilité est que $\zeta(s)$ s'annule en ces points, puisque tous les autres facteurs de l'équation fonctionnelle sont non nuls. Ainsi, on en déduit que $\zeta(s)=0$ pour $s=-2, -4, -6$, etc. Ces valeurs de s sont les «zéros triviaux» de la fonction *zêta*. Ce sont les seuls zéros dont la partie réelle est négative. Le point $s=0$ n'est en revanche pas un zéro, car $\zeta(1-s)$ donne la singularité $\zeta(1)$.

Pour tous les s de partie réelle supérieure à 1, il n'existe, comme le montre la représentation en produit eulérien, aucun autre zéro. C'est donc seulement dans la bande étroite des nombres complexes de partie réelle comprise entre 0 et 1, la «bande critique», que peuvent se trouver d'autres zéros. C'est sur ces zéros «non triviaux» que porte la fameuse hypothèse de Riemann.

Riemann a conjecturé qu'il existe une infinité de zéros non triviaux de la fonction *zêta*. À propos de leur localisation, il a formulé deux assertions précises. L'une concerne leur répartition verticale: le nombre $N(T)$ de zéros dont la partie imaginaire (c'est-à-dire la hauteur au-dessus de l'axe réel) est comprise entre 0 et une valeur T est:

$$N(T)=\frac{T}{2\pi}\left(\ln\left(\frac{T}{2\pi}\right)-1\right)$$
$$+\ \text{terme d'erreur}\,(T)$$

où le terme d'erreur est petit par rapport à T lorsque T est suffisamment grand. Bien que Riemann ait lui-même donné une idée de la preuve, l'assertion ne fut démontrée complètement que trente ans plus tard, en 1893, par Hans von Mangoldt. Ce dernier montra aussi que le terme correctif était au plus de l'ordre de $\ln T$.

Quant à la seconde assertion, elle concerne la répartition des zéros horizontalement. Riemann affirma que les zéros non triviaux ne peuvent se trouver qu'au milieu de la bande critique, c'est-à-dire sur la droite critique; autrement dit, les zéros non triviaux ont pour partie réelle 1/2. C'est cette assertion qui constitue la conjecture de Riemann.

Pourquoi s'intéresse-t-on autant aux zéros de la fonction *zêta*? Parce qu'ils fournissent des informations sur la répartition des nombres premiers. Il s'agit plus précisément d'une formule évaluant le nombre $\pi(x)$ de tous les nombres premiers inférieurs à x. Gauss avait déjà conjecturé que $\pi(x)\simeq x/\ln x$, formule qu'il avait plus tard raffinée en $\pi(x)\simeq \mathrm{li}(x)$, où $\mathrm{li}(x)$ est le «logarithme intégral», défini par $\mathrm{li}(x)=\int_2^x du/\ln u$. Le signe $\simeq$ signifie ici «à un terme correctif près, qui est petit par rapport à $\mathrm{li}(x)$ pour x assez grand». Plus petit est ce terme correctif, meilleure est la précision de la formule.

MIEUX QUE GAUSS

Or Riemann a réussi à améliorer la prédiction de Gauss quant à $\pi(x)$. Le cœur de son idée est une deuxième représentation en produit, elle-même issue de la théorie des polynômes, c'est-à-dire des fonctions de la forme: $f(s)=a_0+a_1s+a_2s^2+\ldots+a_ns^n$

Un polynôme à coefficients a_i complexes et de degré n (n étant la plus haute puissance dont >

> le coefficient correspondant n'est pas nul) a exactement n zéros, ou «racines», complexes – c'est le théorème fondamental de l'algèbre. Et si 0 n'est pas lui-même une racine du polynôme, on peut écrire ce dernier sous la forme $a(1-s/s_1)(1-s/s_2)\ldots(1-s/s_n)$, où les s_i sont les racines et a une constante appropriée.

La fonction *zêta* n'est bien sûr pas un polynôme. Mais Riemann parvint à l'écrire elle aussi comme un produit de facteurs de la forme $(1-s/\rho)$, où ρ parcourt les zéros non triviaux, avec quelques ingrédients supplémentaires :

$$\frac{s-1}{2}\pi^{-s/2}\Gamma(\frac{s}{2})\zeta(s) = \exp(A+Bs)\prod_{\rho}(1-\frac{s}{\rho})\epsilon$$

où A et B sont des constantes. Dans le membre de gauche, on trouve au lieu de $\zeta(s)$ la demi-équation fonctionnelle : celle-ci est multipliée par $(s-1)$, pour éliminer la singularité au point $s=1$.

Riemann a certes pu obtenir cette formule, mais pas la prouver. C'est seulement en 1893 que le mathématicien français Jacques Hadamard y parvint, et ses résultats généraux sur ce sujet constituent maintenant une partie importante de l'analyse complexe.

Riemann disposait ainsi de deux représentations différentes de la même fonction par un produit : le produit eulérien et la formule ci-dessus. En les comparant, il obtint une formule explicite pour la fonction des nombres premiers $\pi(x)$ (*voir l'encadré page ci-contre*). Mais cette formule aussi dut attendre des décennies avant d'être démontrée, par von Mangoldt en 1895.

Les idées et les conjectures de Riemann stimulèrent les recherches dans cette direction et fécondèrent le domaine en plein essor de la théorie des fonctions complexes. Ces efforts furent enfin couronnés de succès avec la preuve en 1896 de la conjecture de Gauss, nommée aujourd'hui «théorème des nombres premiers», par Hadamard et Charles de La Vallée-Poussin, simultanément mais indépendamment.

Pour cette preuve, on doit s'assurer que la fonction *zêta* n'a pas de zéros dans une partie suffisamment grande de la bande critique. Helge von Koch démontra en 1900 la propriété suivante. Plaçons dans la bande critique une droite verticale qui coupe l'axe réel en une valeur α comprise entre 1/2 et 1. Si la fonction *zêta* n'a pas de zéros à droite de cette ligne, alors le terme correctif dans le théorème des nombres premiers est de l'ordre de grandeur de x^{α} et réciproquement (pour être exact : l'exposant dans le terme correctif n'est pas α, mais un nombre un peu supérieur, aussi peu que l'on veut).

Il s'ensuit en particulier que le terme d'erreur ne peut être inférieur en ordre de grandeur à $x^{1/2}$, puisque $\zeta(s)$ a des zéros sur la droite critique. Si la conjecture de Riemann est vraie, le terme d'erreur est minimal et il s'ensuit que les nombres premiers sont répartis aussi régulièrement que possible.

L'importance de l'hypothèse de Riemann pour les mathématiques peut difficilement être surestimée. Des centaines d'articles portent sur ses conséquences et des résultats significatifs ont été obtenus en la supposant vraie. Il existe ainsi des méthodes cryptographiques importantes en pratique dont la sécurité dépend de la validité de la conjecture de Riemann.

La plupart des mathématiciens pensent que l'hypothèse de Riemann est vraie, notamment pour des raisons esthétiques (l'idée d'un ordre dans l'ensemble des zéros de la fonction *zêta* est plaisante), ou parce que Riemann, génie en avance sur son temps, en était lui-même convaincu.

LE SALUT PAR LA PHYSIQUE ?

Une observation surprenante a donné un élan récent aux recherches. Des estimations statistiques sur de nombreux zéros non triviaux de la fonction *zêta* révèlent des motifs analogues à ceux des valeurs propres de matrices aléatoires qui sont étudiées en physique mathématique (les matrices sont des tableaux de nombres utilisés pour représenter des applications linéaires, et les «valeurs propres» sont des nombres qui les caractérisent).

Ces constatations rejoignent certaines idées de Hilbert et du mathématicien d'origine hongroise George Pólya, émises dans les années 1930. Des idées qui ont déjà porté beaucoup de fruits : le Norvégien Atle Selberg a ainsi trouvé vers 1950 des «formules de traces» qui présentent une

BIBLIOGRAPHIE

R. TAZZIOLI, *Riemann, le géomètre de la Nature*, Belin-Pour la Science, 2010.

M. BALAZARD, Un siècle et demi de recherches sur l'hypothèse de Riemann, *Gazette des mathématiciens*, vol. 126, pp. 7-24, 2010.

P. BORWEIN, *The Riemann Hypothesis: A ressource for the afficionado and virtuoso alike*, Springer, 2008.

LA FONCTION GAMMA

On définit d'abord pour tous les nombres complexes s de partie réelle positive la fonction $\Gamma(s)$ par l'intégrale :

$$\Gamma(s) = \int_0^{\infty} u^{s-1}\exp(-u)d$$

Des théorèmes classiques du calcul intégral donnent :

$$\Gamma(1) = \int_0^{\infty} \exp(-u)du =$$

et, par intégration par parties, l'équation fonctionnelle $\Gamma(s+1)=s\,\Gamma(s)$ pour tout s de partie réelle positive. On obtient ainsi $\Gamma(2)=1\times\Gamma(1)=1$, $\Gamma(3)=2\times\Gamma(2)=2$ et, en général, $\Gamma(n+1)=n\times\Gamma(n)=n!$ pour tout entier positif n. L'équation fonctionnelle s'écrit aussi $\Gamma(s)=\Gamma(s+1)/s$. On peut en déduire une valeur de la fonction Gamma pour les nombres de partie réelle comprise entre –1 et 0 à partir des valeurs connues, et donc lui donner un sens. Pour le point $s=0$, on devrait diviser par 0 et donc la fonction Γ n'est pas définie en 0. Le procédé peut être étendu et l'on parvient à définir la fonction Γ pour tous les nombres complexes s à l'exception des entiers négatifs. En ces entiers, la fonction Γ a des singularités, elle prend une valeur infinie.

grande ressemblance avec la formule de Riemann pour la fonction $\pi(x)$ et qui permettent de prouver un analogue de la conjecture de Riemann pour une autre sorte de fonctions *zêta*. Mais en ce qui concerne l'hypothèse de Riemann elle-même, ce type de tentatives n'avait jusqu'à présent fourni aucun résultat.

Depuis 2000, sur la base d'une idée de Jon Keating et Nina Snaith, de l'université de Bristol, on utilise des matrices aléatoires pour modéliser la fonction *zêta* sur la droite critique. En se fondant sur l'analogie entre ces objets complètement différents, les mathématiciens formulent des conjectures qui, espère-t-on, fourniront d'autres pistes pour apporter une réponse définitive à la conjecture de Riemann.

Une autre tentative un peu plus facile à saisir fait appel à une étonnante propriété d'approximation de la fonction *zêta*. En 1975, le mathématicien russe Serguei Voronin prouva que la fonction *zêta* peut approcher aussi précisément qu'on le veut n'importe quelle fonction (suffisamment régulière) sur un petit domaine. C'est le célèbre théorème d'universalité de Voronin. Explicitons un peu ce résultat spectaculaire.

Soit une fonction $f(s)$ définie sur un petit disque K, situé n'importe où dans la moitié droite de la bande critique. Supposons que f n'ait aucun zéro dans K et qu'elle y soit analytique (développable en série de puissances entières). Alors pour tout $\epsilon>0$, aussi petit soit-il, il existe un nombre réel $t>0$ tel que la différence entre $\zeta(s+it)$ et $f(s)$ soit inférieure à ϵ en valeur absolue, et ce pour tout s de K. En d'autres termes, on peut trouver t tel que $\zeta(s+it)$ soit aussi proche que l'on veut de $f(s)$.

UNE PORTE VERS L'UNIVERSALITÉ

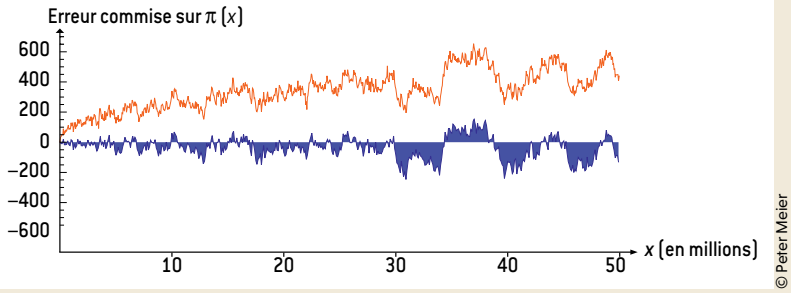
On montre même qu'il existe une infinité de nombres t vérifiant cette approximation pour une fonction f et un nombre ϵ donnés. En quelque sorte, la fonction *zêta* contient donc dans ses valeurs des informations sur toutes ces fonctions f. Un peu comme s'il s'agissait d'un atlas contenant toutes les cartes possibles… C'est pourquoi on résume le théorème d'universalité de Voronin en disant : « Qui connaît la fonction *zêta* connaît le monde. »

Cette propriété d'universalité fournit en retour des renseignements sur la fonction *zêta* elle-même. Si en effet la conjecture de Riemann est correcte, c'est-à-dire que tous les zéros non triviaux de $\zeta(s)$ se trouvent sur la droite critique, on peut appliquer le théorème d'universalité à $\zeta(s)$ et il en résulte que la fonction *zêta* s'approxime elle-même – on en déduit qu'elle est autosimilaire, comme le sont les fractales (figures géométriques qui, quel que soit le grossissement choisi, gardent le même aspect). Réciproquement, si on prouvait que la fonction *zêta* est autosimilaire, la validité de la conjecture de Riemann en découlerait.

LA FORMULE DE RIEMANN POUR $\pi(x)$

$$\pi(x)+\sum_{n=2}^{\infty}\frac{1}{n}\,\pi\left(x^{\frac{1}{n}}\right)=\mathrm{li}(x)-\sum_{\rho}\left(\mathrm{li}(x^{\rho})+\mathrm{li}(x^{1-\rho})\right)+\int_{x}^{\infty}\frac{du}{u(u^2-1)\ln u}-\ln 2$$

Cette formule relative au nombre $\pi(x)$ de nombres premiers inférieurs à x est valable pour tout $x \geqslant 2$ qui n'est pas une puissance d'un nombre premier p (dans ce cas particulier, on doit ajouter à gauche $1/(2k)$ pour la contribution de $x=p^k$). La somme dans le membre de droite est à effectuer sur tous les zéros ρ non triviaux de la fonction *zêta* ayant une partie imaginaire positive. La somme dans le membre de gauche est en réalité finie, car dès que la n-ième racine de x est inférieure à 2, le n-ième terme est nul (ainsi que les termes suivants).
Si l'on veut vraiment calculer $\pi(x)$ à l'aide de cette formule (avec un ordinateur), on doit remplacer les deux sommes par des sommes partielles ne contenant qu'un nombre fini de termes. Or même lorsqu'on ne prend en compte que les 10 premières valeurs de n et les 30 premiers zéros de la fonction *zêta*, on obtient une excellente approximation de $\pi(x)$ *(voir le graphique ci-dessous)*. L'écart entre cette approximation et la valeur exacte *(en bleu)* est à peine supérieur à 200, même autour de $x=50$ millions. En revanche, l'approximation donnée par la formule de Gauss *(en rouge)* devient de plus en plus mauvaise à mesure que x augmente.



© Peter Meier

Le mathématicien danois Harald Bohr (frère du physicien Niels Bohr) est à l'origine de cette observation, dans les années 1920. Mais, faute du théorème d'universalité, il n'avait pu en donner une preuve. Celle-ci a été fournie par le mathématicien indien Bhaskar Bagchi au début des années 1980.

Beaucoup d'autres reformulations de la conjecture de Riemann sont aujourd'hui connues, mais une preuve semble pourtant toujours aussi éloignée. Bien sûr, si la conjecture était fausse, il suffirait de trouver un seul contre-exemple. Les mathématiciens cherchent aussi dans cette direction. Andrew Odlyzko, à l'université du Minnesota, Herman te Riele, au centre de recherche en informatique d'Amsterdam, et d'autres ont calculé jusqu'à présent plus de 100 milliards de zéros de la fonction *zêta* : ils se trouvent tous sur la droite critique $\mathrm{Re}(s)=1/2$.

Mais ces vérifications numériques ne constituent pas une preuve de l'hypothèse de Riemann. Face à l'infinité des nombres, ce à quoi le raisonnement humain et l'ordinateur peuvent accéder n'est qu'une minuscule goutte dans l'immensité de l'océan. Le million de dollars attend toujours son destinataire, mais cette somme ne représentera pas grand-chose comparée à la satisfaction d'avoir résolu le problème. ■

L'ESSENTIEL

- Comment déterminer les nombres premiers ? Depuis l'Antiquité, plusieurs formules ont été proposées pour les calculer.
- Certaines sont élégantes, d'autres plus complexes, mais elles ont souvent pour défaut de ne donner que quelques nombres premiers.
- D'autres encore donnent une infinité (théorique) de nombres premiers, mais les valeurs qu'ils prennent croissent trop vite.
- On peut néanmoins s'en inspirer pour faire mieux, notamment en ajustant très finement les paramètres des formules.

L'AUTEUR

SIMON PLOUFFE
professeur à l'IUT Informatique de Nantes, coauteur de l'Encyclopédie en ligne des suites de nombres entiers (OEIS).

Un record pour les nombres premiers

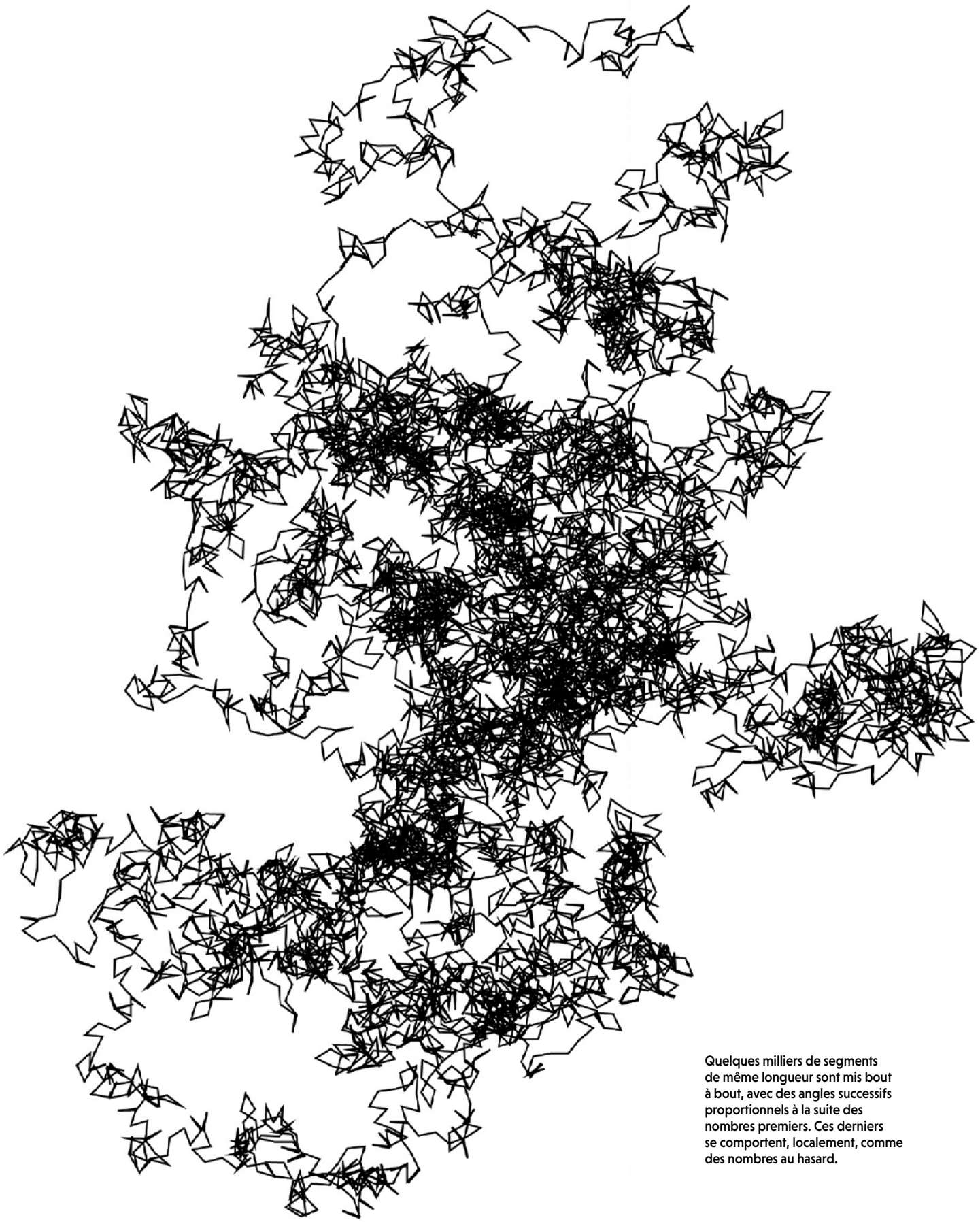
Depuis des millénaires, les mathématiciens conçoivent des formules pour calculer des nombres premiers. En janvier 2019, une formule élaborée par l'auteur a généré une séquence de 100 nombres premiers. C'est un record ! Explications.

Le 7 décembre 2018, un record été battu, celui du plus grand nombre premier connu. $2^{82\,589\,933} - 1$, qui comporte près de 25 millions de chiffres en écriture décimale. On doit cette performance (la vérification est en cours) au *Gimps*, le *Great Internet Mersenne Prime Search*. Ce projet fondé par George Woltman réunit des volontaires mettant à disposition leur ordinateur pour un calcul, distribué, des nombres premiers dits de Mersenne (*voir l'encadré page 79*), c'est-à-dire de la forme $2^p - 1$, p étant un nombre premier. On disposerait donc d'une formule pour déterminer les nombres premiers ?

UNE FORMULE, MAIS LAQUELLE ?

Ce n'est pas aussi simple, notamment parce que tous les nombres premiers ne sont pas de la forme de Mersenne, tant s'en faut. La question se pose donc toujours : y a-t-il une formule pour les nombres premiers ? La réponse est… oui et non.

Et d'abord qu'entend-on par formule ? Par exemple, ce peut être une formule dite close comme celle trouvée par le Suisse Leonhard Euler en 1772 : $p(n) = n^2 + n + 41$. Pour n entre 0 >



Quelques milliers de segments de même longueur sont mis bout à bout, avec des angles successifs proportionnels à la suite des nombres premiers. Ces derniers se comportent, localement, comme des nombres au hasard.

$$\frac{n^6}{72} - \frac{5n^5}{24} - \frac{1493n^4}{72} + \frac{1027n^3}{8} + \frac{100471n^2}{18} - \frac{11971n}{6} - 57347$$

> et 39, elle délivre 40 nombres premiers d'affilée: 41, 43, 47, 53, 61, 71, 83, 97, 113, 131, 151, 173, 197, 223, 251, 281, 313, 347, 383, 421, 461, 503, 547, 593, 641, 691, 743, 797, 853, 911, 971, 1033, 1097, 1163, 1231, 1301, 1373, 1447, 1523 et 1601. De plus, la formule est élégante et simple, mais elle a ses limites. Pour $n = 40$, on trouve 1681... qui est 41^2.

En 2010, François Dress et Bernard Landreau en ont trouvé une meilleure, mais plus compliquée (*voir ci-dessus*). Avec ce polynôme, on obtient des nombres premiers pour n compris entre −42 et 15. La recherche de ce polynôme a tout de même demandé six mois d'efforts avec une batterie d'ordinateurs.

Est-ce donc si difficile de produire une formule qui donnerait quantité de nombres premiers? La question a été close une bonne fois pour toutes en 1947, quand William Mills a publié une formule qui peut donner un nombre arbitraire de nombres premiers. Si A = 1,306377883 8630806904686144926... alors $\lfloor A^{3^n} \rfloor$ donne une suite arbitraire de nombres tous premiers. Ici $\lfloor x \rfloor$ indique que l'on prend la partie entière du nombre x. La suite débute ainsi: 2, 11, 1361, 2521008887... Cependant, les valeurs augmentent très vite, le 8e terme a déjà 762 chiffres, et le 20e environ six milliards!

En 1951, le Britannique Edward Wright en proposait une autre, si $g_0 = \alpha = 1{,}9287800...$ et $g_{n+1} = 2^{g_n}$ alors $\lfloor g_{n+1} \rfloor = \lfloor 2^{...2^{2^\alpha}} \rfloor$ est toujours premier. Les nombres premiers consécutifs sont uniquement représentés par α. La suite obtenue est 3, 13, 16381... le 4e terme a plus de 4932 chiffres et personne n'a osé calculer le 5e...

Ainsi, ces deux suites produisent bien une infinité de nombres premiers, mais le taux de croissance décourage les plus téméraires. Peut-on élaborer des formules fournissant une suite de nombres premiers de longueur arbitraire, mais avec un taux de croissance raisonnable?

Par tous les moyens, on cherche à calculer les nombres premiers, avec une fortune diverse.

Auteur(s)	Année	Commentaire	Efficacité	Nombres calculés
Ératosthène	−276 à −194	Crible d'exclusion	Pratique	Infini calculable
Mersenne	1536	Nombres premiers de la forme 2^p-1.	Pratique, exact	51
Fermat	1640	Petit théorème de Fermat	Produit des premiers probables faibles	Infini calculable
Euler	1772	Polynôme du second degré	Pratique	40
Mills	1947	Double exponentielle	Pratique	Moins de 10
Wright	1951	Super exponentielle	Pratique	Moins de 5
Wilson	vers 1780	Formule qui utilise p!	Théorique	Très peu
Jones, Sato, Wada et Wiens	1976	Polynôme de degré 25 à 26	Théorique	Très peu
John H. Conway	1987	Fractran	Théorique	Très peu
Rowland	2008	Récurrence	Théorique	Très peu
F. Dress et B. Landreau	2010	Polynôme de degré 6	Pratique	58
Benoît Perichon *et al.*	2010	26 premiers en progression arithmétique	Pratique	26
Tomás Oliveira e Silva *et al.*	2019	Programme Primesieve: crible d'Ératosthène optimisé	Le plus rapide connu	Infini calculable sur un ordinateur actuel

LE TABLEAU DE CHASSE

Le «tableau de chasse» ci-contre récapitule des formules et des procédés pour les nombres premiers. L'infini calculable mentionné signifie que le calcul ou procédé peut se dérouler jusqu'à ce que les ressources s'épuisent. Par exemple, le programme Primesieve est le plus rapide. Il peut produire tous les nombres premiers jusqu'à 1000 milliards en 52 minutes sur un ordinateur moyen. Dans sa version courante, la liste peut aller jusqu'à 2^{64}, soit $1{,}844 \times 10^{19}$, mais les nombres réclament 4,1 exaoctets d'espace pour être stockés... Ce programme est fondé sur le crible d'Ératosthène, du nom d'un mathématicien grec du IIIe siècle avant notre ère. Cet algorithme procède par élimination: on supprime parmi les nombres de 2 à N tous les multiples d'un entier de sorte qu'à la fin il ne reste que les nombres premiers.

L'infini calculable du crible d'Ératosthène, à l'époque de son inventeur, était d'un autre ordre, et relevait plus du calcul manuel. La même chose s'applique pour le petit théorème de Fermat selon lequel si p est un nombre premier et si a est un entier non divisible par p, alors $a^{p-1} - 1$ est un multiple de p. Les nombres premiers produits par ce théorème sont probables et faibles. Si p est très grand, il constitue néanmoins un test probabiliste pratique de la primalité d'un nombre candidat.

Quant aux nombres de Mersenne (de la forme $2^p - 1$), ils sont limités par la taille de p. Pour tester un seul exposant dans la liste des candidats, un voire deux mois de calcul intensif sur

LES NOMBRES DE MERSENNE

Marin Mersenne (1588-1648), ou *Marinus Mersenius*, appartenait à l'ordre religieux des Minimes. Érudit, philosophe et mathématicien, il a défini les nombres qui portent son nom. Ils sont de la forme $2^p - 1$. Certains parmi eux sont des nombres premiers. Pour ce faire, p oit lui-même être un nombre premier, cette condition étant nécessaire, mais pas suffisante. Les premiers nombres de Mersenne premiers sont 3 (2^2-1), 7 (2^3-1), 31 (2^5-1), 127 (2^7-1)... Mersenne a calculé (avec quelques erreurs) de tels nombres premiers jusqu'à l'exposant 257. Depuis, c'est la course au plus grand nombre de Mersenne premier, le dernier en date étant pour p = 82 589 933. Avec ses 24 862 048 chiffres, le nombre obtenu est aussi le plus grand nombre premier connu.

Marin Mersenne, un religieux à la culture encyclopédique.

un ordinateur puissant sont nécessaires. Pour cette raison, le *Gimps* distribue les calculs. On peut faire mieux!

Pour ce faire, une première approche consiste à construire une suite basée sur la représentation en base 10 avec, par exemple, $a_{n+1}=10a_n$, et $a_0=7{,}3327334517988679$. On obtient 7, 73, 733, 7333, 73327, 733273... une suite certes de nombres premiers, mais qui s'arrête vite, faute de termes de cette forme qui soient plus grands. C'est l'une des quelques suites connues et la plus étendue. Une autre base bien supérieure à 10, mais de taille fixe, sera forcément prise en défaut, notamment à cause de l'écart entre les nombres premiers qui croît rapidement.

Avec une fonction qui croît plus rapidement, comme n^n on obtient de meilleurs résultats, par exemple avec c=0,265588372943143390897129 45366546... et $a_n = \lfloor cn^n \rfloor$. Elle s'arrête au bout de 19 termes, ici de a_3 à a_{22}. C'est la meilleure qui a été trouvée. Les premiers nombres premiers a_n sont: 7, 67, 829, 12391, 218723, 4455833, 102894377, 2655883729... Et le dernier: 155172317999186449760617 2809.

Encore une fois, et pour les mêmes raisons, le procédé cesse de fonctionner au bout d'un moment. La méthode (*voir l'encadré page suivante*) est fondée sur un programme personnel.

Dans la seconde approche, on considère des formules du type de Mills, celle de Wright étant écartée, car elle croît trop vite. Le problème devient alors de trouver une fonction qui croit suffisamment lentement pour produire une suite de premiers de longueur arbitraire.

Prenons la suite $a_{n+1} = a_n^2 - a_n + 1$, dite de Sylvester (A000058 dans le catalogue OEIS, l'encyclopédie en ligne des suites de nombres entiers). Cette suite commence ainsi, avec a_0=2: a_n = 2, 3, 7, 43, 1807, 3263443, 10650056950807... Tous ne sont pas des nombres premiers ($1807=13\times139$), mais étonnamment, la somme des inverses de ces termes 1/2+1/3 + 1/7+1/43+ 1/1807+1/3263443... est égal à 1. On peut ensuite se demander si l'on peut trouver un a_0 non plus entier, mais réel, qui produise des nombres premiers. Il suffirait d'utiliser la fonction «partie entière» $\lfloor x \rfloor$. La réponse est oui.

Avec a_0=1,6181418093242092, a_n=2, 3, 7, 43, 1811, 3277913, 10744710357637... La croissance est bien inférieure à celle de la formule de Mills et *a fortiori* à celle de Wright. Chaque terme a environ deux fois la taille du précédent, ce qui conduit tout de même à $a_{14} = 9{,}838... \times 10^{1667}$.

Peut-on choisir l'exposant dans la formule précédente de sorte que la croissance soit encore plus lente? Oui, grâce au recuit simulé, on trouve assez rapidement ceci: si a_0=43,80468771580293481... et en utilisant l'arrondi de x noté $\{x\}$, on obtient $S_n=\{a_n\}$ et $a_{n+1}=a_n^{5/4}$. C'est maintenant la suite A323176 du catalogue OEIS: S_n=113, 367, 1607, 10177, 102217...

Cela semble fonctionner! Faisons mieux avec un exposant plus petit et un a_0 choisi soigneusement. Par exemple, si $a_{n+1}= a_n^{11/10}$ et a_0=100000000000000000000000000000049,3 1221074776345... on obtient la suite ci-dessous:

100 000 000 000 000 000 000 000 000 000 049
158 489 319 246 111 348 520 210 137 339 236 753
524 807 460 249 772 597 364 312 157 022 725 894 401
3 908 408 957 924 020 300 919 472 370 957 356 345 933 709
70 990 461 585 528 724 931 289 825 118 059 422 005 340 095 813
3 438 111 840 350 699 188 044 461 057 631 015 443 312 900 908 952 333
48 972 469 000 420 009 426 555 707 142 502 303 667 155 036 417 8496 540 501... >

BIBLIOGRAPHIE

D. FRIDMAN *ET AL.*, A prime-representing constant, *The American Mathematical Monthly*, vol. 126, pp. 70-73, 2019.

Le plus grand nombre premier connu: http://bit.ly/82589933

Le site de Simon Plouffe: http://plouffe.fr

L'OEIS: https://oeis.org/

2
3
5
11
37
223
3 331
192 271
84 308 429
774 116 799 347
681 098 209 317 971 743
562 101 323 304 225 290 104 514 179
13 326 678 220 145 859 782 825 116 625 722 145 759 009
1 538 448 162 271 607 869 601 834 587 431 948 506 238 982 765 193 425 993 274 489

Avec un exposant égal à 3/2 et a_0=2,038239154782... on obtient la suite de nombres premiers ci-dessus.

C'est désormais la suite A323611. Un autre exemple livre les petits nombres premiers. Avec a_0=3,34683553593243081... et un exposant égal à 1,251295195638... la suite (A323065) est: 3, 5, 7, 11, 19, 41, 103, 331, 1423, 8819, 86477, 1504949...

En choisissant a_0 assez grand, on peut utiliser un exposant très petit, comme 101/100. Si a_0=10^{500}+961,4993763378507... on obtient une suite de 100 nombres premiers, le dernier n'ayant que 1340 chiffres. Elle bat ainsi les records de 2010 (58 nombres premiers avec un polynôme et 26 avec une progression arithmétique). Notons néanmoins que lorsque leur taille dépasse 20 chiffres, les nombres obtenus que sont que des premiers probables. Si a_0 est bien choisi, on conjecture que l'exposant peut être aussi près de 1 qu'on le souhaite (pour limiter la croissance).

OBTENIR TOUS LES NOMBRES PREMIERS ?

Avec des formules de ce type, peut-on obtenir tous les nombres premiers? Pour y parvenir, on pourrait par exemple partir d'un nombre premier arbitraire et descendre jusqu'à 2. C'est possible avec un procédé inverse en utilisant 1/α, α étant l'exposant. Ainsi, en partant du nombre premier 10^{100}+267 et avec α =0,38562256415290... on obtient 742123524365563, 542489, 163, 7, 2.

On retrouve la suite inverse en partant à 2 avec a_0=2,1322219996628413452... et l'exposant 1/α=2,5932092490404286167308... Le principe fonctionne dans les deux sens!

Tous ces calculs décrits sont empiriques. En pratique, on arrive à générer un nombre arbitraire de nombres premiers avec une croissance minimale de la suite. Les formules sont bien plus économes que celles Mills et Wright. À partir d'un nombre premier donné, on peut descendre jusqu'à 2 et à partir de 2 on peut obtenir une famille de suites infinies de nombres premiers.

Les records sont faits pour être battus, et avec un matériel informatique adéquat, et un certain temps de calcul, la suite de 100 nombres premiers peut être étendue jusqu'à 1000000 de chiffres. Mieux, lorsque l'exposant est 3/2, on conjecture que tous les nombres premiers peuvent être générés. Reste à le démontrer... ■

UN PROGRAMME MAISON

L'algorithme mis au point procède en trois étapes. D'abord, on choisit la valeur de départ a_0 et l'exposant α, préférablement une fraction simple. Puis on lance un algorithme qui associe la technique de Monte-Carlo (fondée sur des processus aléatoires) et le principe du recuit simulé. Ce principe est inspiré de la métallurgie où l'on alterne les cycles de refroidissement lent et de réchauffage (recuit) afin de minimiser l'énergie d'un matériau. Cette technique évite que l'écart entre chaque nombre premier ne croisse trop vite. Une fois quatre ou cinq valeurs trouvées, on passe à l'étape 3. On utilise une formule qui permet d'aller soit vers l'avant soit vers l'arrière. Vers l'avant, on cherche le plus petit nombre premier après $\{a_p^{\alpha}\}$. C'est assez facile en quelques minutes, même s'il a des milliers de chiffres, grâce à des logiciels, comme Maple ou PFGW. On rebrousse chemin pour vérifier que la formule fonctionne. Pour ce faire, on doit résoudre pour x avec x^{α}- S_{n+1}. Ici S_{n+1} est le prochain nombre premier candidat. C'est ici qu'un α rationnel facilite le calcul.

Des nombres et des énigmes

La suite des énigmes concoctées par Ana Retchman et Sébastien Kernivinen.

La fin page 105. Solutions page 106.


Ana Retchman


Sébastien Kernivinen

ÉNIGME 5

Trouver tous les entiers strictement positifs x et y tels que $6 \times (x! + 3) = y^2 + 5$ (ou $x!$ désigne le produit $1 \times 2 \times 3 \ldots \times x$).

ÉNIGME 6

Trouvez les chiffres a et b de sorte que le nombre à cinq chiffres $32a1b$, soit divisible par 156.

ÉNIGME 7

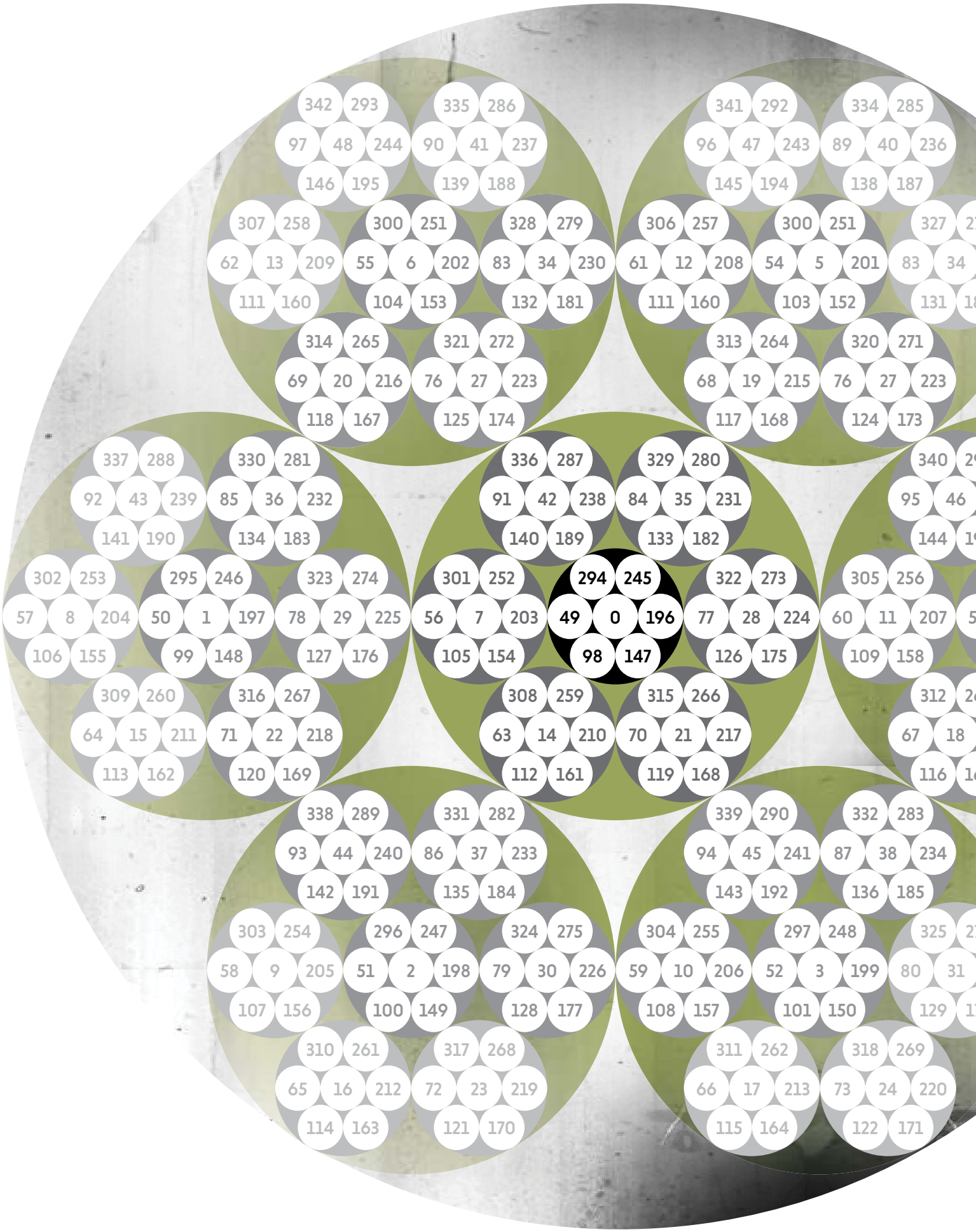
Quel est le plus grand nombre qu'on puisse obtenir en multipliant des nombres entiers positifs dont la somme vaut 8 ?

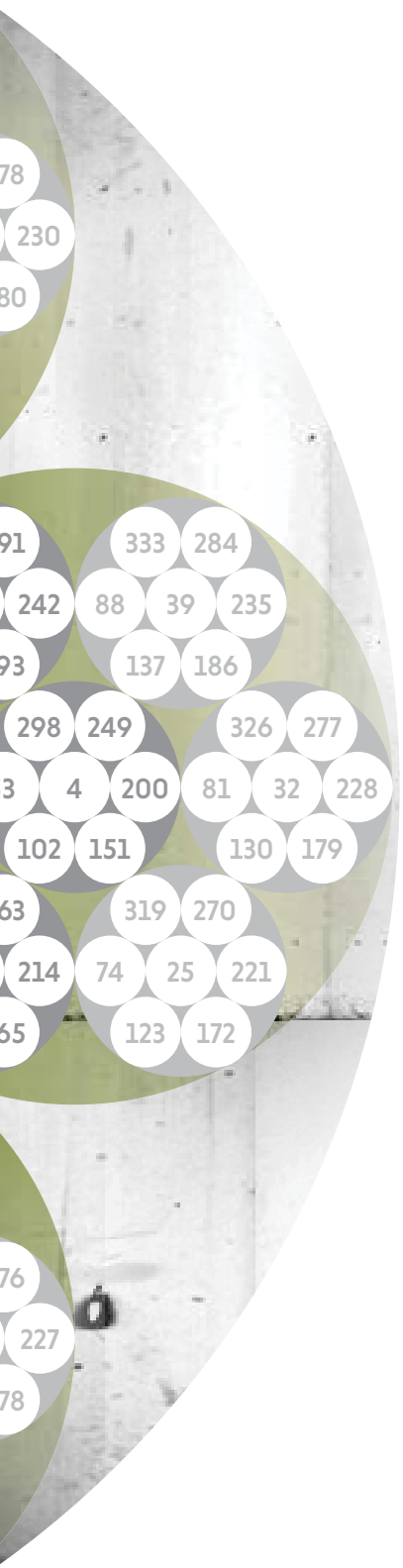
ÉNIGME 8

Si douze nombres strictement positifs $a_1 \leq a_2 \leq \ldots a_{12}$ sont tels que, dès qu'on en choisit trois quelconques parmi eux, on ne peut pas construire de triangle (non plat) dont les côtés aient pour longueurs ces trois nombres, quelle est la plus petite valeur possible de $\frac{a_{12}}{a_1}$?

ÉNIGME 9

La somme de deux nombres entiers positifs vaut 125. Si on multiplie le premier par 4 et qu'on divise le second par 4, on obtient la même somme. Quels sont les deux nombres initiaux ?


342 293 335 286
97 48 244 90 41 237
146 195 139 188
307 258 300 251 328 279
62 13 209 55 6 202 83 34 230
111 160 104 153 132 181
314 265 321 272
69 20 216 76 27 223
118 167 125 174
341 292 334 285
96 47 243 89 40 236
145 194 138 187
306 257 300 251 327
61 12 208 54 5 201 83 34
111 160 103 152 131
313 264 320 271
68 19 215 76 27 223
117 168 124 173
337 288 330 281
92 43 239 85 36 232
141 190 134 183
302 253 295 246 323 274
57 8 204 50 1 197 78 29 225
106 155 99 148 127 176
309 260 316 267
64 15 211 71 22 218
113 162 120 169
336 287 329 280
91 42 238 84 35 231
140 189 133 182
301 252 294 245 322 273
56 7 203 49 0 196 77 28 224
105 154 98 147 126 175
308 259 315 266
63 14 210 70 21 217
112 161 119 168
340
95 46
144
305 256
60 11 207
109 158
312
67 18
116
338 289 331 282
93 44 240 86 37 233
142 191 135 184
303 254 296 247 324 275
58 9 205 51 2 198 79 30 226
107 156 100 149 128 177
310 261 317 268
65 16 212 72 23 219
114 163 121 170
339 290 332 283
94 45 241 87 38 234
143 192 136 185
304 255 297 248 325
59 10 206 52 3 199 80 31
108 157 101 150 129
311 262 318 269
66 17 213 73 24 220
115 164 122 171



© Patrick Cœuru

DES HOMMES ET DES NOMBRES

Parmi les résultats les plus importants obtenus en mathématiques ces dernières années, beaucoup concernent la théorie des nombres. Et derrière ces exploits se cachent des mathématiciens aux tempéraments variés, aux approches différentes… Mais tous ont en commun d'avoir pris à bras-le-corps des problèmes ardus et de les avoir explorés de façon nouvelle. Avec à la clé, pour ces hommes de nombres, les récompenses les plus prestigieuses, comme la médaille Fields ou le prix Abel.

Les nombres 7-adiques (ici, les $7 \times 7 \times 7 = 343$ premiers) sont arrangés de façon fractale révélant leur proximité (cette notion prend un sens différent ce celui qu'on lui connaît habituellement). Dans le disque noir central, on distingue les multiples de $7 \times 7 = 49$, puis dans les disques autour les entiers de la forme $n \times 7 \times 7 + 7$, $n \times 7 \times 7 + 14$…

Peter Scholze, avec sa médaille Fields qu'il vient de recevoir.

L'ESSENTIEL

- Peter Sholze, mathématicien allemand d'à peine 30 ans, a reçu la médaille Fields en 2018.
- Il a été récompensé notamment pour les espaces perfectoïdes, des objets mathématiques construits à partir des nombres *p*-adiques, une extension abstraite des nombres naturels arithmétiques.
- Ces espaces permettent de transposer des problèmes complexes dans des domaines où l'arithmétique est bien plus simple.

L'AUTEURE

ERICA KLARREICH
docteure en mathématiques de l'université Stony Brook, dans l'État de New York, elle contribue régulièrement au magazine *Quanta*.

L'oracle de l'arithmétique

Peter Scholze fut l'un des quatre lauréats de la médaille Fields en 2018, la plus prestigieuse récompense en mathématiques. Avec le concept de perfectoïde, il a mis au jour des liens profonds entre la théorie des nombres et la géométrie.

Quanta magazine

Cet article a d'abord été publié en anglais par *Quanta Magazine*, une publication en ligne indépendante soutenue par la *Simons Foundation* afin de favoriser la diffusion des sciences : http://bit.ly/QM-Scholze

En 2010, une rumeur étonnante circule au sein de la communauté des théoriciens des nombres. Un étudiant de l'université de Bonn, en Allemagne, aurait publié un article qui redémontrait une conjecture impénétrable en théorie des nombres en seulement 37 pages, là où les deux mathématiciens Michael Harris et Richard Taylor avaient eu besoin de 288 pages. À 22 ans, Peter Scholze, l'étudiant en question, avait réussi à contourner l'une des parties les plus compliquées de la démonstration, celle ayant trait à une connexion générale entre la théorie des nombres et la géométrie.

UNE LEÇON D'HUMILITÉ

« C'était incroyable qu'un résultat aussi révolutionnaire vienne de quelqu'un d'aussi jeune, s'enflamme Jared Weinstein, théoricien des nombres à l'université de Boston, âgé de 38 ans. Ce fut une sacrée leçon d'humilité ! »

À l'université de Bonn, qui proposa à Peter Scholze un poste de professeur à peine deux ans plus tard, les mathématiciens avaient déjà perçu ses extraordinaires capacités. Après son article sur les travaux de Harris et Taylor, c'est l'ensemble des experts en théorie des nombres et en géométrie qui en fut convaincu.

Depuis, Peter Scholze s'est fait un nom dans la communauté des mathématiciens tout entière. Certains disent déjà de lui qu'il est « un des mathématiciens les plus influents du monde » et « un talent rare qui n'émerge que toutes les quelques décennies ». De fait, il a reçu en août 2018 la médaille Fields, la plus prestigieuse récompense en mathématiques, décernée tous les quatre ans lors du Congrès international des mathématiciens.

L'innovation majeure de Peter Scholze – une classe de structures fractales qu'il appelle les espaces perfectoïdes – n'a que quelques années d'existence, mais elle a déjà de vastes ramifications en géométrie arithmétique, un domaine où la théorie des nombres et la géométrie se rejoignent. « Dans ses travaux, Peter Scholze fait preuve de "prescience", admire Jared Weinstein : il peut voir les développements avant même qu'ils ne se produisent. » >

Face aux découvertes de Peter Scholze, beaucoup de mathématiciens réagissent avec «un mélange d'admiration, de peur et d'euphorie», explique Bhargav Bhatt, de l'université du Michigan. Sa personnalité n'est pas en cause, car il est unanimement reconnu comme quelqu'un de généreux. «Il ne vous prend jamais de haut», confie Eugen Hellmann, à l'université de Bonn.

Le plus déconcertant est sa vision en profondeur de la nature des phénomènes mathématiques. Contrairement à la plupart de ses confrères, il commence rarement à réfléchir à un problème particulier. Il privilégie plutôt des concepts insaisissables qu'il veut comprendre pour ce qu'ils sont. «Mais ensuite, raconte Ana Caraiani, à l'université de Princeton, les structures qu'il crée s'avèrent avoir des applications dans une multitude de directions qui n'avaient pas été anticipées, simplement parce qu'elles étaient le bon objet auquel il fallait réfléchir.»

APPRENDRE L'ARITHMÉTIQUE

Peter Scholze a commencé à apprendre seul les mathématiques de niveau universitaire à l'âge de 14 ans, alors qu'il était au lycée Heinrich-Hertz, à Berlin. Dans cet établissement, «vous n'étiez pas vu comme un marginal si vous vous intéressiez aux mathématiques», confie-t-il.

BIBLIOGRAPHIE

P. SCHOLZE, Perfectoid spaces, *Publications mathématiques de l'IHÉS*, vol. 116, pp. 245-313, 2012.

J.-M. FONTAINE, Perfectoïdes, presque pureté et monodromie-poids (d'après Peter Scholze), «Séminaire Bourbaki, 64e année 2011/2012», exposés 1043-1058, vol. 352, *Société mathématique de France*, 2013.

B. BHATT, What is a perfectoid space ?, *Notices AMS*, vol. 61(9), octobre 2014.

À 16 ans, il apprend que dix ans plus tôt, en 1995, Andrew Wiles avait prouvé le fameux dernier théorème de Fermat, selon lequel l'équation $x^n+y^n=z^n$ n'a pas de solution entière non nulle si n est supérieur à 2 (*voir L'hypothèse qui valait un million, par P. Meier, page 68*). Peter Scholze se rue sur la preuve, sauf qu'elle fait appel aux mathématiques les plus compliquées. «Je n'y comprenais rien, mais c'était fascinant», dit-il.

Alors il fait marche arrière, essayant de déterminer ce qu'il devait apprendre pour comprendre la preuve de Wiles. «C'est plus ou moins comme ça que j'ai appris jusqu'ici», détaille-t-il. «En fait, je n'ai jamais vraiment appris les choses basiques comme l'algèbre linéaire. Je les ai seulement assimilées en m'intéressant à d'autres notions.»

À mesure qu'il étudiait la preuve de Wiles, Peter Scholze se passionna pour les objets mathématiques utilisés – les formes modulaires et les courbes elliptiques, qui réunissent des domaines disparates de la théorie des nombres, de l'algèbre, de la géométrie et de l'analyse. Comprendre les objets mathématiques en jeu était plus intéressant que le problème lui-même.

Aujourd'hui encore, Peter Scholze travaille sur des problèmes ancrés dans des équations simples impliquant des nombres entiers. De là, même les structures mathématiques les plus ésotériques qui en découlent restent concrètes à ses yeux. «Je m'intéresse surtout à l'arithmétique», explique-t-il. Il se dit très heureux lorsque ses constructions abstraites le conduisent à de petites découvertes sur les nombres entiers.

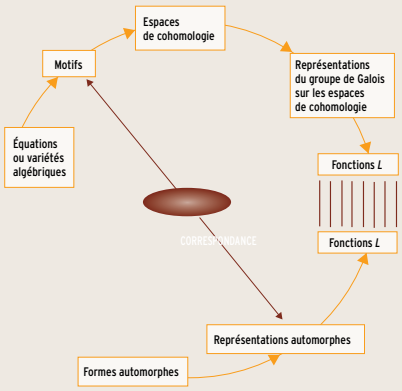
À l'université, Peter Scholze persévère dans la théorie des nombres et la géométrie. Là, son camarade de classe, Eugen Hellmann, se souvient que pendant les cours de mathématiques, Peter ne prenait jamais de notes. Il comprenait le contenu du cours en temps réel. «Mais pas seulement en surface; il comprenait en profondeur, si bien qu'il n'oubliait rien.»

Peter Scholze a commencé ses recherches en géométrie arithmétique, où des outils de géométrie aident à approcher les solutions entières d'équations polynomiales (par exemple, $xy^2+3y=5$), qui n'impliquent que des nombres entiers, des variables et des exposants.

Pour certaines équations de ce type, il est utile de déterminer si elles ont des solutions dans des ensembles de nombres alternatifs dits p-adiques qui, comme les réels, sont construits en «remplissant les intervalles» entre les entiers et les fractions (*voir l'encadré page 88*). Mais ces corps de nombres sont fondés sur des notions non standard d'intervalles et de proximité. Dans un système p-adique, deux nombres sont proches, non pas si leur différence est petite, mais si elle est divisible de nombreuses fois par p (p étant un nombre premier). C'est étrange, mais utile ! Ainsi, les nombres 3-adiques offrent un moyen naturel d'étudier

LE PROGRAMME DE LANGLANDS

Une part substantielle des recherches menées ces dernières décennies en théorie des nombres et en géométrie algébrique s'est déroulée sous l'impulsion d'un tissu de conjectures, dont Robert Langlands, de l'Institut des études avancées, à Princeton, aux États-Unis, avait formulé certaines dans une longue lettre adressée à André Weil en 1967. Cet ensemble de conjectures, les unes précises, les autres un peu floues, est surnommé aujourd'hui «programme (ou correspondance) de Langlands». Il dresse des ponts entre la théorie des nombres et d'autres parties des mathématiques, notamment la théorie des représentations des groupes et la théorie de certaines fonctions nommées formes automorphes. Il a été fructueux, dans la mesure où plusieurs résultats importants ont été démontrés au fil des ans : la démonstration du théorème de Fermat, en 1994, en est l'un de ces résultats les plus marquants. Pour autant, l'exploration et la démonstration de cette «correspondance» sont loin d'être achevées : elles représentent toujours, pour les mathématiciens, un défi à relever.



Le programme de Langlands relie deux grands édifices, l'un construit à partir des équations ou variétés algébriques, l'autre à partir de fonctions modulaires ou automorphes. Il conjecture une correspondance entre motifs et représentations automorphes, deux ensembles d'objets auxquels on sait associer des «fonctions L», fonctions qui contiennent des informations de nature arithmétique.

des équations comme $x^2=3y^2$, pour lesquelles les multiples de 3 sont la clé.

Les nombres *p*-adiques vont «bien au-delà de ce que notre sens commun nous permet de concevoir», explique Peter Scholze. Avec les années, ils lui sont finalement devenus naturels. «Désormais, je trouve les nombres réels bien plus perturbants que les *p*-adiques!»

Les mathématiciens avaient remarqué dans les années 1970 que beaucoup de problèmes concernant les nombres *p*-adiques deviennent plus simples si on étend le corps des nombres *p*-adiques en ajoutant successivement les racines *p*-ièmes de *p*, créant ainsi une «tour infinie» de nombres, où chacun englobe les précédents, avec les nombres *p*-adiques à la base. Au «sommet» de cette tour infinie se trouve un objet fractal qui est l'exemple le plus simple des espaces perfectoïdes que Peter Scholze a développé par la suite.

Il s'est fixé l'objectif de comprendre pourquoi cette construction enveloppante infinie facilite tant les problèmes mettant en jeu des nombres *p*-adiques et des équations polynomiales. «J'essayais de comprendre le cœur de ce phénomène», explique-t-il. «Il n'existe aucun formalisme général qui peut expliquer cela.»

Il s'est finalement rendu compte qu'il est possible de construire des espaces perfectoïdes pour une grande variété de structures mathématiques, et notamment pour les corps de nombres *p*-adiques et les corps de polynômes. Il a montré que ces espaces permettent de transposer des problèmes liés aux équations polynomiales avec les nombres *p*-adiques dans des structures basées sur des polynômes, où l'arithmétique est bien plus simple (par exemple, lors d'une addition, les retenues ne sont pas nécessaires). «La propriété la plus étrange des espaces perfectoïdes est leur capacité à se transposer comme par magie entre les deux systèmes», explique Jared Weinstein.

Avec cette idée, Peter Scholze a prouvé un cas particulier d'une conjecture complexe à propos des solutions *p*-adiques aux équations polynomiales, émise par le mathématicien Pierre Deligne et appelée la conjecture monodromie-poids, qui a fait l'objet de sa thèse en 2012. Elle «avait des implications si vastes qu'elle est devenue un sujet de groupes d'études à travers le monde», selon Jared Weinstein.

Pour Eugen Hellmann, «Peter Scholze a trouvé précisément le moyen le plus propre et le plus correct d'intégrer tous les travaux précédents avec une formulation élégante, et par conséquent le moyen d'aller bien plus loin que les résultats déjà connus».

Malgré la complexité des espaces perfectoïdes, Peter Scholze est connu pour la clarté de ses discours et de ses publications. «Je ne comprends vraiment tout cela que lorsque Peter me l'explique», confie Jared Weinstein.

JE N'AI JAMAIS VRAIMENT APPRIS LES CHOSES BASIQUES. JE LES AI ASSIMILÉES EN M'INTÉRESSANT À D'AUTRES NOTIONS

Pour Ana Caraiani, Peter Scholze met un point d'honneur à essayer d'expliquer ses idées à un niveau d'étudiant de second cycle. «Il a cette attitude d'ouverture et de générosité lorsqu'il s'agit de parler de ses idées», explique-t-elle. «Et il ne le fait pas qu'avec quelques séniors. Il est vraiment très accessible pour beaucoup de jeunes.» Cette attitude fait de lui un chef de file idéal pour le domaine, selon Ana Caraiani. Une fois, alors qu'elle participait à une randonnée difficile avec lui et un groupe de mathématiciens, «il était celui qui allait et venait en s'assurant que tous les autres allaient bien et arrivaient à suivre», raconte-t-elle.

AU-DESSUS DE LA JUNGLE

Pourtant, même avec les explications de Peter Scholze, les espaces perfectoïdes sont difficiles à appréhender pour beaucoup. Selon Eugen Hellmann, «si vous vous éloignez un petit peu du chemin, vous vous retrouvez au milieu d'une jungle de notions où il est très difficile de se repérer. Peter, en revanche, ne s'y perd jamais. Il n'essaie pas de se frayer un chemin, il est plutôt à la recherche d'une vue globale de l'ensemble, d'un concept plus clair.»

Peter Scholze évite le chaos luxuriant de la jungle de l'arithmétique en la survolant. À l'université, il préférait travailler sans rien écrire. Ce qui signifie qu'il devait formuler ses idées le plus clairement possible. «Nos capacités cérébrales sont d'une certaine façon limitées, donc on ne peut pas faire de choses trop compliquées», explique Scholze.

Alors que d'autres mathématiciens commencent à s'approprier les espaces perfectoïdes, certaines des découvertes les plus fondamentales à leur sujet viennent, sans surprise, de Peter Scholze et de ses collaborateurs. En 2013, un résultat publié en ligne «a stupéfié la communauté», d'après Jared Weinstein. «Nous n'imaginions pas qu'un tel théorème soit envisageable.»

Le résultat de Scholze a étendu la portée des relations qu'on appelle lois de réciprocité. Elles gouvernent le comportement d'équations polynomiales qui font appel à l'arithmétique modulaire. Cette arithmétique (dont une illustration simple est le compte «modulo 12» des heures sur une horloge, où 8 heures + 5 heures = 1 heure, par exemple) est le système de nombres finis le plus naturel et le plus étudié.

Les lois de réciprocité sont une généralisation de la loi de réciprocité quadratique, une pierre angulaire de la théorie des nombres démontrée par Gauss en 1801 et l'un des théorèmes préférés de Peter Scholze. La loi de réciprocité quadratique stipule que lorsqu'on a deux nombres premiers *p* et *q*, dans la plupart des cas, *p* est un carré >

modulo q si q est un carré modulo p sur une horloge ayant p heures. Par exemple, 5 est un carré parfait modulo 11, puisque $5=16=4^2$ et 11 est un carré modulo 5, puisque $11=1=1^2$.

«Je trouve cela très surprenant», confie Peter Scholze. «À première vue, ces deux choses n'ont rien en commun.» «Vous pouvez interpréter beaucoup de théories algébriques modernes comme de simples tentatives de généraliser cette loi», explique Jared Weinstein.

Au milieu du XX^{e} siècle, les mathématiciens ont découvert un lien étonnant entre les lois de réciprocité et ce qui avait l'air d'être un sujet totalement différent: la géométrie hyperbolique (un exemple de modèle d'espace hyperbolique est le pavage «Anges et démons», d'Escher). Ce lien fait partie intégrante du programme de Langlands (*voir l'encadré page 86*), une série de conjectures et de théorèmes interconnectés portant sur les relations entre la théorie des nombres, la géométrie et l'analyse. Quand ces conjectures sont prouvées, elles se révèlent souvent extrêmement puissantes. Par exemple, la preuve du dernier théorème de Fermat a consisté à résoudre une petite – mais loin d'être triviale – partie du programme Langlands.

Les mathématiciens ont progressivement pris conscience que ce programme s'étend bien au-delà du cas du disque hyperbolique: il peut aussi être étudié dans des espaces hyperboliques de dimension supérieure et d'autres contextes variés. Peter Scholze a montré comment

L'ÉTRANGE MONDE *P*-ADIQUE

Notre manière habituelle (décimale) d'écrire des nombres consiste à les représenter comme une somme de puissances de dix avec des facteurs (des coefficients) compris entre 0 et 9. Ainsi, 347 est une forme abrégée de $3\times10^2+4\times10^1+7\times10^0$.

En fait, on peut identifier tout nombre réel avec la suite de ses chiffres: $a_n a_{n-1}\ldots a_1 a_0, a_{-1} a_{-2} a_{-3}\ldots$ est essentiellement identique à: $a_n\times10^n+a_{n-1}\times10^{n-1}\ldots a_1\times10+a_0+a_{-1}\times10^{-1}+a_{-2}\times10^{-2}+a_{-3}\times10^{-3}\ldots$ les chiffres a_j étant compris entre 0 et 9. Dans ce contexte, les séquences à l'infini de chiffres 0,999... et 1,000... représentent le même nombre.

De manière générale, en mathématiques, une suite est un ensemble de quantités, par exemple de nombres, dont les éléments sont pourvus de numéros (des indices): a_n désigne l'élément de rang n d'une suite, du coefficient de 10^n dans l'exemple précédent.

Habituellement, les indices vont de 1 à l'infini: a_1, a_2, $a_3\ldots$ C'est différent avec les nombres réels qui peuvent nécessiter une infinité de coefficients à indice négatif. Par exemple, $\pi=3{,}14159$ s'écrit: $3\times10^0+1\times10^{-1}+4\times10^{-2}+1\times10^{-3}+5\times10^{-4}+9\times10^{-5}\ldots$ où $a_0=3$, $a_{-1}=1$, $a_{-2}=4$, $a_{-3}=1$, $a_{-4}=5$, $a_{-5}=9\ldots$

Le fait que la base soit 10 n'a aucune signification mathématique. Dans ce qui suit, il sera même plus intéressant de choisir pour base un nombre premier p. Un nombre réel écrit en base p est donc une suite de chiffres entre 0 et p-1, qui peut en contenir un nombre infini d'éléments d'indice négatif (après la virgule), mais seulement un nombre fini d'indice positif. Peut-on imaginer l'inverse? Quels seraient les nombres obtenus en autorisant une infinité de termes à gauche de la virgule, mais seulement un nombre fini de termes à sa droite? Ces nombres sont dits p-adiques. Leur comportement déconcerte et réclame du temps pour s'y s'habituer. Et contrairement aux nombres réels, ils sont complètement inadaptés pour décrire les processus naturels. Néanmoins, on peut calculer avec eux presque comme on a l'habitude de le faire depuis l'école primaire. Ainsi, pour les nombres 5-adiques, comme pour les nombres habituels en base 5, on a $4+1=10$. Cependant, on a aussi ... $4444+1=0$, car il y a une retenue à chaque addition, qui se propage à l'infini vers la gauche. La division doit également être effectuée dans l'ordre inverse de celui de la méthode scolaire.

Les nombres p-adiques forment un corps, c'est-à-dire un ensemble où les quatre opérations arithmétiques de base peuvent être effectuées sans restriction – sauf la division par zéro. On désigne ce corps par le symbole $\mathbb{Q}_p$.

Quand dit-on de deux nombres réels qu'ils sont proches? Lorsque leur différence a un zéro avant la virgule et beaucoup de zéros après. La question est plus complexe avec deux nombres p-adiques: ils sont proches quand leur différence a beaucoup de zéros avant la virgule (et seulement des zéros derrière) ou, ce qui revient au même, est divisible par une puissance élevée de p. Le fait qu'il existe encore une infinité de chiffres plus à gauche est sans importance. Avec cette définition de la proximité, on peut définir des suites de nombres p-adiques ainsi que leurs limites. Toutefois, on ne peut pas ordonner les nombres p-adiques sur une ligne aussi facilement que les nombres réels.

Le calcul de puissances, définies par multiplication répétée d'un nombre, compte parmi les opérations qui sont toujours possibles dans un corps. Ce n'est pas le cas des racines. Parmi les nombres réels, il n'existe pas de x ayant la propriété $x^2=-1$. Les mathématiciens remédient à ce défaut en ajoutant, quasiment par décret, un nouveau nombre appelé i, dont ils ne demandent rien d'autre que la propriété $i^2=-1$ (ils «ajoutent au corps des nombres réels une racine de -1»). Ainsi, ils construisent à partir des nombres réels les nombres complexes

Un procédé similaire est possible avec les nombres p-adiques. On ajoute de préférence au corps $\mathbb{Q}_p$ une racine p-ième de p. Cependant, contrairement au cas des nombres complexes, ceci ne résout pas une fois pour toutes le problème du calcul de racines. Il s'avère nécessaire d'ajouter également la p-ième racine de la p-ième racine, la p-ième racine de ce nombre, et ainsi de suite. Cela conduit à l'extension de corps infinie de $\mathbb{Q}_p$, la «tour infinie» évoquée dans le texte principal.

Le corps $\mathbb{Q}_p$ des nombres p-adiques a une autre propriété remarquable: on peut pourvoir ses éléments (des suites de chiffres entre 0 et $p-1$, dont une infinité a un indice positif, mais seulement un nombre fini à indice négatif sont non nuls) de nouvelles règles de calcul, ce qui conduit à un corps complètement différent.

Ces nouvelles règles de calcul viennent de la théorie de l'analyse complexe (la théorie des fonctions). On y étudie de préférence des fonctions représentables par des séries entières, c'est-à-dire des sommes infinies de la forme $f(z)=a_0+a_1z+a_2z^2+a_3z^3\ldots$

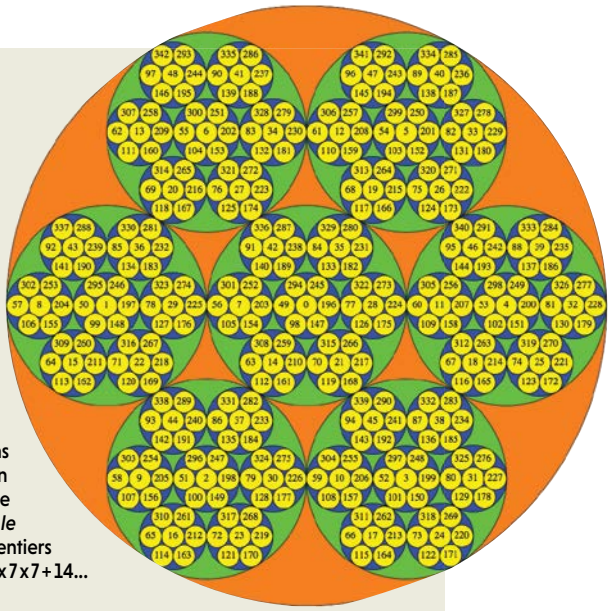
Si l'on ne veut pas exclure des fonctions telles que $1/z$ ou $2/z^3+3z^2$, on doit étendre les sommes à des «séries de Laurent», où des coefficients d'indice négatif peuvent apparaître. Pour $1/z$, on a alors $a_{-1}=1$, et pour $2/z^3+3z^2$, $a_{-3}=2$ et $a_2=$.

l'étendre à une grande variété de structures dans les espaces hyperboliques de dimension 3 (des espaces de courbure négative généralisant le disque hyperbolique) et au-delà. En construisant le perfectoïde d'un espace hyperbolique de dimension 3, Scholze a découvert une série complètement nouvelle de lois de réciprocités.

« Les travaux de Peter ont complètement transformé ce qui est possible, et ce à quoi nous avons accès », explique Ana Caraiani. Pour Jared Weinstein, les résultats de Peter Scholze montrent que le programme Langlands est « bien plus profond que ce que nous pensions... il est plus systématique et partout présent. »

Discuter de mathématiques avec Peter Scholze, c'est comme consulter un « oracle de la vérité », selon Jared Weinstein. « S'il dit que quelque chose va marcher, vous pouvez être confiant. S'il dit non, vous devriez abandonner tout de suite; et s'il ne sait pas – ce qui peut arriver –, vous êtes chanceux, car alors, vous avez entre les mains un problème très intéressant. »

Pourtant, collaborer avec lui n'est pas une expérience aussi intense qu'on pourrait le croire, explique Ana Caraiani. Quand elle travaillait avec lui, il n'y avait jamais de précipitation. « J'avais le sentiment qu'on faisait toujours ce qu'il fallait de la bonne façon – nous prouvions les théorèmes les plus généraux possible, le mieux possible, grâce à des constructions qui permettraient d'éclairer les choses. »



Les nombres 7-adiques (ici, les 7 x 7 x 7 = 343 premiers) sont arrangés de façon fractale révélant leur proximité (une notion qui a ici un sens différent de celui qu'on lui prête d'habitude). Dans le disque bleu central, on distingue les multiples de 7 x 7 = 49, entourés (*dans le disque vert central*) des entiers de la forme $n \times 7 \times 7 + 7$, $n \times 7 \times 7 + 14$...

Les fonctions de cette classe (dites méromorphes) sont complètement décrites par la suite de leurs coefficients a_{-n}, $a_{-(n-1)}$... a_{-1}, a_0, a_1, a_2...
L'addition et la multiplication de telles fonctions peuvent s'exprimer par l'intermédiaire de ces coefficients. En principe, ces coefficients sont des nombres complexes, mais rien n'empêche d'utiliser à leur place des nombres d'un autre corps. Dans le cas qui nous intéresse, le corps s'appelle $\mathbb{F}_p$: il comprend les nombres 0, 1... $p-1$, avec lesquels on calcule « modulo p », c'est-à-dire que l'on commence par les ajouter ou les multiplier de la façon habituelle, puis on prend le reste de leur division euclidienne par p. Les questions de convergence et de différentiabilité, qui jouent un rôle central en analyse complexe, sont devenues sans objet lors du passage vers le corps fini $\mathbb{F}_p$, voire même plus du tout formulables. Mais par les « séries de Laurent formelles sur $\mathbb{F}_p$ », on obtient une nouvelle structure de corps pour le même ensemble, qui formait déjà le corps $\mathbb{Q}_p$.
En interprétant le même objet d'une part comme un élément de l'un des corps, et d'autre part comme un élément de l'autre corps, on aboutit à des résultats de très grande portée. C'est de cette astuce que le concept d'espace perfectoïde développé par Peter Scholze tire toute sa puissance.

CHRISTOPHE PÖPPE (*SPEKTRUM DER WISSENSCHAFT*), TRADUIT PAR NILS BERGLUND, DE L'INSTITUT DENIS-POISSON, À L'UNIVERSITÉ D'ORLÉANS

MATHS ET PATERNITÉ

Toutefois, en une occasion, Peter Scholze a effectivement travaillé dans la précipitation: en 2013, il essayait de finir un article à temps avant la naissance de sa fille. Pour lui, c'est une bonne chose qu'il se soit dépêché. « Je n'ai pas fait grand-chose après. » Devenir père l'a poussé à se discipliner dans la gestion de son temps, explique-t-il. Mais il n'a pas de problème pour trouver du temps dévolu à la recherche – les mathématiques remplissent simplement tous les moments libres entre ses autres obligations. « Les mathématiques sont ma passion. J'y pense sans cesse. »

Pour autant, il ne souhaite pas tellement s'étendre sur cette passion. Quand on lui demande s'il était fait pour devenir mathématicien, il dément: « C'est une idée bien trop philosophique. » Plutôt secret, il n'est pas très à l'aise avec sa célébrité. En 2016, il est devenu le plus jeune lauréat du prix Leibniz, la plus haute distinction scientifique en Allemagne, qui s'accompagne d'une bourse de recherche de 2,5 millions d'euros pour les sciences expérimentales, et 900000 euros pour les théoriciens. « Parfois, c'est un peu accablant », confie-t-il.

Peter Scholze continue d'explorer les espaces perfectoïdes, mais il s'est aussi ouvert à d'autres domaines des mathématiques et touche à la topologie algébrique, qui utilise l'algèbre pour étudier la forme des objets. « L'année dernière, Peter est devenu maître du sujet. Il a changé la façon dont les experts l'abordent », explique Bhargav Bhatt.

Selon lui, quand Peter Scholze s'intéresse à leur domaine, cela peut être effrayant, mais aussi excitant pour les autres mathématiciens. « Cela signifie que le sujet va avancer rapidement. Je suis très enthousiaste à l'idée qu'il travaille sur un domaine proche du mien, puisque je peux assister au recul des frontières de nos connaissances. »

Toutefois, pour Peter Scholze, ces travaux jusqu'à maintenant ne sont qu'un échauffement. « Je suis encore dans une phase où j'essaie d'apprendre ce qui existe, en le reformulant à ma manière », se confie-t-il. « Je n'ai pas le sentiment d'avoir vraiment commencé mes recherches. » ■

L'ESSENTIEL

- L'Indo-Australien Akshay Venkatesh a reçu en 2018 une médaille Fields.
- Malgré un passé brillant, il ne s'est épanoui dans la recherche en mathématiques que tardivement.
- Il s'est illustré dans l'étude de la subconvexité, un problème lié aux généralisations de la fonction *zêta* de Riemann, en inventant des méthodes radicalement nouvelles.
- Il explore aujourd'hui des liens nichés au cœur du programme de Langlands, qui relie théorie des nombres, géométrie et analyse.

L'AUTEURE

ERICA KLARREICH
docteure en mathématiques de l'université Stony Brook, dans l'État de New York. Elle contribue régulièrement au magazine *Quanta*.

Un mathématicien bâtisseur de ponts

Akshay Venkatesh, lauréat en 2018 de la médaille Fields, n'aime rien tant que se perdre dans des contrées mathématiques inexplorées, peu balisées, en quête de liens cachés entre différents domaines. Et il en trouve !

Quanta magazine

Cet article a d'abord été publié en anglais par *Quanta Magazine*, une publication en ligne indépendante soutenue par la *Simons Foundation* afin de favoriser la diffusion des sciences : http://bit.ly/QM-Venka

Par un après-midi de mai, sur l'aire de jeu du campus de l'Institut d'études avancées, à Princeton, aux États-Unis, le mathématicien Akshay Venkatesh poussait sa petite fille de 4 ans sur la balançoire (son autre fille, 7 ans, se promenait avec ses amis) tout en méditant sur le mythe du génie.

« Ce stéréotype ne rend pas service à la discipline, explique-t-il. Je pense qu'il ne reflète pas les diverses façons par lesquelles on peut contribuer aux mathématiques. »

Venant de l'université Stanford, en Californie, à l'autre bout des États-Unis, Akshay Venkatesh a séjourné pendant un an à Princeton, en tant que professeur visiteur. Depuis août 2018, il y est devenu permanent, ajoutant son nom à une longue liste de résidents prestigieux : Albert Einstein, Kurt Gödel et quelques titulaires de la médaille Fields.

Coïncidence. Akshay Venkatesh s'est vu décerner cette médaille, la plus haute distinction en mathématiques. Il est honoré pour ses « contributions majeures à un éventail exceptionnellement vaste de sujets en mathématiques » et