

POUR LA

édition française de Scientific American

SCIENCE

HORS-SERIE

+
14

ENIGMES
DIFFICILES
À RÉSOUDRE !



CRYPTO
LES DERNIERS
RÉSULTATS
FABULEUX

RÉCOMPENSES
LES MATHS DES
MÉDAILLES
FIELDS

SIMON PLOUFFE
DES NOMBRES
PREMIERS ET
DES RECORDS

NOMBRES STAR
LES SURPRISES
DU NOMBRE
D'OR ET DE PI

GRAND
TÉMOIN
ÉTIENNE
GHYS

L'ORDRE CACHÉ DES NOMBRES

Un champ mathématique en pleine effervescence



M 0130 - 101 - 7,90 € - RD
N° 103 MAI-JUIN 2015

Apprenez les mathématiques par les jeux !

NOUVEAUTE

Apprendre les mathématiques par les jeux. Cette idée vous paraît farfelue ? Détrompez-vous : les jeux ont de tout temps contribué à la création et au développement des mathématiques et de l'informatique.

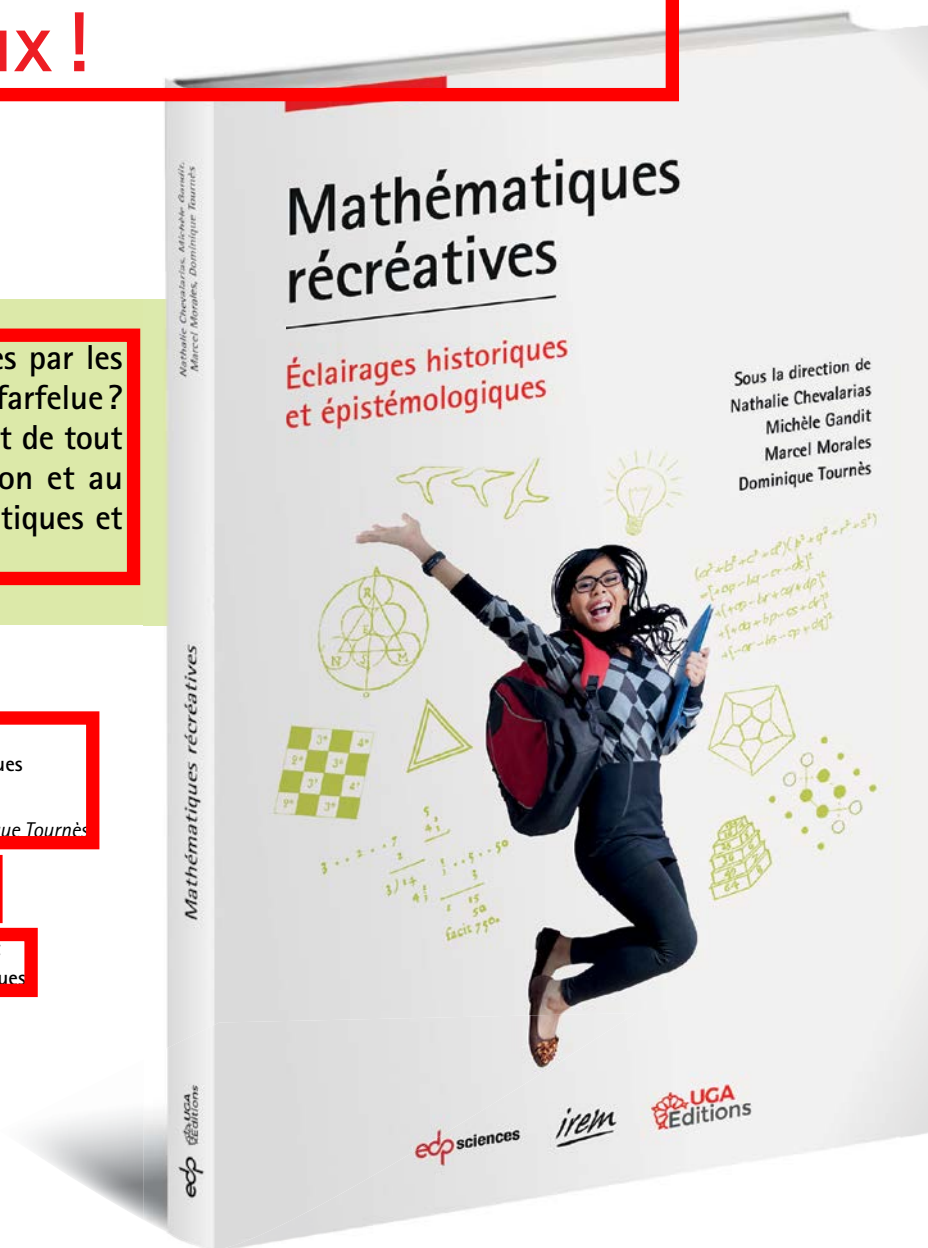
Mathématiques récréatives

Éclairages historiques et épistémologiques

*Sous la direction de Nathalie Chevalarias,
Michèle Gandit, Marcel Morales, Dominique Tournès*

SBN : 978-2-7598-2318-5 – Prix : 25 €
Format : 16 x 24 cm – 256 pages

Public : enseignants du second degré et de l'université, curieux des mathématiques



À PARAÎTRE

L'apprentissage de la critique

Laurence Viennot & Nicolas Décamp

Lisez ce livre si vous voulez (mieux) savoir à quoi vous en tenir sur les explications de phénomènes physiques qui vous sont livrées.

SBN : 978-2-7598-2355-0 – Prix : 25 €

COLLECTION
Enseigner les sciences

EN VENTE EN LIBRAIRIE ET SUR laboutique.edpsciences.fr

www.pourlascience.fr

70 bis boulevard du Montparnasse – 75014 Paris
Tél. 01 55 42 84 00

ÉQUIPE POUR LA SCIENCE

Directrice des rédactions: Cécile Lestienne

HORS-SERIE POUR LA SCIENCE

Rédacteur en chef adjoint: Loïc Mangin

Maquettiste: Patrick Cœurin

POUR LA SCIENCE

Rédacteur en chef: Maurice Mashaal

Rédactrice en chef adjointe: Marie-Neige Cordonnier

Rédacteurs: François Savatier, Sean Bailly

Développement numérique: Philippe Ribeau-Gésippe

Community manager: Aëla Kervhuel

Conception graphique: William Londiche

Directrice artistique: Céline Lapert

Maquette: Pauline Bilbault, Raphaël Queruel,
Patrick Cœurin

Révisseuse: Anne-Rozenn Jouble

Marketing & diffusion: Arthur Peys

Direction du personnel: Olivia Le Prévost

Direction financière: Cécile André

Fabrication: Marianne Sigogne et Olivier Lacam

Directeur de la publication et gérant: Frédéric Mériot

Anciens directeurs de la rédaction: Françoise Pétry et
Philippe Boulanger

Conseiller scientifique: Hervé This

Ont également participé à ce numéro:

Nils Berglund, Jean-François Colonna, Chantal Ducoux,
Sébastien Kernivinen, Philinne Michel et William Rowe-Pirri

PRESSE ET COMMUNICATION

Susan Mackie

susan.mackie@pourlascience.fr • Tél. 01 55 42 85 05

PUBLICITÉ France

stephanie.jullien@pourlascience.fr

ABONNEMENTS

Abonnement en ligne: <http://boutique.pourlascience.fr>

Courriel: pourlascience@abopress.fr

Tél.: 03 67 07 98 17

Adresse postale: Service des abonnements

Pour la Science – 19 rue de l'Industrie – BP 90053

77402 Illkirch Cedex

Tarifs d'abonnement 1 an (16 numéros)

France métropolitaine: 79 euros – Europe: 95 euros

Reste du monde: 114 euros

DIFFUSION

Contact kiosques: À Juste Titres ; Stéphanie Troyard

Tél. 04 88 15 12 48

Information/modification de service/réassort:

www.direct-editeurs.fr

SCIENTIFIC AMERICAN

Editor in chief: Mariette DiChristina

President: Dean Sanderson

Executive Vice President: Michael Flore

Toutes demandes d'autorisation de reproduire, pour le public français ou francophone, les textes, les photos, les dessins ou les documents contenus dans la revue « Pour la Science », dans la revue « Scientific American », dans les livres édités par « Pour la Science » doivent être adressées par écrit à « Pour la Science S.A.R.L. », 62 rue du Faubourg Saint-Denis, 75010 Paris.

« Pour la Science S.A.R.L. » Tous droits de reproduction, de traduction, d'adaptation et de représentation réservés pour tous les pays. La marque et le nom commercial « Scientific American » sont la propriété de Scientific American, Inc. Licence accordée à « Pour la Science S.A.R.L. ». En application de la loi du 11 mars 1957, il est interdit de reproduire intégralement ou partiellement la présente revue sans autorisation de l'éditeur ou du Centre français de l'exploitation du droit de copie (20 rue des Grands-Augustins, 75006 Paris).

Origine du papier: Italie

Taux de fibres recyclées: 0%

Eutrophisation ou « Impact sur l'eau » :

total 0,008 kg/tonne

Le produit est issu de forêts gérées durablement

et de sources contrôlées



ÉDITORIAL



LOÏC MANGIN
Rédacteur
en chef adjoint

Happy *pi*-day!

Le 14 mars dernier, que faisiez-vous? Plus précisément à 1 heure 59? Vous avez oublié? D'autres s'en souviennent parfaitement: ils mangeaient une *pi*-zza, buvaient une *pi*-ñacolada... Tout leur était bon pour fêter la Journée de pi, le célèbre nombre dont les premiers chiffres sont connus de tous. 3,14159... Ce même jour, Google Cloud annonçait qu'une de ses informaticiennes, Emma Haruka Iwao, avait calculé 31415926535897 décimales de π (soit $\pi \times 10^{13}$). Elle battait un record: le précédent, obtenu en 2016, était de $2,2 \times 10^{12}$.

Ainsi, en 2019, un nombre connu depuis plusieurs millénaires continue de faire parler de lui et de mettre le monde en émoi. Cette effervescence illustre le pouvoir de fascination des nombres, π en tête, sur le grand public. Les mathématiciens ne sont pas en reste, eux qui n'en finissent pas de révéler les propriétés insoupçonnées de ce nombre.

C'est même tout l'univers des nombres qu'ils explorent, en quête d'une compréhension intime des lois qui y règnent, à commencer par celle de la répartition des nombres premiers parmi les entiers. Cela passe souvent par la mise au jour de liens avec d'autres domaines, un passage qui semble désormais obligé pour obtenir de beaux résultats, parfois récompensés par les prix les plus prestigieux.

Si vous avez manqué le 14 mars, vous pourrez vous rattraper le 22 juillet, une «journée de π approximatif», car le nombre 22/7 est assez proche de la valeur de π . D'ici là, après la lecture de ce *Hors-Série*, vous en saurez plus sur ce nombre, et les autres.

SOMMAIRE

SCIENCE
HORS-SÉRIE

N° 103

Mai-Juin 2019

L'ordre caché des nombres

UN CHAMP MATHÉMATIQUE
EN PLEINE EFFERVESCENCE

Constituez
votre collection
de *Hors-Séries*
Pour la science
Tous les numéros
depuis 1996

pourlascience.fr



P. 6 Repères

Glossaire, schémas...

Indispensable pour apprécier ce numéro

P. 10 Avant-propos ÉTIENNE GHYS

« Les mathématiques sont
jubilaires quand
des branches indépendantes
se rencontrent pour
en faire une nouvelle »



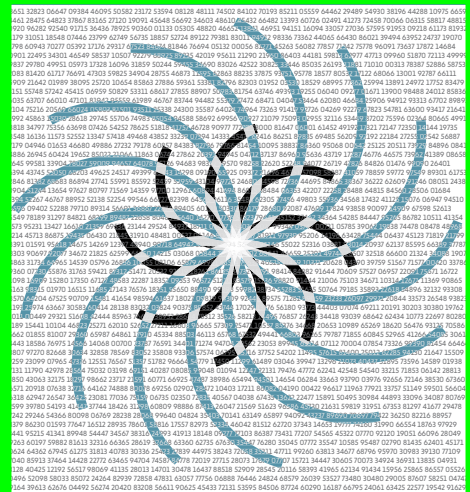
En couverture :
Patrick Cour

+
14

ENIGMES
DIFFICILES
À RÉSOUDRE !

pages 49, 81 et 105

Réponses et solutions
pages 106 et 107



DES NOMBRES D'EXCEPTION

P. 16

Le nombre π est partout

Jean-Paul Delahaye

L'ubiquité de π ne cesse d'étonner. Récemment,
il est apparu là où personne ne l'attendait !

P. 24

Jouons avec les palindromes

Jean-Paul Delahaye

Faciles à identifier, les nombres palindromes
offrent des problèmes de tous niveaux.

P. 30

Élémentaire, mais redoutable

Shalom Eliahou

La conjecture de Syracuse, accessible à tous
dans son énoncé, défie les chercheurs.

P. 38

Des centenaires plein d'avenir

Shalom Eliahou

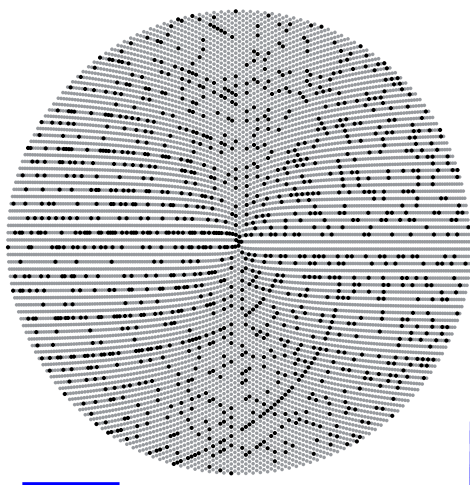
Les nombres de Schur sont si mystérieux que
l'on ne sait encore rien sur eux... ou presque.

P. 44

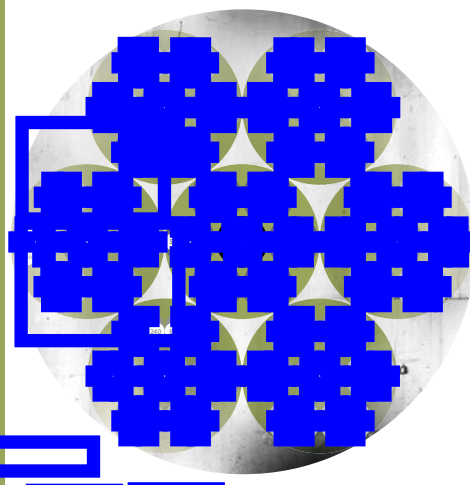
Le nombre d'or fait (encore) parler de lui

Férom Buzzi

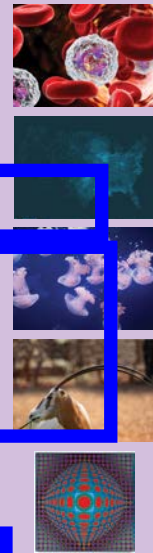
On pensait en avoir fini avec nombre d'or. C'était
sans compter sur ses propriétés de symétrie.



LES PREMIERS DE LA CLASSE



DES HOMMES ET DES NOMBRES



RENDEZ-VOUS sur LOIC MANGU

P. 52

Une nouvelle merveille cryptographique !

Jean-Paul Delahaye

Comment confier des calculs à un tiers sans
lui dévoiler ni les données ni les résultats ?

P. 60

Des jumeaux, des cousins et... des nombres sexy

Bruno Martin

La conjecture des nombres premiers jumeaux
est l'un des problèmes les plus populaires.

P. 68

L'hypothèse qui valait un million

Peter Meier et Jörn Steuding

La clé de la répartition des nombres premiers
résiste aux assauts des mathématiciens.

P. 76

Un record pour les nombres premiers

Simon Plouffe

En 2019, une formule a généré une séquence
de 100 nombres premiers. C'est un record !

P. 84

L'oracle de l'arithmétique

Erica Klarreich

Peter Scholze a mis au jour des liens profonds
entre la théorie des nombres et la géométrie.

P. 90

Un mathématicien bâtisseur de ponts

Erica Klarreich

Akshay Venkatesh traque des liens cachés
entre différents domaines mathématiques

P. 96

Entretien

« Il y a un roman derrière le grand théorème de Fermat »

Cédric Villani

P. 98

Le tombeur de Fermat

Giulio Giorello et Corrado Sinigaglia

L'épopée du théorème de Fermat, démontré
en 1995, fut riche en rebondissements.

P. 108

À lire en plus

P. 110

Rebondissements

Une restauration rapide,
mais dans le désordre •
La musique nuit gravement
à la créativité • Se coller
pour mieux décoller •
Un modèle pour la
dynamique d'Alzheimer •

P. 114

Données à voir

Dù est passé
l'Ananas express ?

P. 116

Les incontournables

Des livres, des expositions,
des sites internet,
des vidéos, des podcasts...
à ne pas manquer.

P. 118

Spécimen

L'oryx, bon sang
mais c'est bien sûr

P. 120

Art & Science

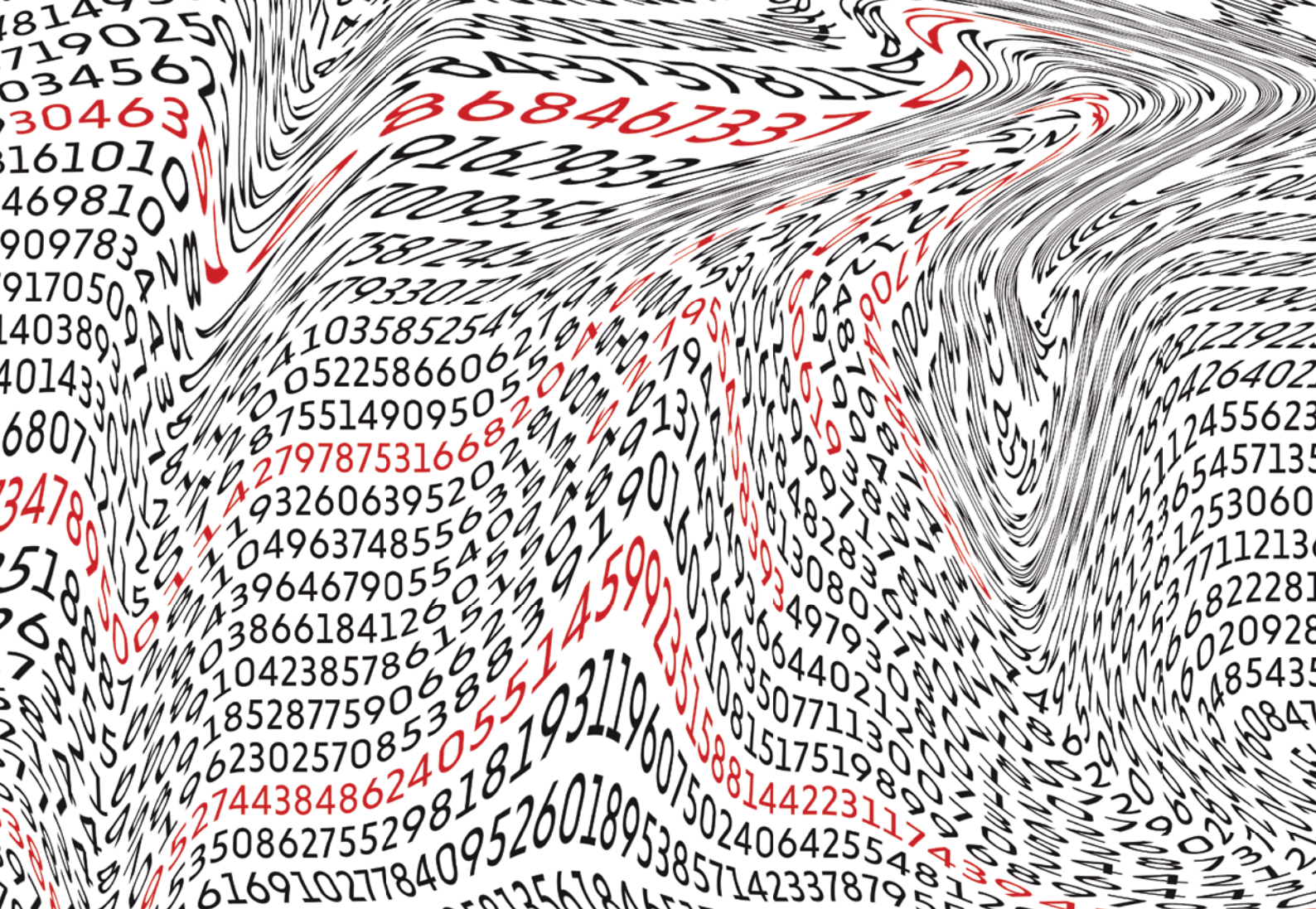
Du petit carré
à l'Univers en entier

[illegible]

Sans nombre, impossible d'évaluer, de comparer, de mesurer, de se localiser, d'ordonner... Le nombre est donc indispensable. Pour pratiquer leur art, et étendre le monde de leurs investigations, les mathématiciens distinguent et même ont créé quantité de types de nombres. Un vrai bestiaire ! Inventaire non exhaustif.

es poupées russes. Les nombres sont réunis dans les ensembles souvent emboîtés, mais pas toujours





CHIFFRE OU NOMBRE ?

Les chiffres sont des signes, des éléments d'écriture, utilisés pour représenter les nombres. Notre système décimal est bâti sur les chiffres indo-arabes (0, 1, 2, 3, 4, 5, 6, 7, 8 et 9). On connaît aussi les chiffres romains : I, V, X, L, C...

SYSTEME DECIMAL

Le système de numération en base 10 est fondé sur les chiffres de 0 à 9 dans une notation dite positionnelle. Dans l'écriture d'un nombre, la position d'un chiffre correspond à une puissance de 10 dont le chiffre lui-même est un coefficient multiplicateur : $263 = 2 \times 10^2 + 6 \times 10^1 + 3 \times 10^0$. En informatique, on rencontre le système binaire, c'est-à-dire en base 2 (seulement les chiffres 0 et 1), et le système hexadécimal avec les 16 « chiffres » : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E et F. Le nombre binaire 1101 est égal en système décimal à $1 \times 2^3 + 1 \times 2^2 + 0 \times 2^1 + 1 \times 2^0$, soit 13. Le nombre hexadécimal 15AACF7 est égal en système décimal à $1 \times 16^6 + 5 \times 16^5 + 10 \times 16^4 + 10 \times 16^3 + 12 \times 16^2 + 15 \times 16^1 + 7 \times 16^0$, soit 22719735.

NOMBRES ENTIERS NATURELS

Des nombres non décimaux (c'est-à-dire sans virgule) et positifs : 10, 159, 32 548 965... L'ensemble des entiers naturels est noté $\mathbb{N}$.

NOMBRES ENTIERS RELATIFS

Toujours sans virgule, ces nombres incluent les entiers naturels (donc positifs) et les entiers négatifs : -15, -4 958, 3, 159... L'ensemble des entiers relatifs est noté $\mathbb{Z}$.

NOMBRES ENTIERS DÉCIMAUX

Les nombres (positifs ou négatifs) incluent les entiers relatifs et ceux qui ont des chiffres après la virgule, mais uniquement une suite finie : $2/5$, $-5/4$, 0,153, $-0,2...$ L'ensemble des entiers décimaux est noté $\mathbb{D}$.

NOMBRES RATIONNELS

Les nombres incluent les précédents, ainsi que tous ceux qui s'expriment sous la forme d'un quotient de deux nombres entiers a et b (b est non nul), sans restriction sur le nombre de chiffres après la virgule : $-2/3$, $22/7...$ Ils auraient été conçus la première fois par les Égyptiens. La suite de nombres après la virgule est toujours périodique. L'ensemble des rationnels est noté $\mathbb{Q}$.

NOMBRES IRRATIONNELS

Les nombres, qui cette fois n'incluent pas les précédents, ne peuvent pas s'écrire sous la forme d'une fraction a/b . Les premiers nombres irrationnels (les racines carrées) auraient été découverts par les Grecs entre le V^e et le IV^e siècle avant notre ère, même si l'on en trouve également la trace dans des documents indiens datés du VIII^e au V^e siècle avant notre ère. On distingue plusieurs types d'irrationnels : les irrationnels constructibles, les nombres algébriques, les nombres transcendants...

IRRATIONNELS CONSTRUCTIBLES

Un nombre irrationnel constructible peut s'obtenir avec une règle et un compas. C'est le cas du nombre $\sqrt{2}$ découvert par les Grecs, ainsi que du **nombre d'or**.

NOMBRES ALGÈBRIQUES

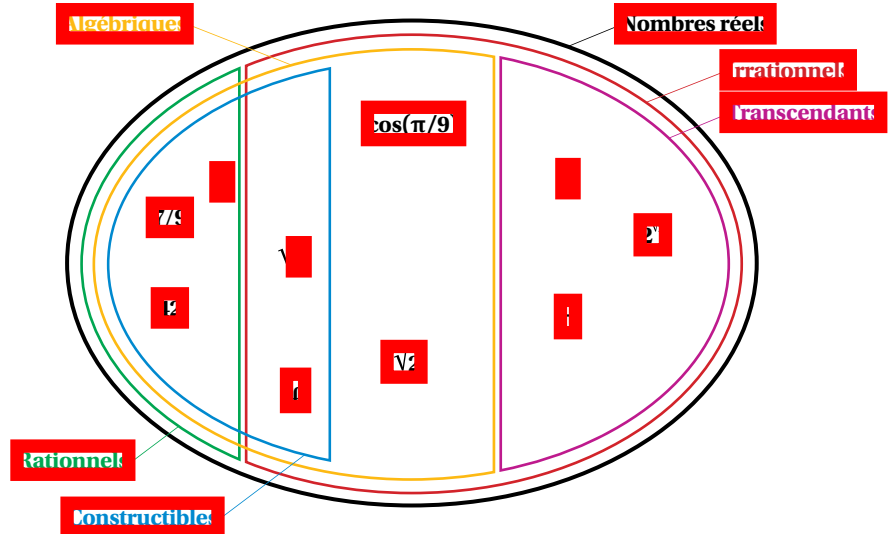
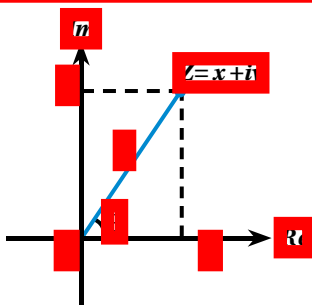
Les nombres, qui incluent les précédents, sont les solutions des équations polynomiales à coefficients rationnels de la forme $a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 = 0$, tous les a_i appartenant à $\mathbb{Q}$. Par exemple, $\sqrt{2}$ (**constructible**) est solution de $x^2 - 2 = 0$. $\sqrt{2}/2$ est aussi algébrique, **irrationnel**, mais non constructible.

NOMBRES TRANSCENDANTS

Les nombres irrationnels ne sont pas solutions d'équations polynomiales à coefficients rationnels. Les plus connus de ces nombres sont π et e . Le nombre de Champernowne 0,12345678910111213... est aussi transcendant. L'existence de tels nombres a été prouvée pour la première fois en 1844 par Joseph Liouville.

NOMBRES COMPLEXES

L'ensemble des nombres complexes est une extension de l'ensemble des **nombres réels**, contenant un nombre imaginaire noté i tel que $i^2 = -1$. Le carré de $(-i)$ est aussi égal à -1 : $(-i)^2 = -1$. Tout nombre complexe z s'écrit sous la forme $x + iy$ où x et y sont des nombres réels et nommés respectivement « partie réelle » (Re) et « partie imaginaire » (Im). On peut représenter les nombres complexes dans un plan dit complexe avec pour abscisse les parties réelles x et en ordonnées les parties imaginaires y . Un nombre complexe $z = x + iy$ s'écrit aussi sous la forme $z = re^{i\theta}$ ou bien $z = r(\cos(\theta) + i\sin(\theta))$ où r est le module de z et θ son argument. Un nombre complexe peut être **algébrique**.



NOMBRES RÉELS

Les nombres englobent l'ensemble des nombres rationnels et irrationnels. Ils peuvent avoir une liste finie ou infinie de décimales. L'ensemble des réels est noté $\mathbb{R}$. En 1874, Georg Cantor démontra que les nombres **algébriques** réels sont dénombrables et les nombres réels sont non dénombrables. Les nombres réels sont des nombres **complexes** dont la partie imaginaire est égale à zéro.

π (PI)

Le nombre π a été initialement défini comme le rapport constant de la circonférence d'un cercle à son diamètre dans un plan euclidien. Sa valeur approchée est 3,141592653... Il est connu depuis l'Antiquité : dès 2000 avant notre ère, les Babyloniens avaient obtenu pour π une valeur de 3,125. L'ubiquité de π en fait l'une des plus importantes constantes en mathématiques. La **transcendance** de π (qui est par définition non constructible) a permis de prouver l'impossibilité de résoudre la quadrature du cercle.

e

Le nombre e (nommé nombre d'Euler ou constante de Néper) est la base des logarithmes népériens (noté $\ln$), c'est-à-dire le nombre défini par $\ln(e) = 1$, ce qui en fait la base de la fonction exponentielle e^x . Euler a défini e comme : $1 + 1/1 + 1/(1 \times 2) + 1/(1 \times 2 \times 3) + 1/(1 \times 2 \times 3 \times 4) \dots$. En 1873, Charles Hermite a montré que le nombre e est **transcendant**.

NOMBRES P-ADIQUES

Les nombres p -adiques ont été inventés par Kurt Hensel en 1897 pour mieux comprendre les nombres habituels. Ils sont définis sur la base d'un nombre premier p . Par construction, ils peuvent avoir un nombre infini de chiffres à gauche de la virgule.

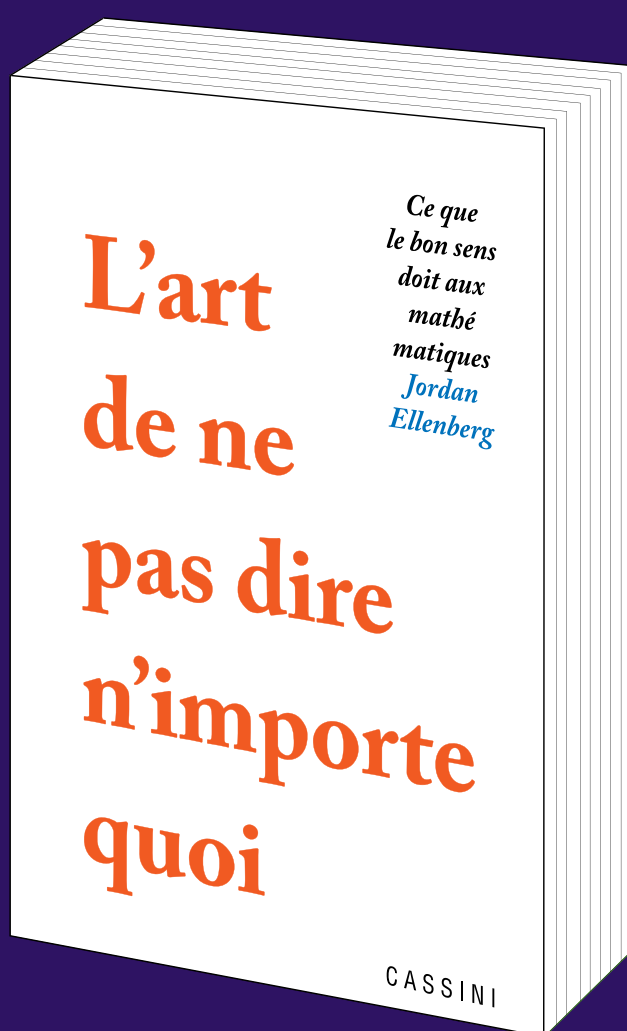
NOMBRES PREMIERS

Un tel nombre est un entier qui n'a que deux diviseurs, 1 et lui-même. Les premiers nombres premiers sont : 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37... Ce sont les nombres élémentaires à partir desquels on peut fabriquer tous les autres entiers (en les additionnant ou en les multipliant). Ils sont utiles en cryptographie, car il est très difficile de trouver les facteurs premiers d'un nombre très grand. Le plus grand nombre premier connu est $2^{77232917} - 1$, qui comporte plus de 23 millions de chiffres en écriture décimale. C'est un nombre de Mersenne, car il est de la forme $2^p - 1$, où p est premier. Beaucoup de conjectures portent sur les nombres premiers.

NOMBRE D'OR (φ)

Le nombre d'or (noté ϕ), aussi nommé section dorée, proportion dorée et divine proportion, a été défini comme l'unique rapport a/b entre deux longueurs a et b telles que $(a+b)/a = a/b$. Ce nombre **irrationnel** est l'unique solution positive de l'équation $x^2 = x + 1$. Il vaut environ 1,618... On le retrouve dans la suite de Fibonacci, les pavages quasi-périodiques. Il était probablement connu dès l'Antiquité, en particulier par les pythagoriciens, et on le retrouve dans les *Éléments* d'Euclide.

Facile, intelligent, drôle, voici un livre que les amoureux des mathématiques dévoreront, et qui apportera une agréable surprise à ceux qui les ont en horreur. Il vous fera mieux comprendre le monde qui vous entoure, et vous aidera, n'en doutez pas, à ne plus dire n'importe quoi.



« Ce livre est une merveille, un des meilleurs livres de vulgarisation des mathématiques. Je ne trouve pas de mots assez forts pour exprimer ma reconnaissance à l'auteur. »

Philippe Boulanger,
Pour la science, avril 2018.

L'art de ne pas dire n'importe quoi a reçu le Prix Tangente 2018.

Jordan Ellenberg

L'art de ne pas dire n'importe quoi

Ce que le bon sens doit aux mathématiques

534 p., 24 €

Retrouvez nos autres publications sur www.cassini.fr



CASSINI

ÉTIENNE
GHYS



« Les mathématiques sont
jubilatoires quand des branches
indépendantes se rencontrent
pour en faire une nouvelle »

Quelle place tient le nombre dans les mathématiques ?

Étienne Ghys : De façon caricaturale, on distingue en général la géométrie d'une part et l'algèbre d'autre part, dédié aux nombres. Ils représenteraient donc la moitié des mathématiques ! À la vérité, les nombres et la géométrie jouent au chat et à la souris depuis plus de trois mille ans. Même si je n'aime pas trop dissocier l'algèbre de la géométrie, personnellement les nombres m'intéressent plus sous leur aspect géométrique.

De fait, beaucoup de grandes avancées, parfois récompensées par des prix prestigieux, ne résultent-elles pas de liens tissés entre différents domaines ?

Étienne Ghys : Cette dichotomie entre algèbre et géométrie était pratique par le passé, mais elle a perdu de son sens. Le mathématicien américain Dennis Sullivan utilise une analogie. Il pense aux

BIO EXPRESS

1954
Naissance à Lille

1988
Directeur de recherche au CNRS, à l'École normale supérieure de Lyon.

2009
Rédacteur en chef de *l'Images des Mathématiques*.

2019
Secrétaire perpétuel pour la première division de l'Académie des sciences.

mathématiques comme à une tapisserie à laquelle on ajoute sans cesse de nouvelles pièces. Les mathématiques ne se développent pas, comme on pourrait le penser, sous forme arborescente où les ramifications se succèdent. Le modèle de l'arbre est un peu triste, car les branches qui se séparent ne se rencontrent plus par la suite.

Les mathématiques sont jubilatoires, on peut employer ce mot-là, précisément, quand des branches se rencontrent pour en faire une nouvelle, insoupçonnée auparavant. L'image qui me vient est celle de ces arbres touffus et denses où l'on ne sait plus où sont les branches, où sont les racines.

Et quand deux branches indépendantes depuis longtemps fusionnent, on assiste à un grand moment. C'est arrivé à l'algèbre et à la géométrie à l'occasion d'événements historiques.

Selon moi, le premier de ces moments forts a été l'invention par Descartes de ses fameuses coordonnées cartésiennes. Grâce à lui, avec son livre *La Géométrie*, on

comprend que l'on peut traiter de géométrie à partir des coordonnées (des nombres donc) et qu'à l'inverse, on peut étudier des courbes (de la géométrie) à partir de leurs équations. La géométrie devient en quelque sorte la même chose que l'algèbre!

Un deuxième grand moment, inverse, a eu lieu dans la deuxième moitié du 19^{e} siècle. Au lieu d'expliquer la géométrie par l'algèbre, au lieu de décrire un cercle par son équation $x^2 + y^2 = 1$ (c'est l'approche cartésienne), Alexandre Grothendieck, et bien d'autres, ont expliqué les nombres par la géométrie. Les nombres entiers forment des espaces sur lesquels on peut faire de la géométrie! Sans cette vision géométrique de l'arithmétique, par exemple, on ne serait jamais arrivé à démontrer le théorème de Fermat.

En construisant sans cesse des passerelles, ne va-t-on pas aboutir à une sorte d'unité globale?

Etienne Ghys: J'aime les mathématiques sans aucun doute à cause de cette unité. Les mathématiques explosent en quantité, les connaissances augmentent de façon exponentielle (ce que l'on sait aujourd'hui est sans commune mesure avec ce que l'on connaissait il y a seulement cent ans), mais elles conservent une cohérence indiscutable. Les mathématiques ont réussi à croître non pas comme un arbre, mais plutôt comme une nébuleuse connexe: il y a des passerelles dans tous les sens, je trouve ça vraiment remarquable. La structure des mathématiques évoque un graphe expenseur, un sujet mathématique aujourd'hui très à la mode.

De quoi s'agit-il?

Etienne Ghys: Lors du dernier congrès international de mathématiques, plusieurs conférences plénières en parlaient. Imaginons un graphe en forme d'arbre. En retirant un sommet à l'intérieur, on obtient deux morceaux, deux graphes plus petits. Les graphes expenseurs sont à l'opposé: on a du mal à les couper en deux morceaux de taille significative. On a beau retirer des sommets, le graphe reste d'un seul tenant. Les graphes expenseurs ont une propriété d'hyperconnectivité. Internet, un graphe d'environ 10 milliards de sommets, est un exemple. Le nombre de pages Internet qu'il faudrait fermer pour couper le monde en deux parties de grande taille qui ne communiqueraient plus est très grand.

Le mathématicien russe Gregori Margulis, aujourd'hui à l'université Yale, aux États-Unis, en a construit

dans les années 1980. C'est un sujet vraiment intéressant et qui, en passant, est relié à l'arithmétique.

De quelle façon?

Etienne Ghys: Au début, dans les années 1970, on avait démontré l'existence de tels graphes par des moyens probabilistes, mais on n'en connaissait aucun que l'on pouvait décrire de façon explicite. Finalement, Gregori Margulis y est parvenu en utilisant les nombres premiers et les graphes dits de Cayley (qui encodent la structure d'un groupe). En d'autres termes, aujourd'hui on peut construire explicitement de grands graphes expenseurs grâce aux nombres premiers.

Gregori Margulis est un grand mathématicien. Médaille Fields en 1978, il n'a pas pu venir chercher sa récompense à Helsinki, parce que l'Union soviétique ne l'a pas autorisé à sortir de son pays. Il a donc envoyé sa conférence par la poste et c'est Jacques Tits, Prix Abel en 2008, qui l'a lue. Elle annonçait la démonstration du théorème d'arithmétique, un résultat absolument extraordinaire. Il continue à travailler aujourd'hui, sur de nombreux sujets.

Est-ce que les nombres ont leur place dans votre spécialité, la géométrie et les systèmes dynamiques?

Etienne Ghys: Et comment! C'est justement un de ces nombreux exemples de connexion entre des domaines qu'on pensait indépendants. Dans ce cas précis, les systèmes dynamiques ont remis de l'ordre dans les nombres.

Il s'agit d'une question d'approximation diophantienne. L'idée est d'approcher un nombre irrationnel et de s'intéresser à la qualité de l'approximation. Par exemple, je peux approcher le nombre π par $22/7$, mais aussi par $355/113$. Quel est le lien entre l'erreur commise et la taille du numérateur et du dénominateur du nombre rationnel? Cette question est un sujet majeur.

Les mathématiques explosent en quantité, le savoir augmente de façon exponentielle

Certains nombres, dits de Liouville, sont très bien approchés par des nombres rationnels. Pourquoi? Par exemple, construisons le nombre suivant: un «0», une virgule, un «1», 10 000 «0», un «1», un million de «0», un «1», un milliard de «0», un «1», un milliard de milliards de milliards de milliards de «0», encore un «1»... Dans son écriture décimale, ce nombre est essentiellement constitué de «0», avec de temps en temps, et de plus en plus rarement un «1». Il est bien sûr irrationnel, car les décimales ne sont pas périodiques, mais il est extrêmement bien approché par un nombre rationnel puisque si je m'arrête par exemple au dix millièmes «1», les «0» qui suivent sont tellement nombreux que l'erreur commise en le tronquant à ce niveau est microscopique. Ce nombre est presque rationnel. Or un très ancien théorème de Liouville, de la fin 19^{e} siècle, affirme qu'un tel nombre est nécessairement transcendant. C'était la première fois que l'on mettait en évidence cette propriété!

Elle signifie que le nombre en question ne peut pas être solution d'une équation à coefficients entiers. C'est le cas de π , de e . Mais à cette époque, on l'ignorait.

Maintenant, à l'opposé, on trouve... le nombre d'or. Le nombre d'or est irrationnel, Platon le savait, Euclide en parle... Et il est très mal approché par des rationnels. On parle alors de nombres diophantiens.

Un autre théorème du début du 19^{e} siècle va nous conduire à la dynamique. Il stipule que le nombre d'or (ainsi que quelques autres qui lui sont très reliés) est le pire de ces nombres diophantiens: aucun autre nombre n'est aussi loin des rationnels. L'image est saisissante!

A cette aune, quel nombre suit le nombre d'or? C'est le nombre d'argent, qui correspond à $\sqrt{2}$. Il est très mal approché par les nombres rationnels, mais l'est un peu mieux que le nombre d'or. Viennent

Ensuite le nombre de bronze, et d'autres encore. Ils forment ensemble la suite de Markov et convergent vers une limite. Ils constituent tout un domaine d'étude, qu'on appelle le spectre de Markov et de Lagrange.

J'en viens au rapport avec la dynamique. Les tout derniers théorèmes qui décrivent la nature de ces nombres mal approchés par des rationnels sont le fruit de l'école brésilienne. Leurs énoncés parlent de nombres, mais dès la première ligne de démonstration, on parle de systèmes dynamiques, d'orbites qui convergent, ou pas... Ce courant a été initié pour l'essentiel par Gregori Margulis, encore lui, dans les années 1980. Marina Ratner, décédée il y a peu, a également joué un rôle important.

Le lien entre différents domaines, et tous les autres, que disent-ils de la nature des mathématiques ?

Étienne Ghys : Difficile de répondre... Ces multiples connexions disent peut-être que les mathématiques sont importantes. Elles refusent d'être coupées en morceaux, alors que depuis trois mille ans, beaucoup ont cherché à le faire.

La distinction fréquente entre les mathématiques pures et appliquées en est une bonne illustration. À certaines périodes de l'histoire, cette différence ne faisait aucun sens. Carl Friedrich Gauss, par exemple, était-il théoricien ou non ? Astronome ou mathématicien ? Impossible de trancher. Le génie des *Disquisitiones Arithmeticae* (un texte fondamental de théorie des nombres), l'inventeur du théorème de représentation conforme et l'arpenteur du royaume de Hanovre sont un seul et même Gauss. Dans son esprit, il n'y a ni mathématiques pures ni appliquées.

À d'autres moments, la situation change. Ainsi, je pense qu'Henri Poincaré faisait une différence entre les deux, même s'il s'est illustré dans les deux registres. Ensuite, une bonne partie des mathématiques françaises du xx^e siècle ont séparé le pur et l'appliqué, ce qui a d'ailleurs eu un certain nombre d'avantages pendant un temps.

Du point de vue de la politique scientifique, le CNRS a un temps envisagé de scinder en deux la section de mathématiques. Cela ne s'est heureusement pas fait, et aujourd'hui, plus personne n'y pense. Mais on peut encore repérer quelques réminiscences de ce débat. Ce modèle s'applique même à la science tout entière, où l'on essaie d'opposer la recherche fondamentale et la recherche appliquée.

Si les mathématiques se dispersaient dans tous les sens et perdaient leur cohésion, alors on en déduirait que l'objet central situé derrière n'existe pas. J'ai plutôt le sentiment que la cohérence, confirmée depuis des siècles, prouve que l'on parle de quelque chose d'unique, que l'on appelle « mathématique ».

En tant qu'adepte de la diffusion, le nombre a-t-il un statut particulier lorsqu'il s'agit de partager les mathématiques avec le grand public ?

Étienne Ghys : Première remarque, nous manipulons des nombres tous les jours, à peu près correctement. Ensuite, tout le monde croit savoir ce qu'est un nombre (pourant, rien n'est moins sûr), mais presque personne ne s'est jamais vraiment posé la question. Pour ces raisons, les nombres ont en effet un rôle important dans la diffusion des sciences et des mathématiques en particulier : ce sont des objets à la fois familiers et méconnus.

Par exemple, sur le site *Images des mathématiques*, que j'ai contribué à créer en 2009, l'article le plus lu, et de très loin, est consacré aux... tables de multiplication ! Ça fait réfléchir. Pourquoi celui-là ? En regardant de plus près la fréquentation, on observe un pic à chaque rentrée scolaire. C'est passionnant. Les parents se posent des questions pour leurs enfants. Il y a une demande dans nos rapports aux nombres.

Un grand nombre de mathématiciens pendant plusieurs siècles. Je crois qu'il faudrait commencer par dire ça aux enfants : ils sont les héritiers d'un passé très riche.

Jusqu'au Moyen Âge, les additions étaient faisables, mais les multiplications restaient très compliquées, même avec le système décimal. Dans une lettre, un riche marchand allemand demande conseil à un universitaire pour orienter son fils. L'universitaire répond que s'il s'agit pour son fils de ne faire que des additions, alors une université allemande devrait suffire. Mais s'il faut multiplier, le fils doit partir étudier en Italie. Des techniques se développaient donc progressivement.

Pour résumer, le nombre est essentiel pour la diffusion car les gens sont intéressés. Les enfants adorent qu'on leur explique comment multiplier facilement avec les doigts. Et l'on peut s'adapter à tous les auditoires. Pour un public plus averti, on peut par exemple aborder la cryptographie, les nombres premiers... Le nombre sert en toute occasion !

Parmi les grands problèmes qui restent à résoudre en théorie des nombres, lesquels vous semblent être une sorte de graal ?

Étienne Ghys : Je ne vais pas être très original, mais il y a bien sûr l'hypothèse de Riemann sur les nombres premiers qui reste centrale depuis très longtemps.

Tout le monde croit savoir ce qu'est un nombre, mais qui s'est vraiment posé la question ?

Dans cet article, j'explique des choses très simples, comme les méthodes employées à l'école primaire pour les additions et les multiplications. Et je commence par une question : « Comment les Romains pouvaient-ils multiplier CXXIV par XXIX ? » C'est impossible.

À l'école, un enfant apprend des algorithmes, pas très compliqués, pour faire des opérations. Il bénéficie des progrès conceptuels gigantesques dus au travail

Intrinsèquement, pour quelles raisons est-elle si importante ?

Étienne Ghys : Parce que les nombres premiers sont les briques élémentaires de l'arithmétique, c'est-à-dire, on l'a dit, de la moitié des mathématiques. La distribution asymptotique des nombres premiers parmi les nombres entiers, c'est vraiment la base. Tous les nombres entiers sont fabriqués à partir de ces nombres premiers. On comprend alors

que l'on veuille les compter, ça me paraît indiscutable.

En ce moment, nous fêtons les 150 ans du tableau périodique des éléments de Mendeleïev, une classification de tous les atomes existants sur la base de leurs constituants et qui sous-tend leurs propriétés chimiques. L'hypothèse de Riemann est du même niveau: elle mettrait de l'ordre dans les «atomes des nombres». Aucun doute, c'est une question centrale, qui dépasse même le cadre de la théorie des nombres. D'ailleurs, il est possible de la reformuler en termes de systèmes dynamiques.

Quel autre grand problème peut-on citer ?

Etienne Ghys: J'aime bien ce problème $3n+1$, ou conjecture de Syracuse: à partir d'un nombre entier strictement positif, on le divise par 2 s'il est pair, sinon, on le multiplie par 3 et on ajoute 1, et on recommence avec le résultat. Arrivera-t-on toujours à 1 ?

Je n'ai aucune idée de sa place dans le paysage mathématique (en fait, je ne vois pas très bien en quoi il est important), mais il se prête volontiers à la diffusion: on peut tout à fait en parler avec n'importe qui, évoquer ce problème en tant que tel, son histoire, les progrès quant à sa résolution... Au passage, on balaie une idée reçue selon laquelle tous les problèmes mathématiques ont été résolus par les Grecs. Non, il existe bel et bien des problèmes encore non résolus!

Cette conjecture offre également l'occasion, lors d'une conférence ou en discutant plus simplement, de mettre en évidence de vrais liens structurels entre mathématiques et informatique.

Avec le problème $3n+1$, on multiplie par trois, on divise par 2, on ajoute 1... et l'on se demande si l'on peut arriver à la case 1. De même, lorsqu'un mathématicien raisonne, il met bout à bout un certain nombre de raisonnements élémentaires, des syllogismes, et regarde où ils le mènent, l'objectif étant d'arriver à l'équivalent d'une case 1, en l'occurrence une case «Oui, c'est démontré».

Syracuse permet d'illustrer des questions sur ce que peut être un algorithme qui ne finit jamais, un problème fondamental en informatique, un domaine dans lequel justement, on doit prouver qu'un algorithme, comme Parcours Sup, conduit à une conclusion dans tous les cas.

Pour cela, le problème $3n+1$ a des vertus pédagogiques que je trouve

très intéressantes. On peut expliquer ce que sont les mathématiques, un algorithme, et même qu'il existe des énoncés pour lesquels on a beau développer tous les syllogismes que l'on veut, on n'arrivera jamais à dire s'ils

Suite au discours d'Edouard Philippe, un comité se réunit à l'Académie et transmettra aux autorités différentes recommandations. Par le passé, l'Académie s'est souvent exprimée sur des sujets divers, comme les enfants et les écrans, les

Aujourd'hui, les enfants sont les héritiers d'un passé mathématique très riche

sont vrais ou faux. Ils sont indécidables. C'est le fameux théorème de Gödel.

Le problème $3n+1$ permet d'aller très loin, et en cela, c'est un outil de choix pour transmettre les mathématiques. Et cet aspect est très important pour moi.

Depuis janvier 2019, vous êtes secrétaire perpétuel de l'Académie des sciences. Quel est votre rôle ?

Etienne Ghys: L'Académie des sciences, créée en 1666 par Colbert, est investie de plusieurs missions: parmi elles, on peut citer diffuser la science, conseiller le gouvernement, favoriser l'enseignement des sciences... La vie de l'Académie est organisée par un bureau constitué d'un président (aujourd'hui Pierre Corvol), d'un vice-président (Patrick Flandrin) et de deux secrétaires perpétuels. Je suis l'un d'eux (l'autre est Pascale Cossart). En quelques mots, mon rôle est simplement d'orienter l'action de cette académie.

Par exemple, le Premier ministre a récemment prononcé un discours annonçant un plan pluriannuel pour la science. Or dans notre académie, un grand nombre de scientifiques réfléchissent au fonctionnement de la science, au rôle du programme d'investissements d'avenir, de l'Agence nationale de la recherche (ANR), du CNRS dont on fête les quatre-vingts ans cette année... Ces structures doivent être repensées régulièrement. Par exemple comment harmoniser les rôles des chercheurs CNRS et des enseignants-chercheurs universitaires?

mathématiques à l'école primaire, la réforme du baccalauréat...

Êtes-vous en lien avec en lien avec l'Office parlementaire d'évaluation des choix scientifiques et technologiques (OPECST) ?

Etienne Ghys: Oui, avec cette instance présidée par Gérard Longuet et dont Cédric Villani est le premier vice-président, nous organisons des petits-déjeuners mensuels qui réunissent parlementaires et scientifiques autour d'un thème particulier. Le prochain traitera de la cybersécurité.

Par ailleurs l'Académie organise un nombre de colloques, parfois importants notamment celui à venir sur les insectes. Certaines de ses manifestations sont destinées au grand public, comme les «5 à 7» dont je m'occupe particulièrement. À chaque fois, la grande salle des séances où ils se déroulent est pleine à craquer. Le dernier était dédié aux femmes de science oubliées, comme Alicia Boole, une mathématicienne britannique du ^{xx}e siècle que personne ne connaît.

Nous nous préparons aussi à commémorer les cinq cents ans de la mort de Léonard de Vinci, en mettant à l'honneur douze de ses codex dont l'Institut est propriétaire.

Une dernière chose. L'Académie des sciences décerne chaque année des dizaines de prix, généralement bien dotés. La sélection des lauréats est un travail gigantesque. ■

Pronos recueillis par Loïc Mangin

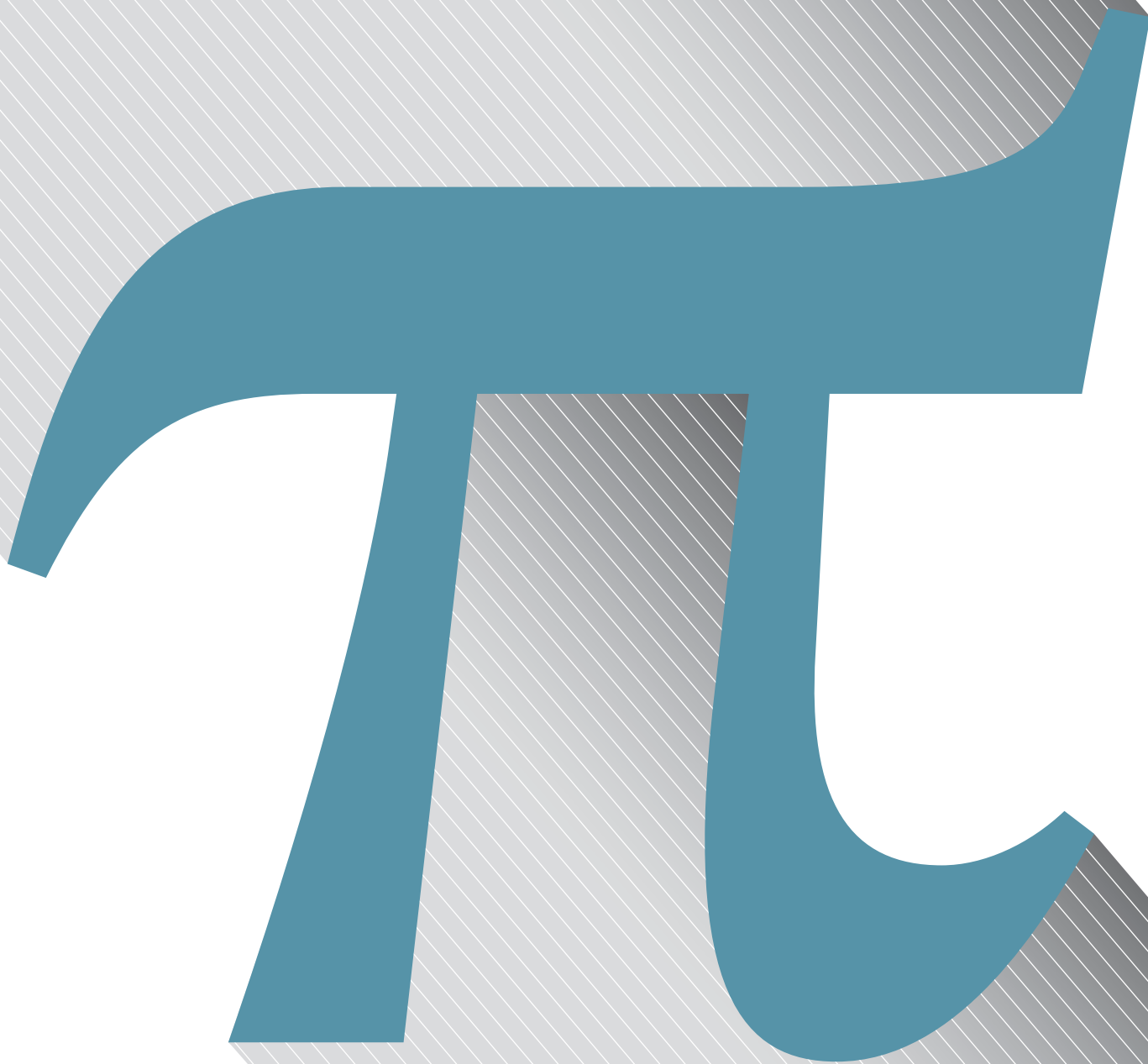
8,14159 26535 89793 23846 26433 83279 50288 41971 69399 37510 58209 74944 59230 78164 06286 20899 86280
08651 32823 06647 09384 46095 50582 23172 53594 08128 48111 74502 84102 70193 85211 05559 64462 29489 54
34461 28475 64823 37867 83165 27120 19091 45648 56692 34603 48610 45432 66482 13393 60726 02491 41273 72
20920 96282 92540 91715 36436 78925 90360 01133 05305 48820 46652 13841 46951 94151 16094 33057 27036 5
61179 31051 18548 07446 23799 62749 56735 18857 52724 89122 79381 83011 94912 98336 73362 44065 66430 860
21798 60943 70277 05392 17176 29317 67523 84674 81846 76694 05132 00056 81271 45263 56082 77857 71342 75778
40901 22495 34301 46549 58537 10507 92279 68925 89235 42019 95611 21290 21960 86403 44181 59813 62977 47
99837 29780 49951 05973 17328 16096 31859 50244 59455 34690 83026 42522 30825 33446 85035 26193 11881 71
32083 81420 61717 76691 47303 59825 34904 28755 46873 11595 62863 88235 37875 93751 95778 18577 80532 1712
95909 21642 01989 38095 25720 10654 85863 27886 59361 53381 82796 82303 01952 03530 18529 68995 77362 23
13151 55748 57242 45415 06959 50829 53311 68617 27855 88907 50983 81754 63746 49393 19255 06040 09277 01
16035 63707 66010 47101 81942 95559 61989 46767 83744 94482 55379 77472 68471 04047 53464 62080 46684 23
52104 75216 20569 66024 05803 81501 93511 25338 24300 35587 64024 74964 73263 91419 92726 04269 92279 67
21992 45863 15030 28618 29745 55706 74983 85054 94588 58692 69956 90927 21079 75093 02955 32116 53449 87
98818 34797 75356 63698 07426 54252 78625 51818 41757 46728 90977 77279 8000 81647 06001 61452 49192 173
68548 16136 11573 52552 13347 57418 49468 43852 33239 07394 14333 62416 86251 89835 69485 56209 921
67179 04946 01653 46680 49886 27232 79178 60857 84383 82796 79181 81454 10095 38837 86360 95068 00342 2
34886 26945 60424 19652 85022 21066 11863 07124 27862 20391 69445 04712 37137 86960 95636 43719 17287 46
32645 99581 33904 78027 59009 94657 64078 91226 94683 98351 49570 98258 22620 52248 94077 26719 47826 84
36394 43745 53050 68203 49625 24517 49399 61243 14298 09111 65925 09372 21691 92387 41059 78
92846 81382 68683 86894 27741 55991 85592 51259 53959 43111 99725 24680 91278 72736 44695 84865 38367 36
43904 51244 13654 97627 80797 71569 14359 91110 12961 60811 41694 86811 38484 06353 42207 22258 28488 64
27394 52267 46767 88952 52138 52254 99546 66111 82398 64561 96116 35113 62305 77456 49803 55936 34568 174
96596 09402 52288 79710 89314 56691 36867 22111 89405 60111 50330 91179 28680 92087 47609 17824 93858 9
65549 78189 31297 84821 68299 89487 22658 80481 5640 14271 17755 1323 79641 91111 87462 34364 54285 844
73573 95231 13427 16610 21359 69551 23144 29524 81111 18711 01111 10311 149344 05711 1731 05785 390
33214 45713 86875 19435 06430 21811 31910 48481 00311 14681 11111 81911 97939 95206 11111 63428 75
98391 01591 95618 14675 14269 12391 8940 90718 64942 31111 95146 55022 52316 03811 23014 20
08303 90697 92077 34672 21825 62599 11111 14215 03068 03844 71111 02681 146659 25201 49744 1507 3
04863 31734 64965 14539 05796 26856 10111 28106 65879 69811 35111 340525 11111 59 10371 20628 11111 90 3
99360 07230 55876 31763 59421 87312 51471 20511 11111 86125 17321 791 98414 11111 882 91644 70609 575
91098 16909 15280 17350 67127 48583 22287 18352 09353 96572 51211 133579 11111 36 98820 11111 44 21006 75103 346
35163 98315 01970 16515 11685 17143 76576 18351 55650 88490 99111 3 59982 11111 734 55283 31111 5 50764 79185 358
98570 64204 67525 90709 15481 41654 98594 61637 18027 09810 11111 309 9244 11111 9575 71282 81111 59 23233 26097 29
91193 25974 63667 30583 60414 28138 83032 03824 90375 89111 43744 17029 11111 76 56180 93111 44403 07074 692
11011 00449 29321 51608 42444 85963 71111 38952 28111 11111 35526 58215 11111 495 76857 26111 3 34418 93039 68
73189 15441 10104 46823 25271 62010 52652 27211 10803 96665 57309 25477 11111 557 85376 34611 3 20653 10989 652
35662 01855 81007 29360 65987 64861 17910 45334 88503 46113 65768 67111 49441 66803 11111 265 79787 71855 60
34443 18586 76975 14566 14068 00700 23787 76591 34401 71274 94704 21111 32 23053 89945 61111 14 07112 70004 07
58807 97270 82668 30634 32858 78569 83052 35808 93306 57574 06761 11111 3716 37752 54202 11495 57615 81400 250
79259 23099 07965 47376 12551 76567 51357 51782 96664 54779 11111 11299 61489 03046 39947 13296 21073 404
97131 11790 42978 28564 75032 03198 69151 40287 08085 99048 01094 12147 22131 79476 47772 62241 42548 545
75850 43063 32175 18297 98662 23717 21591 60771 66925 47487 38986 65494 94501 14654 06284 33663 93790 03
96571 20918 07638 32716 64162 74888 80078 69256 02902 28472 10403 17211 86082 04190 00422 96617 11963 77
96318 62947 26547 36425 23081 77036 75159 06735 02350 72835 40567 04038 67435 13622 22477 15891 50495 309
32599 39780 54193 41447 37744 18426 31298 60809 98886 87413 26047 21569 51623 96586 45730 21631 59819 31
67242 29246 54366 80098 06769 28238 28068 99640 04824 35403 70141 63149 65897 94092 43237 89690 70697
38379 86230 01593 77647 16512 28935 78601 58816 17557 82973 52334 46042 81512 62720 37343 14653 19777 74160
33441 95215 41341 89948 54447 34567 38316 24993 41913 18148 09277 77103 86387 73431 77207 54565 45322 07770
09263 60197 59882 81613 32316 66365 28619 32668 63360 62735 67630 35447 76280 35045 07772 35547 10585 954
30624 64362 67945 61275 31813 40783 30336 25423 27839 44975 38243 72058 35311 47711 99260 63813 34677 6879
37040 85913 37464 14428 22772 63465 94704 74587 84778 72019 27715 28073 17679 07707 15721 34447 30605 70073
63128 40425 12192 56517 98069 41135 28013 14701 30478 16437 88518 52909 28545 20116 58393 41965 62134 914
90496 52098 58033 85072 24264 82939 72858 47831 63057 77756 06888 76446 24824 68579 26039 53527 73480 30
09164 39613 62676 04492 56274 20420 83208 56611 90625 45433 72131 53595 84506 87724 60290 16187 66795 24
91930 64553 77991 40373 40432 87526 28889 63995 87947 57291 74642 63574 55254 07909 14513 57111 36941 091

34825 34211 70679 82148
 4930 38196 44288 10975 66593
 458 70066 06315 58817 48815
 7595 91953 09218 61173 81932
 21 39494 63952 24737 19070
 3 96091 73637 17872 14684
 713 09960 51870 72113 49999
 010 00313 78387 52886 58753
 2 68066 13001 92787 66111
 994 13891 24972 17752 83479
 671 13900 98488 24012 85836
 5906 94912 93313 67702 89891
 823 54781 63600 93417 21641
 7202 75596 02364 80665 49911
 21 72147 72350 14144 19735
 92 22184 27255 02542 56887
 5125 20511 73929 84896 08412
 776 46575 73962 41389 08658
 4826 01476 99090 26401
 8859 59772 97549 89301 61753
 6222 62609 91246 08051 24388
 4815 84560 28506 01684
 32 41125 15076 06947 94510
 0097 14909 67598 52613
 47 95265 86782 10511 41354
 62 19838 74478 08478 48968
 444 06437 45123 71819 21799
 0937 62137 85595 66389 37787
 2518 66600 21324 34088 19071
 9759 51567 71577 00420 33786
 27 06957 22091 75671 16722
 71 10314 12671 11369 90865
 93 22618 54896 32132 93308
 9971 20844 33573 26548 93823
 211 20191 30203 30380 19762
 642 62434 10773 22697 80280
 269 18620 56476 93125 70586
 845 52965 41266 54085 30614
 854 73326 99390 81454 66464
 012 62285 94130 21647 15509
 37 51895 73596 14589 01938
 40 33215 71853 06142 28813
 976 92656 72146 38530 67360
 921 33757 51149 59501 56604
 84 44893 33096 34087 80769
 951 67353 81297 41677 29478
 79422 36250 82216 88957
 0 31990 66554 18763 97929
 0 92120 19051 66096 28049
 487 02790 81435 62401 45171
 6 95970 30983 39130 77109
 3 34924 36931 13835 04931
 434 15956 25865 86557 05526
 480 29005 87607 58251 04747
 061 63425 22577 19542 91629
 19 39325 19107 60208 285318

DES NOMBRES D'EXCEPTION

Le nombre d'or et π sont parmi les plus célèbres. Connus depuis l'Antiquité, ils n'ont pourtant pas encore révélé tous leurs secrets. D'ailleurs, on découvre qu'ils surgissent où on ne les attend pas : dans les quasi-cristaux, dans du sable jeté sur le sol, dans des fractales... Ces deux stars ne doivent pas occulter la richesse d'autres nombres parés de tout aussi extraordinaires propriétés : les nombres palindromes, ceux de Schur...

Un peu plus de six mille décimales de π sur lesquelles se déploient deux séries de spirales : huit dans un sens et treize dans l'autre. Ces nombres sont deux termes consécutifs de la suite de Fibonacci, où le rapport de deux termes consécutifs tend vers le nombre d'or.



ESSENTIEL

On sait calculer avec une efficacité plusieurs milliards de décimales de π grâce à des formules complexes.

Des méthodes plus rustiques, et moins performantes, existent aussi, par exemple en jetant du sable sur un carré, ou bien en tirant un fusil sur une cible.

On a récemment découvert d'autres moyens inattendus. Ainsi, le choc de billes près d'un mur révèle les premières décimales de π .

Ce nombre se cache aussi dans l'ensemble fractal de Mandelbrot et dans le jeu de la vie de John Conway.

AUTEUR



JEAN-PAUL DELAHAYE est professeur émérite à l'université de Lille et chercheur au Centre de recherche en informatique, signal et automatique de Lille (Cristal).

Le nombre π est partout !

L'ubiquité du nombre π ne cesse d'étonner. On peut l'approcher avec du sable, des aiguilles, un fusil... Et récemment encore, il est apparu là où personne ne l'attendait !

L

es staphylocoques sont des bactéries ubiquitaires, du microbiote intestinal jusqu'aux sols. Le Bien et le Mal sont ubiquitaires dans la littérature. Certaines roches le sont aussi. L'ubiquité, c'est-à-dire «le fait d'être présent partout à la fois ou en plusieurs lieux en même temps», existe même en mathématiques. Ainsi, parmi les nombres, π est celui qui jouit le plus spectaculairement de

cette propriété: on le rencontre sans cesse. L'une des conséquences est qu'on découvre encore de nouvelles façons de calculer π .

Il est devenu difficile de battre les formules qui évaluent très vite ce nombre, parce que les meilleures méthodes connues résultent de recherches approfondies, qu'elles sont d'une grande subtilité, et qu'elles sont d'une époustouflante efficacité. Aujourd'hui, le record de calcul donne 31 415 milliards de décimales de π et se fonde sur plusieurs formules, comme celle-ci, due aux frères David et Gregory Chudnovsky («!» se lit factorielle: $n! = 1 \times 2 \times \dots \times n$)

$$\frac{1}{\pi} = \frac{1}{6k} \left(\frac{1}{(k!)^3} \left(\frac{13591409 + 545140134k}{(6k)!(k!)^3 (640320)^{3k+3/2}} \right) \right)$$

Les étranges et nouvelles méthodes de calcul de π ne peuvent rivaliser avec cette extraordinaire formule (en se limitant au terme $k=0$, on trouve $\pi=3,1415926535897342\dots$, ce qui est correct jusqu'au 14^e chiffre), mais

elles valent que l'on s'y intéresse pour le défi, la beauté et même l'amusement.

Certaines méthodes utilisent des procédés physiques (voir l'encadré ci-dessous). La méthode de Monte-Carlo pour calculer π se fonde sur un principe simple: la surface d'un disque de rayon r est πr^2 . On fait tomber au hasard des grains de sable sur un carré de côté r ; si les grains le recouvrent uniformément, la proportion de grains tombés dans le quart de disque de rayon r donne une valeur approchée de $\pi/4$. On obtient ainsi quelques décimales de π par l'expérience.

TIRER π AU FUSIL

En pratique, cette méthode souffre d'un grave défaut: elle suppose que l'on sache disposer des grains de sable uniformément sur le carré. Or en les lançant vers le centre, par exemple, les grains de sable auront une distribution plus dense vers le centre et plus éparse sur les bords. Le calcul sera faussé!

Des méthodes statistiques corrigent cette non-uniformité. L'une d'elles consiste à compter le nombre de grains P en affectant à chacun un coefficient inversement proportionnel au nombre de grains situés dans un petit cercle autour de lui. Les grains situés dans une zone

dense sont ainsi moins comptés, ce qui corrige la non-uniformité.

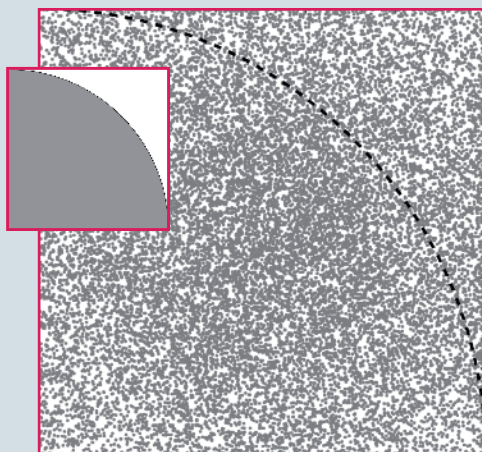
Dans une expérience plus agressive, Vincent Dumoulin et Félix Thouin, de l'université de Montréal, ont utilisé une méthode de ce type en tirant sur une cible distante de 20 mètres avec un fusil. Les expérimentateurs ont ainsi créé 30857 trous dans la cible. Le calcul, avec correction de la non-uniformité, a donné $\pi=3,131$, ce qui correspond à une erreur de 0,3 %.

DES AIGUILLES ET DES BILLES

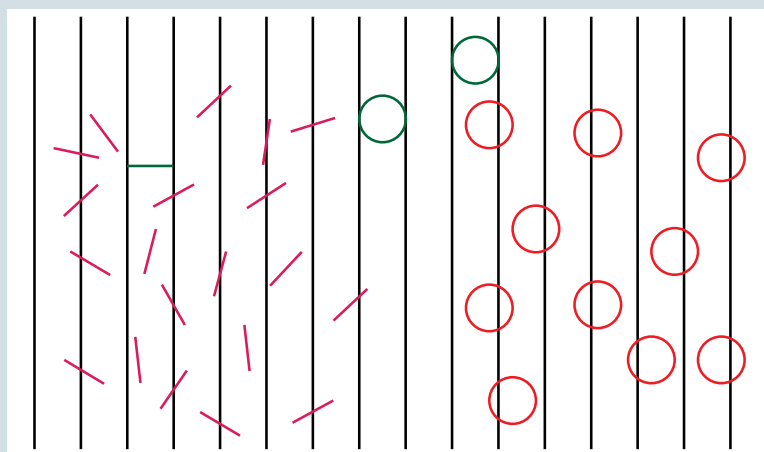
Les aiguilles de Buffon constituent un autre moyen d'approcher π par la physique. On lance n aiguilles de longueur L sur un parquet dont la largeur des lattes est L ; on compte le nombre k d'aiguilles coupant les lignes parallèles de jonction entre lattes; le quotient $2n/k$ est une valeur approchée de π . Cette méthode très classique, comme celle des coups de fusil, ne donnera jamais plus de quatre décimales exactes de π .

La méthode proposée par Gregory Galperin, de l'université de l'Illinois, est plus intéressante et surprenante. Elle n'utilise que des chocs entre billes respectant les lois de la physique classique et produisant les décimales de π les unes après les autres. Non seulement le dispositif imaginé

CALCULER π PAR LA PHYSIQUE



en comptant les points ou grains de sable supposés uniformément étalés sur un quart de disque inscrit dans un carré, et en faisant le rapport entre le nombre obtenu et le nombre total de grains de sable dans le carré, on obtient une valeur approchée de $\pi/4$. Lorsque les points sont choisis par des méthodes numériques (par exemple des générateurs de nombres pseudo-aléatoires), on parle de méthode de Monte-Carlo. Si la répartition des points n'est pas uniforme, un ajustement statistique est nécessaire.



La méthode du naturaliste Buffon consiste à lancer aléatoirement n aiguilles de longueur L sur un tracé constitué de droites parallèles espacées de la même longueur L : la probabilité de l'intersection d'une aiguille avec une droite est $2/\pi$: en lançant beaucoup d'aiguilles et en comptant la proportion d'intersections, on en tire une approximation de π .

Pour comprendre, supposons que, en moyenne, le nombre de points d'intersection d'une courbe quelconque avec les droites soit proportionnel à sa longueur. Pour un cercle de diamètre L , ce nombre est toujours égal à 2; alors le nombre de points d'intersection pour l'aiguille sera en moyenne $2L/\pi L = 2/\pi$.

donne π , mais il le donne écrit en base 10, et cela sans qu'aucun calculateur mécanique ou électronique ne soit mêlé à l'affaire.

Par rapport à celle de Buffon et du fusil, la méthode de Galperin se dispense de hasard : le procédé déterministe donne donc, non pas une approximation de π , mais exactement les premiers chiffres de π ... pour peu que le dispositif matériel soit conforme au modèle théorique.

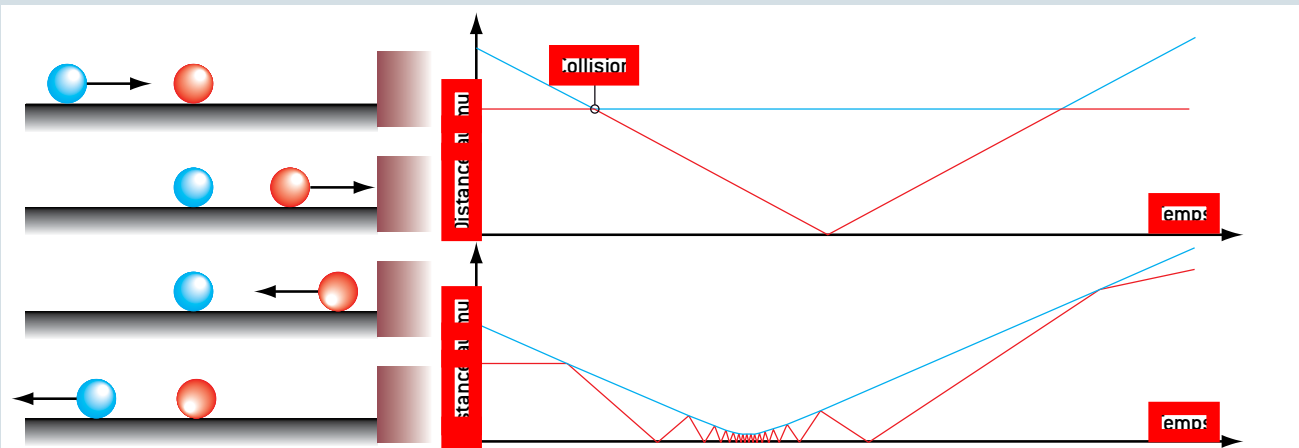
Pour comprendre, commençons par le cas le plus simple (voir l'encadré ci-dessous). On considère deux billes A et B de masse identique (en fait, des masses ponctuelles, la rondeur des billes ne joue aucun rôle). La bille A est immobile à une distance L d'un mur plat M. On lance la bille B perpendiculairement au mur M dans la direction de A. Elle cogne la bille A de façon parfaitement élastique (conservation de l'énergie cinétique et de la quantité de mouvement). La bille B s'immobilise donc, et A part vers le mur M avec la vitesse qu'avait B et qu'elle lui a transmise. La bille A cogne le mur, rebondit (le choc est toujours parfaitement élastique) et repart vers B, toujours avec la même vitesse. La bille A cogne B, A s'immobilise et B repart en s'éloignant du mur. On suppose qu'il n'y a pas de frottement. Il y a eu trois chocs : deux entre les billes A et B

et un entre la bille A et le mur. Le chiffre 3 est le premier de π . Ce n'est pas un hasard !

Si maintenant on refait l'expérience avec une bille B dont la masse est 100 fois celle de A, le schéma des collisions est plus compliqué. Avant que B et A ne se séparent définitivement, le nombre de chocs entre A et B et de la bille A avec le mur est 31. Ce sont les deux premiers chiffres décimaux de π . Plus généralement, si le rapport des masses entre B et A est 10^{2n} , alors le nombre de chocs donnera exactement les $n+1$ premiers chiffres décimaux de π . Ainsi, pour un rapport de masse de 10000, il y a 314 chocs ; pour un rapport 1000000, il y a 3141 chocs ; etc.

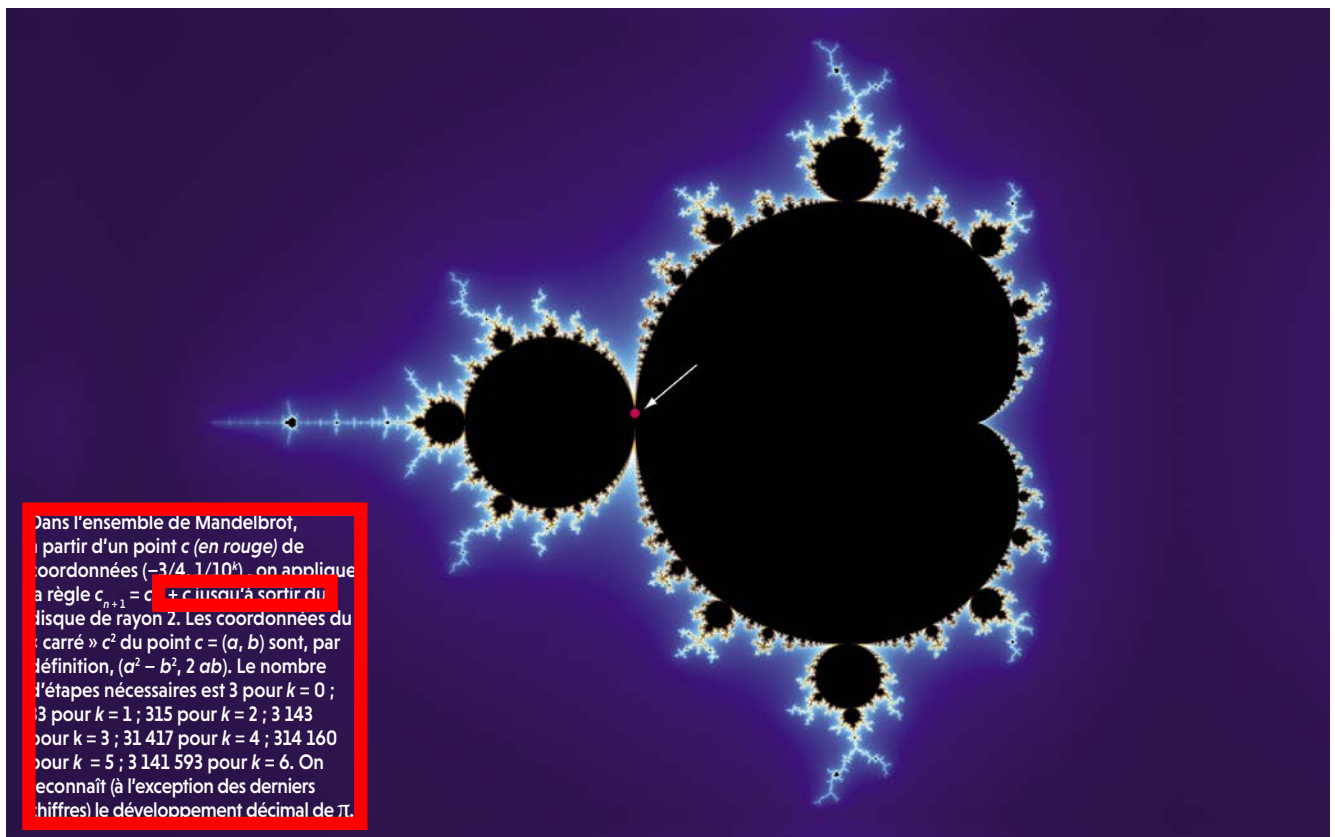
UNE BELLE METHODE. MAIS...

Pour les premières valeurs de n , on peut écrire de petits programmes qui confirment les affirmations indiquées. Le résultat général est cependant démontré de manière parfaitement rigoureuse. Il nécessite juste une petite hypothèse : les $2n$ premiers chiffres de π ne doivent pas se terminer par $n-1$ fois le chiffre 9. On sait que c'est vrai pour n plus petit que 5650000000000, puisqu'on connaît explicitement les décimales de π , mais pour n tendant vers l'infini, nul ne sait le démontrer. Cette



Des chocs entre billes π peut aussi surgir. Prenons une bille bleue et une bille rouge de même masse. La bille rouge est immobile (à gauche). La bille bleue la frappe selon un choc élastique. La bille bleue s'immobilise et la bille rouge se précipite sur un mur où elle rebondit et repart vers la bille bleue. Après le choc, la bille rouge est à nouveau immobile et la bille bleue s'éloigne indéfiniment. Il y a eu 3 chocs (à droite, en haut) : 3 est

le premier chiffre de π . Avec des masses dans un rapport 100, il y a non plus 3, mais 31 chocs (à droite, en bas). Plus généralement, si le rapport des masses est 10^{2n} , alors le nombre de chocs reste fini, et c'est l'entier correspondant aux $n+1$ premières décimales de π . Ainsi, pour $n = 5$, on aura 314 159 chocs : ce sont les 6 premiers chiffres de π .



SUR LE WEB

Animation montrant les 31 chocs de deux billes dont le rapport des masses est 100 :

<https://youtu.be/4UhPTrHIprk>

Expérience en ligne sur les aiguilles de Buffon : experiences.math.cnrs.fr/Calcul-de-Pi-avec-des-aiguilles-et.html

propriété est jugée plus que probable, mais elle reste inaccessible à nos techniques de preuve.

La méthode est magnifique et a étonné les spécialistes des systèmes dynamiques. En revanche, sur le plan pratique, la méthode est d'un intérêt limité. Comment ajuster les masses de A et de B avec la précision exigée ? On ne peut espérer faire beaucoup plus que le nombre d'Avogadro, soit environ 10^{24} , ce qui ne donnera que 12 décimales, et les autres mesures sont à l'avenant. Comment être certain de lancer les billes perpendiculairement au mur avec toute l'exactitude nécessaire ? Comment s'assurer que les chocs soient parfaitement élastiques et qu'il n'y ait aucun frottement ?

Pas plus que la méthode de Buffon ou du fusil, on ne tirera de celle de Galperin un grand nombre de chiffres de π . Si l'on veut s'en tenir à des méthodes physiques, le mieux est peut-être simplement de mesurer avec soin le périmètre et le diamètre d'un cercle assez grand et de faire le quotient. En réalité, rien ne vaut les calculs purs ne s'appuyant pas sur des hypothèses et des mesures physiques qu'on ne parvient jamais à mener avec plus de quelques chiffres significatifs. Venons-en donc aux méthodes mathématiques.

Archimède est né, a vécu et est mort à Syracuse, en Sicile. Il fut le premier à proposer une méthode mathématique permettant de calculer les chiffres du nombre π aussi loin qu'on

le souhaite. En mathématiques, Syracuse est aussi le nom d'une conjecture qui intéresse beaucoup de monde à cause de sa simplicité.

J'AIMERAIS TANT VOIR SYRACUSE

Cette «conjecture de Syracuse» ou «conjecture de Collatz» propose de partir d'un entier positif quelconque n : s'il est pair, on le divise par 2 ; s'il est impair, on le remplace par $3n + 1$. Et on recommence. La conjecture affirme que quel que soit l'entier initial n , on finit toujours par arriver à 1 (voir *Élémentaire, mais redoutable*, par S. Eliahou, page 30). Personne n'a su la démontrer. Expérimentalement, elle a été vérifiée jusqu'à 10^{20} . À priori, elle n'a rien à voir avec π , malgré son nom qui semble faire écho à Archimède. La Syracuse de la conjecture est en fait la ville américaine de Syracuse, dans l'État de New York, dont l'université a joué un rôle important dans la diffusion de la conjecture au monde entier.

Aucun lien avec π ? Pourtant, le Français Roland Yéléhada a mis au point une méthode de calcul de π à partir de la conjecture de Syracuse. Le principe est le suivant. On calcule la suite de Syracuse pour tous les nombres jusqu'à une certaine borne n , par exemple 100. Pour chacune des suites calculées, par exemple [13, 40, 20, 10, 5, 16, 8, 4, 2, 1], on évalue la longueur, ici 10, et la somme des éléments de la suite, ici 119. On teste si les deux nombres obtenus (10 et 119) ont un

diviseur commun plus grand que 1; ce n'est pas le cas ici. On prend alors le nombre a de fois où la réponse a été NON, puis on divise a par n , ce qui donne un nombre b . La racine carrée c de $6/b$ est une valeur approchée de π !

La méthode ne donne pas très rapidement les chiffres de π , mais on a des raisons de croire qu'elle converge vers π , car la longueur et la somme d'une suite de Syracuse, à cause de comportements imprévisibles des suites, sont comme deux nombres entiers tirés au hasard. Or on sait, d'après un résultat de 1881 démontré par Ernesto Cesaro, que la probabilité que deux entiers tirés au hasard n'aient pas de diviseur commun supérieur à 1 est $6/\pi^2$. Bien qu'aujourd'hui aucune preuve mathématique rigoureuse n'ait été donnée du résultat quand n tend vers l'infini, les expériences effectuées en écrivant de petits programmes confirment qu'il s'agit bien d'une méthode de calcul de π . Pour $n=100$, on obtient $a=66$, $b=0,66$, $c=3,01511...$ Pour $n=1000$, on obtient $a=606$, $b=0,606$, $c=3,146583...$

Bien évidemment, il s'agit d'un jeu et pour disposer de beaucoup de décimales de π , ce procédé n'est pas plus recommandable que les méthodes de Buffon, du fusil ou de Galperin. Une méthode toute aussi étonnante peut-elle faire mieux ? Oui, et elle est plus simple encore à mettre en œuvre.

π CACHÉ DANS UNE FRACTALE

L'ensemble de Mandelbrot est la plus célèbre des fractales (voir la figure page ci-contre). Sa définition, succincte, tient en quelques mots: c'est l'ensemble des points c du plan complexe tels que la suite $c_0=0$, $c_1=c$, $c_2=c^2+c$, ..., $c_{n+1}=c_n^2+c$, ... reste dans une partie bornée du plan; autrement dit, c'est l'ensemble des points c tels que la distance de c_n à 0 ne tend pas vers l'infini quand n tend vers l'infini.

Si vous n'avez jamais entendu parler du « plan complexe », il suffit, pour comprendre

LA PROBABILITÉ

QUE DEUX ENTIERS

TIRÉS AU HASARD

N'AIENT PAS DE DIVISEUR

COMMUN SUPÉRIEUR

À 1 EST $6/\pi^2$

tout ce qui nous occupe ici, de savoir que le carré d'un point de coordonnées (a, b) (représentant le nombre complexe $c=a+ib$) dans le plan complexe est le point de coordonnées $(a^2-b^2, 2ab)$.

Les outils nécessaires à la visualisation de l'ensemble de Mandelbrot, et surtout les puissances de calcul suffisantes (en chaque point il faut calculer la suite c_n), ne sont devenus disponibles qu'au début des années 1980. Grâce à quoi on a pris conscience de la richesse de cet ensemble et du découpage infiniment fin de sa frontière. Adrien Douady, de l'université Paris-Sud, et John Hubbard, de l'université Cornell aux États-Unis, ont montré en 1981 que cet ensemble est connexe, c'est-à-dire d'un seul tenant: on peut passer d'un point à un autre de l'ensemble en utilisant un chemin qui y reste tout le temps.

En 1991, Dave Boll, étudiant en informatique à l'université d'État du Colorado, explore l'ensemble de Mandelbrot et tente de savoir si un point unique sépare la partie de cet ensemble à droite du point $c = (-3/4, 0)$ de la partie qui se trouve à sa gauche (en rouge sur la figure page ci-contre). Il prend donc des valeurs de c de plus en plus proches du point c et calcule combien de points de la suite il faut considérer avant que c_n sorte du cercle de rayon 2. On sait en effet que dès que la suite c_n sort de ce cercle, elle part inévitablement à l'infini.

Il essaie donc comme point de départ $c = (-3/4, 1)$ et trouve que 3 itérations suffisent pour que la suite sorte du cercle. Il essaie $c = (-3/4, 1/10)$, il en faut maintenant 33. Avec $c = (-3/4, 1/100)$, il en faut 315. Avec $c = (-3/4, 1/1000)$, il en faut 3143. Avec $c = (-3/4, 1/10000)$, il en faut 31417. Avec $c = (-3/4, 1/100000)$, il en faut 314160. Avec $c = (-3/4, 1/1000000)$, il en faut 3141593... Stupéfaction! Les chiffres des

La naissance de π

Une fantastique configuration des cellules du jeu de la vie a été conçue par Adam Goucher

fonctionnement « Naissance si 3 voisins vivants, survie si 2 ou 3 voisins vivants », elle calcule π . Bien mieux, elle écrit en diagonale le résultat sous la forme d'une configuration stable qui énumère les chiffres décimaux de π . La configuration initiale est téléchargeable ici : <http://bit.ly/1S7PwJw> Et pour la faire fonctionner, le logiciel gratuit Golly est disponible ici : <http://golly.sourceforge.net>

3.141592651

ombres calculés sont, à l'exception des derniers, ceux de π écrit en base 10: 314159... Les calculs à programmer pour le vérifier sont particulièrement simples (*voir ci-contre*).

David Boll découvre aussi que, partant de $(1/4+c, 0)$ et en prenant des valeurs de c de plus en plus petites (cette fois, il commence par $c = 1/100$ et divise par 100 à chaque nouvel essai), on tombe sur les entiers suivants: 30, 312, 3140, 31414, 314157, etc. À nouveau, c'est π !

Notons que rien, dans la définition de l'ensemble de Mandelbrot, n'a de rapport avec la géométrie du cercle. Pourtant, une simple itération partant d'un nombre choisi de plus en plus petit donne assez rapidement les décimales de π .

Notons aussi que, par cette méthode, calculer 20 décimales de π demanderait plus de 10^{20} itérations, ce qui est la limite de ce qu'on peut espérer faire aujourd'hui, même en mobilisant les plus puissants ordinateurs. Cette méthode, aussi simple et élégante qu'elle soit, ne peut donc pas rivaliser avec les meilleures méthodes connues de calcul de π , qui sont plus compliquées, mais beaucoup plus efficaces.

LE JEU DE LA VIE ÉCRIT π

Un exploit de calcul d'une autre nature concernant π est lié au célèbre «jeu de la vie» de John Conway. Ce réseau d'automates cellulaires est l'un des moyens les plus élémentaires de mener des calculs. Chaque case du plan infini, muni d'un quadrillage, est occupée par un microcalculateur confronté à une seule alternative:

- Si, à l'instant t , une case est dans l'état *mort* (de couleur blanche), alors le microcalculateur examine ses 8 voisines; si 3 exactement sont vivantes, la case passe à l'état *vivant* (en noir) à l'instant $t+1$; sinon, elle reste dans l'état *mort*.

- Si, à l'instant t , une case est dans l'état *vivant*, alors le microcalculateur examine ses 8 voisins; si 2 ou 3 sont dans l'état *vivant*, la case reste dans l'état *vivant* à l'instant $t+1$; sinon, elle meurt. En résumé: «Naissance si 3 voisins vivants, survie si 2 ou 3».

Le pouvoir de calcul d'un tel réseau est bien supérieur à ce que l'on peut imaginer, et d'ailleurs John Conway a montré qu'on pourrait calculer avec cet automate cellulaire tout ce qui est calculable par algorithme. Pour cela, il faut la bonne configuration initiale et ne pas être pressé!

En 2010, Adam Goucher, prenant au sérieux le résultat théorique de John Conway, a conçu une configuration du jeu de la vie comportant 1389325 cases vivantes. En évoluant génération après génération, la configuration calcule les chiffres de π écrit en base 10 et, c'est le plus étonnant, va les écrire en diagonale à l'aide de cases vivantes déposées qui dessinent les chiffres en écriture habituelle (*voir l'encadré page précédente*)!

UN PROGRAMME POUR DÉBUSQUER π

Pour chaque entier k à partir de zéro, définissez la suite de couples de nombres réels (a_n, b_n) :
 $t_0 = 0, b_0 = 0$,
 $t_1 = -3/4, b_1 = -1/10^k$
 $t_{n+1} = a_n - b_n - 3/4, b_{n+1} = 2a_n b_n + 1/10^k$
 et déterminez le premier n tel que $a_n + b_n$ soit supérieur à 4.
 Les nombres n calculés seront les nombres 3, 33, 315, 3143, 31417, 314160, 3141593...

BIBLIOGRAPHIE

-P. DELAHAYE, *Le fascinant nombre Pi*, Belin, 2^e éd., 2018.

J. DUMOULIN ET F. THOUIN, A ballistic Monte Carlo approximation of π , 2014. arxiv.org/pdf/1404.1499.pdf

G. GALPERIN, Playing pool with π (the number π from a billiard point of view), *Regular and Chaotic Dynamics*, vol. 8(4), pp. 375-394, 2003.

A. KLEBANOFF, π in the Mandelbrot set, *Fractals*, vol. 9(4), pp. 393-402, 2001.

H.-H. STØLUM, River meandering as a self-organization process, *Science*, vol. 271, pp. 1710-1713, 1996.

L'exploit est inouï, mais, une fois encore, c'est un jeu: au bout de plusieurs heures de fonctionnement avec mon ordinateur, la configuration d'Adam Goucher a réussi à écrire 3,14159265. L'obtention d'autres décimales demanderait des jours ou des semaines. Le calcul utilise un produit infini et progresse en $O(n^6)$, ce qui veut dire que s'il faut k heures de calcul pour avoir n décimales, en avoir le double demandera $2^6 = 64$ fois plus de temps, à supposer que la mémoire disponible sur l'ordinateur ne fasse pas défaut.

π NE COULE PAS DE SOURCE!

Pour terminer, signalons deux méthodes illusoire de calcul de π , parfois présentées comme sérieuses, mais qui en réalité ne vous donneront jamais rien.

La première pourrait être qualifiée de géographique. Dans un article publié dans la revue *Science* en mars 1996, Hans-Henrik Stølum, de l'université de Cambridge, décrit un modèle d'écoulement des cours d'eau. Il tire de son modèle l'affirmation qu'en moyenne, le rapport entre la longueur d'un fleuve et la distance à vol d'oiseau entre la source et l'endroit où le fleuve se jette à la mer est le nombre π . En se fondant sur ce résultat, on pourrait donc tenter de calculer π en prenant un grand nombre de fleuves, et en calculant la moyenne des rapports entre leur longueur et la distance parcourue à vol d'oiseau entre la source et l'embouchure.

Malheureusement, tous ceux qui, à partir de bases de données géographiques ont essayé, arrivent à des valeurs sensiblement plus petites que π . Il semble bien que le modèle théorique soit inexact.

L'autre méthode illusoire est celle liée à la théorie économique de Martin Armstrong. Cet Américain est l'auteur d'une théorie (*Economic Confidence Model*) selon laquelle l'économie est soumise à des ondes cycliques tous les 8,6 ans et que les prendre en compte permet de prévoir les crises. La durée de 8,6 ans correspond à 3 141 jours, soit 1000 π . On a du mal à comprendre ce que π , avec une précision de 4 chiffres, vient faire dans les cycles économiques, mais Martin Armstrong prétend avoir annoncé, grâce à sa théorie, la crise de 1987 au jour près.

Plus récemment, Martin Armstrong avait annoncé une nouvelle crise pour le 1^{er} octobre 2015. Elle ne s'est pas produite! Tout cela ne semble pas très sérieux et, si les mathématiciens sont bien persuadés de l'importance et de l'ubiquité de π , ils n'ont pas la naïveté de croire en de telles théories dont, d'ailleurs, aucune justification n'est présentée. C'est un plaisir de jouer avec π et de le découvrir partout, mais c'est avant tout un amusement qu'il est sage de ne pas transformer en superstition numérolologique.

LA STAR DES MATHÉMATIQUES ET DE LA PHYSIQUE



belin-editeur.com



Belin:

Jouons avec les palindromes

121, 404, 123 454 321... faciles à identifier, les nombres palindromes offrent des problèmes de tous niveaux et quelques défis ardu.

ESSENTIEL

Les nombres palindromes sont une infinité et on sait parfaitement les dénombrer.

On connaît des formules qui engendrent une infinité de nombres palindromes.

Les nombres premiers palindromes

sont probablement une infinité, mais on ne sait pas les dénombrer.

Le plus beau résultat récemment établi au sujet des nombres palindromes est que tout entier est la somme de trois nombres palindromes

VAUTEUR



JEAN-PAUL DELAHAYE est professeur émérite à l'université de Lille et chercheur au Centre de recherche en informatique, signal et automatique de Lille (Cristal).

L

es mots «gag», «elle», «rotor» sont des palindromes: ils se lisent de droite à gauche aussi bien que de gauche à droite. «Ressasser» et «rotavator» sont les plus longs mots palindromes en français. Allons plus loin. En négligeant les espaces, les accents, les majuscules et la ponctuation, on sait composer des phrases et même des textes palindromes: *Élu par cette crapule* (Hippolyte Laverdan); *Rue Verlaine gela le génial rêveur* (Jacques Perry-Salkow); *Éric notre valet alla te laver ton ciré* (Maître Capelo qui ajoutait que Luc pouvait remplacer Éric)...

4321

Georges Perec a composé un texte palindromique de 1247 mots. Plus récemment, Frédéric Schmitter et Jacques Perry-Salkow ont écrit un récit palindromique, *Sorel Éros*, qui comporte 10001 lettres. Romain Seignovert a trouvé des palindromes pour toutes les langues européennes (voir figure ci-dessous).

Jolis exploits mais qui ne concernent guère le mathématicien. Ce dernier préfère envisager les nombres palindromes. En trouver est facile, puisque toute suite de chiffres ne commençant pas par 0 est un nombre et qu'on peut donc sans difficulté en écrire qui soient des palindromes: 242, 10001 ou 12321. Leur liste, bien sûr infinie, se programme aisément. C'est la suite A002113 de l'encyclopédie en ligne des suites numériques OEIS (<https://oeis.org/A002113>) l'encyclopédie des suites de nombres entiers. En voici le début: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 11, 22, 33, 44, 55, 66, 77, 88, 99, 101, 111, 121, 131, 141, 151, 161, 171, 181, 191, 202, 212, 222, 232, 242, 252, 262, 272, 282, 292, 303, 313, 323, 333, 343...

Les jeux et problèmes que les mathématiciens envisagent à propos des nombres palindromes sont aussi variés et difficiles que ceux d'autres pans de la discipline... et certains restent irrésolus.

COMBIEN SONT-ILS ?

Commençons par des questions faciles. Combien existe-t-il de nombres palindromes en base 10 composés de n chiffres? Si n est pair, pour avoir un nombre palindrome à n chiffres décimaux, il suffit de choisir comme on le veut les $n/2$ premiers chiffres en imposant que le premier ne soit pas 0, et de les répéter en ordre inverse. Pour $n = 6$, on choisit par exemple 247, qui donne 247742. On en déduit que le nombre de palindromes à n chiffres, n pair, est exactement $9 \times 10^{n/2-1}$, soit 900 pour $n = 6$.

Pour $n = 1$, il y a 10 nombres palindromes: 0, ..., 9. Si n est impair supérieur à 1, en raisonnant

L'Europe des palindromes. Romain Seignovert, fervent défenseur de l'idée d'une Europe unie, propose cette carte où chaque pays porte un palindrome dans sa langue.



comme dans le cas pair, on trouve que le nombre de palindromes à n chiffres est $9 \times 10^{(n-1)/2}$. On en tire que le nombre de nombres palindromes inférieurs à 10^n pour $n = 1, 2, 3, 4...$ est, respectivement: 10, 19, 109, 199, 1099, 1999, 10999, 19999... (ce qui est toujours supérieur à $10^{n/2}$).

Leur densité (leur fréquence) devient nulle à l'infini et elle est sensiblement inférieure à celle des nombres premiers, ce que l'on démontre ou que l'on constate en examinant le nombre de nombres premiers inférieurs à 10^n pour $n = 1, 2, 3, 4, ...$ qui est 4, 25, 168, 1229,

9592, 78498, 664579, 5761455... (en ordre de grandeur: $10^n/n$). La série des inverses des nombres palindromes converge vers la limite 8,37018..., alors que la série des inverses des nombres premiers a une somme infinie, marque d'une densité assez forte.

Autre propriété élémentaire: si un nombre palindrome est formé d'un nombre pair de chiffres, alors il est divisible par 11, et n'est donc pas un nombre premier (sauf 11 lui-même). Pour le démontrer, on applique le critère de divisibilité par 11: «Un entier est divisible par 11 si et seulement si la différence entre la somme de ses chiffres de rang pair et la somme de ses chiffres de rang impair est un multiple de 11» (par exemple, 915123 est un multiple de 11 puisque $(9+5+2) - (1+1+3) = 11$). Pour un nombre palindrome N ayant un nombre pair de chiffres, les deux sommes en question sont égales; leur différence est nulle, donc N est multiple de 11.

Quittons les rivages de la facilité... Qu'en est-il des nombres palindromes ayant un nombre impair de chiffres? Peuvent-ils être des nombres premiers? Plus généralement, qu'en est-il des diviseurs des nombres palindromes?

Voici d'abord le début de la suite des nombres premiers palindromes (<https://oeis.org/A002385>): 2, 3, 5, 7, 11, 101, 131, 151, 181, 191, 313, 353, 373, 383, 727, 757, 787, 797, 919, 929, 10301, 10501, 10601, 11311, 11411, 12421, 12721, 12821, 13331, 13831, 13931, 14341... Le plus grand nombre premier palindrome connu aujourd'hui est $10^{474500} + 999 \times 10^{237249} + 1$, qui est formé de 474 501 chiffres.

On cherche à démontrer qu'il existe une infinité de nombres premiers palindromes. Cela semble probable, car les deux propriétés «être un nombre premier» et «être un palindrome», au moins pour les nombres composés d'un nombre impair de chiffres, semblent indépendantes. Cependant, cette intuition un peu vague n'a pas pu être confirmée par une démonstration et donc l'affirmation «Il existe une infinité de nombres premiers palindromes» reste une conjecture.

Il existe des méthodes pour construire des nombres palindromes qui ne sont pas des nombres premiers. En voici une.

$1 \times 1 = 1$
 $11 \times 11 = 121$
 $111 \times 111 = 12321$
 $1111 \times 1111 = 1234321$
 $11111 \times 11111 = 123454321$
 $111111 \times 111111 = 12345654321$
 $1111111 \times 1111111 = 1234567654321$
 $11111111 \times 11111111 = 123456787654321$
 $111111111 \times 111111111 = 12345678987654321$

Malheureusement, la méthode ne fonctionne plus au-delà, car $1111111111 \times 1111111111 = 1234567900987654321$.

Le sixième des nombres de cette série est vraisemblablement le premier palindrome à avoir attiré l'attention d'un mathématicien. En effet, il est mentionné par Mahāvīra, un mathématicien indien du IX^e siècle. Dans son ouvrage en sanskrit *Ganita-sāra-sangraha*, il évoque ce carré parfait en le décrivant comme un nombre «commençant par 1 et allant jusqu'à 6, puis décroissant en ordre inverse».

Une série de formules donnent elles une infinité de nombres palindromes composés

$11 \times 11 \times 11 = 1331$
 $11 \times 11 \times 111 = 13431$
 $11 \times 11 \times 1111 = 134431$
 $11 \times 11 \times 11111 = 1344431$
 $11 \times 11 \times 111111 = 13444431$

Ajoutons encore deux séries infinies:
 $11 \times 111 \times (11 \dots 11) = 13566 \dots 66531$
 $111 \times 111 \times (11 \dots 11) = 136899 \dots 9998631$

FACTEURS ET NOMBRES PREMIERS

William Banks a démontré que des nombres palindromes ont un nombre de facteurs premiers aussi grand que souhaité. Des nombres palindromes ont donc, par exemple, plus de 1000 facteurs premiers. Il a aussi établi que des nombres palindromes ont des facteurs premiers aussi longs qu'on le désire; ainsi, des nombres palindromes ont un facteur premier composé de plus de 1 million de chiffres.

Une autre étude, cette fois de William Banks, Derrick Hart et Mayumi Sakata, établit que la proportion d'entiers premiers parmi les

LES NON-PALINDROMES

Les nombres strictement non palindromes sont, par définition, les entiers n qui ne sont

avec $2 \leq b \leq n-2$. On impose la limite $b-2$ car, en base $n-1$, le nombre n s'écrit 11 et est donc toujours palindrome. La suite des nombres strictement non palindromes commence par: 0, 1, 2, 3, 4, 6, 11, 19, 27, 53, 79, 103, 137, 139, 149, 163, 167, 179, 223, 263, 269, 283, 293... qui est la suite A016038 de l'encyclopédie des suites numériques de Neil Sloane. Une propriété intéressante des nombres strictement non palindromes est que ce sont tous des nombres premiers, à l'exception de 4 et 6. En voici la démonstration.

On se donne un nombre composé quelconque $n \geq 6$ et on montre que n est

palindrome dans une base bien choisie.

Si n est pair, n s'écrit 22 dans la base $b = n/2 - 1$, car $n = 2(n/2 - 1) + 2$.

Si n est impair, on écrit $n = pm$, où p est le plus petit facteur premier de n . Nécessairement, $p \leq m$.

Si $p = m = 3$, alors $n = 9$ s'écrit 1001 en base $b = 2$.

Si $p = m > 3$, alors n s'écrit 121 en base $b = p-1$, car $121_{p-1} = 1 + 2(p-1) + (p-1)^2 = 1 + 2p - 2 + p^2 - 2p + 1 = p^2 = n$.

Le cas $p = m-1$ est impossible, car p et m sont impairs.

Si $p < m-1$, alors n est le palindrome pp en base $b = m-1$, car $p(m-1) + p = pm$.

On contrôle à chaque fois que la base proposée vérifie $2 \leq b \leq n-2$ et que les chiffres du palindrome proposé sont des nombres entiers entre 0 et $b-1$.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
1																				
2	5643																			
3		10																		
4		3	2	4																
5			2	4	5															
6		3		3	2	2														
7			2	5	8	152	12													
8		2	10	10	105	30	10	152												
9	10	3	2	3	3	3	2	2	19											
10		25	242	25	4	160	2	3	50	23										
11		5	8	5	2	102	8	5	2	18	27									
12		31	2	4	2	23	152	10	22	32	32									
13		4	1210	4	108	13	13	4	30	32	50	25	375							
14		59	7	26	161	30	7	37	30	32	48	24	117	136						
15		7	5	7	119	18	3	70	13	35	22	117	70	37	19					
16		14	182	14	8	211	10	8	52	25	7	290	27	20	42	567				
17		32	173	8	9	205	9	32	205	17	13	462	205	32	16	13	53			
18		181	20	112	128	30	10	260	20	567	50	167	40	50	30	112	180	102		
19	20	2	1602	2	126	2	1942	5	27	257	32	161	9	101	12	77	127	14	18	

Le nombre de premiers nombres palindromes tend vers 0 quand n croît. On sait, d'après le théorème d'Hadarnard et de La Vallée-Poussin, que la proportion de nombres premiers parmi les n premiers entiers est environ $1/\ln(n)$, où $\ln(x)$ désigne le logarithme népérien de x . On conjecture donc, sans toutefois savoir le démontrer, un résultat analogue pour les nombres palindromes: la proportion d'entiers premiers parmi les n premiers nombres palindromes serait $1/\ln(n)$.

Une conjecture intéressante a été imaginée en 2014 par Ivan Ianakiev: les seuls nombres palindromes premiers dont le numéro d'ordre dans la suite des nombres premiers est un nombre premier palindrome sont 3 (qui est deuxième), 5 (qui est troisième) et 11 (qui est cinquième). La conjecture a été testée pour les huit premiers millions de nombres premiers ayant des numéros d'ordre qui sont des nombres premiers palindromes.

Par jeu, le mathématicien brésilien-canadien Paulo Ribenboim a proposé de dénommer «nombre premier triplement palindrome» un nombre premier palindrome de m chiffres décimaux, où m est un nombre premier palindrome de n chiffres décimaux, où n est lui-même un

Voici les plus petits entiers palindromes dans deux bases a et b la fois, a et b variant de 2 à 20 ($a < b$). Ce tableau a été établi par Rich Friedman. Ainsi, pour $a = 2$ et $b = 3$, il faut aller jusqu'à 6 643 pour trouver un nombre qui convient: $6643_{10} = 110011111011_2 = 100101001_3$.

nombre premier palindrome. Le plus petit de ces nombres, nécessairement rares, est 10 000 500 001, qui comporte 11 chiffres; 11 est un nombre premier palindrome lui-même constitué de 2 chiffres, 2 étant un nombre premier palindrome.

Plus intéressant, $10^{11510} + 4661664 \times 10^{632} + 1$ est formé de 11311 chiffres, le nombre 11311 étant un nombre premier palindrome qui a lui-même 5 chiffres, 5 étant encore un nombre premier palindrome. Bien évidemment, on ignore s'il existe une infinité de ces nombres premiers triplement palindromes.

La notion de nombre palindrome dépend bien sûr de la base de numération, et jusqu'ici nous n'avons envisagé que la base 10. Que se passe-t-il pour les autres bases?

CHANGÉONS LES BASES

Les calculs du nombre de palindromes faits pour la base 10 se généralisent à toute base $b > 1$. La propriété «Les palindromes ayant un nombre pair de chiffres en base 10 sont multiples de 11» devient: «Les palindromes ayant un nombre pair de chiffres en base b sont multiples de $(b+1)$ ». Par exemple, le nombre N dont l'écriture en base 5 est 123321₅ est divisible par 6: $123321_5 = 5^5 + 2 \times 5^4 + 3 \times 5^3 + 3 \times 5^2 + 2 \times 5^1 + 1 = 4836 = 806 \times 6$.

Nombre de chiffres	Formule	Palindrome
1		9
2	$9 + 2$	11
3	$9 \times 7 + 2$	343
4	$9 \times (9 \times 9 + 2)$	747
5	$9 \times 9 \times 9 \times 9 - 5$	6 556
6	$9 \times 7 \times 7 \times 8 \times 8 \times 8$	65 856
7	$9 \times 8 \times 8 \times 8 \times 9 \times (9 + 2)$	405 504
8	$9 \times 9 \times 9 \times 9 \times 9 \times 9 - 2$	4 251 524
9	$8 \times 8 \times (5 \times 6 \times 8 \times 8 \times 9 + 2)$	8 847 488
10	$9 \times 7 \times 7 \times 8 \times (7 \times 8 \times 8 \times 9 - 4)$	88 499 488
11	$6 \times 8 \times 8 \times 8 \times 9 \times (6 \times 7 \times 9 \times 9 + 8)$	846 747 648
12	$9 \times 8 \times 8 \times 8 \times 9 \times (4 \times 7 \times 7 \times 9 \times 9 - 3)$	4 095 995 904
13	$9 \times 9 \times 9 \times 9 \times 9 \times (6 \times 7 \times 7 \times 9 \times 9 - 8)$	68 899 199 886
14	$(9 \times 9 \times 9 \times 9 \times 5 + 4) \times (8 \times 8 \times 8 \times 8 \times 9 - 5)$	97 955 055 979
15	$9 \times 8 \times (5 \times 9 \times 9 \times 9 \times 9 - 7) \times (8 \times 9 \times 9 \times 9 \times 9 - 7)$	867 685 586 768

A VOS CRAYONS !

On recherche les combinaisons de chiffres qui, multipliés ou additionnés en utilisant

qu'on veut, donnent le plus grand nombre palindrome.
Par exemple, avec 4 chiffres, la formule $9 \times (9 \times 9 + 2)$ donne 747, qui est le plus grand nombre palindrome.

qu'on peut obtenir ainsi.
Le tableau ci-dessus est dû à Erich Friedman (www2.stetson.edu/~efriedma/mathmagic/0699.html).
Saviez-vous le poursuivre ?
Ces résultats sont prouvés jusqu'à 15 chiffres utilisés. Le Français Marc Lapiere a mené les calculs pour les trois dernières lignes.

Une étrange curiosité a été notée pour le nombre 5 et la base 24. Parmi les petites puissances de 5, 10 sont des palindromes en base 24: $5^0 = 1_{24}$; $5^1 = 5_{24}$; $5^2 = 11_{24}$; $5^3 = 55_{24}$; $5^4 = 121_{24}$; $5^5 = 5A5_{24}$; $5^6 = 1331_{24}$; $5^7 = 5FF5_{24}$; $5^8 = 14641_{24}$; $5^9 = 15151_{24}$ (en base 24, on convient de noter les 24 chiffres 0, 1, 2, ..., 7, 8, 9, A, B, C, ..., L, M, N, ce qui explique la présence des lettres dans ces formules).

Une question vient naturellement à l'esprit: « Existe-t-il des nombres n qui sont palindromes dans plusieurs bases de numération b à la fois? » Remarquons d'abord que si n est un nombre quelconque, il est palindrome dans toutes les bases b où $b > n$, car n s'y écrit alors avec un seul chiffre. C'est un peu facile! Il n'est donc intéressant que de considérer des bases $b \leq n$.

La question devient: « Existe-t-il des nombres n qui sont palindromes dans plusieurs bases de numération b à la fois, avec $b < n$? » Une petite exploration montre aisément que oui. Un bel exemple est 105. En effet: $105_{10} = 1221_4 = 151_8 = 77_{14} = 33_{34}$. Le tableau de la figure 3 donne les plus petits entiers palindromes dans deux bases a et b à la fois, pour a et b variant de 2 à 19. Il a été établi par Erich Friedman, de l'université Stetson, en Floride.

Il est aussi intéressant de savoir si les nombres de la suite F_n de Fibonacci ($F_0 = 1$, $F_1 = 1$, $F_n = F_{n-2} + F_{n-1}$ pour $n > 1$) sont parfois des palindromes. Les seuls connus jusqu'à présent sont 0, 1, 1, 2, 3, 5, 8, 55. On démontre que la densité des entiers n tels que F_n est un palindrome est nulle à l'infini, mais on se demande si en réalité les termes palindromes de la suite cités au-dessus ne sont pas les seuls: encore une conjecture!

En additionnant trois nombres premiers au plus, on peut obtenir tout entier impair. C'est la « conjecture faible de Goldbach », qui est maintenant un théorème puisqu'elle a été démontrée en 2013 par le mathématicien péruvien Harald Helfgott, chercheur du CNRS à Paris. Lorsqu'on additionne deux nombres premiers, il semble possible d'obtenir tout nombre pair à partir de 4. C'est la fameuse conjecture de Goldbach qui, elle, attend toujours une démonstration.

LES SOMMES DE PALINDROMES

Qu'en est-il des sommes de nombres palindromes? Donnent-elles tous les entiers? Combien faut-il de palindromes pour obtenir tout entier dans le pire cas? Les nombres palindromes étant plus faciles à maîtriser que les nombres premiers, on connaît aujourd'hui les réponses à ces questions.

Le premier résultat est que les sommes de deux nombres palindromes ne donnent pas tous les entiers. Voici la suite des nombres entiers (la suite A035137 de l'encyclopédie de Neil Sloane) qui ne s'écrivent pas comme la somme de deux palindromes: 21, 32, 43, 54, 65, 76, 87, 98, 201, 1031, 1041, 1042, 1051, 1052, 1053, 1061, 1062, 1063, 1064, 1071, 1072, 1073, 1074, 1075, 1081, 1082, 1083.

Comment le vérifier? On considère les $n+1$ façons d'écrire n comme une somme $a+b$ de deux entiers, et on constate que a et b ne sont jamais simultanément palindromes.

Joseph DeVincentis et Ulrich Schimke ont démontré qu'il existe une infinité d'entiers qui ne sont pas somme de deux nombres palindromes. L'affaire est entendue: en effectuant la somme de deux nombres palindromes, on n'obtient qu'une petite partie des entiers.

Le plus beau résultat concernant les sommes de palindromes est récent, mais lui aussi tout aussi définitif: « Tout nombre entier est somme de trois nombres palindromes au plus. » Le nombre 2000, par exemple, est la somme de 516, 383 et 1001. Le résultat a été obtenu en deux temps. D'abord, en 2015, William Banks a démontré qu'en base 10, tout entier est somme d'au plus 49 nombres palindromes. Il semblait alors qu'on était au début d'une série de résultats où, progressivement, on remplacerait 49 par des entiers de plus en plus petits.

En fait, l'affaire fut magistralement traitée d'un seul coup. Javier Cilleruelo, de l'université

LESSSENTIEL

Le énoncé est simple: « Quand on part d'un entier positif n quelconque et que, de manière répétée, on le divise par 2 s'il est pair et on le remplace par $3n+1$ s'il est impair, on finit toujours par tomber sur 1. »

Pourtant, cette conjecture dite le Syracuse, ou $3n+1$, n'a toujours pas été démontrée. Mais elle a été vérifiée jusqu'à $n = 5 \times 10^{18}$.

De nombreux travaux portent sur des variantes du problème ou sur certaines parties, notamment sur la longueur des cycles dans les valeurs rencontrées.

La longueur d'un tel cycle est soit 3 soit supérieure à 17 026679261 ! La démonstration de ce résultat est déjà une prouesse.

L'AUTEUR



SHALOM ELIAHOU est professeur à l'université du Littoral Côte d'Opale, à Calais.

26

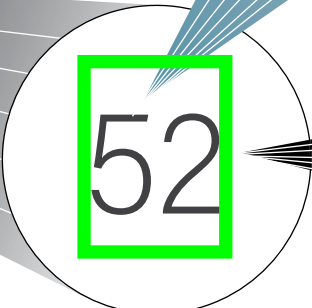
13

40

10

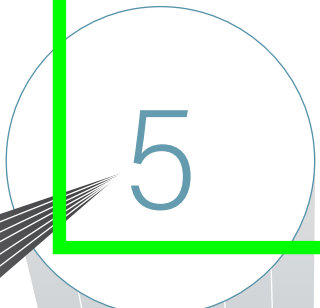
20

Prenez un nombre quelconque. S'il est pair, divisez-le par 2, sinon multipliez-le par 3 et ajoutez 1. Puis recommencez avec le nouveau nombre obtenu. Vous tomberez toujours sur 1. Enfin, on le suppose, car on n'a jamais su le démontrer.



52

Élémentaire, mais redoutable



5

Parmi tous les problèmes mathématiques actuellement non résolus, quel est celui dont l'énoncé est le plus élémentaire ? C'est peut-être bien la conjecture de Syracuse : accessible à tous dans son énoncé, elle défie les chercheurs depuis des décennies.

D

ans les années 1960, une conjecture a occupé tant de mathématiciens que, dans l'ambiance de la guerre froide, certains y ont vu une conspiration soviétique destinée à détourner les esprits américains. Cette conjecture a reçu les noms Collatz, Kakutani, $3n+1$, Syracuse... Et c'est sous ce dernier qu'elle est la plus connue, car l'université de Syracuse (rien à voir avec la Sicile), aux États-Unis, a joué un rôle important dans la popularisation du problème.

Pourquoi est-il si célèbre ? Sans doute parce que le problème $3n+1$ offre un contraste saisissant : il est d'un côté extrêmement simple à énoncer et de l'autre, particulièrement difficile à résoudre. De quoi s'agit-il ? On définit la règle de transformation sur les nombres entiers $1, 2, 3, \dots$ suivante : étant donné un entier naturel n non nul quelconque, si n est pair, on le divise par 2 ; si n est impair, on le multiplie par 3 et on ajoute 1 ($3n+1$). Par exemple, avec le nombre 14, cette transformation donne 7 ; et appliquée à 7 elle donne 22. On écrira $14 \rightarrow 7 \rightarrow 22$, et plus généralement $n \rightarrow m$ si appliquée à n elle donne m . La transformation est dite de Collatz, du nom de son inventeur, dans les années 1930 semble-t-il.

Le problème $3n+1$ se pose en ces termes : partons d'un nombre entier positif quelconque, et appliquons-lui cette transformation de façon répétée (on parle de trajectoire).

Est-il vrai que l'on finira tôt ou tard par tomber sur 1? Tous les calculs faits à ce jour confirment cette prédiction. Mais voilà, personne jusqu'à présent ne sait comment la démontrer, et ce n'est pas faute d'avoir essayé. D'ailleurs, selon le grand Paul Erdős, les mathématiques ne seraient pas encore assez mûres pour espérer résoudre cet innocent petit problème. En 1995, en Hongrie, j'ai essayé d'engager une discussion avec lui sur ce problème. Sa réaction fut sans appel: «C'est sans espoir».

Duelques exemples s'imposent. Partons d'abord de 1 lui-même. Sa trajectoire est

$1 \rightarrow 4 \rightarrow 2 \rightarrow 1 \rightarrow 4 \rightarrow 2 \rightarrow 1 \rightarrow \dots$

On obtient un cycle de longueur 3 ($1 \rightarrow 4 \rightarrow 2$) qui se répète. Ce cycle est dit trivial.

Second exemple, en partant de $n = 3$, on retrouve le même cycle.

$3 \rightarrow 10 \rightarrow 5 \rightarrow 16 \rightarrow 8 \rightarrow 4 \rightarrow 2 \rightarrow 1 \rightarrow \dots$

Enfin, avec $n = 7$, on obtient:

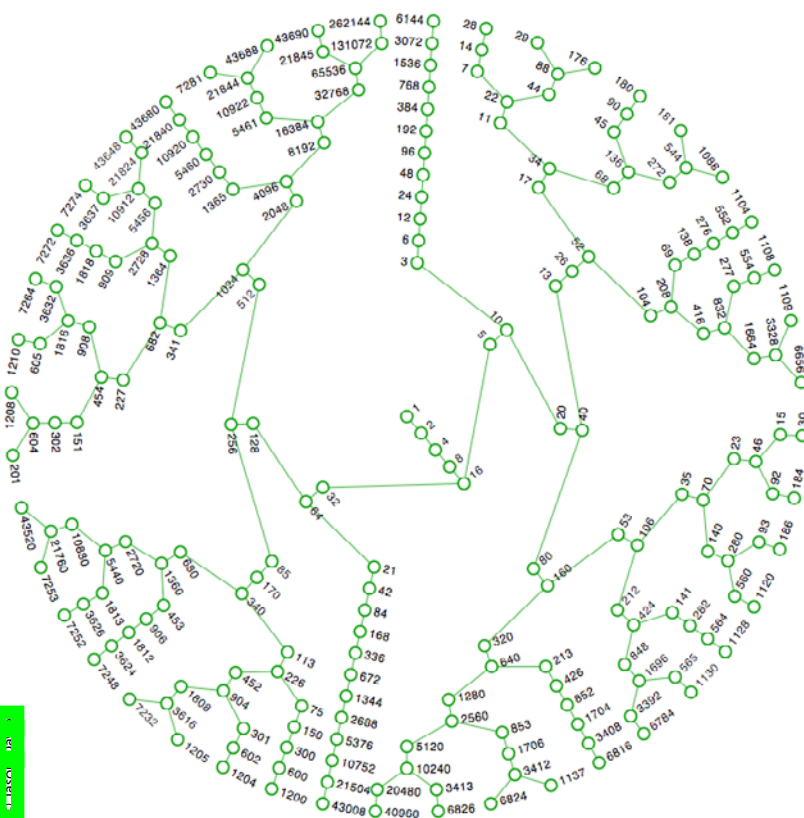
$7 \rightarrow 22 \rightarrow 11 \rightarrow 34 \rightarrow 17 \rightarrow 52 \rightarrow 26 \rightarrow 13 \rightarrow 10 \rightarrow 20 \rightarrow 10 \rightarrow 5 \rightarrow 16 \rightarrow 8 \rightarrow 4 \rightarrow 2 \rightarrow 1 \rightarrow \dots$

Encore 1!

Certaines trajectoires sont spectaculaires et valent le détour. Celle de $n = 27$, par exemple, est une montagne russe qui monte vers des hauteurs inattendues (jusqu'à 9232). Mais rien n'y fait, après 111 étapes (c'est la durée de vol), elle retombe sur 1. Vous pouvez expérimenter ici: <http://l.pellegrino.free.fr/vracuse/index.php>

Depuis 2009, Tomás Oliveira e Silva, de l'université d'Aveiro, au Portugal, détient le

Cet arbre relie les nombres qui, par la transformation de Collatz, aboutissent à 1 via des trajectoires inférieures à 20 étapes.



sur $3 \times (-1) + 1 = -2$ par la transformation de Collatz. De même, on a $-2 \rightarrow -1$. On observe ainsi, sur les entiers négatifs, un cycle de longueur 2. Or là, surprise, ce n'est pas le seul! On en connaît même deux autres:

La trajectoire de -5 est un cycle de longueur 5: $-5 \rightarrow -14 \rightarrow -7 \rightarrow -20 \rightarrow -10 \rightarrow -5...$ Quant à -17 , il donne un cycle de longueur 18 (voir la figure ci-contre). Cette présence de trois cycles différents sur les entiers négatifs (on pense que ce sont les seuls) rend d'autant plus intéressante la prédiction selon laquelle il n'y aurait qu'un seul cycle sur les entiers positifs.

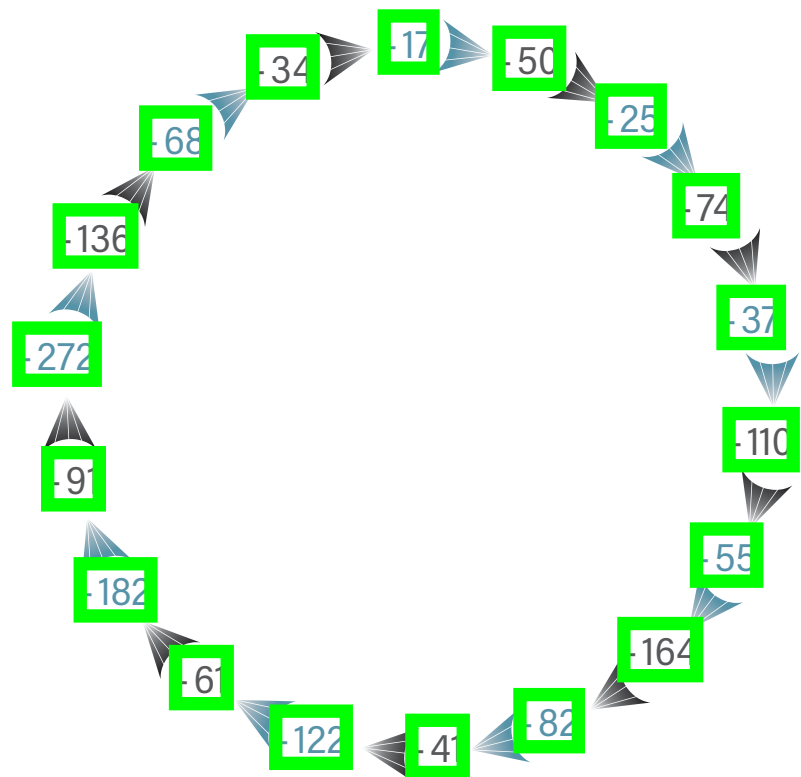
DIVERGENTE OU NON ?

Une variante de la transformation de Collatz, où l'on remplace $3n+1$ par $5n+1$, illustre simultanément les deux sous-problèmes (voir l'encadré ci-dessous). La différence est légère... et pourtant!

Pourquoi semble-t-il y avoir des trajectoires divergentes avec $(5n+1)/2$, mais pas avec $3n+1$ ni avec, ce qui revient au même, $(3n+1)/2$? Ce ne sont encore que des observations empiriques qui demandent à être formellement prouvées; mais d'où peut bien venir cette différence de comportement?

Voici une explication intuitive possible, fondée sur quelques approximations, une hypothèse osée mais plausible et, en fin de compte, sur le fait que $5/4$ est supérieur à 1 alors que $3/4$ ne l'est pas.

Cheminons le long de la trajectoire de 7 par exemple, d'abord pour la transformation $\rightarrow$. Pour passer d'un terme au suivant, on le multiplie par $1/2$ s'il est pair, ou par environ $5/2$ s'il



Avec des nombres négatifs, la transformation de Collatz peut créer des cycles, ici de longueur 18.

est impair. Admettons que, lors de ce cheminement, on rencontre à peu près autant de pairs que d'impairs (c'est l'hypothèse osée!). Alors, si l'on marche jusqu'au 21 millionième terme par exemple, celui-ci devrait valoir environ: $7 \times (1/2)^{10500000} \times (5/2)^{10500000}$, soit $7 \times (5/4)^{10500000}$.

Or $5/4$ étant plus grand que 1, ses puissances successives grandissent sans limites. Le nombre ci-dessus compte d'ailleurs 1017556 chiffres avant la virgule, ce qui en fait une assez bonne approximation du vrai 21 millionième terme de la trajectoire de 7 avec ses 1016568 chiffres.

En revanche, le même raisonnement avec la transformation $\rightarrow$ ferait intervenir une grosse puissance de $3/4$. Celui-ci étant inférieur à 1, ses puissances successives tendent vers 0. C'est cela qui semble empêcher l'existence de trajectoires divergentes pour la transformation de Collatz.

Parmi les résultats partiels connus sur le problème $3n+1$, l'un affirme que si, contre toute attente, il existait un cycle autre que $(1 \rightarrow 4 \rightarrow 2)$, de longueur 3, alors il serait forcément gigantesque. Un théorème précise les choses: la transformation de Collatz n'admet, sur les entiers positifs, aucun cycle de longueur comprise entre 4 et environ 17000000000.

Comment prouver une telle affirmation? D'abord, en montrant qu'il n'existe aucun cycle de longueur 5 pour la transformation de Collatz sur les entiers positifs. L'intérêt de cette preuve est d'être assez élémentaire, tout en contenant déjà l'idée essentielle pour la suite: la mise en évidence d'une équation très contraignante associée à un cycle. Pour la longueur 5,

LA VARIANTE $5n+1$

Pour étudier les cycles et la divergence du problème $3n+1$, on peut s'intéresser à une variante: $5n+1$. En fait, pour accélérer un peu le cheminement dans les trajectoires, on remplace $5n+1$ par $(5n+1)/2$ si n est pair, et $5n+1$ si n est impair.

Si n est impair, on l'envoie sur $(5n+1)/2$. On utilisera le symbole $\rightarrow$ pour dénoter cette nouvelle transformation. Voici par exemple la trajectoire de 1: $1 \rightarrow 3 \rightarrow 8 \rightarrow 4 \rightarrow 2 \rightarrow 1...$ Un beau cycle de longueur 5.

Voici un autre cycle, cette fois de longueur 7:

$3 \rightarrow 33 \rightarrow 83 \rightarrow 208 \rightarrow 104 \rightarrow 52 \rightarrow 26 \rightarrow 13...$ Partons maintenant de $n=7$.

À un nouveau phénomène se manifeste. En effet, les 16 premiers termes de la trajectoire sont:

$7 \rightarrow 18 \rightarrow 9 \rightarrow 23 \rightarrow 58 \rightarrow 29 \rightarrow 73 \rightarrow 183 \rightarrow 458 \rightarrow 229 \rightarrow 573 \rightarrow 1433 \rightarrow$

$3583 \rightarrow 8958 \rightarrow 4479 \rightarrow 1198$. Cela grimpe vite.

Allons un peu plus loin. Le 1000^e terme de cette trajectoire est:

5857007305798959806990948240228589098703203749.

Un nombre à 46 chiffres! On continue? Jonathan Chappelon a bien voulu pousser le calcul de cette trajectoire jusqu'à son 21 millionième terme.

Le nombre obtenu n'est même plus monstrueux: il a plus d'un million de chiffres exactement 1016568! Il y a donc une très forte présomption que la trajectoire de 7 diverge; mais personne à ce jour ne sait le démontrer. Pire: on pense que la plupart des trajectoires de cette transformation sont divergentes, mais personne ne sait prouver qu'il en existe au moins une qui le soit vraiment.

procédons par l'absurde, et supposons qu'un tel cycle existe. En le manipulant, on révélera une équation qui lui est associée et l'on constatera que cette équation est insoluble.

Remarquons que pour un hypothétique cycle de la transformation de Collatz sur les entiers positifs, le plus petit élément est forcément impair. En effet, notons C ce cycle et m son plus petit élément. Bien sûr, C est la trajectoire de m . Notons maintenant m' le nombre obtenu à partir de m par transformation de Collatz. Alors m' est lui aussi dans C , puisque C est la trajectoire de m , et il est plus grand que m , puisque m est minimal dans C . Or si m était pair, on aurait $m' = m/2$ qui est plus petit que m : cette contradiction montre bien que m est impair.

LE CAS DE LONGUEUR 5

L'hypothétique cycle de longueur 5 serait de la forme: $a_1 \rightarrow a_2 \rightarrow a_3 \rightarrow a_4 \rightarrow a_5 \rightarrow a_1$. Quitte à renommer les indices, on peut supposer que le plus petit est a_1 , forcément impair, nous l'avons vu, et différent de 1, puisque la trajectoire de 1 donne un cycle de longueur 3. En fin de compte, a_1 est supérieur ou égal à 3.

La transformation de Collatz appliquée aux éléments du cycle a_1, a_2, a_3, a_4 et a_5 donne la même liste décalée d'un cran (puisque c'est un cycle): a_2, a_3, a_4, a_5 et a_1 . Ce cycle est ainsi stable par transformation de Collatz. C'est évident, mais crucial pour la suite.

Pour savoir concrètement comment la transformation de Collatz agit sur $a_1 \dots a_5$, on doit savoir lesquels sont pairs et lesquels sont impairs. On sait déjà que a_1 est impair. Qu'en est-il des autres termes?

Puisque a_1 est impair, $a_2 = 3a_1 + 1$ est pair. Serait-il que $a_3 = a_2/2 = (3a_1 + 1)/2$ soit pair? Si c'était le cas, on aurait alors $a_4 = a_3/2$. En enchaînant avec ce que l'on sait sur a_2 et a_1 , on obtiendrait: $a_4 = a_3/2 = a_2/4 = (3a_1 + 1)/4$. Le terme a_4 faudrait donc environ les trois quarts de a_1 : il serait donc plus petit que a_1 (puisque celui-ci est supérieur ou égal à 3). C'est en contradiction avec la minimalité de a_1 . On conclut que a_3 est forcément impair.

En conséquence, $a_4 = 3a_3 + 1$ et il est donc pair. Et $a_5 = a_4/2$? Il est pair. En effet, a_5 doit être plus grand que a_1 . La seule possibilité est donc que a_5 soit pair et donc que $a_1 = a_5/2$. Car dans le cas contraire $(3a_5 + 1) = a_1$ serait plus grand que a_5 , ce qui est exclu. Nous connaissons maintenant l'exacte répartition des pairs et des impairs du cycle: a_1 et a_3 sont impairs; a_2, a_4 et a_5 sont pairs.

Résumons les formules obtenues en chemin, exprimant chaque terme du cycle en fonction du précédent: $a_1 = a_5/2$; $a_2 = 3a_1 + 1$; $a_3 = a_2/2$; $a_4 = 3a_3 + 1$; $a_5 = a_4/2$.

L'étape suivante consiste à prendre le produit P de ces 5 termes: $P = a_1 \times a_2 \times a_3 \times a_4 \times a_5$. Avec les formules précédentes, on obtient: $P = (a_5/2) \times (3a_1 + 1) \times (a_2/2) \times (3a_3 + 1) \times (a_4/2)$.

A partir de ces deux expressions différentes de P , on parvient à l'équation annoncée. La voici dans une première version brute:

$$a_1 \times a_2 \times a_3 \times a_4 \times a_5 = (a_5/2) \times (3a_1 + 1) \times (a_2/2) \times (3a_3 + 1) \times (a_4/2).$$

Cette équation contient des informations intéressantes, mais pour les révéler, quelques manipulations algébriques s'imposent, au terme desquelles on obtient:

$$8 = (3 + 1/a_1)(3 + 1/a_3)$$

C'est l'équation annoncée, sous sa forme épurée, associée à n'importe quel hypothétique cycle de longueur 5. Nous pouvons maintenant conclure: a_1 et a_3 étant supposés positifs, l'équation ci-dessus est impossible à satisfaire, puisqu'à droite on obtient un nombre supérieur à 9, alors qu'à gauche on n'a que 8. On vient de prouver que la transformation de Collatz n'admet aucun cycle de longueur 5 sur les entiers positifs.

Une bizarrerie reste à comprendre: le développement ci-dessus reste valable sur les entiers négatifs, à condition de remplacer les

**La conjecture
a occupé tant
de mathématiciens
américains que
certains y ont vu...
une conspiration
soviétique**

comparaisons de grandeur par des comparaisons de grandeur *en valeur absolue*. Comment se fait-il que, malgré cela, il existe bien un cycle de longueur 5 dans les entiers négatifs?

La solution de cette apparente contradiction tient à l'ultime argument de la preuve: bien qu'insoluble dans les entiers positifs, l'équation associée admet quand même des solutions dans les entiers négatifs! En effet, posons $a_1 = -5$ et $a_3 = -7$. Un calcul montre qu'on a bien $8 = (3 + 1/(-5))(3 + 1/(-7))$. Et

On retrouve bien le cycle que nous avons vu auparavant: $-5 \rightarrow -14 \rightarrow -7 \rightarrow -20 \rightarrow -10 \rightarrow -5$.

À part les trajectoires de -1 et de -5 , on connaît encore un autre cycle pour la transformation de Collatz sur les entiers négatifs. C'est la trajectoire de -17 , qui est de longueur 18.

Revenons aux entiers positifs pour lesquels on ne connaît de cycle que le trivial ($1 \rightarrow 4 \rightarrow 2$). Nous sommes désormais armés pour le théorème: la transformation de Collatz n'admet, sur les entiers positifs, aucun cycle de longueur comprise entre 4 et 17 000 000 000, et plus précisément 17 026 679 261!

DE 5 A 17 026 679 261...

Notre preuve d'exclusion de la longueur 5 pour les cycles de Collatz dans les entiers positifs repose sur deux piliers: la stabilité du cycle présumé sous l'action de la transformation de Collatz; une équation très contraignante associée à ce cycle.

Pour exclure de plus grandes longueurs de cycles, le premier ingrédient se généralise facilement. En revanche, le second avait découlé d'une description précise de la répartition des pairs et des impairs dans le cycle. Or il est illusoire d'espérer obtenir une telle description en longueur supérieure, pour des raisons d'explosion combinatoire. Comment surmonter cet obstacle? Grâce à un petit saut dans l'abstraction, en acceptant d'introduire une notation spécifique distinguant les pairs des impairs dans le cycle présumé.

Pour un hypothétique cycle de Collatz C ($a_1 \rightarrow a_2 \rightarrow a_3 \dots a_N \rightarrow a_1$) dans les entiers positifs de longueur N , on notera p le nombre d'éléments pairs et q le nombre de ses éléments impairs. On ignore tout *a priori* de p et q , si ce n'est qu'ils satisfont l'égalité $p + q = N$. Poursuivant sur notre lancée, on notera $b_1 \dots b_p$ la liste des éléments pairs de C , et $c_1 \dots c_q$ celle de ses éléments impairs. Enfin, m sera le plus petit élément de C . Forcément impair, ce nombre jouera un rôle particulier. Que deviennent dans ce cadre plus général, les deux piliers de la preuve?

Le premier est la stabilité. Si l'on applique la transformation de Collatz à la liste des éléments du cycle C , on retombe sur la liste d'origine, juste décalée cycliquement d'un cran. Le cycle C est donc bien stable par transformation de Collatz.

Le second ingrédient est l'équation associée au cycle C . On ignore comment se répartissent les termes pairs $b_1 \dots b_p$ et impairs $c_1 \dots c_q$ dans C . Mais, en les agrégeant, la liste $b_1 \dots b_p, c_1 \dots c_q$ obtient n'est rien d'autre qu'un réarrangement de la liste des éléments de C . Or, celle-ci est globalement stable par transformation de Collatz. De plus, on sait exactement ce que donne cette transformation sur chacun des termes b_i et c_j , puisqu'on connaît leur parité! Faisons-le. En appliquant la transformation de Collatz à la liste $b_1 \dots b_p, c_1 \dots c_q$, on obtient $b_1/2 \dots b_p/2, 3c_1 + 1 \dots 3c_q + 1$.

Ces deux listes contiennent exactement les mêmes éléments à l'ordre près, ceux de C .

Pour l'équation, comme pour le cycle de longueur 5, prenons le produit P des termes de C . En utilisant chacune des deux listes ci-dessus représentant C , on obtient à nouveau deux expressions de P : $P = b_1 \times b_2 \dots b_p \times c_1 \times c_2 \dots c_q$ et $P = b_1/2 \times b_2/2 \dots b_p/2 \times (3c_1 + 1) \times (3c_2 + 1) \dots (3c_q + 1)$. De cette double expression, on déduit l'équation associée à C , dans sa version brute: $b_1 \times b_2 \dots b_p \times c_1 \times c_2 \dots c_q = b_1/2 \times b_2/2 \dots b_p/2 \times (3c_1 + 1) \times (3c_2 + 1) \dots (3c_q + 1)$.

Après quelques manipulations algébriques, l'équation devient, sous une forme épurée:

$$2^p = (3 + 1/c_1) (3 + 1/c_2) \dots (3 + 1/c_q).$$

Pour $N = 3$, on a le cycle trivial ($1 \rightarrow 4 \rightarrow 2$). On voit que $p = 2$ et $q = 1$, la liste des impairs se réduisant à $c = 1$. On vérifie que $2^2 = (3 + 1/1)$.

Pour $N = 5$, en supposant que le minimum du cycle est a_1 , on avait trouvé trois pairs (a_2, a_4 et a_5) et deux impairs (a_1 et a_3), donnant donc $p = 3$ et $q = 2$. On retrouve l'équation $8 = (3 + 1/a_1) (3 + 1/a_3)$ avec laquelle on avait exclu les cycles de Collatz de longueur 5 dans les entiers positifs.

L'équation en question fournit un encadrement de 2^p très contraignant. Avec $c_1 \dots c_q$ les éléments impairs de C et m son minimum, on a donc $c_i \geq m$, pour tout indice i entre 1 et q . En inversant, puis en ajoutant 3, on obtient $3 < 3 + 1/c_i \leq 3 + 1/m$ pour tout i , sachant que les c_i sont strictement positifs. En prenant le produit de ces q termes, on obtient les inégalités suivantes: $3^q < (3 + 1/c_1) \dots (3 + 1/c_q) \leq (3 + 1/m)^q$.

Par l'équation associée au cycle, le terme du milieu est égal à 2^p . On obtient donc l'encadrement

$$3^q < 2^p \leq (3 + 1/m)^q$$

pour un cycle de Collatz C dans les entiers positifs, avec p pairs, q impairs, et de minimum m .

Voici pourquoi on peut tirer des informations de cet encadrement: plus le minimum m de C est grand, plus son inverse $1/m$ est petit, et plus il sera difficile de trouver une puissance de 2 coincée entre une puissance de 3 et une autre de $3 + 1/m$ avec un exposant commun q . Cela suffit déjà pour exclure la longueur 18.

... EN PASSANT PAR 18

La trajectoire de -17 est un cycle de Collatz de longueur 18 dans les entiers négatifs. Au contraire, il n'existe pas de cycle de cette longueur dans les entiers positifs. Montrons-le. Les symboles p , q et m sont compris relativement à cet hypothétique cycle C . En particulier, le minimum m de C est strictement plus grand que 1, puisque la trajectoire de 1 est un cycle de longueur 3 et non pas 18. Comme $p + q = 18$, on a $p = 18 - q$, et l'encadrement de 2^p devient: $3^q < 2^{18-q} \leq (3 + 1/m)^q$.

Puisque $m > 1$, $(3 + 1/m)$ est donc inférieur à 4. Le terme de droite est donc dominé par 4^q . On obtient ainsi les inégalités strictes $3^q < 2^{18-q} \leq 4^q$. Quelles valeurs de q satisfont ces deux inégalités?

Si q est trop grand, alors 3^q dépassera 2^{18-q} et q ne conviendra pas. De même, si q est trop petit, alors $18-q$ sera trop grand et 2^{18-q} dépassera 4^q . q ne conviendra donc pas non plus. Concrétisons ces observations avec une calculatrice. On trouve $3^7 = 2187$ et $2^{11} = 2048$, donnant l'inégalité $3^7 > 2^{11}$. Donc les valeurs de q supérieures ou égales à 7 sont interdites.

Dans l'autre sens, on a $2^{15} > 4^5$, puisque $4^5 = 2^{10}$. Les valeurs de q inférieures ou égales à 5 sont donc interdites également. Reste une unique valeur permise, à savoir $q=6$, ce qui donne $18-q=12$. Or on a $2^{12} = 4^6$, en contradiction avec l'inégalité stricte $2^{18-q} < 4^q$ requise plus haut. Conclusion: il n'existe aucun cycle de Collatz de longueur 18 dans les entiers positifs.

Pour aller au-delà de l'exclusion de la longueur 18, nous avons besoin d'outils afin de mieux exploiter la force de l'encadrement de 2^p obtenu plus haut. L'idée est de faire «descendre» les exposants p et q afin de les manipuler plus aisément. Pour ce faire, l'outil tout indiqué est le logarithme. De fait: $\log(x^r) = r \log(x)$.

Une propriété du logarithme qui nous intéresse ici est sa continuité: si x et y sont très proches, alors $\log(x)$ et $\log(y)$ le sont aussi.

L'ENCADREMENT DE P/Q

On va déduire un encadrement de p/q à partir de celui de 2^p obtenu précédemment: $3^q < 2^p \leq (3 + 1/m)^q$. En appliquant le logarithme, qui **respecte** l'ordre, on obtient: $\log(3^q) < \log(2^p) \leq \log((3 + 1/m)^q)$. En «descendant» les exposants et après quelques manipulations, on parvient à l'encadrement:

$$\frac{\log(3)}{\log(2)} < \frac{p}{q} \leq \frac{\log(3+1/m)}{\log(2)}$$

Encore une fois, plus m est grand, plus $1/m$ est petit et, par continuité, plus $\log(3+1/m)$ est proche de $\log(3)$. Autrement dit, le rapport p/q se retrouve coincé entre deux nombres d'autant plus proches que m est grand. Ces contraintes vont se révéler très fortes.

Pour un hypothétique cycle de Collatz non trivial C dans les entiers positifs, de minimum m , on a forcément $m > 5 \times 10^{18}$. Ce nombre découle de la vérification du problème $3n+1$ sur ordinateur par Tomás Oliveira e Silva jusqu'à cette borne: pour tout entier n inférieur à 5×10^{18} , sa

trajectoire finit par atteindre 1. Celle-ci ne peut donc contenir un cycle autre que le cycle trivial de longueur 3. On en déduit alors que: $\log(3)/\log(2) < n/q \leq \log(3 + 2 \times 10^{-19})/\log(2)$.

En effet, notant toujours m le minimum de C , on a $m > 5 \times 10^{18}$. En prenant les inverses, l'ordre s'inverse, ce qui donne $1/m < 1/(5 \times 10^{18})$, ou encore, puisque $1/5 = 0,2 = 2 \times 10^{-1}$, $1/m < 2 \times 10^{-19}$. Reste, de chaque côté, à ajouter 3, à prendre le logarithme et à diviser par $\log(2)$ pour parvenir à: $\log(3+1/m)/\log(2) < \log(3+2 \times 10^{-19})/\log(2)$. Combinée à l'encadrement de p/q obtenu plus haut, on obtient celui annoncé.

Concrètement, le rapport p/q est compris entre 1,5849625007211561814537389 et 1,5849625007211561815499186. La différence ne se manifeste qu'à partir de la 19^e décimale! On en déduit que si C est un cycle de Collatz non trivial dans les entiers positifs, avec p termes pairs et q impairs, alors p/q appartient à l'intervalle: $]1,58496250072115618145, 1,58496250072115618155[$.

UN INTERVALLE DE PLUS EN PLUS RÉDUIT

En quoi le fait de savoir que p/q est contraint d'habiter dans un intervalle aussi petit peut-il nous être utile? Assez curieusement parce que toute fraction appartenant à I est tenue d'avoir ses numérateur et dénominateur très grands. Concrètement, on peut montrer que pour tout rationnel s/t de I , avec s et t entiers positifs, on a forcément $s \geq 10439860591$ et $t \geq 6586818670$.

En particulier, ces seuils s'appliqueront à p et q respectivement, puisque p/q appartient à I . Il en découle aussitôt que la longueur de notre présumé cycle C doit dépasser la somme de ces seuils, à savoir 17026679261!

Ainsi, tout hypothétique cycle de Collatz non trivial C dans les entiers positifs doit

contenir au moins 17 milliards d'éléments, s'il existe. Cela ne répond pas à notre question initiale. Mais on peut s'en satisfaire, en attendant mieux.

Et un mieux viendra peut-être bientôt. En effet, cette borne de 17 milliards repose sur la vérification

actuelle du problème $3n+1$ jusqu'à 5×10^{18} . Avec du nouveau matériel informatique, on espère pouvoir vérifier la conjecture jusqu'à $2,17 \times 10^{20}$, dans quelques années sans doute (sauf si un cycle est découvert!). La borne inférieure sur les longueurs de cycles sautera alors de 17 milliards à... 186 milliards, d'un seul coup (c'est un saut d'un facteur 10)! Si vous êtes impatients, sachez que nous venons de passer en revue tous les ingrédients théoriques et numériques suffisants pour s'en convaincre. Vous êtes prêts pour le vérifier? Alors, à vos calculatrices! ■

Cet article est adapté de celui paru sur le site du CNRS Images des Mathématiques : <http://images.math.cnrs.fr/> Nous en remercions les équipes de nous avoir autorisé à le reproduire

BIBLIOGRAPHIE

1. LAGARIAS, The Ultimate Challenge: The $3x+1$ Problem, *American Mathematical Society*, 2010.

2. ELIAHOV, The $3x+1$ problem: new lower bounds on nontrivial cycle lengths, *Discrete Mathematics*, vol. 118, pp. 45-56, 1993.

L'ESSENTIEL

En étudiant une démonstration liée au grand théorème de Fermat dans des conditions particulières, le mathématicien Issai Schur a défini une suite de nombres qui portent son nom.

Le nombre $S(n)$ est le plus grand nombre N pour lequel on peut colorier en n couleurs les entiers de 1 à N tout en évitant

des triplets monochromatiques de la forme $(a, b, a+b)$ avec a, b et $a+b$ compris entre 1 et N .

Étonnamment, on ne connaît que les cinq premiers nombres de Schur. La valeur $S(5) = 160$ n'a été établie qu'en 2018, par ordinateur, avec une preuve pesant... 2 pétaoctets. Et on ignore tout de $S(6)$!

L'AUTEUR



SHALOM ELIAHOUCHE
Professeur à l'université du Littoral Côte d'Opale, Calais.

Des centenaires pleins d'avenir

En 1916, le grand mathématicien Issai Schur donnait naissance à une suite de nombres entiers. Ils sont si mystérieux que, même plus de cent ans après, on ne sait encore rien sur eux... ou presque

V

En 1910, le mathématicien américain Leonard Eugene Dickson travaille sur le dernier théorème de Fermat. Il stipule que pour tout exposant n supérieur ou égal à 3, il n'existe aucun triplet d'entiers non-nuls x, y, z vérifiant l'équation $x^n + y^n = z^n$. Resté à l'état de conjecture

pendant des siècles, ce n'est qu'en 1995 qu'il a été démontré, par Andrew Wiles, avec une contribution de Richard Taylor pour corriger un point dans une version initiale de la preuve (voir *Le tombeur de Fermat*, par G. Giorrello, page 08).

Dickson avait démontré que, pour $n \geq 3$ donné, des solutions non nulles de l'équation de Fermat $x^n + y^n = z^n$ existent non pas en arithmétique ordinaire (il n'y en a que pour $n = 2$), mais en arithmétique *modulo* p pour tout nombre premier p suffisamment grand par rapport à n . En arithmétique *modulo* p , on ne s'intéresse pas aux nombres, mais aux restes après leur division par un certain entier (ici n) nommé module.



prenez les entiers naturels,
coloriez-les en respectant quelques
contraintes... vous entrez alors dans
le monde des nombres de Schur,
un monde pour l'essentiel inconnu.



Intrigué par la preuve assez compliquée de Dickson, le mathématicien juif allemand Issai Schur en a cherché et découvert une plus simple, entièrement nouvelle, de nature combinatoire. C'est à l'occasion de ce travail qu'il définit une suite de nombres entiers $S(1), S(2), S(3)...$ Ces nombres de Schur $S(n)$ sont encore très mystérieux, même après plus d'un siècle d'existence. Il ne s'agit pourtant que de colorier les entiers naturels en respectant quelques contraintes...

De fait, on ne connaît exactement que les cinq premiers nombres de Schur, de $S(1)$ à $S(5)$. Et à partir du sixième, on en sait si peu qu'on ne dispose même pas de conjectures spécifiques quant à leurs valeurs possibles !

L'existence même de ces mystères révèle les lacunes profondes dans notre compréhension collective des choses mathématiques. Vouloir les percer peut avoir des conséquences bien au-delà des seuls nombres de Schur. Car, comme partout en sciences, la recherche ou la découverte de nouvelles approches pour résoudre un problème donne parfois des progrès inattendus dans les tout autres domaines.

Levons un coin du voile. Les quatre premiers nombres de Schur, les seuls connus jusqu'en 2017: $S(1)=1$, $S(2)=4$, $S(3)=13$ et $S(4)=44$. Quant à $S(5)$, une conjecture datant de l'an 2000 stipulait qu'il devait valoir 160. Cette conjecture a été validée en 2018 seulement, par ordinateur, par Marijn Heule, de l'université du Texas, à Austin. Comment ces fameux nombres de Schur sont-ils donc définis ? Un peu de patience...

COLORIER LES ENTIERS

Commençons par fixer un nombre n de couleurs, par exemple $n = 2$. Comme palette de couleurs, prenons rouge et bleu. Ce qui compte, c'est leur nombre. Maintenant, assignons à chaque entier naturel une couleur de notre palette. Par exemple, colorions en rouge les entiers impairs et en bleu les pairs. Les entiers impairs forment alors un sous-ensemble monochromatique, c'est-à-dire d'une seule couleur. Les entiers pairs aussi.

A l'opposé de ce premier exemple, prenons un coloriage aussi aléatoire et irrégulier que possible, comme celui-ci: 1,2,3,4,5,6,7,8,9,10... La question qui nous intéresse est la suivante: malgré l'aspect arbitraire et irrégulier d'un tel coloriage, trouvera-t-on forcément des régularités monochromatiques? De quoi s'agit-il?

Pour Schur, ces régularités sont les triplets de nombres (a, b, c) tels que $c = a + b$; autrement dit, les triplets de la forme $(a, b, a + b)$ comme $(1, 1, 2)$ ou $(3, 5, 8)$ par exemple.

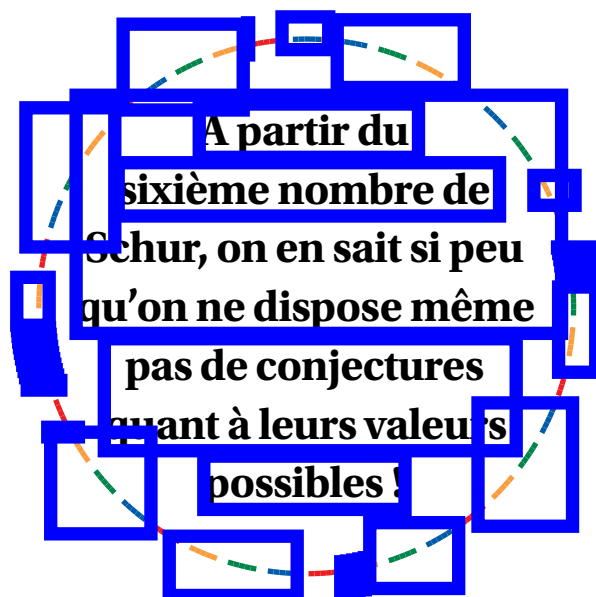
La question est donc: quel que soit le coloriage en deux couleurs des entiers naturels, aussi irrégulier soit-il, trouvera-t-on forcément un tel triplet $(a, b, a + b)$ qui soit

monochromatique? Dans l'exemple 1,2,3,4,5,6,7,8,9,10... précédent, la réponse est oui: $(1, 7, 8)$, $(2, 8, 10)$ et $(3, 6, 9)$.

C'est le cœur du sujet, mais pour un nombre fini n quelconque de couleurs. La question devient: pour un coloriage arbitraire en n couleurs des entiers naturels, trouvera-t-on forcément un triplet monochromatique de la forme $(a, b, a + b)$?

La réponse est positive! C'est le théorème de Schur, énoncé en 1916. Soit n un nombre donné de couleurs: pour tout coloriage en n couleurs des entiers naturels 1,2,3..., on trouvera forcément trois entiers naturels a, b, c de même couleur tels que $c = a + b$, c'est-à-dire un triplet monochromatique de la forme $(a, b, a + b)$.

Précisons qu'il n'est pas interdit d'avoir $b = a$. Dans ce cas, le triplet $(a, b, a + b)$ devient $(a, a, 2a)$. Si a et $2a$ sont de même couleur, alors le triplet $(a, a, 2a)$ sera à la fois monochromatique et de la forme spécifiée $(a, b, a + b)$.



Une version équivalente de ce théorème donne quelques précisions supplémentaires et conduit enfin aux nombres de Schur $S(n)$.

Ce nouveau théorème, lui aussi de 1916, stipule que, pour n donné, il existe un nombre $S(n)$ défini ainsi: c'est le plus grand entier N pour lequel il est possible de colorier en n couleurs les entiers de 1 à N de façon à exclure tout triplet monochromatique de la forme $(a, b, a + b)$ avec a, b et $a + b$ compris entre 1 et N .

Que les deux versions du théorème de Schur soient équivalentes n'a rien d'évident. Un petit supplément d'information s'impose. La première version affirme l'inévitabilité d'un triplet $(a, b, a + b)$ monochromatique pour un coloriage en n couleurs de tous les entiers naturels, tandis que pour atteindre la même conclusion dans la seconde version.

On peut se restreindre à un coloriage en n couleurs des $S(n)$ premiers entiers naturels seulement. La seconde version entraîne donc la première. L'inverse est plus subtil et repose sur un principe général fort utile, le principe de compacité.

Avec la définition, voyons ce que vaut le nombre de Schur $S(2)$. À partir d'une palette de deux couleurs (rouge et bleu), on doit répondre à la question : jusqu'à quel entier maximal N peut-on colorier en rouge ou bleu chaque entier de 1 à N de façon à éviter l'émergence de triplets $(a, b, a+b)$ monochromatiques ? Ce N maximal sera la réponse : $S(2)=N$.

Nous avons vu que $S(2)=4$. Pour le prouver, quelques observations et un peu de raisonnement suffisent. D'abord, identifions tous les triplets de la forme $(a, b, a+b)$ dont les éléments constitutifs a, b et $a+b$ sont compris entre 1 et 4 : $(1,1,2)$, $(1,2,3)$, $(1,3,4)$, $(2,2,4)$. Cette liste est complète, excepté $(2,1,3)$ et $(3,1,4)$ que l'on peut froidement ignorer, puisque l'ordre entre les deux premiers termes a et b ne joue aucun rôle.

Peut-on colorier les entiers 1,2,3,4 en deux couleurs de sorte qu'aucun de ces quatre triplets $(a, b, a+b)$ ne soit monochromatique ? Oui, la preuve : 1,2,3,4. Les quatre triplets concernés deviennent $(1,1,2)$, $(1,2,3)$, $(1,3,4)$, $(2,2,4)$. Manifestement, aucun n'est monochromatique !

Ne peut-on pas construire un tel «bicoloriage» pour $N = 5$? Assignons à 1 la couleur rouge. Pour empêcher que $(1,1,2)$ ne soit monochromatique, il faut colorier 2 en bleu. Mais pour empêcher que $(2,2,4)$ ne soit monochromatique, le 4 doit être rouge. 1 et 4 sont donc tous les deux rouges. La seule façon d'empêcher que le triplet $(1,3,4)$ ne soit monochromatique est alors de colorier 3 en bleu. L'état actuel de notre coloriage des entiers de 1 à 4, le seul possible à ce stade pour exclure les triplets $(a, b, a+b)$ monochromatiques est : 1,2,3,4.

Quelle couleur peut-on assigner à 5 tout en continuant à exclure les triplets $(a, b, a+b)$ monochromatiques ? Ni rouge ni bleu, à cause des triplets $(1,4,5)$ et $(2,3,5)$, tous deux de la forme spécifiée ! Bref, en bicoloriant chaque entier de 1 à 5 en rouge ou en bleu, il s'avère impossible d'éviter l'émergence d'un triplet $(a, b, a+b)$ monochromatique.

Ainsi, il est possible de colorier les entiers de 1 à 4 en deux couleurs tout en excluant les triplets $(a, b, a+b)$ monochromatiques, mais il est impossible de faire de même pour les entiers de 1 à 5. On vient de démontrer que $S(2)=4$.

Quid de $S(3)=13$? Pour le démontrer, et comme pour la détermination de $S(2)$, deux étapes sont nécessaires. D'abord, construire un coloriage des entiers de 1 à 13 en trois couleurs excluant les triplets

monochromatiques de la forme $(a, b, a+b)$. Le coloriage est le suivant :

1, 4, 10, 13

2, 3, 11, 12

5, 6, 7, 8, 9

On vérifie qu'aucun triplet $(a, b, a+b)$ n'est soit tout rouge, soit tout bleu, soit tout vert.

Ensuite, il faut démontrer que 13 est maximal pour cette propriété, c'est-à-dire prouver que pour tout coloriage des entiers de 1 à 14 en trois couleurs, il est impossible d'éviter l'émergence d'au moins un triplet monochromatique de la forme $(a, b, a+b)$. Nous ne donnerons pas de démonstration, mais tout un chacun, moyennant suffisamment d'essais et de patience, un peu comme face à une grille de sudoku de niveau difficile, peut tenter d'en établir une.

Quant à démontrer que $S(4)=44$, on doit d'une part montrer que $S(4) \geq 44$ et, d'autre part, que $S(4) \leq 44$. Pour la première inégalité $S(4) \geq 44$, considérons le coloriage suivant en quatre couleurs des entiers de 1 à 44 :

1, 3, 5, 15, 17, 19, 26, 28, 40, 42, 44

2, 7, 8, 18, 21, 24, 27, 33, 37, 38, 43

4, 6, 13, 20, 22, 23, 25, 30, 32, 39, 41

9, 10, 11, 12, 14, 16, 29, 31, 34, 35, 36

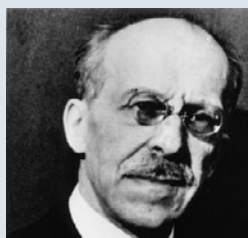
Avec une bonne dose de patience, on peut vérifier que pour ce coloriage, il n'existe aucun triplet $(a, b, a+b)$ monochromatique. Voici quelques triplets : $(1,3,4)$, $(1,5,6)$, $(3,5,8)$, $(2,7,9)$, $(4,6,10)$, $(9,10,19)$... L'inégalité $S(4) \geq 44$ est donc vérifiée.

Pour démontrer l'inégalité inverse, soit $S(4) \leq 44$, il faut s'assurer que pour tous les coloriages possibles en quatre couleurs des entiers de 1 à 45, il y aura toujours au moins un triplet $(a, b, a+b)$ monochromatique.

Les outils théoriques à notre disposition pour ce faire s'avèrent insuffisants : c'est

QUI ÉTAIT ISSAI SCHUR ?

Issai Schur est né à Moguilev, en Biélorussie, le 10 janvier 1875. Il a surtout travaillé en Allemagne, à Berlin et à Bonn, et s'est illustré par bien d'autres résultats que la seule découverte des nombres $S(n)$: l'algèbre, l'arithmétique, la décomposition, l'inégalité, le lemme, le polynôme... portent son nom, dans tous les grands domaines des maths. Comme pour tant de savants juifs d'Europe de cette période, ses contributions fondamentales ne l'ont pas protégé de l'antisémitisme nazi, qui l'a obligé à fuir l'Allemagne in extremis début 1939.



Il se réfugia en Palestine ; il est décédé à Tel Aviv le 10 janvier 1941, jour de son soixante-sixième anniversaire. Un colloque scientifique en sa mémoire s'est tenu en décembre 2000 à l'institut Weizmann à Rehovot, en Israël. En octobre 2016, le centenaire de la naissance des nombres de Schur a été célébré lors d'un colloque à Séville, en Espagne, dédié à la Théorie de Ramsey.

accompagné d'un certificat informatique de validité pesant quelques... 2 pétaoctets en format comprimé ! Bref, on connaît désormais $S(5)$, il vaut 160 exactement.

Malgré cette avancée spectaculaire, le mystère entourant $S(5)$ n'est que partiellement levé. En effet, sans ordinateur, on ne sait toujours pas dire plus que : $S(5)$ se situe quelque part entre 160 et 305. Réduire cette grosse marge d'incertitude grâce à des avancées théoriques serait hautement souhaitable, et permettrait sans doute d'en savoir plus sur les insaisissables nombres de Schur suivants.

VERS $S(6)$ ET AU-DELÀ...

Que sait-on sur $S(n)$ pour $n \geq 6$? Pas grand-chose, à part un encadrement de $S(n)$ entre deux bornes (ici légèrement simplifié) démontré par Schur lui-même, et pas substantiellement amélioré depuis : $(3^n - 1)/2 \leq S(n) \leq 3 \times n! - 1$. Le symbole $n!$ se lit « n factorielle » et est défini par $n! = 1 \times 2 \times \dots \times n$.

Contrairement au cas de $S(5)$, on ne dispose d'aucune conjecture raisonnable quant à la valeur exacte de $S(6)$, et plus généralement de $S(n)$ pour tout $n \geq 6$; même après plus d'un siècle, on en sait encore trop peu pour s'y oser.

L'écart entre les deux bornes encadrant $S(n)$ croît très vite en fonction de n

	$(3^n - 1)/2$	$3 \times n! - 1$
1	1	2
2	4	5
3	13	14
4	40	47
5	121	150
6	364	455
7	1093	1512
8	2800	20959

seulement grâce à une vérification exhaustive par ordinateur qu'on arrive à l'établir. Le premier à l'avoir fait est Leonard Baumert en 1961.

Venons-en à $S(5)$... Jusqu'en 2017, on savait seulement qu'il se situait quelque part entre 160 et 305. On disposait néanmoins de la conjecture formulée par Harold Fredricksen et Melvin Sweet en 2000 selon laquelle $S(5)$ vaut *probablement* 160.

Pour démontrer l'inégalité $S(5) \geq 160$, il suffit d'exhiber un coloriage en 5 couleurs des entiers de 1 à 160 excluant les triplets monochromatiques de la forme $(a, b, a+b)$. Un tel coloriage a été trouvé par Geoffrey Exoo en 1994 par ordinateur :

1. 6. 10. 18. 21. 23. 26. 30. 34. 38. 43. 45. 50. 54. 65. 74...

2. 3. 8. 14. 19. 20. 24. 25. 36. 46. 47. 51. 62. 73...

4. 5. 15. 16. 22. 28. 29. 39. 40. 41. 42. 48. 49. 59...

7. 9. 11. 12. 13. 17. 27. 31. 32. 33. 35. 37. 53. 56. 57. 61. 79...

14. 52. 55. 58. 60. 63. 64. 66. 67. 68. 69. 70. 71. 72. 75. 76. 77. 78. 80...

Ce coloriage est symétrique, c'est-à-dire qu'il assigne la même couleur à un entier x et à son symétrique $161 - x$. Les couleurs des entiers de 1 à 80 suffisent donc à définir le coloriage.

Peut-on pousser d'un cran et trouver un coloriage similaire en 5 couleurs des entiers de 1 à 161 évitant complètement les triplets monochromatiques de la forme $(a, b, a+b)$? On l'ignorait jusqu'à peu !

Puis la réponse est tombée en 2018. Non, c'est impossible : quel que soit le coloriage en 5 couleurs des entiers de 1 à 161, on trouvera forcément un triplet $(a, b, a+b)$ monochromatique, c'est inévitable. Ce résultat a été obtenu par Marijn Heule via un calcul massif sur ordinateur, grâce à de nouvelles méthodes d'attaque de problèmes de logique booléenne. Il vient

Cet article est adapté de celui paru sur le site du CNRS Images des Mathématiques : <http://images.math.cnrs.fr/> Vous en remercions les équipes qui nous ont autorisé à le reproduire

BIBLIOGRAPHIE

M. Heule, Schur Number Five, The Thirty-Second AAAI Conference on Artificial Intelligence, La Nouvelle-Orléans, 2-7 février 2018.

Par conséquent, l'incertitude concernant la valeur précise de $S(n)$ dans l'intervalle ainsi délimité croît elle aussi très vite en fonction de n , du moins en l'état actuel des connaissances.

Les nombres de Schur s'inscrivent dans une théorie générale, la théorie de Ramsey, développée vers 1930 par l'Anglais Frank Plumpton Ramsey. Utilisée en informatique théorique, cette théorie concerne la question suivante : étant donné un objet mathématique quel qu'il soit, si on colorie ses éléments en un nombre fini de couleurs, existera-t-il forcément un sous-objet d'un type spécifié à l'avance – dont tous les éléments sont d'une même couleur, c'est-à-dire monochromatique ? Les nombres de Schur sont précisément une manifestation, avant la lettre, de ce type de problématique. ■

Quand les nombres se la racontent...

Vivre avec la main d'un homme mort

une histoire de poker et de mathématiques

Ronan Quarez



Échappées

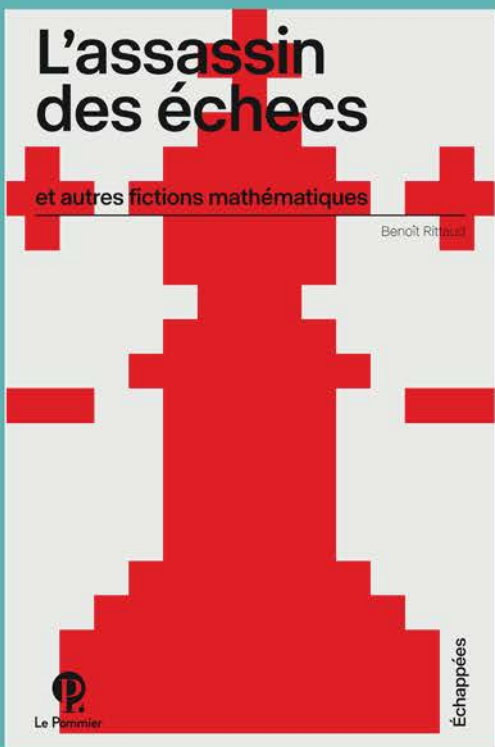
Ronan Quarez 268 p. - 17€

A tous ceux dont
la curiosité se nourrit
d'histoires et de
récits, la collection
« Echappées »
propose des œuvres
de fiction qui parlent
de mathématiques –
autrement.

L'assassin des échecs

et autres fictions mathématiques

Benoît Rittaud



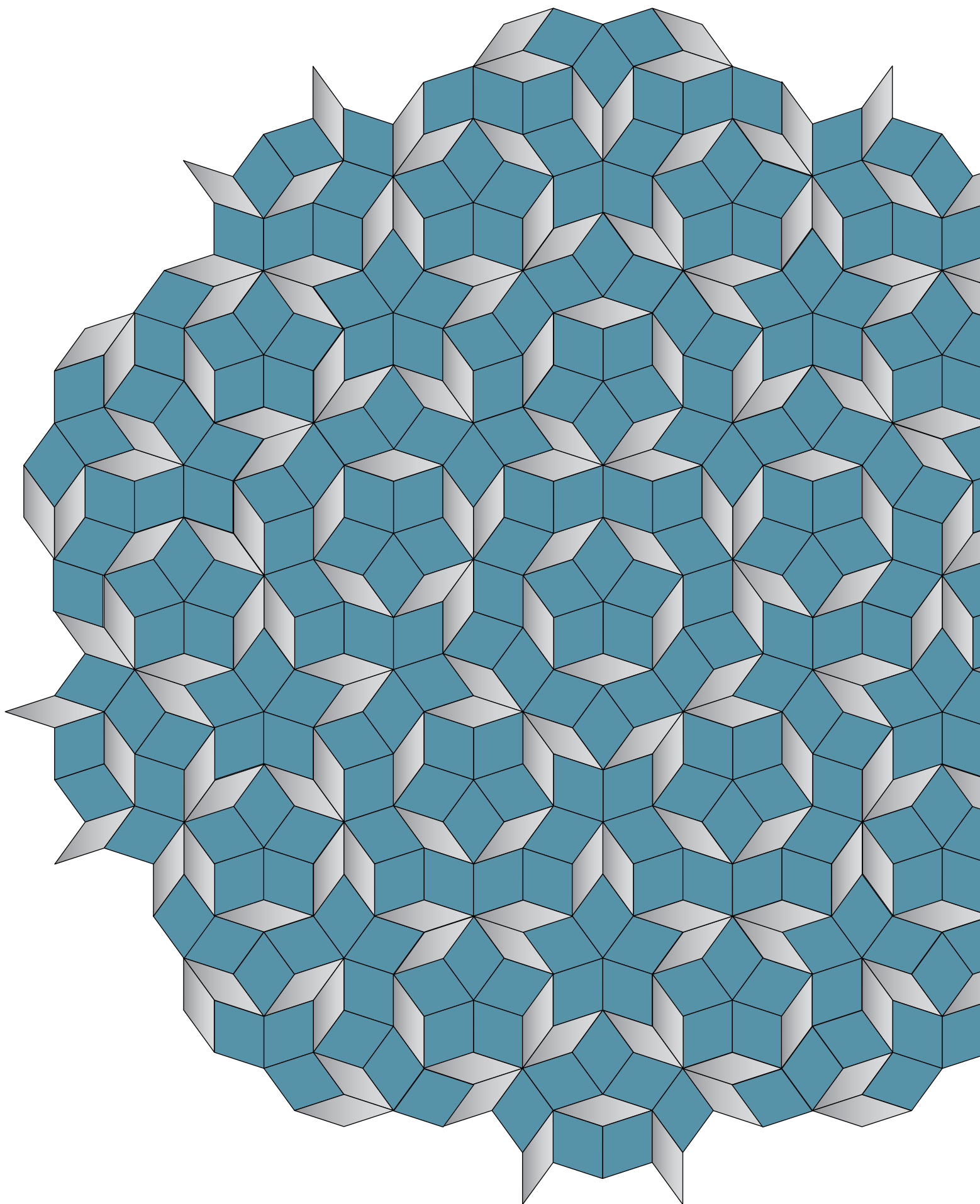
Échappées

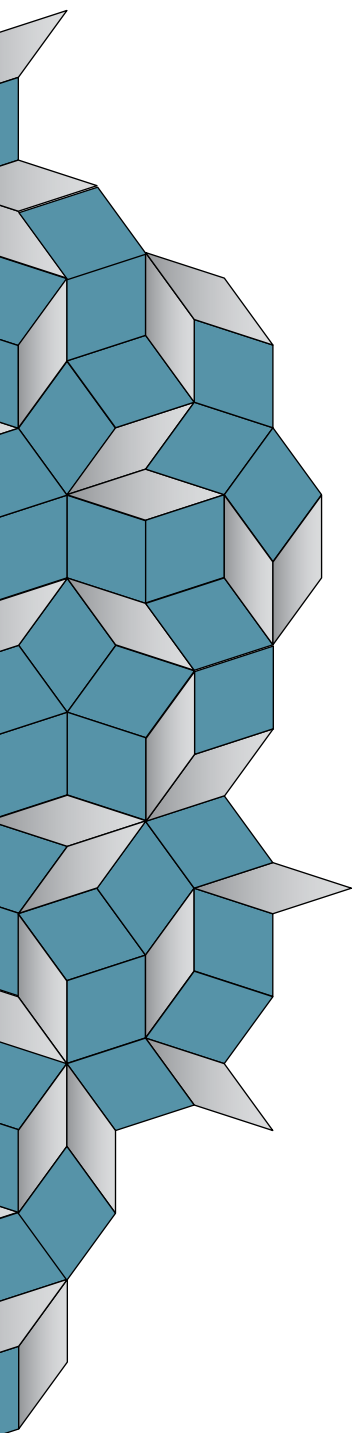
Benoît Rittaud 336 p. - 17€

Retrouvez toutes nos nouveautés sur notre site
www.editions-lepommier.fr



Le Pommier





ESSENCE

Le nombre d'or, ou ϕ , surait souvent la ou on ne l'attend pas en mathématiques.

Ainsi, de par la particularité de l'équation qu'il vérifie, on le retrouve dans des objets fractals, comme l'ensemble de Cantor.

L'équation caractérisant le nombre d'or permet

la construction d'un ensemble de points quasi-périodique, un modèle des «quasi-cristaux», des nouveaux matériaux découverts récemment.

Ces liens du nombre d'or avec la physique soulèvent plusieurs questions mathématiques.

VALEUR



JÉRÔME BUZZI
Directeur de recherches CNRS, travaille au Laboratoire de mathématiques d'Orsay, à l'université Paris-Sud.

Le nombre d'or fait (encore) parler de lui

Le nombre d'or est connu depuis l'Antiquité et l'on pensait en avoir fini avec lui. C'était sans compter sur ses propriétés de symétrie qui expliquent l'intérêt de ce nombre pour la recherche mathématique d'aujourd'hui.

L

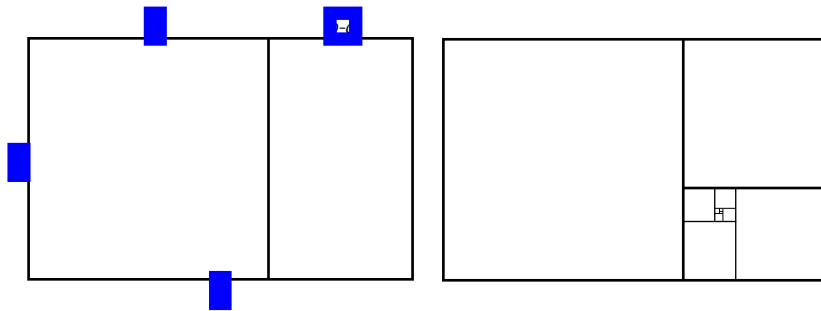
e nombre d'or, désigné par la lettre grecque ϕ (prononcée *fi*), fascine depuis plus de deux millénaires. Identifié dès l'Antiquité, par exemple par les pythagoriciens, on le retrouve à toutes les époques : dans les écrits du mathématicien perse Al-Khawarizmi au VIII^e siècle, dans *La divine proportion*, de

Luca Pacioli et illustré par Léonard de Vinci, à la fin du XV^e siècle, dans les poèmes de Paul Valéry au début du XX^e siècle... Ce sont aussi bien ses propriétés mathématiques que son symbolisme quasi-mystique qui intéressent. De là à penser que tout a été dit sur le nombre d'or, il n'y a qu'un pas... que nous ne franchissons pas, car ce n'est pas le cas !

Aujourd'hui encore, le nombre d'or est au cœur de recherches actives. Grâce aux liens que ϕ entretient avec l'idée de symétrie, elles empruntent des chemins inattendus qui mènent à l'étude des quasi-cristaux, des cristaux découverts au début des années 1980 dont la structure n'est pas périodique, à l'inverse de celle des cristaux classiques. Cette découverte d'ordre physique soulève des questions mathématiques.

Parmi les différentes façons de définir le nombre d'or (voir l'encadré page 48), la plus simple stipule que ϕ est le rapport entre la longueur b et la largeur a d'un rectangle R tel que, si on enlève de R le plus grand carré qu'il contient (de côté a), le rectangle restant R'

Un pavage de Penrose est non périodique. Les dimensions des pavés qui le constituent sont fondées sur le nombre d'or.



de longueur a et de largeur $b-a$, est semblable au rectangle initial, c'est-à-dire que le rapport entre longueur et largeur, φ donc, est le même que pour R (voir la figure ci-dessus).

De cette construction, on peut établir une équation. Les longueurs des côtés du sous-rectangle sont a et $b-a$, on doit donc avoir: $b/a = \varphi$ et $b/a = a/(b-a)$. Ceci donne $\varphi = 1/(\varphi - 1)$, soit $\varphi^2 - \varphi = 1$. C'est une équation du second degré dont les solutions sont: $(1 + \sqrt{5})/2$ et $(1 - \sqrt{5})/2$. Cette dernière solution, inférieure à 0, ne peut pas être φ (le rapport de la longueur sur la largeur). On en déduit que $\varphi = (1 + \sqrt{5})/2$, soit environ 1.618.

Comme le sous-rectangle R' est semblable au rectangle de départ R , on peut répéter la construction, c'est-à-dire enlever le plus grand carré possible du sous-rectangle R' . Et on peut recommencer indéfiniment.

La figure obtenue (prolongée à l'infini) est auto-similaire: dilatée de φ et tournée de 90° , on retrouve la même figure. C'est une forme de symétrie, une notion mathématique qui nous mènera jusqu'aux quasi-cristaux, des objets presque réguliers découverts en 1984.

BIENVENUE EN SYMETRIE

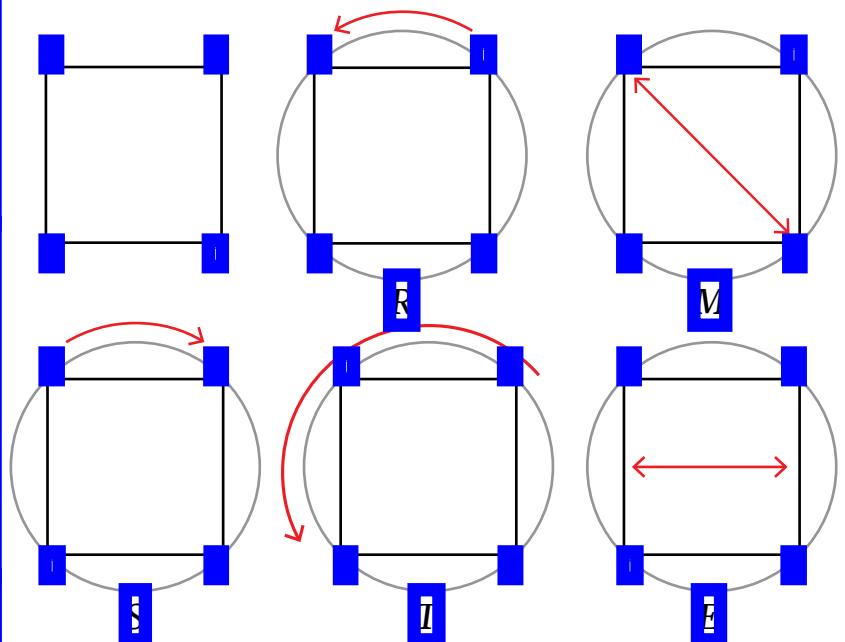
La symétrie est une des grandes idées des mathématiques. Un objet est symétrique quand de «bonnes» transformations le laissent inchangé. Ce sont en l'occurrence des isométries, c'est-à-dire les transformations du plan qui ne modifient pas les distances. Par exemple, si on tourne un carré de 90° autour de son centre, on obtient la même figure, même si tous les points du carré ont été déplacés (voir la figure ci-contre).

La rotation R d'angle 90° autour du centre du carré est une symétrie du carré. Un carré est aussi symétrique par rapport à l'une de ses diagonales: il est invariant par la transformation correspondante M . Si on nomme A, B, C et D les sommets du carré, alors M est caractérisé parmi les isométries du plan par: $M(A) = A$, $M(B) = D$, $M(C) = C$ et $M(D) = B$. En clair, après M , A et C ne changent pas de position, B et D échangent les leurs. Outre R et M , on peut définir la rotation S de -90° , la rotation T d'angle 180° et la symétrie E d'axe vertical.

Les trois symétries S, T et E peuvent en fait être fabriquées à partir des deux

Le nombre d'or φ est le rapport entre la longueur b et la largeur a d'un rectangle (à gauche) tel que, si on enlève le plus grand carré qu'il contienne (de côté a), le rapport entre longueur et largeur reste inchangé. En répétant indéfiniment la construction (à droite), on obtient une figure auto-similaire.

Le carré dispose de nombreuses symétries qui le laissent inchangé: R, M, S, T et E .



premières, R et M , indépendamment de toute considération géométrique. En effet, S est l'inverse de R : l'image par S d'un point x du carré $ABCD$ est le point y dont l'image par R est x ; $S(x) = y$ quand $x = R(y)$. Ainsi, l'inverse d'une symétrie est une symétrie. On note $\bar{U}$ l'inverse d'une symétrie U . On observe que $U(\bar{U}(x)) = \bar{U}(U(x)) = x$, ce que les mathématiciens aiment résumer par $U\bar{U} = \bar{U}U = \text{Id}$ où Id est la transformation identité qui ne fait... rien: $\text{Id}(x) = x$ pour tout x .

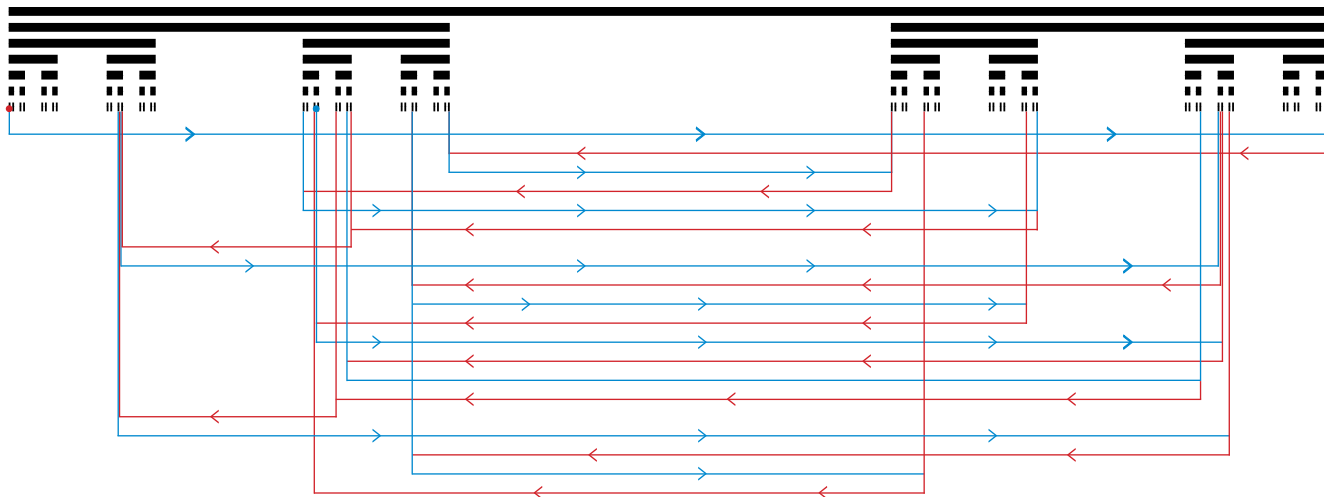
La symétrie d'axe vertical E est la composée de deux symétries, une symétrie M autour de la diagonale suivie d'une rotation R de 90° , ce qui s'écrit $E(x) = R(M(x))$ pour tout x ou, plus brièvement, $E = RM$. Notons que la composée de deux symétries est automatiquement une symétrie.

On peut donc fabriquer des symétries à partir de symétries déjà déterminées, simplement en prenant des inverses ou des composées de celles-ci, indépendamment de la nature géométrique du problème. On peut recommencer tant qu'on obtient de nouvelles symétries. Dans notre exemple, en partant de S et M , on obtient finalement huit symétries: $R, M, \bar{R}, \bar{M}, \text{Id}, RM, MR$ et RRM .

Cet ensemble est le groupe du carré, au sens mathématique du terme, engendré par S et M . Un groupe est un ensemble de transformations tel que l'inverse ou la composée de n'importe lequel de ses éléments est encore un élément de celui-ci.

L'ESPACE DE CANTOR

Poursuivons notre exploration de la symétrie avec l'un des premiers fractals découverts par les mathématiciens: l'ensemble de Cantor (accompagné de copies décalées par les nombres entiers). Il a été étudié par le mathématicien



Allemand Georg Cantor en 1883, mais il avait déjà été remarqué par d'autres notamment le Britannique Henry John Stephen Smith en 1874. Une façon de le mettre en évidence consiste à partir du segment $[0, 1]$ dont on ôte le tiers central, opération que l'on répète sur les deux segments restants, et ainsi de suite (voir la figure ci-dessus). On peut aussi voir dans cet ensemble une partie de la droite construite à partir de symétries définies par deux transformations S et T de la droite. S dilate la droite à partir d'un point origine A d'un facteur trois tandis que T effectue une symétrie autour d'un autre point B .

Si on introduit des coordonnées bien choisies, les points de la droite sont représentés par des nombres et on peut faire en sorte que A corresponde à 0 et B à $1/2$. Les transformations S et T correspondent alors aux formules: $S(x) = 3x$ et $T(x) = 1-x$ où x est un nombre quelconque. Les points A et B deviennent des points fixes de respectivement S et T , car $S(0) = 0$ et $T(1/2) = 1/2$.

Le groupe G engendré par ces deux transformations s'obtient, on l'a vu, en ajoutant à S et T les inverses et les compositions: $\tilde{S}$, $\tilde{T}$, ST , TS , $\tilde{S}\tilde{T}$, $\tilde{T}\tilde{S}$, SST , STS ... Le groupe G est infini, contrairement à celui des symétries du carré. Par exemple composer n fois S avec lui-même donne la transformation qui envoie x sur $3^n x$: S , SS , SSS , $SSSS$... sont des transformations distinctes (à l'inverse des transformations du carré). L'ensemble de Cantor s'obtient en calculant l'image de 0 par tous les éléments du groupe G (voir la figure ci-dessus).

A partir du groupe G nous avons construit un ensemble K , l'ensemble de Cantor. Réciproquement cet ensemble K a pour groupe de symétries G exactement. Si K est un objet compliqué (un fractal), G est fabriqué à partir de transformations très simples qui permettent son analyse. On peut ainsi calculer à partir de G la dimension fractale d de K : $d = \log 2 / \log 3$, soit environ 0.631...

L'ensemble de Cantor (en noir) se construit à partir du segment $[0, 1]$ dont on ôte le tiers central, opération que l'on répète sur les deux segments restants, et ainsi de suite. On peut aussi obtenir cet ensemble à partir des transformations $S(x) = 3x$ et $T(x) = 1-x$, ainsi que leurs inverses et leurs compositions: ce sont les transformations du groupe G . A partir de 0 (le point rouge), on calcule l'image par chacune des transformations de G . Ici, une vingtaine d'images successives sont représentées, où T (en bleu) et $\tilde{S}$ (en rouge) alternent jusqu'au point bleu.

Le 2 correspond au nombre d'éléments (S et T) générant le groupe et le 3 correspondant au facteur de dilatation de S . Il est temps désormais de revenir au nombre d'or...

L'équation établie au début de cet article $\varphi^2 - \varphi - 1 = 0$ peut se réécrire ainsi $\varphi^2 = \varphi + 1$ et s'interpréter géométriquement comme: la dilatation par un facteur φ d'un intervalle de longueur φ est l'union d'un intervalle de longueur φ et d'un intervalle de longueur 1. Désignons par T la transformation de dilatation-subdivision qui prend un découpage d'un segment de la droite en sous-segments de longueurs 1 ou φ , le dilate d'un facteur φ et découpe les sous-segments de longueur φ^2 en un segment de longueur φ suivi d'un de longueur 1. Si on part du segment $[0, \varphi]$, on obtient successivement par application répétée de T la figure ci-dessous.

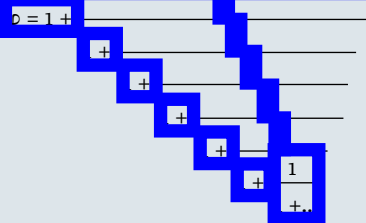
A la limite on obtient une partition R de la demi-droite qui est invariante par la transformation T de dilatation et subdivision. Cette invariance confère à R de curieuses propriétés. D'abord, R n'est pas périodique. Autrement dit, aucune translation de R vers la gauche ne redonne exactement R lui-même. Ensuite, R est quasi-périodique, c'est-à-dire qu'il existe des translations de R qui coïncident avec R sur une longueur arbitrairement grande.

L'IMAGE DU 8 AVRIL 1982

L'ensemble R intéresse les physiciens, car il ressemble à un cristal aperiodique. De quoi s'agit-il? Un cristal se reconnaît expérimentalement à partir de sa figure de diffraction des rayons X. Celle-ci se présente en effet comme un réseau de points brillants alors que les matériaux non-cristallins produisent une figure diffuse. Tout a changé le 8 avril 1982 avec une figure de diffraction étonnante: un réseau de points brillants (comme dans le cas d'un cristal) présentant une symétrie d'ordre 10 (c'est-à-dire invariante par la rotation d'angle 36°). Or un cristal, étant un

LE NOMBRE D'OR EST PARTOUT

Le nombre d'or $\varphi = (1 + \sqrt{5})/2$, soit environ 1,618. Il est certes une des solutions de l'équation $x^2 - x = 1$, mais on le trouve dans beaucoup d'autres situations. Par exemple, dans un rectangle dont la longueur sur la largeur est égale à φ . Cela se traduit par l'égalité $2 \cos(\pi/5) = \varphi$. De l'équation précédente, on peut également montrer que :



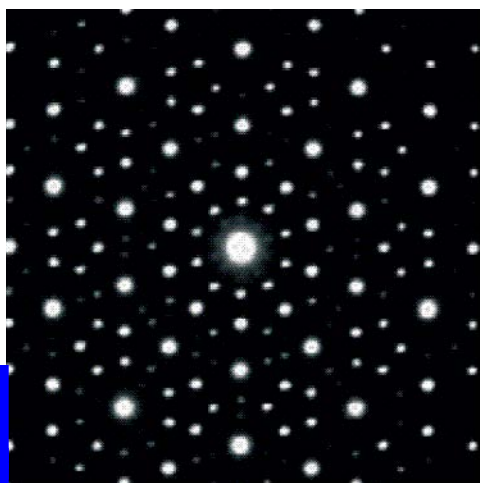
Le nombre d'or se cache aussi dans la suite de Fibonacci ainsi définie : $F_0 = 0, F_1 = 1, F_{n+2} = F_{n+1} + F_n$. Chaque terme (à part les deux premiers) est la somme des deux précédents : 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144... Au XVI^e siècle, l'astronome Kepler a remarqué que le rapport F_{n+2}/F_{n+1} de deux termes consécutifs de la suite de Fibonacci tend vers φ à mesure n croît. Le nombre d'or se

trouve enfin dans le monde végétal. Les écailles des pommes de pin, les fleurons des tournesols et des marguerites, les feuilles le long d'une tige s'agencent en deux séries de spirales. Lorsqu'on les compte, on trouve deux nombres consécutifs de la suite de Fibonacci, et donc une approximation du nombre d'or !



motif périodique de dimension 3, ne peut avoir de symétries que d'ordre 2, 3, 4 ou 6 d'après un théorème similaire à celui qui limite les solides réguliers aux cinq solides platoniciens. C'était inconcevable et pendant plusieurs années la communauté scientifique refusa d'y croire.

Pourtant, des expériences ont confirmé la présence de cette symétrie « impossible » (voir la figure ci-dessous). On avait donc découvert une nouvelle organisation de la matière : ordonnée comme des cristaux, mais sans être périodique comme eux. La découverte de ces « quasi-cristaux » a valu le prix Nobel de chimie, en 2011, à Dan Shechtman, l'auteur de l'image du 8 avril. L'ensemble R offre un modèle (très simplifié) de ces objets physiques quasi-périodiques.



Cet article est adapté de celui paru sur le site du CNRS *Images des Mathématiques* : <http://images.math.cnrs.fr/> Nous en remercions les équipes qui nous ont autorisé à le reproduire.

BIBLIOGRAPHIE

M. BAAKE ET U. GRIMM, *Aperiodic Order*, vol. 1. A Mathematical Invitation, Cambridge University Press, 2013.

R. PENROSE, Tilings and quasicrystals : a nonlocal growth problem? in M. Jaric (Ed.) Introduction to the Mathematics of Quasicrystals, Academic Press, pp. 53-58, 1989.

D. SHECHTMAN ET AL., Metallic phase with long-range orientational order and no translational symmetry, *Phys. Rev. Lett.*, vol. 53, no. 1951-1953, 1984.

L'image par laquelle on a découvert les quasi-cristaux. Les points brillants sont organisés selon un motif régulier à symétrie d'ordre 5, ce qui est impossible avec des cristaux classiques.

Une question mathématique fondamentale, à ce jour non résolue, est de classer les quasi-cristaux comme on a su au XIX^e siècle classer les cristaux par leurs groupes de symétries. La dilatation-subdivision T définie par le nombre d'or φ est une piste suivie pour y parvenir. Elle est à l'origine de plusieurs procédés de construction de quasi-cristaux, notamment les pavages de Penrose du plan, qui font aussi intervenir le nombre d'or (voir la figure page 44).

PENROSE ET LE NOMBRE D'OR

Ces pavages du plan, dont certains ont une symétrie d'ordre 5, ont été découverts par le Britannique Roger Penrose dans les années 1970. Les pièces de base de ces pavages sont des triangles isocèles (des triangles d'or) dont certains côtés ont pour longueur φ .

Parmi les autres procédés fondés sur T , citons la dilatation-division liée à d'autres nombres particuliers différents de φ , la projection de points à coordonnées entières en grande dimension, les règles de compatibilité entre plus proches voisins... Ces constructions sont également utilisées en informatique théorique.

Les mathématiciens s'efforcent aujourd'hui de préciser les propriétés de ces différentes constructions : lesquelles produisent la même classe d'objets? Quand obtient-on bien une figure de diffraction conforme à celles des quasi-cristaux? Peut-on reconnaître la construction à partir des figures de diffraction? Quels sont les liens entre combinatoire et géométrie? Le nombre d'or n'a pas fini de faire parler de lui ! ■

Des nombres et des énigmes

Êtes-vous prêts pour des énigmes difficiles ? Ana Retchman, maîtresse de conférences à l'université de Strasbourg, et Sébastien Kernivinen, enseignant en mathématiques, à Rennes, vous en proposent 14. Elles sont extraites, pour la plupart, des *Défis du calendrier 2018*, d'Ana Retchman.

Suite des énigmes page 81. Solutions page 106

Ana
Retchman



Sébastien
Kernivinen



ENIGME 1

Jusqu'à quel nombre N est-il possible de colorier en rouge ou bien en bleu les nombres entiers de 1 à N sans que deux nombres quelconques distincts de la même couleur ne redonnent, en les additionnant, un nombre de la même couleur ?
Indice : c'est un cube

ENIGME 2

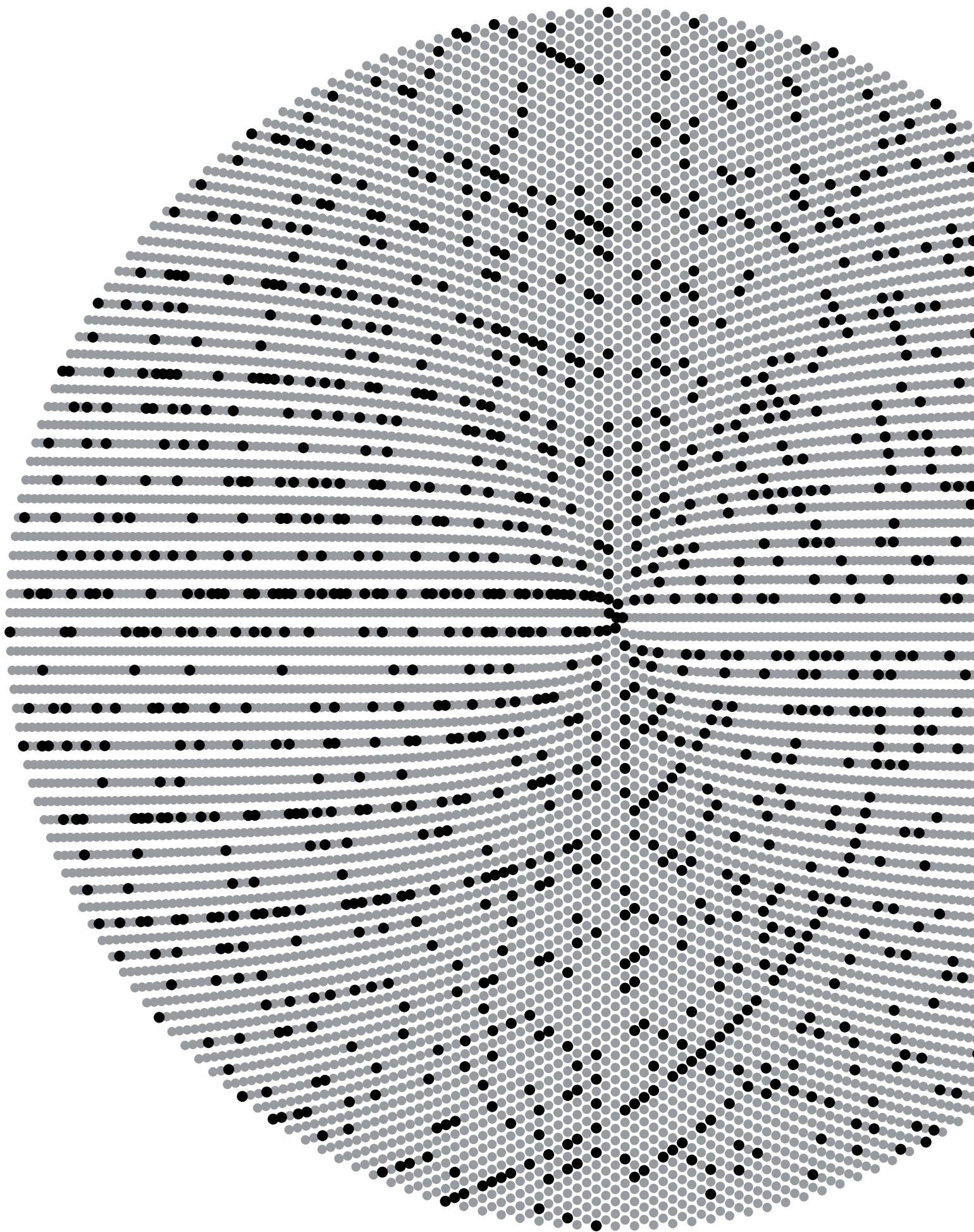
Combien y a-t-il de « randonnées » partant du nombre entier 1 et arrivant au nombre entier 10 en ajoutant successivement ou bien 1 ou bien 2 à chaque pas ?

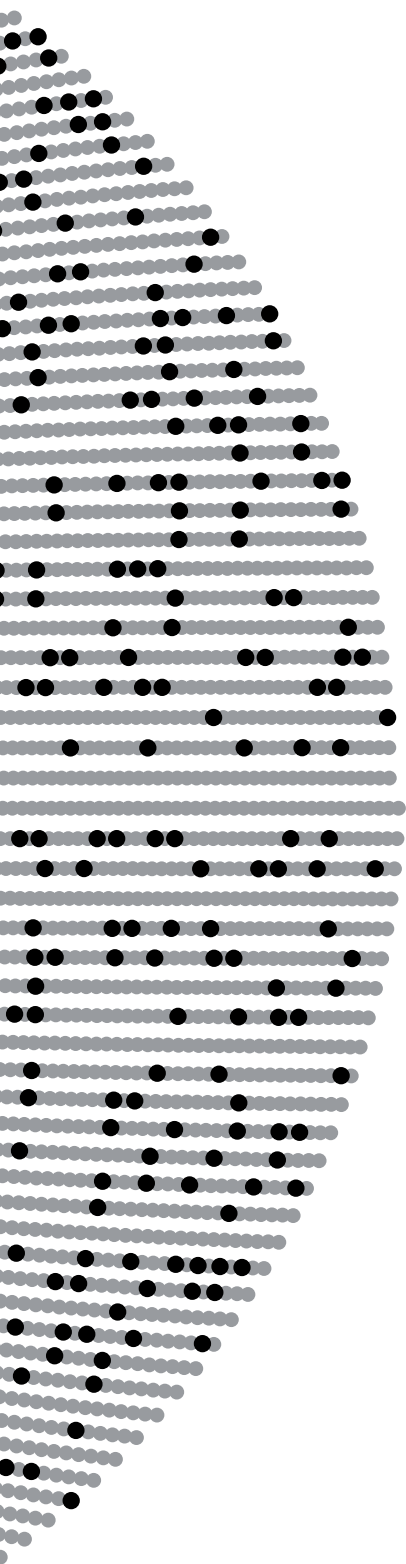
ENIGME 3

Trouvez dix entiers positifs distincts tels que chacun d'entre eux divise la somme de ces dix nombres.

ENIGME 4

Quels sont les nombres rationnels positifs r tels que $r + \frac{1}{r}$ soit un entier ?





LES PREMIERS DE LA CLASSE

Les nombres premiers sont aux nombres ce que les atomes sont à toutes les molécules : leurs constituants élémentaires. Ils sont donc l'objet de toutes les attentions de la part des mathématiciens, qui aimeraient les comprendre en profondeur. Y a-t-il une infinité de nombres premiers jumeaux (séparés par 2), cousins (par 4), sexy (par 6) ? Peut-on élaborer une formule mathématique qui donnerait quantité de nombres entiers ? Et, quête absolue, comment se répartissent ces nombres premiers parmi les entiers ? Cette dernière question est mise à prix un million de dollars, une somme dérisoire comparée à la gloire qu'apportera la solution à celui qui la trouvera.



Le graal de la cryptographie, faire exécuter un calcul par un opérateur extérieur qui ignore ce qu'il calcule, sera-t-il bientôt possible ?

ESSENTIEL

Comment calculer et manipuler des données sans les connaître?

Pour des calculs simples, les solutions sont faciles. Mais on est vite limité, par exemple pour identifier parmi des nombres ceux qui sont premiers.

On peut aller plus loin avec des méthodes de chiffrement

pleinement homomorphe que les travaux de Craig Gentry ont rendus possibles.

Avec des versions partielles, on peut déjà sécuriser des votes électroniques. Mais des progrès restent nécessaires pour rendre «pleinement» utilisable le chiffrement pleinement homomorphe.

AUTEUR



JEAN-PAUL DELAHAYE est professeur émérite à l'université de Lille et chercheur au Centre de recherche en informatique, signal et automatique de Lille (Cristal).

Une nouvelle merveille cryptographique!

Vous confiez des calculs à un tiers, il les effectue et vous transmet les résultats, mais sans avoir pu connaître ni les données du calcul ni ses résultats. On peut parler de prodige!

S

Si vous êtes prudent, vous chiffrez vos données avant de les confier à un service de sauvegarde extérieur, dans le *cloud* par exemple. Comment demander alors à ce service de prendre les données d'un fichier et d'en calculer la moyenne, ou d'en extraire des informations particulières? Pour calculer et manipuler des données, vous devez les connaître!

Eh bien, non! C'est tout l'enjeu des systèmes de chiffrement homomorphe: un tiers peut calculer avec vos données qu'il ne connaît pas, et il produit un résultat qui lui est illisible, mais que vous savez déchiffrer.

UNE METHODE TRES SIMPLE

Si les calculs à effectuer sont simples, il est facile d'imaginer une solution. Vous choisissez un nombre C que vous seul connaissez. Vous multipliez toutes vos données par C , et ce sont ces données que vous transmettez à l'opérateur extérieur (noté $\odot$) chargé de les sauvegarder. Pour connaître, par exemple, la moyenne de vos données ou de certaines d'entre elles, vous demandez à $\odot$ de calculer la moyenne sur les données dont il dispose et

de vous transmettre le résultat. Puis vous divisez le résultat par C : vous avez votre moyenne, car la moyenne de $Cd_1, Cd_2, \dots, Cd_n$ est C fois la moyenne de $d_1, d_2, \dots, d_n$.

Avec ce procédé, vous pouvez faire exécuter par l'opérateur extérieur d'autres types de calculs. Pour connaître le nombre de données qui dépassent un certain nombre B , vous lui demanderez le nombre de données qui dépassent CB . Le tri de vos données par ordre croissant est aussi faisable, puisque si C est positif, le tri de $Cd_1, Cd_2, \dots, Cd_n$ exige les mêmes permutations que $d_1, d_2, \dots, d_n$.

Toutes les moyennes pondérées, par exemple la moyenne $(d_1 + 2d_2 + 5d_3 + d_4)/9$, sont aussi possibles sans dévoiler C , car le résultat sur les données multipliées par C est égal à C fois le résultat attendu. Certaines opérations un peu plus compliquées sont envisageables: pour le calcul de $d_1d_2 + d_3d_4 + d_5d_6$, il suffira de diviser le résultat que $\mathcal{O}$ fournit par C^2 .

Cependant, vous ne pourrez pas demander $d_1 + d_2d_3$ et, finalement, ce n'est qu'un faible sous-ensemble de calculs que vous saurez faire exécuter à l'extérieur sans avoir à divulguer vos secrets. En particulier, pas question de faire opérer des algorithmes complexes sur vos données, comme l'identification, parmi les nombres confiés, de ceux qui sont des nombres premiers.

Remarquons aussi que le chiffrement de vos données en les multipliant par une constante C laisse transparente certaines informations que vous ne souhaitez peut-être pas que l'opérateur $\mathcal{O}$ connaisse: le numéro de la donnée la plus grande ou la plus petite, les valeurs égales, les données classées, etc. Le problème sera résolu si vous disposez

d'une méthode de chiffrement permettant à la fois de bien masquer toute l'information et autorisant l'exécution d'additions et de multiplications sans rien révéler: avec ces deux opérations, on reconstitue tout calcul.

DES CHIFFREMENTS PLEINEMENT HOMOMORPHES

Notons aussi qu'il n'est pas essentiel que l'opération effectuée par $\mathcal{O}$ soit identique à celle que vous voulez au final. En effet, supposons que le chiffrement de la donnée d soit $\mathcal{C}(d)$ et que le déchiffrement (que vous seul savez effectuer) soit l'opération $\mathcal{C}': \mathcal{C}'(\mathcal{C}(d)) = d$. Pour réussir à faire exécuter toutes sortes de calculs par un opérateur extérieur, il suffirait qu'il existe une opération $*_1$ et une opération $*_2$ (pas nécessairement l'addition et la multiplication habituelles) vérifiant:

$$\begin{aligned}\mathcal{C}(d_1 + d_2) &= \mathcal{C}(d_1) *_1 \mathcal{C}(d_2) \quad (\text{propriété 1}) \\ \mathcal{C}(d_1 \times d_2) &= \mathcal{C}(d_1) *_2 \mathcal{C}(d_2) \quad (\text{propriété 2}).\end{aligned}$$

En exécutant $*_1$ et $*_2$ à la place de $+$ et $\times$, l'opérateur 2 produira à partir des données chiffrées un résultat qui, après le déchiffrement par $\mathcal{C}'$, sera exactement ce que vous voulez.

Par exemple, si vous souhaitez connaître $d_1 + d_2d_3$ sans le calculer vous-même (ce qui est impossible avec la méthode de multiplication par C), vous enverrez vos données chiffrées $\mathcal{C}(d_1), \mathcal{C}(d_2), \mathcal{C}(d_3)$ à l'opérateur en lui demandant de calculer $\mathcal{C}(d_1) *_1 (\mathcal{C}(d_2) *_2 \mathcal{C}(d_3))$ et de vous renvoyer le résultat R . Grâce à l'opération $\mathcal{C}'$, vous obtiendrez alors la valeur de $d_1 + d_2d_3$, puisque:

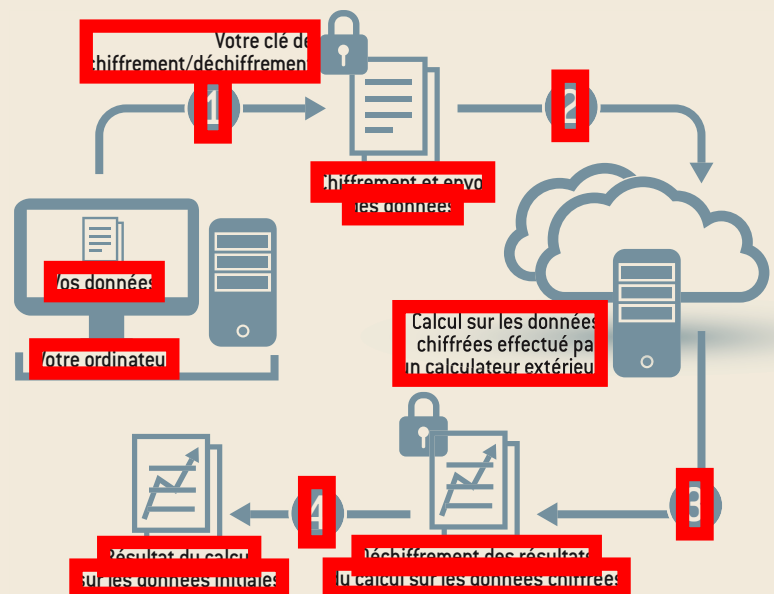
$$\begin{aligned}\mathcal{C}'(R) &= \mathcal{C}'(\mathcal{C}(d_1) *_1 (\mathcal{C}(d_2) *_2 \mathcal{C}(d_3))) = \\ &= \mathcal{C}'(\mathcal{C}(d_1)) + \mathcal{C}'(\mathcal{C}(d_2) *_2 \mathcal{C}(d_3)) = \\ &= d_1 + \mathcal{C}'(\mathcal{C}(d_2) \times \mathcal{C}(d_3)) = d_1 + d_2d_3.\end{aligned}$$

La méthode fonctionnera pour toute

CALCUL DÉLOCALISÉ

Avec les chiffrements dits homomorphes, un opérateur calcule sur des données chiffrées dont il n'a pas connaissance.

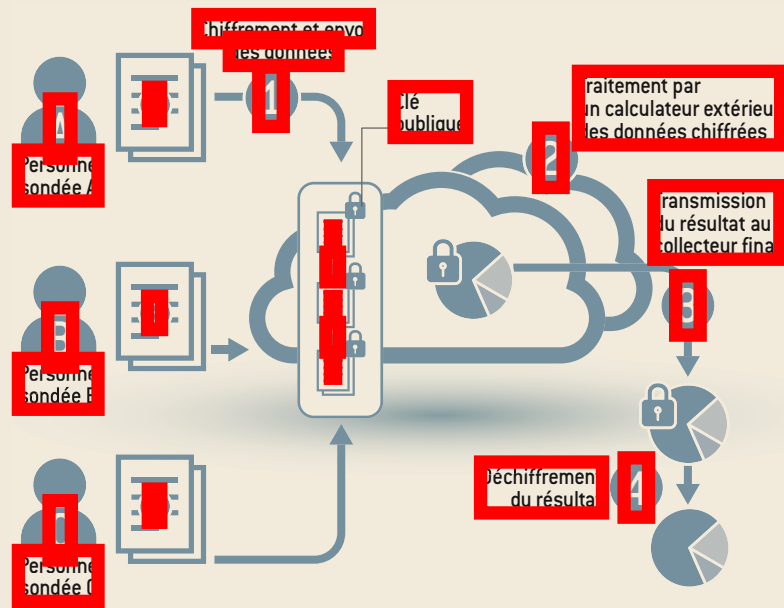
Connaître le résultat trouvé, que seul le commanditaire du calcul déchiffre. Vous chiffrez vos données avec une clé secrète et vous les envoyez à l'opérateur extérieur (1). L'opérateur effectue des calculs avec les données chiffrées et vous envoie les résultats chiffrés sans avoir eu connaissance de la clé (2, 3). Vous déchiffrez les résultats reçus grâce à la clé secrète (4): vous avez ainsi connaissance des résultats d'un calcul que vous n'avez pas fait, résultats auxquels l'opérateur n'a pas pu avoir accès. Pour des calculs simples, des séries d'additions et de soustractions, la mise au point d'applications réelles telles que les systèmes de vote est possible.



PRÉSERVER LA CONFIDENTIALITÉ

Imaginons que l'on souhaite établir une statistique sur un sujet délicat en utilisant Internet et en garantissant à chacune des

individuelles contenues dans les réponses ne seront pas divulguées. La procédure est la suivante. Chaque personne chiffre ses réponses avec la clé publique du collecteur final et les envoie à un ordinateur extérieur (1). Ce dernier traite ces données chiffrées et envoie le résultat au collecteur final (2, 3). Ce dernier déchiffre le résultat et obtient la statistique souhaitée (4). Le collecteur extérieur ne peut pas accéder aux informations privées des sujets de l'enquête, car il ne dispose pas de la clé privée de déchiffrement, et le collecteur final ne peut pas accéder aux données individuelles car il n'a pas eu accès aux informations chiffrées individuelles transmises.



expression, aussi compliquée soit-elle, constituée d'additions et de multiplications. Puisque dès qu'on sait mener des additions et des multiplications de cette façon, on peut exécuter tout algorithme, le problème des calculs secrets par un tiers se ramène à celui de trouver $\mathcal{C}$, $\mathcal{C}'$, $\mathcal{E}_1$, $\mathcal{E}_2$ vérifiant les propriétés 1 et 2.

Les méthodes de chiffrement vérifiant les propriétés 1 et 2 sont dites «pleinement homomorphes». Le terme vient du langage mathématique où les homomorphismes sont des fonctions qui transforment une opération en une autre, comme l'indique par exemple la propriété 1.

Ces homomorphismes jouent un rôle important en mathématiques et chacun connaît le logarithme qui vérifie $\log(a \times b) = \log(a) + \log(b)$ et qui transforme donc des multiplications en additions (ici, $+$ est l'addition habituelle). Avant l'avènement des ordinateurs, c'était le moyen le plus efficace pour mener à la main des calculs numériques, et c'est pourquoi on dressait des tables de logarithmes contenant des millions de données.

En mathématiques, on connaît de nombreux homomorphismes, mais aucun des homomorphismes classiques ne peut servir à concevoir un chiffrement $\mathcal{C}$ homomorphe car l'opération de déchiffrement $\mathcal{C}'$ est alors trop simple; or une bonne méthode cryptographique est une méthode où il est difficile de trouver $\mathcal{C}'$. Le problème des systèmes de chiffrement pleinement homomorphes n'était donc pas évident au moment où, en 1978, l'idée en a été envisagée par les Américains Ron Rivest et Leonard Adleman et le Grec Michael Rortouzos. On s'est longtemps demandé si de

elles méthodes existaient. Le problème a par trois fois été qualifié de «problème de la cryptographie».

UNE PERCÉE DÉCISIVE

Une percée décisive a été réalisée en 2009 par Craig Gentry, de l'université Stanford et aujourd'hui au centre Thomas Watson d'IBM à New York. Craig Gentry a proposé une méthode qui résout théoriquement le problème et a pour cela reçu une bourse de 625 000 dollars de la fondation MacArthur. La méthode qu'il a initialement proposée n'est pas applicable, car elle exige des calculs trop volumineux au moment du chiffrement (la transformation des données avant de les envoyer) et du déchiffrement. De plus, la taille des données que doit manipuler l'opérateur extérieur $\mathcal{C}$, et donc la quantité de calculs qu'il doit mener, est des millions de fois celle nécessaire quand les données ne sont pas chiffrées.

Depuis 2009, une multitude de recherches ont été faites pour trouver des schémas plus économiques. En quelques années, les progrès ont rendu envisageables certaines applications, et l'espoir de méthodes encore plus économiques et faciles à mettre en œuvre suscite de nombreux travaux parmi les spécialistes.

Avant de donner des précisions sur les données de la percée décisive de Craig Gentry, revenons sur les applications des chiffrements pleinement homomorphes ou même partiellement homomorphes.

L'algorithme RSA (conçu en 1977 par Ronald Rivest, Adi Shamir et Leonard Adleman) est une méthode de chiffrement à clé publique: pour chiffrer un message, on utilise la clé publique de

CRAIG GENTRY, LE PIONNIER

En proposant en 2009 le premier système de cryptage complètement homomorphe

chez IBM, a révolutionné le domaine. Il a déclenché une multitude de travaux qui, petit à petit, ouvrent des voies pour rendre utilisable son idée, initialement théorique pour l'essentiel. Confier de façon massive des calculs à des opérateurs extérieurs qui ne peuvent pas accéder aux données n'est pas aujourd'hui envisageable. En revanche, peu à peu, il est devenu possible de résoudre des problèmes



particuliers n'exigeant qu'une petite quantité de calculs homomorphes (comme pour un vote). Les applications de ces méthodes devraient rapidement s'étendre et aider à accroître la sécurité des réseaux et la protection des données... ce dont on a un grand besoin !

son correspondant, et lui seul peut déchiffrer le message grâce à sa clé secrète. C'est un bon algorithme, aujourd'hui très utilisé. Il a la propriété d'être homomorphe pour la multiplication: on en déduit une méthode de chiffrement homomorphe pour l'addition, comme celle évoquée au début de l'article, méthode ayant cette fois l'avantage que les données sont correctement masquées à l'opérateur extérieur.

LES VOTES SECRETS

Avec un système additivement homomorphe de ce type, on peut opérer des votes secrets sur le réseau sans se rencontrer. Décrivons un tel procédé.

Il y a trois types d'intervenants: les votants (au plus $N-1$), l'opérateur calculeur, et l'opérateur de dépouillement. L'opérateur de dépouillement choisit un couple clé publique/clé privée et communique la clé publique à chaque votant. Chaque votant choisit alors un nombre entier V de la forme Nk (k entier) s'il veut voter OUI, ou $Nk+1$ (k entier) s'il veut voter NON; puis il chiffre le nombre V choisi avec la clé publique et transmet le nombre chiffré $\mathcal{E}(V)$ à l'opérateur de calcul. Ce dernier fait la somme S de tous les nombres qu'il reçoit et communique S à l'opérateur de dépouillement, lequel déchiffre le résultat grâce à la clé privée, qu'il est seul à connaître. Il trouve ainsi un nombre de la forme $Mk+p$, où p est le nombre de personnes ayant voté NON. Le résultat du vote est alors communiqué à tous.

L'opérateur calculeur, qui ne connaît pas la clé de déchiffrement, ne peut pas connaître les votes individuels; l'opérateur de dépouillement, qui n'a pas eu connaissance des nombres transmis individuellement, ne peut pas lui non plus connaître les votes individuels. Les votants peuvent contrôler le travail de l'opérateur de

calcul, s'ils acceptent de se communiquer les $\mathcal{E}(V)$, ce qui ne compromet pas le secret du vote.

Avec un tel système, même si les votants sont séparés par des milliers de kilomètres et ne communiquent que par messages, aucun vote ne circule de manière lisible, et personne ne sait comment les autres ont voté. On peut encore perfectionner de tels systèmes, comme l'expliquent Véronique Cortier et Steve Kremer dans un article de 2013.

Ce type d'applications de la cryptographie partiellement homomorphe est aujourd'hui arrivé à maturité et le système de vote Helios est un logiciel libre développé par les chercheurs de l'université Harvard et de l'université catholique de Louvain. On l'a utilisé pour l'élection du recteur de l'université catholique de Louvain et plusieurs fois lors d'élections étudiantes. L'Association internationale des chercheurs en cryptographie (IACR) l'utilise pour choisir les membres de son bureau. Il est fondé sur le système de chiffrement El Gamal, qui est additivement homomorphe.

UNE ARITHMETIQUE « SECRETE »

Voici maintenant la description d'une version du chiffrement pleinement homomorphe de Craig Gentry. Cette version est due à Marten van Dijk, Craig Gentry, Shai Halevi et Vinod Vaikuntanathan. Les idées sont simples et n'impliquent que des calculs élémentaires effectués avec des entiers.

La méthode utilise le fait que, pour créer un système de chiffrement pleinement homomorphe, il suffit de définir un système qui chiffre les bits, des 0 et des 1, et de savoir faire exécuter par l'opérateur extérieur un nombre quelconque d'opérations logiques du type XOR (OU exclusif) et ET entre de tels bits chiffrés.

La clé secrète du système, que l'utilisateur doit garder pour lui, comme le C de l'exemple du début de l'article, est ici un long nombre entier impair p , mettons de 500 chiffres binaires. Dans toute la description de la méthode, la taille des entiers manipulés est importante; les opérations ne sont pas faisables à la main, mais ce n'est aujourd'hui pas un problème, puisque n'importe quel téléphone peut manipuler des nombres de plusieurs millions de chiffres.

Un multiple «approximatif» de p est un nombre de la forme $qp+e$, où e est un nombre d'une vingtaine de chiffres binaires introduisant une sorte de bruit. Retrouver p à partir de la donnée d'un ou plusieurs multiples approximatifs de p nécessite des calculs si longs qu'ils sont impossibles à réaliser pratiquement en un temps raisonnable. C'est sur cette impossibilité pratique que se fonde le chiffrement pleinement homomorphe que nous décrivons. Si q comporte beaucoup de chiffres (par exemple plusieurs millions de chiffres binaires), un attaquant

ignorant p ne peut pas faire la différence entre $qp + e$ et un nombre quelconque de même taille.

De ce fait, chiffrer un bit b ($b=0$ ou 1) par $\mathcal{E}(b) = pq + b + 2r$ où r a une vingtaine de chiffres et q plusieurs millions est une bonne méthode : celui qui connaît p n'a aucun mal à retrouver q en faisant la division par n .

Le reste de la division est $b + 2r$, qui est pair si $b=0$ et impair si $b=1$. Ainsi, celui qui connaît p saura sans mal déchiffrer $\mathcal{E}(b)$. Et celui qui ne connaît pas p ne voit dans $\mathcal{E}(b)$ qu'un nombre quelconque dont il ne tire rien. Ce système de chiffrement est homomorphe pour le XOR et le ET et est donc pleinement homomorphe. Le vérifier est une simple question d'arithmétique. En voici les détails, que vous pouvez passer si vous trouvez cela fastidieux.

Soient b_1 et b_2 deux bits. Chiffrons-les : $\mathcal{E}(b_1) = c_1 = q_1p + 2r_1 + b_1$ et $\mathcal{E}(b_2) = c_2 = q_2p + 2r_2 + b_2$ avec des entiers r_1 et r_2 d'une vingtaine de chiffres, p d'environ 500 chiffres et q_1 et q_2 de plusieurs millions de chiffres. Celui qui connaît p peut calculer le reste de la division par p de : $c_1 + c_2 = (q_1 + q_2)p + 2(r_1 + r_2) + (b_1 + b_2)$. Ce reste est $2(r_1 + r_2) + (b_1 + b_2)$; puisque $2(r_1 + r_2)$ est pair, connaître le reste donne la parité de $(b_1 + b_2)$ c'est-à-dire le XOR entre b_1 et b_2 . Additionner $\mathcal{E}(b_1)$ et $\mathcal{E}(b_2)$ donne donc, si l'on connaît p , le XOR entre b_1 et b_2 ($b_1 + b_2$ n'est impair que si l'un ou l'autre est impair, mais pas les deux, et est pair dans les deux autres cas). On peut donc faire calculer à un opérateur extérieur des XOR sans qu'il connaisse ni les données b_1 et b_2 , ni le résultat qu'il calcule. C'est la propriété d'homomorphisme additif. Notons que le « bruit » sur $c_1 + c_2$ est passé de r_1 et r_2 à $2(r_1 + r_2)$, il a donc à peu près doublé.

Pour la multiplication, l'opérateur extérieur calcule : $c_1c_2 = (q_1q_2p + 2q_1r_2 + q_1b_2 + 2q_2r_1 + q_2b_1)p + 2(2r_1r_2 + r_1b_2 + r_2b_1) + b_1b_2$.

La division par p donne le reste $2(2r_1r_2 + r_1b_2 + r_2b_1) + b_1b_2$ et donc la parité de b_1b_2 , c'est-à-dire le ET entre b_1 et b_2 (b_1b_2 est impair si b_1 et b_2 le sont). C'est la propriété d'homomorphisme multiplicatif. Notons cependant que le bruit sur le résultat est maintenant de l'ordre de $4r_1r_2$.

NETTOYER LE « BRUIT »

Cette méthode est donc parfaite à un détail près. Plus on fera de calculs successifs de XOR et de ET, plus le bruit introduit par les $2r$ augmentera en taille et cela en particulier à cause des ET. Ce n'est pas grave si l'on n'effectue que quelques opérations, mais cela devient très ennuyeux si le bruit atteint la taille de p , car alors on ne peut plus retrouver $(b_1 + b_2)$ et b_1b_2 .

En effet, si le bruit devient supérieur à p , le reste n'est plus comme il faut (car le quotient augmente de 1 ou plus) pour connaître la somme et le produit des deux bits codés. La méthode n'est bonne qu'à la condition d'opérer

VERS DES MACHINES À VOTER SÛRES ?

La question de savoir s'il faut développer l'utilisation de machines à voter est

exige

que des cryptologues compétents et des techniciens très qualifiés s'en occupent... ce qui n'est pas toujours le cas. Des appels à la prudence ont été émis par de nombreuses personnalités et mouvements. En France, un rapport du Sénat datant de 2014 préconisait le maintien du moratoire sur les machines à voter décidé en 2007.

La Cnil a aussi exprimé des réserves sur le vote électronique.

Les incidents et problèmes semblent trop nombreux pour qu'on envisage aujourd'hui de remplacer au niveau national le bulletin de vote, l'isoloir et l'urne fermée à clé par des ordinateurs s'échangeant des messages et que les citoyens devraient manipuler pour effectuer leurs devoirs électoraux.

Le site *Ordinateurs de vote* (www.ordinateurs-de-vote.org/) et le récent rapport *Ethics and electronic voting* de Chantal Enguehard (<https://hal.archives-ouvertes.fr/hal-01016256/document>) détaillent les raisons et les faits montrant qu'il faut être prudent et patient.

Cependant, rien n'interdit de chercher à concevoir des méthodes de vote

aussi rigoureuses que possible, permettant des contrôles *a posteriori* tout en garantissant l'anonymat des votes. Le calcul homomorphe présenté dans le présent article semble une voie sérieuse : il donne des garanties convenables concernant la protection du secret des votes et autorise le contrôle et le recalculation des résultats, tout en permettant à chacun d'être certain que son bulletin est pris en compte. Le système de vote par Internet Helios (<https://vote.heliosvoting.org/>), fondé sur le calcul homomorphe et développé par l'université Harvard et l'université catholique de Louvain, est disponible gratuitement et librement.

L'association internationale des chercheurs en cryptographie (IACR) l'utilise pour choisir les membres de son bureau... ce qui est un argument sérieux pour croire en ses qualités. Il faut se méfier de toutes les solutions précipitées en la matière, et il ne faut renoncer à aucune des garanties données par les procédures classiques de vote. Il ne fait cependant pas de doute qu'il y aurait des avantages à pouvoir voter de chez soi, et que si c'était possible de manière sûre, le coût de l'organisation d'élections en serait, en terme, considérablement réduit.



Machine à voter électronique utilisée à Aulnay-sous-Bois en 2007

CALCUL FLOU ET BOOTSTRAPPING

Le système de calcul homomorphe initialement conçu par Craig Gentry se retrouve dans tous les systèmes de calcul homomorphe inventés et perfectionnés depuis. La première idée est que les données doivent être chiffrées d'une manière floue, ce flou ne pouvant être effacé que par celui qui connaît la clé de déchiffrement. À mesure que les calculs homomorphes s'effectuent, le flou s'accroît – comme l'illustration ci-contre le symbolise. Après un certain nombre d'opérations, le flou devient si important que même avec la clé de déchiffrement, il est impossible d'accéder aux résultats. La seconde idée est qu'en s'y prenant bien (en demandant au système homomorphe d'exécuter l'opération de déchiffrement sur ses données, donc sans en prendre connaissance, et sans prendre connaissance des résultats), on réussit à effacer le flou

| | | | |
|--------------|--------------------|---------------|---------------------|
| $2 + 3 = 5$ | $5 \times 10 = 50$ | $50 + 2 = 52$ | $52 \times 5 = 260$ |
| $5 + 5 = 10$ | $5 \times 10 = 50$ | $50 + 2 = 52$ | $52 \times 5 = 260$ |
| $2 + 3 = 5$ | $5 \times 10 = 50$ | $50 + 2 = 52$ | $52 \times 5 = 260$ |
| $5 + 5 = 10$ | $5 \times 10 = 50$ | $50 + 2 = 52$ | $52 \times 5 = 260$ |
| $2 + 3 = 5$ | $5 \times 10 = 50$ | $50 + 2 = 52$ | $52 \times 5 = 260$ |
| $5 + 5 = 10$ | $5 \times 10 = 50$ | $50 + 2 = 52$ | $52 \times 5 = 260$ |

qui risquait de devenir irrécupérable. C'est le **bootstrapping**, opération miraculeuse analogue à celle du baron de Münchhausen qui s'élevait dans les airs en tirant sur ses bottes. Soigneusement conçu et réalisé, le nettoyage périodique des données est réellement possible et permet alors de mener des calculs homomorphes sans limitations de complexité : dès que le flou devient trop grand, on le réduit par **bootstrapping**.

Cela semble assez fou et cela ressemble à l'opération consistant à s'élever dans les airs en tirant sur ses bottes... c'est d'ailleurs pour quoi le nom donné à cette phase du calcul est **bootstrapping**. Pour que la phase de **bootstrapping** soit possible, il faut qu'un minimum d'opérations soient faisables sans que le bruit qui s'introduit soit devenu trop grand, et cela oblige à prendre des nombres entiers très longs pour p et les q_i , mais cela marche, et on dispose donc d'une méthode de calcul pleinement homomorphe comme on en rêvait. L'opération de **bootstrapping**, en nettoyant autant de fois que nécessaire les calculs partiels, rend possible des séries d'opérations aussi longues qu'on le souhaite de XOR et de ET; et on peut donc faire exécuter tout calcul par un opérateur extérieur qui ignorera ce qu'il calcule.

Puisque la taille des bits chiffrés $\ell(b)$ est nécessairement grande, les calculs effectués par l'opérateur extérieur sont très lourds, énormes comparés à ce qu'il faudrait faire si on ne souhaitait rien cacher, mais le but est atteint : on sait déléguer des calculs sans dévoiler ni les données ni le résultat.

ENCORE QUELQUES ORDRES DE GRANDEUR À GAGNER

Les travaux très nombreux sur ce sujet menés depuis 2009 ont visé à réduire les surcoûts en taille et en lourdeur de calcul des systèmes homomorphes. On progresse et des réalisations logicielles utilisant les idées mathématiques de ces travaux tentent de rendre les systèmes utilisables en pratique. La série d'opérations nécessaires au chiffrement de données par l'algorithme AES (Advanced Encryption Standard), très largement utilisé dans le monde entier, sert de repère pour mesurer les progrès des différents programmes de chiffrement homomorphe. On est ainsi passé, pour l'exécution de ce calcul test par un système homomorphe, de plusieurs heures (sur une machine courante) à quelques secondes.

C'est remarquable, mais pour que réellement on puisse envisager de confier massivement les calculs qu'on veut faire sur des données confidentielles à des opérateurs extérieurs qui les exécuteraient sans rien y voir, il faudra encore attendre un long moment, que le surcoût ait diminué de plusieurs ordres de grandeur. Certains experts tels que l'Américain Bruce Schneier restent réservés tant les surcoûts sont encore élevés. Aujourd'hui, la formidable idée de la cryptographie homomorphe est utile, par exemple pour la conception de systèmes de vote. Cependant, malgré une série d'idées intéressantes qui ont prouvé qu'elle était possible dans sa forme la plus générale, sa mise en œuvre pour tous, permettant plus de sécurité et une meilleure confidentialité sur les réseaux, devra encore attendre un peu. ■

un nombre limité d'opérations successives. Pour un calcul dépendant de plusieurs dizaines de bits $b_1, b_2, \dots, b_k$ présents dans une expression complexe utilisant beaucoup de XOR et de ET, le résultat obtenu par l'opérateur extérieur risque d'être devenu illisible à celui qui lui a confié le calcul. La méthode sans le perfectionnement qui va venir ne fonctionne qu'avec des calculs assez limités. C'est là qu'intervient la deuxième idée majeure de Craig Gentry. Elle consiste à nettoyer périodiquement le bruit pour éviter qu'il ne devienne trop important.

Pour cela, on fait déchiffrer le résultat du calcul partiel avant qu'il ne soit trop brouillé. Ce nettoyage enlève tout le bruit. On l'effectue en demandant à l'opérateur extérieur d'appliquer la fonction de déchiffrement sur le résultat partiel, c'est-à-dire de diviser par p et examiner la parité du reste obtenu. Suprême astuce : puisqu'on ne fait pas confiance à l'opérateur extérieur, on ne lui communique pas la clé de déchiffrement (le nombre p), mais on lui demande de faire ce déchiffrement par un calcul homomorphe utilisant la méthode qu'on vient de décrire ! Ce n'est possible bien sûr que si ce calcul homomorphe du déchiffrement n'est pas trop complexe, c'est-à-dire n'exige pas, une fois traduit en XOR et en ET, une succession trop longue de calculs : on s'en assurera.

BIBLIOGRAPHIE

K. YI ET AL., *Homomorphic Encryption and Applications*, Springer, 2014.

J. CORTIER ET S. KREMER, *Vote par Internet*, *Interstices*, 2013. https://interstices.info/jcms/nt_68258/vote-par-internet

M. VAN DIJK ET AL., *Fully homomorphic encryption over the integers*, *Advances in Cryptology - EUROCRYPT 2010*, Springer, pp. 24-43, 2010.

C. GENTRY, *Fully homomorphic encryption using ideal lattices*, *Proceedings of the 41st ACM Symposium on Theory of Computing*, pp. 169-178, 2009.

R. RIVEST ET AL., *On data banks and privacy homomorphisms*, *Foundations of Secure Computation*, Academic Press, pp. 169-180, 1978.

U N



N E M E U R T

J A M A I S.

EN TRIANT VOS JOURNAUX,
MAGAZINES, CARNETS, ENVELOPPES,
PROSPECTUS ET TOUS VOS AUTRES
PAPIERS, VOUS AGISSEZ POUR UN MONDE
PLUS DURABLE. DONNONS ENSEMBLE
UNE NOUVELLE VIE À NOS PRODUITS.

CONSIGNESDETRI.FR

CITEO

Le nouveau nom d'Eco-Emballages et Ecofolio

ESSENTIEL

Deux nombres premiers sont jumeaux, cousins ou sexy selon qu'ils sont respectivement séparés par 2, 4 ou 6.

Combien y en a-t-il ? Une infinité ? Probablement, mais les mathématiciens ne savent pas encore le démontrer.

Pourtanto, on peut s'intéresser à leur régularité au sein des

nombres entiers et étudier leur fréquence à partir de celle des nombres premiers.

On se rapproche peut-être de la preuve tant attendue avec un résultat récent selon lequel il y a une infinité de paires de nombres premiers consécutifs distants d'au plus 246. Reste à remplacer ce 246 par 2...

L'AUTEUR



BRUNO MARTIN
Maître de conférences
au laboratoire de recherche
en Mathématiques de l'université
du Littoral-Côte-d'Opale,
Calais.

Des jumeaux, des cousins et... des nombres sexy

La conjecture des nombres premiers jumeaux est l'un des problèmes non résolus les plus populaires en mathématiques. Des progrès extraordinaires ont été récemment accomplis, mais la route vers une démonstration est encore longue...

P

etit exercice : recherchez tous les nombres premiers inférieurs à 60. Comment avez-vous procédé ? Peut-être avez-vous testé pour chaque nombre s'il était divisible par un autre nombre que lui-même et 1, en faisant appel aux tables de multiplication ou même en utilisant une calculatrice ? Cela fonctionne, mais

c'est long ! Une technique plus rapide est le crible d'Ératosthène. Elle consiste à éliminer, parmi tous les nombres, les multiples de 2, puis de 3, de 5... afin de ne conserver que les nombres premiers. On peut ensuite visualiser la disposition des nombres premiers au sein des nombres entiers de plusieurs manières, l'une des plus originales et surprenante étant la spirale d'Ulām (voir l'encadré page 62).

Grâce au crible ou tout autre moyen, listons les nombres premiers plus petits que 200 : 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197 et 199. Devant cette liste, on peut s'interroger : existe-t-il une règle permettant de passer d'un nombre premier au suivant ? Par exemple, peut-on connaître le

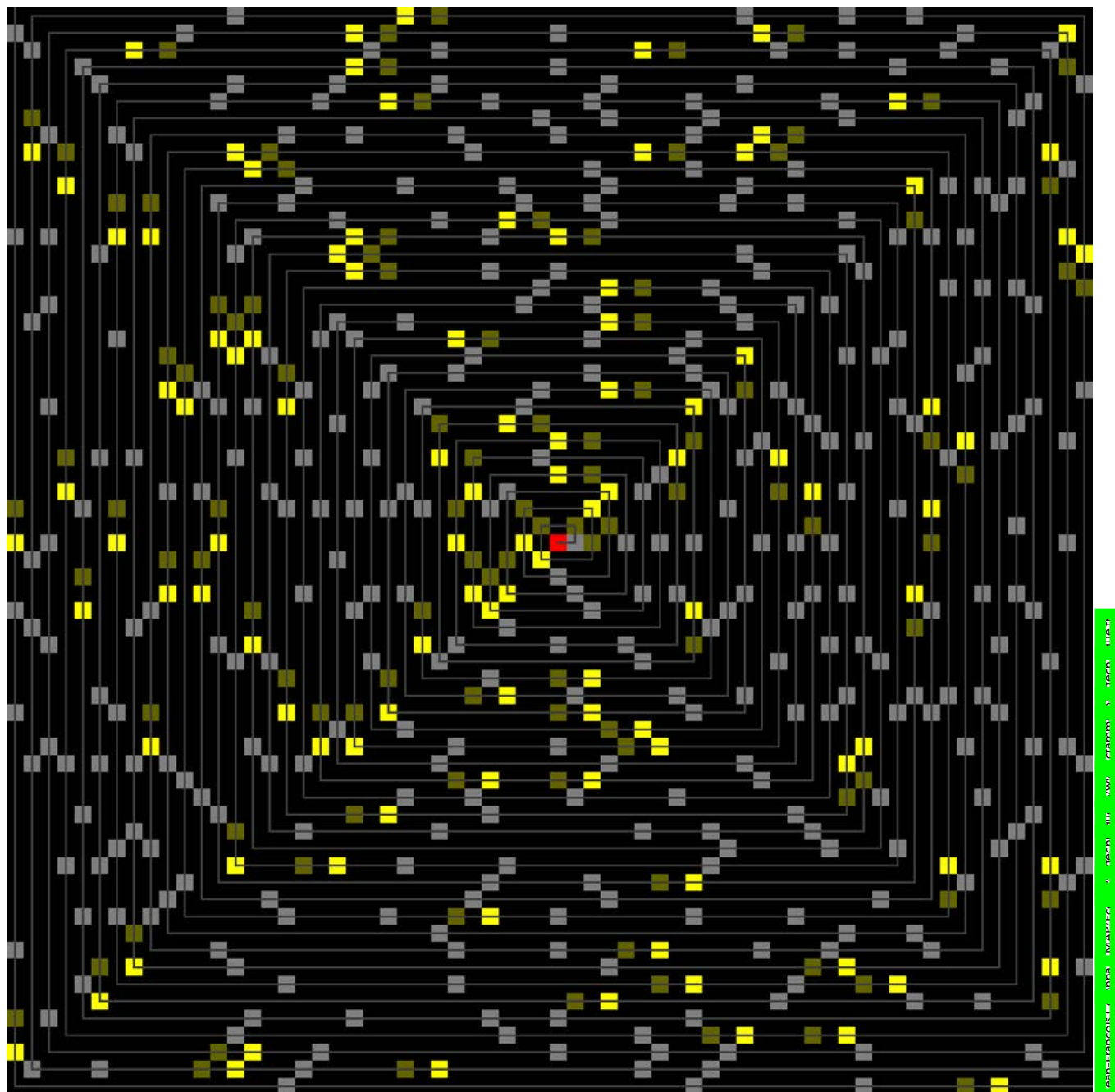


Illustration : J. Lagarias / The New York Times

nombre premier qui vient juste après 199 sans rester un par un les nombres qui suivent?

Au fait, est-on sûr qu'un nombre premier vient après 200? Rien *a priori* ne permet de l'affirmer. Bien sûr, en testant 201, 202, 203, 204... et on finit par ajouter 211 à la liste des nombres premiers. Le répit est de courte durée, car la question se repose immédiatement: y a-t-il un nombre premier après 211? Et ainsi de suite... En d'autres termes, la liste des nombres premiers s'arrête-t-elle à un moment donné?

UNE INFINITE DE PREMIERS

La réponse, certaine, est non. On sait prouver, depuis l'Antiquité, que la liste des nombres premiers est infinie. Le réservoir de nombres premiers est donc intarissable. Qu'en est-il alors d'une règle pour passer d'un nombre

Pour cette spirale d'Ulam le long de laquelle les entiers se suivent (1, en rouge), les paires de nombres premiers jumeaux apparaissent en jaune (sombre pour le premier de la paire, et vif pour le second).

premier au suivant? Pour répondre, intéressons-nous à l'écart entre deux nombres premiers consécutifs, par exemple, celui entre 3 et 5 (2), entre 7 et 11 (4), et entre 53 et 59 (6). Cet écart obéit-il à des règles particulières?

A l'exception de 2, tous les nombres premiers sont impairs. Donc l'écart entre deux nombres premiers consécutifs est toujours un nombre pair, sauf bien sûr celui entre 2 et 3.

Et à part ça? Ecrivons la liste des écarts successifs entre les nombres premiers consécutifs plus petits que 200: 1, 2, 2, 4, 2, 4, 2, 4, 6, 2, 6, 4, 2, 6, 4, 2, 6, 4, 6, 8, 4, 2, 2, 2, 4, 14, 4, 6, 8, 2, 10, 2, 6, 6, 4, 6, 6, 2, 10, 2, 4, 2... Aucune logique apparente. On remarque que l'écart le plus fréquent est 2 (il apparaît 16 fois), mais rien ne dit que cette prédominance se maintiendra lorsque l'on poursuivra

➤ a liste. Et d'ailleurs, est-on certain de voir apparaître le nombre 2 une 17^e fois? une 18^e? et ainsi de suite? Autrement dit: est-on certain de continuer inexorablement à rencontrer des nombres premiers consécutifs avec un écart de 2 comme 3 et 5, 5 et 7, 11 et 13, 17 et 19, 29 et 31, 41 et 43? De tels nombres sont des nombres premiers jumeaux. Nouvelle question: la liste des nombres premiers jumeaux s'arrête-t-elle?

On l'ignore. Les mathématiciens penchent pour la négative, et misent sur une infinité de nombres premiers jumeaux, mais personne n'est en mesure d'en donner une preuve irréfutable! Pourtant ce n'est pas faute d'avoir essayé. Si l'origine exacte de ce problème n'est pas certaine (la source la plus ancienne serait un article du mathématicien français Alphonse de Polignac écrit en 1849), on peut dire qu'il est l'objet de recherches intensives depuis plus de cent ans. C'est dire la difficulté!

Pour aborder ce problème, une première idée est de dire que nous ne sommes pas allés suffisamment loin dans l'expérimentation: nous n'avons observé que les nombres premiers jusqu'à 200. Avec un ordinateur, on peut aller bien au-delà et se faire une idée peut-être plus précise de l'évolution de la quantité de nombres premiers et des écarts entre nombres premiers consécutifs à mesure que l'on observe des nombres de plus en plus grands.

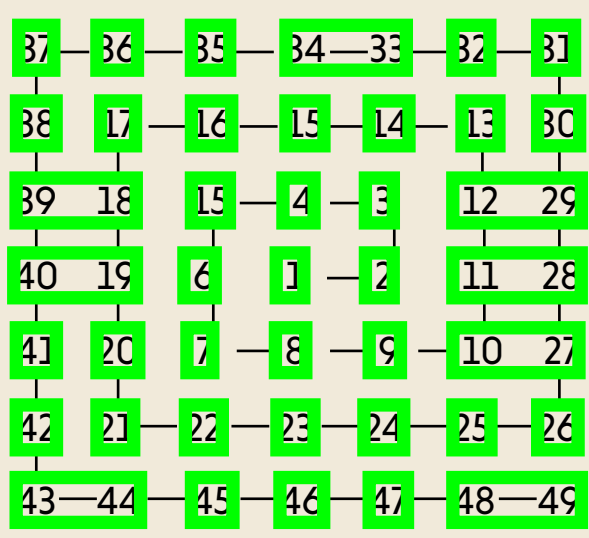
Une autre idée est d'examiner très attentivement les preuves connues de l'infinitude des nombres premiers, puis tenter d'adapter l'une de ces preuves pour en extraire des informations sur la liste des nombres premiers jumeaux.

Explorons d'abord la première piste, avec un ordinateur, pour aller au-delà de 200, par exemple jusqu'à 1 000 000. Les résultats: il y a 78 948 nombres premiers plus petits que 1 000 000. Et 8 169 paires de nombres premiers jumeaux parmi eux. C'est «beaucoup», mais ces chiffres seuls ne nous apprennent pas grand-chose. Il se pourrait par exemple que ces 78 948 nombres premiers soient tous situés entre 1 et 500 000 et qu'entre 500 000 et 1 000 000, il n'y en ait aucun, ce qui laisserait présager qu'au-delà de 500 000 il n'y a plus de nombres premiers.

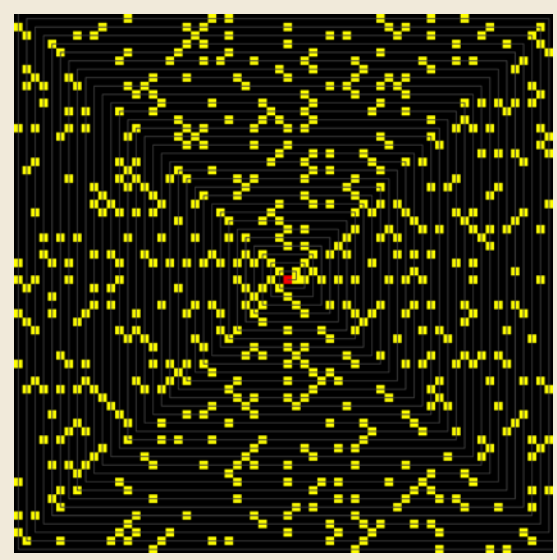
L'ESCALIER DES PREMIERS

Il est plus intéressant de suivre l'évolution de la quantité de nombres premiers rencontrés à mesure que nous progressons dans la suite des nombres entiers. Pour le visualiser, imaginons un promeneur qui avance sur un axe horizontal indexé par les nombres entiers. Dès qu'il tombe sur un nombre premier, il s'élève d'une marche, puis poursuit sa trajectoire à l'horizontale jusqu'à ce qu'il rencontre le nombre premier suivant. La hauteur à laquelle se trouve le promeneur

LA SPIRALE D'ULAM

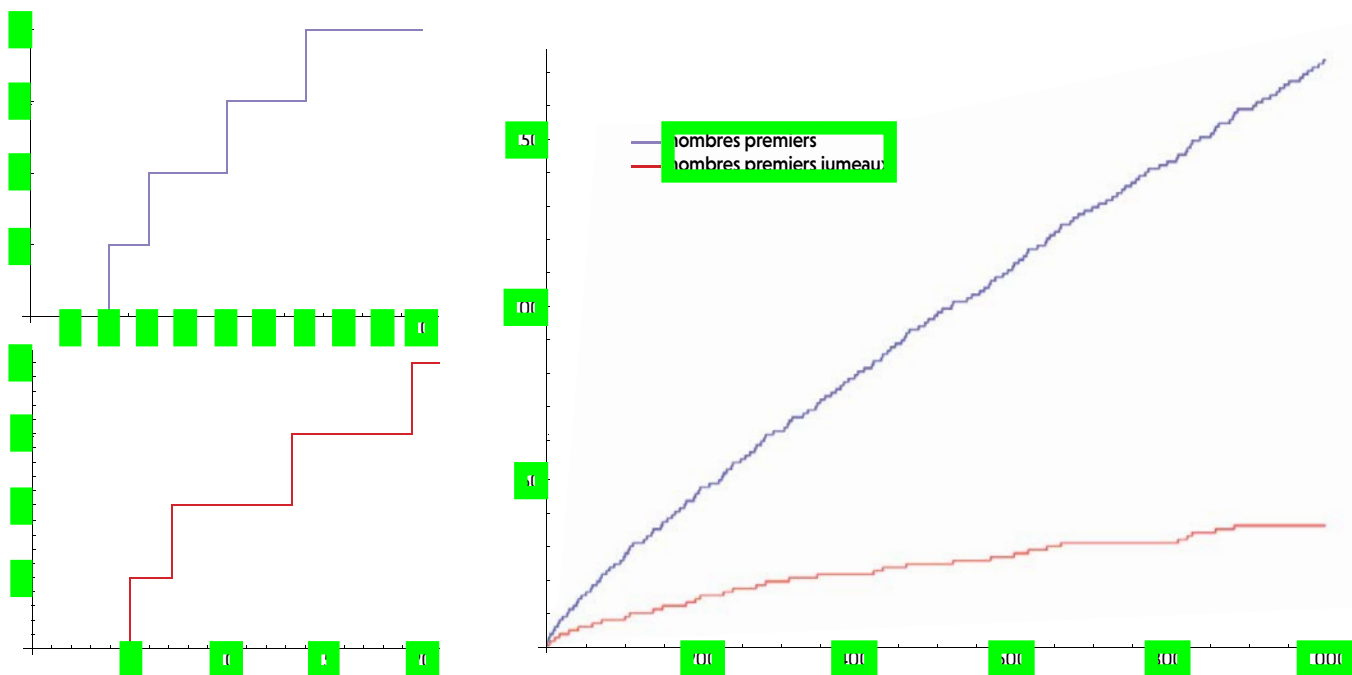


La légende raconte qu'un jour, s'ennuyant fermement lors d'une conférence, le mathématicien d'origine polonaise Stanisław Ulam, passa le temps en inscrivant sur un papier les entiers selon une spirale



En entourant les nombres premiers, il eut la surprise de les voir s'aligner, pour certains, le long de diagonales. Il y aurait donc un semblant de régularité, partielle, dans la répartition des nombres premiers.

CHANGEMENTS DE LA SPIRALE D'ULAM



correspond donc à la quantité de nombres premiers rencontrés depuis le début du parcours (voir la figure ci-dessus).

Au début (jusqu'à 10), les marches sont disposées de façon assez irrégulière, exactement comme le laisse prévoir la disposition d'apparence désordonnée des nombres premiers. Cependant, à mesure que l'on progresse vers 100, 1000... 1000000, et que l'on recule pour embrasser l'escalier du regard, l'ascension prend l'allure d'une courbe qui croît régulièrement et semble se confondre avec une droite : étonnant ! Cela signifierait-il que la quantité de nombres premiers rencontrés évolue à une vitesse quasi constante ? Y a-t-il autant de nombres premiers entre 1000 et 10000 qu'entre 10000 et 20000 ? entre 20000 et 30000 ?

Il n'en est rien. Voici quelques chiffres. On compte 1229 nombres premiers entre 1 et 10 000, 1033 entre 10000 et 20000, 983 entre 20000 et 30000, 958 entre 30000 et 40000. On devine un phénomène intrigant : on rencontre de moins en moins de nombres premiers. D'autres chiffres abondent dans ce sens. On croise 25 nombres premiers, soit 25%, entre 1 et 100, 170 (17%) entre 1 et 1000, 78498 (environ 7,8%) entre 1000 et 1000000...

La proportion de nombres premiers rencontrés semble donc diminuer progressivement à mesure que l'on parcourt la suite des nombres entiers. Autrement dit les nombres premiers semblent se raréfier ! Chose extraordinaire, on sait démontrer que ce phénomène de raréfaction a bien lieu. Mieux, il peut être quantifié grâce à une célèbre fonction des mathématiques, le logarithme népérien noté $\ln$, introduit dans un tout autre but par John Napier au XVII^e siècle. En effet,

les nombres premiers (en bleu) et les nombres premiers jumeaux (en rouge) semblent au départ progresser de façon erratique (en haut), mais avec du recul (en bas), on devine une certaine régularité.

en mettant en œuvre des idées lumineuses exposées par Riemann en 1852, Hadamard et La Vallée-Poussin ont démontré indépendamment en 1896 qu'à mesure que x croît, le nombre de nombres premiers plus petits que x , souvent noté $\pi(x)$, tend à se comporter comme $x/\ln x$ (plus précisément, le rapport des deux tend vers 1). Ce magnifique résultat porte le nom de «Théorème des nombres premiers», il établit avec certitude que les nombres premiers se raréfient et précise à quelle vitesse. Étudier plus précisément l'écart entre $\pi(x)$ et $x/\ln(x)$ est une question fascinante et difficile, liée à l'un des problèmes ouverts les plus importants en mathématiques, connu sous le nom d'hypothèse de Riemann (voir *L'hypothèse qui valait un million*, par P. Meier, page 68).

Retenons en définitive que le nombre de nombres premiers progresse avec une certaine régularité, pour peu que l'on s'aventure vers des nombres suffisamment grands. La succession des nombres premiers paraissait imprévisible, et voilà qu'avec un peu de recul, la répartition des nombres premiers ne paraît plus si chaotique !

DU CÔTÉ DES JUMEAUX...

On peut s'intéresser aux nombres premiers jumeaux avec la même approche, celle de l'escalier où chaque marche correspond à une paire de nombres premiers jumeaux. Échauffons-nous doucement. Jusqu'à 20, le nouvel escalier est élevé de quatre marches, ce qui correspond aux quatre premières paires (3, 5), (5, 7), (11, 13) et (17, 19) de nombres premiers jumeaux.

À mesure que l'on parcourt les entiers, l'escalier des nombres premiers jumeaux semble davantage irrégulier que celui des nombres premiers (voir la figure ci-dessus). Il comporte

quelques marches relativement longues, sortes de déserts de nombres premiers jumeaux. L'allure laisse même penser que le nombre de nombres premiers jumeaux ne va pas dépasser 50! Se dirige-t-on vers une extinction des nombres premiers jumeaux?

Non. En atteignant 1000000, on constate que l'escalier des nombres premiers jumeaux continue de s'élever, lentement mais apparemment sûrement. Il semble raisonnable de conjecturer que la liste des nombres premiers jumeaux ne s'arrête jamais. Et parmi les nombres premiers, quelle est la proportion de nombres premiers jumeaux? Et comment évolue cette proportion?

A l'instar des nombres premiers parmi les entiers, les nombres premiers jumeaux se raréfient au sein des nombres premiers. Qui plus est, ce comportement semble lui aussi relié à la fonction logarithme népérien. Seulement voilà, dans le cas des nombres premiers jumeaux, on ne dispose d'aucune démonstration à l'appui de ces observations. Rien ne nous permet de garantir que ces phénomènes (apparition de nombres premiers jumeaux, leur raréfaction...) perdurent indéfiniment.

.. ET DES COUSINS SEXY

Nous en sommes venus à parler des nombres premiers jumeaux après avoir observé le caractère en apparence aléatoire des écarts entre nombres premiers successifs. Que se passe-t-il pour les nombres premiers consécutifs distants de 4 (les nombres premiers cousins)? de 6 (les nombres premiers sexy)? Ces deux listes sont-elles aussi infinies? Là encore, on pense que c'est le cas, mais le mystère plane tout autant.

On peut aussi se poser la question: y a-t-il plus de nombres premiers jumeaux ou de nombres premiers cousins, c'est-à-dire plus souvent des sauts de 2 ou de 4? Jusqu'à 1000, les escaliers correspondant aux nombres premiers jumeaux et aux nombres premiers

la progression relative des nombres premiers jumeaux (en rouge), cousins (en vert) et sexy (en violet) semble incertaine au départ (à gauche). Les choses s'éclaircissent (à droite): les sexy l'emportent largement.

cousins se dépassent mutuellement à plusieurs reprises (voir la figure ci-dessous). Ce phénomène de chevauchement se poursuit-il? Avec plus de marches (jusqu'à 1000000), les deux courbes semblent confondues! En zoomant, on observerait que les deux courbes semblent poursuivre ce jeu de dépassements successifs.

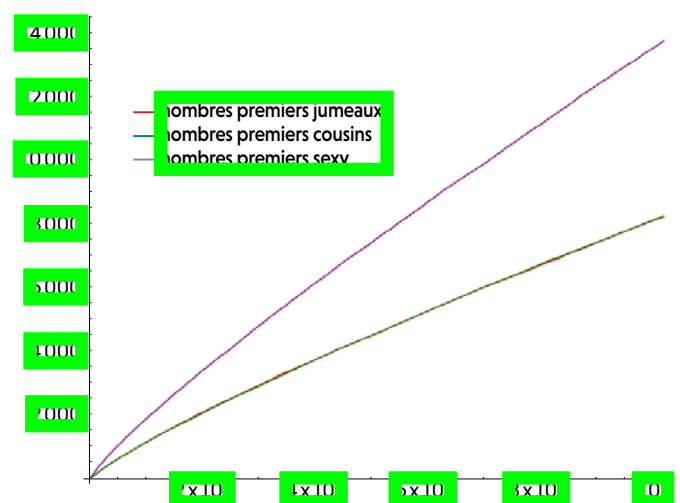
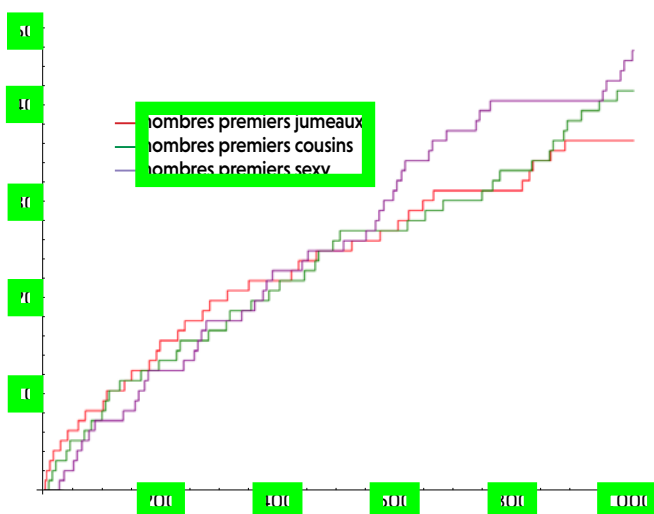
Qu'en est-il lorsque les nombres premiers sexy sont de la partie? Ils sont légèrement en tête à 1000 et s'imposent définitivement, et de manière très nette, au-delà. Entre les écarts 2, 4 et 6, ce dernier serait ainsi prépondérant. Nous pourrions poursuivre nos observations et multiplier les conjectures, sur la base de calculs numériques, en nous intéressant à tous les écarts possibles (tous les nombres pairs!). Privilégions plutôt un détour par les probabilités.

Dans ce domaine, les mathématiciens partent d'un constat audacieux: certes, la répartition des nombres premiers est parfaitement déterminée par leur définition, mais cette répartition n'est finalement pas si éloignée de ce que l'on obtiendrait en jouant à la loterie pour savoir quel nombre est premier.

Pas n'importe quelle loterie bien sûr! Le fonctionnement schématique est le suivant: on connaît la proportion de nombres premiers entre 1 et disons 1000000, soit environ 7,8%. Imaginez alors que pour chaque nombre, on tire la pile ou face pour décider son statut, premier ou pas, sachant que notre pièce est truquée de façon à donner pile dans seulement 7,8% des cas. Notre loterie est en fait un peu plus compliquée car on ne veut pas se limiter à 1000000, et elle fait intervenir le logarithme.

A partir de cette hypothèse d'apparence farfelue, les mathématiciens se livrent à des calculs de probabilité, relativement aisés, et aboutissent à des formules qui sont généralement en accord avec les expérimentations numériques: incroyable!

Pour résumer, tout se passe comme si les mathématiciens, partant d'une observation erronée, mais pas si éloignée de la réalité,



avaient construit une boule de cristal (on dit un modèle) permettant de réaliser des prédictions (ou des conjectures!) sur les nombres premiers, jumeaux, cousins... qui semblent fiables. Cette boule de cristal prédit par exemple qu'il y a une infinité de nombres jumeaux, qu'ils apparaissent régulièrement, et même qu'il finit par y avoir plus de nombres premiers sexy que de jumeaux. En revanche, elle reste muette quand à ces dépassements perpétuels entre cousins et jumeaux.

Pouvons-nous faire une confiance aveugle à cette boule de cristal? Non, ces considérations probabilistes ne fournissent pas la moindre démonstration. Quel est leur intérêt en ce cas? De nous aiguiller dans ce que l'on croit être la bonne direction, ce qui n'est pas rien. Il s'agit maintenant de construire les outils théoriques qui jetteront un pont entre probabilité et réalité! Mais le gouffre qui sépare les deux semble infranchissable aujourd'hui, tout du moins pour la conjecture des nombres premiers jumeaux.

Nous avons précédemment conjecturé qu'il y a une infinité de paires de nombres jumeaux, une hypothèse que nous avons étayée par plusieurs graphiques. Mais la question reste entière: comment démontrer cette conjecture? Commençons par oublier que ce problème est sans solution depuis près de deux siècles...

UN PROBLÈME « FACILE »

Une idée naturelle dans cette situation est de se mesurer à un autre problème, assez similaire mais plus simple. Puis, une fois le problème « facile » résolu, on cherche à modifier adéquatement la solution pour qu'elle s'applique au problème de départ. Ici le problème « facile » est tout trouvé: sait-on démontrer que la liste de tous les nombres premiers ne s'arrête jamais?

Mais avant même d'attaquer la première étape – bien comprendre une preuve du fait qu'il y a une infinité de nombres premiers –, concentrons-nous sur la notion délicate d'infinité. Comment démontrer que la liste d'une certaine famille de nombres ne s'arrête jamais?

Partons d'une situation familière. Les enfants demandent souvent: « Quel est le plus grand nombre? » « Il n'y en a pas, car ça ne s'arrête jamais », leur répond-on, et c'est souvent le début d'une réflexion silencieuse ou d'une avalanche de questions. Un moyen de les convaincre est d'ajouter: « Prends n'importe quel nombre. Tu peux toujours ajouter 1 pour obtenir un nombre plus grand. »

Avec cette « recette » (ajouter 1), on fabrique une infinité de nombres. Grâce à cette technique, on peut prouver que certaines familles de nombres sont de taille infinie, comme celle des nombres impairs avec, par exemple, la recette: prenez un nombre impair et ajoutez 2. Peut-on trouver une recette de ce

genre pour prouver que la liste des nombres premiers ne s'arrête pas? C'est difficile.

LA RECETTE D'EUCLIDE

Le mathématicien grec Euclide en a le premier trouvé une satisfaisante, qu'il a consignée dans son traité *Les Éléments*, vers 300 avant notre ère. La recette est astucieuse et nécessite quelques efforts. Mais le résultat en vaut la chandelle!

Nous allons avoir l'usage d'une propriété toute simple: deux nombres consécutifs n'ont qu'un seul diviseur en commun, le nombre 1. Par exemple, 99 et 100 ont pour diviseurs respectifs (1, 3, 11, 33, 99) et (1, 2, 4, 5, 10, 20, 25, 50, 100). On le démontre ainsi. Prenez deux nombres consécutifs et considérez un nombre qui les divise tous les deux. Il divisera aussi leur différence. Or cette différence vaut 1. Donc ce diviseur commun aux deux nombres de départ

Au-delà de 1 000,
les nombres sexy
s'imposent définitivement
face aux nombres
jumeaux et cousins

divise 1, ce qui nous laisse peu de doutes sur son identité: ce diviseur vaut 1.

Une autre propriété cruciale est que tout nombre est divisible par (au moins) un nombre premier. Ce sera la clé de voûte de la preuve d'Euclide. Quelques exemples vont guider notre démonstration. La liste des diviseurs de 45 est (1, 3, 5, 9, 15, 45), parmi lesquels 3 et 5 sont premiers. La liste des diviseurs de 61 est (1, 61): c'est un nombre premier. La liste des diviseurs de 32 est (1, 2, 4, 8, 16, 32) et 2 est bien un nombre premier.

La démonstration repose sur l'observation suivante: si l'on dresse la liste des diviseurs strictement plus grands que 1 d'un nombre, le plus petit d'entre eux est toujours un nombre premier, les exemples précédents en attestent. Imaginons que ce plus petit

diviseur, notons-le $n^{\circ} 1$, ne soit pas premier. Puisqu'il n'est pas premier, $n^{\circ} 1$ est donc divisible par un nombre, $n^{\circ} 2$, strictement plus petit que $n^{\circ} 1$ et strictement plus grand que 1. Mais ce $n^{\circ} 2$ divise $n^{\circ} 1$ qui lui-même divise le nombre de départ. Donc $n^{\circ} 2$ divise le nombre de départ. Voilà qui est gênant : deux nombres différents se disputent la place de plus petit diviseur du nombre de départ. Notre hypothèse de départ (le plus petit diviseur n'est pas premier) ne tient pas la route : ce plus petit diviseur est forcément premier.

Nous sommes maintenant en mesure de donner cette recette d'Euclide qui montre que la liste des nombres premiers est inépuisable. Prenons un exemple avec les nombres premiers 2, 3 et 5, et formons le produit $2 \times 3 \times 5$ (sans effectuer le calcul). Ce nombre est divisible par 2, 3 et 5. Maintenant ajoutons 1 : $2 \times 3 \times 5 + 1$. Les deux nombres $2 \times 3 \times 5$ et $2 \times 3 \times 5 + 1$ sont bien consécutifs. D'après la première propriété, ils n'ont donc aucun diviseur en commun si ce n'est 1. Le nombre $2 \times 3 \times 5 + 1$ n'est donc divisible ni par 2, ni par 3, ni par 5. Pourtant la deuxième propriété nous dit qu'il possède un diviseur qui est un nombre premier. Nous venons de montrer qu'il se trouve un nombre premier qui est différent de 2, 3 et 5. Inutile de savoir de quel nombre il s'agit : il existe et il est différent des nombres premiers 2, 3, 5 déjà connus. C'est tout ce que l'on voulait.

Voici donc une recette de fabrication d'un nouveau nombre premier à partir de plusieurs autres : prenez plusieurs nombres premiers, multipliez-les entre eux, ajoutez 1 au résultat et vous obtenez un nombre divisible par un nouveau nombre premier différent de ceux du départ. Avec cette recette, la liste des nombres premiers pourra toujours être agrandie : il y a une infinité de nombres premiers.

LE PROBLEME RESTE ENTIER

La première étape de notre plan, résoudre un problème « facile » est franchie. Passons à la deuxième. Peut-on s'inspirer de cette recette de fabrication de nombres premiers pour en former une qui produise des nombres premiers jumeaux ? Peut-être, mais jusqu'à présent personne n'y est parvenu. Et l'on ignore toujours s'il y a une infinité de nombres premiers jumeaux.

Après Euclide, d'autres mathématiciens ont produit de nouvelles démonstrations du fait qu'il y a une infinité de nombres premiers. Des chercheurs très inventifs s'en sont inspirés pour essayer de prouver qu'il existe une infinité de nombres premiers jumeaux. Cela a débouché sur la construction de théories mathématiques incroyablement élaborées qui n'ont pourtant pas encore permis de résoudre ce problème.

Néanmoins on s'en rapproche... la preuve avec un résultat récent obtenu par les efforts

conjointes de plusieurs chercheurs. Prenez la liste des nombres premiers jumeaux, celle des nombres premiers cousins, celle des sexy et regroupez-les dans une même liste. On n'est pas encore capable de montrer que cette nouvelle liste ne s'arrête pas. Ajoutez les nombres premiers consécutifs distants de 8, puis ceux de 10, puis ceux de 12... jusqu'à ajouter les nombres premiers consécutifs distants de 246. Et bien la liste ainsi obtenue ne se termine pas, on sait maintenant le prouver !

DE 70 000 000 A 246

De façon synthétique, on peut dire qu'il y a une infinité de paires de nombres premiers consécutifs distants d'au plus 246. Ce résultat peut paraître curieux, et peu étonnant. Il est pourtant qualifié d'extraordinaire par les experts des nombres premiers. En fait, il y a encore six ans, personne n'était capable de prouver un résultat de ce type, même en remplaçant 246 par un entier N beaucoup plus grand.

Pourquoi 246 ? Dans un premier temps, en 2013, le mathématicien chinois Yitang Zhang a établi le résultat pour $N = 70\,000\,000$ qui a stupéfait et passionné la communauté mathématique. Pouvait-on améliorer la preuve d'Yitang Zhang et remplacer 70 000 000 par un nombre bien plus petit ? Plusieurs chercheurs se sont lancés dans l'aventure et ont entamé une collaboration intensive via un forum public de discussion sur Internet. Cette pratique, relativement neuve dans le milieu, avait été conceptualisée et lancée par le mathématicien anglais Tim Gowers sous le nom de *Polymaths*. Chaque projet *Polymath* réunit virtuellement un groupe plus ou moins important de chercheurs intéressés autour d'un problème ouvert bien précis, et pour un laps de temps plus ou moins long. Toute publication qui en résulte est signée sous le pseudonyme collectif D. H. J. Polymath.

Après une succession d'améliorations, une nouvelle percée du jeune mathématicien anglais James Maynard, puis de nouvelles améliorations, le projet *Polymath* n° 8 parvint à ce fameux 246. Mais même avec ces progrès extraordinaires, établir la conjecture des nombres premiers jumeaux (ce qui en somme consisterait à remplacer ce 246 par 2) semble hors d'atteinte actuellement aux dires des spécialistes.

Le chemin qui mène à une démonstration de cette conjecture semble donc encore bien long. Et pire encore, une telle preuve, si elle venait à être trouvée, resterait probablement incompréhensible à toute personne n'ayant pas un solide bagage mathématique. Alors que vous veniez juste de vous attaquer au problème avec un papier et un crayon... ■

Cet article est adapté de celui paru sur le site du CNRS *Images des Mathématiques* : <http://images.math.cnrs.fr/> Nous remercions les équipes de nous avoir autorisé à le reproduire

BIBLIOGRAPHIE

J.-P. DELAHAYE, *Merveilleux nombres premiers. Voyage au cœur de l'arithmétique*, Belin, 2013.

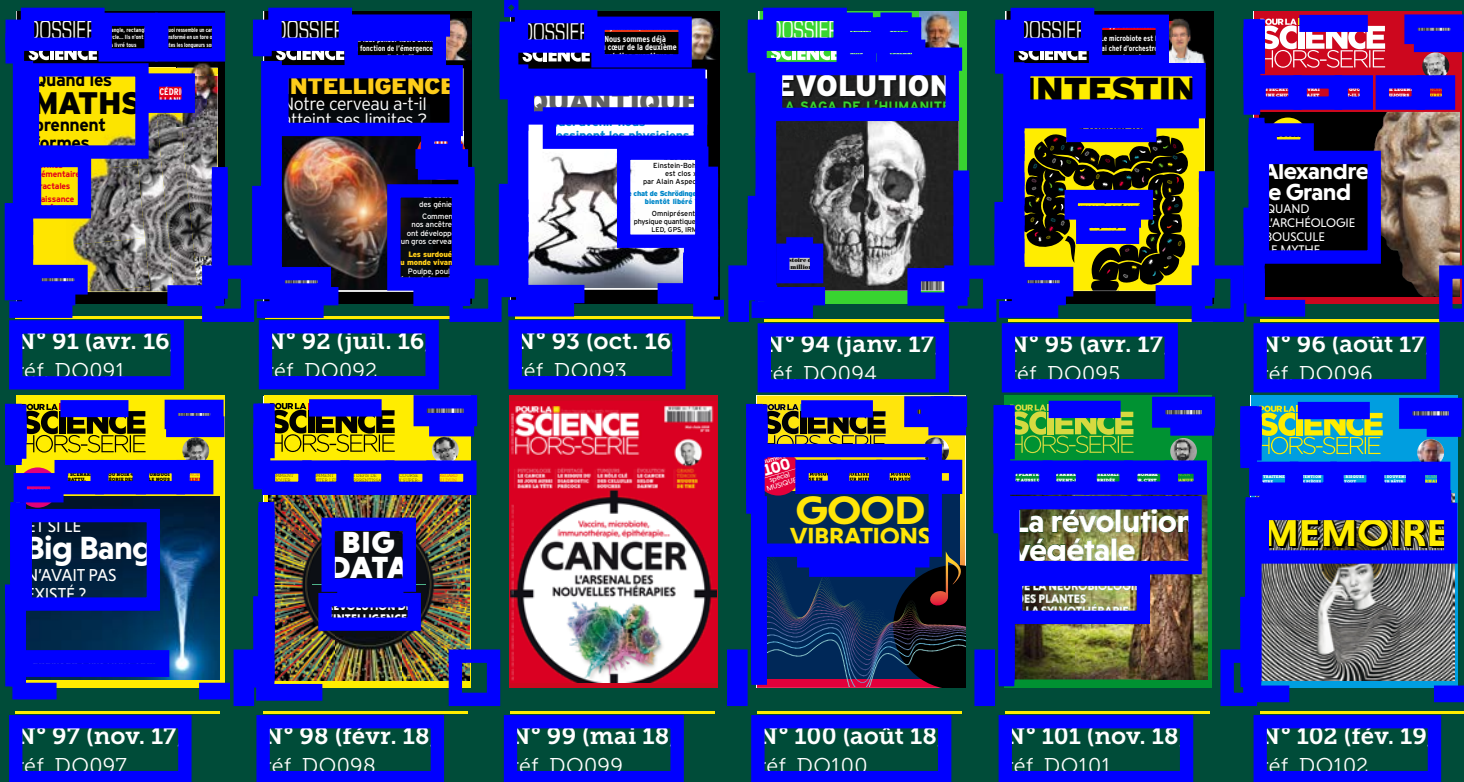
M. DU SAUTOY, *La symphonie des nombres premiers*, Seuil, 2007

J. DERBYSHIRE, *Dans la jungle des nombres premiers*, Dunod, 2007.

POUR LA SCIENCE HORS-SERIE

Edition française de Scientific American

COMPLÉTEZ VOTRE COLLECTION DÈS MAINTENANT!



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

Je retournerai accompagné de votre règlement à :

Pour la Science - Service VPC - 15 rue de Montparnasse - BP 20055 - 75042 Paris Cedex 12 - email: bonnasscience@lapresse.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 :

| | | | | | | |
|----------------------|-------|----------------|-------|-----------|-------|---|
| 1 ^{re} réf. | _____ | 2 ^e | _____ | 10,90 € = | 10,90 | € |
| 2 ^e réf. | _____ | 3 ^e | _____ | 10,90 € = | _____ | € |
| 3 ^e réf. | _____ | 4 ^e | _____ | 10,90 € = | _____ | € |
| 4 ^e réf. | _____ | 5 ^e | _____ | 10,90 € = | _____ | € |
| 5 ^e réf. | _____ | 6 ^e | _____ | 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 vous poser toute question concernant le traitement de vos données personnelles), vous pouvez nous contacter par courriel à bonnasscience@lapresse.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 : 10 bis, boulevard du Montparnasse - CS20012 - 75680 Paris Cedex 14 - Sarl au capital de 32000 € - RCS Paris B 3117 97 393 - Siren 3117 97 393 000 23 - APE 5814



PLUS SIMPLE. PLUS RAPIDE

ABONNEZ-VOUS SUR BOUTIQUE.POURLASCIENCE.FR

ESSENTIEL

La répartition des nombres premiers est un défi pour les mathématiciens. La fonction ζ de Riemann apporte des informations sur cette répartition.

► Cette fonction ζ , au départ définie pour

une variable complexe s , la partie réelle $\text{Re}(s)$ 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 ζ s'annule) se trouvent tous sur la droite verticale $\text{Re}(s)=1/2$. 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.



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

L'hypothèse qui valait un million

La fonction ζ 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.

L

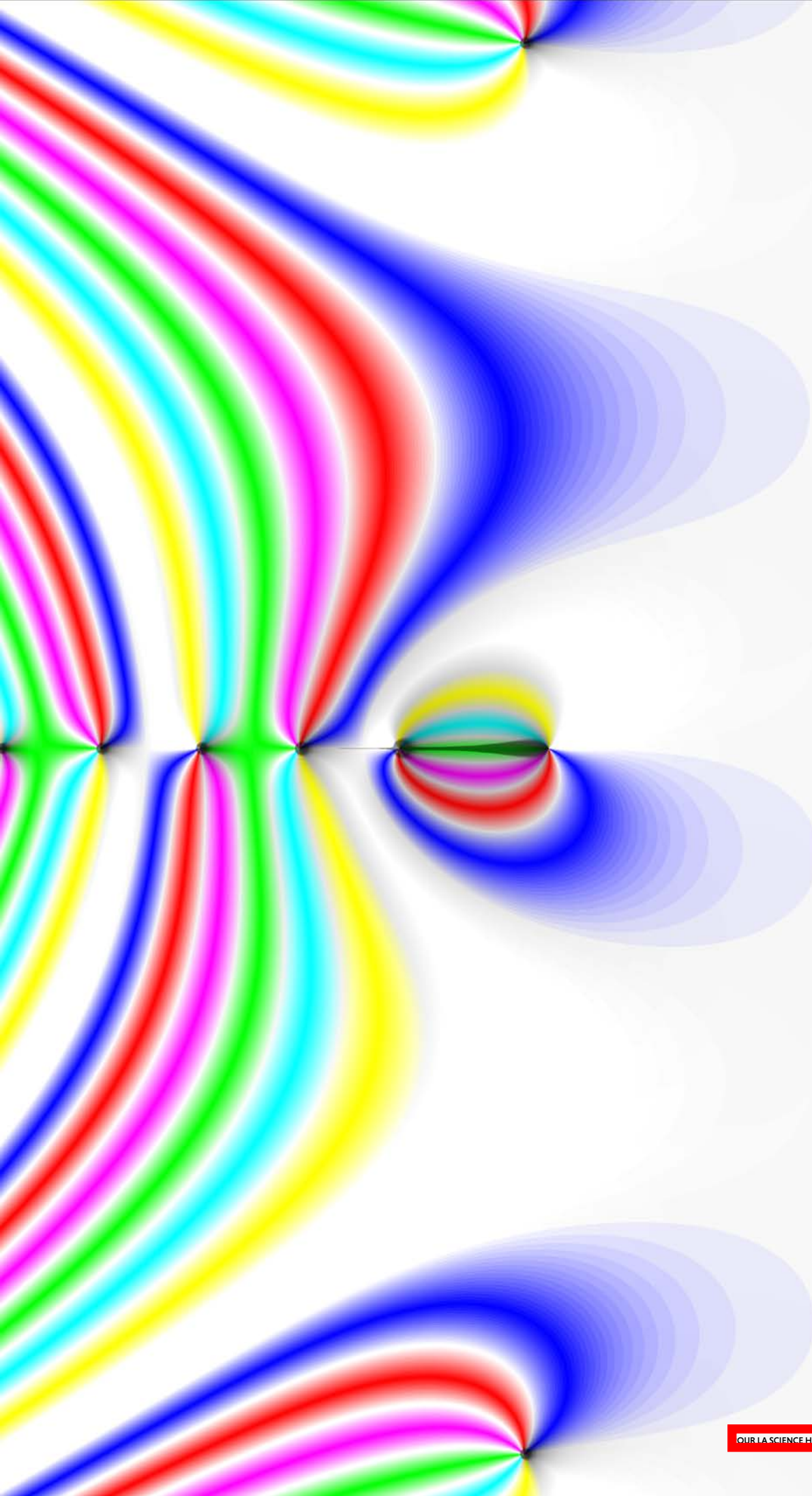
ors du deuxième Congrès international des mathématiciens, à Paris, en août 1900, le mathématicien David Hilbert dresse une liste de vingt-trois problèmes alors irrésolus. Selon lui, ils montraient la voie vers le xx^e siècle. Où en est-on aujourd'hui? Quelques-uns, environ une dizaine, ont été résolus.

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 IMPRESSIONNANT

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 ζ de Riemann, ζ , est calculée pour des points du plan complexe $s=x+iy$. Dans le domaine représenté, 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 :

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

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

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

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 »

Domage... 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 jumeaux*, 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 :

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

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 :

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

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 :

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \frac{1}{p^{3s}} + \dots \right)$$

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) :

$$\zeta(2) = 1 + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \dots = \frac{\pi^2}{6}$$

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'IDEE CLE 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 : $\exp(z) = e^z = 1 + z/1! + z^2/2! + z^3/3! + \dots$

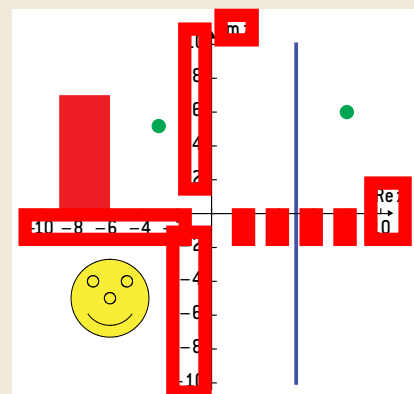
Certaines choses changent peu dans cette extension aux nombres complexes. La série d'Euler converge pour s réel supérieur à 1; cette condition devient maintenant que la partie réelle de s , notée $\text{Re}(s)$, soit supérieure à 1. Sur la droite réelle, le point 1 est la barrière qui bloque la convergence 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, $i^2 = -1$. 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 » $\text{Re}(z)$ de z et b sa « partie imaginaire » $\text{Im}(z)$. 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 : $f(z) = a_0 + a_1(z - z_0) + a_2(z - z_0)^2 + \dots$ La valeur de f en chaque point z (complexe) est donc définie par une somme infinie. Les coefficients a_n 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 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 1 (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 $s=1$.

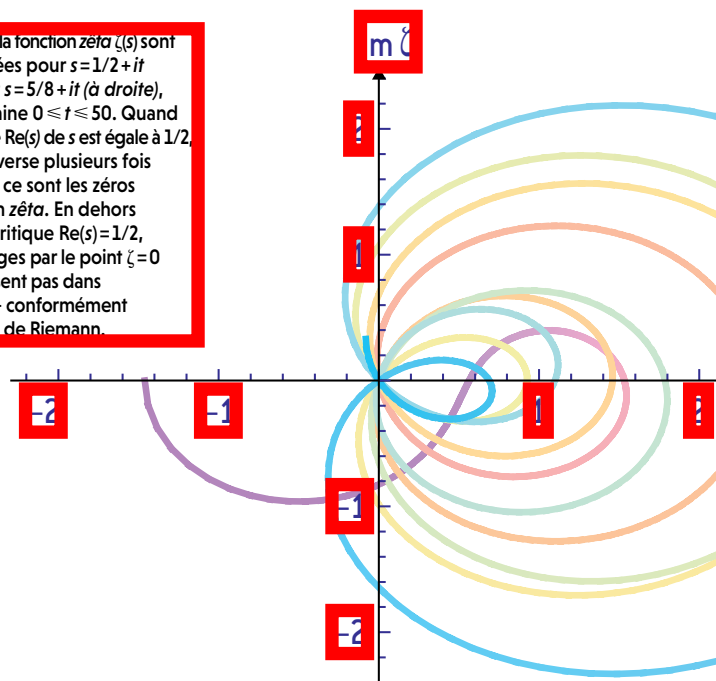
La valeur $s=1$ est pour la fonction zêta ce que le mathématicien nomme une singularité. La fonction prend ici inévitablement une valeur infinie. Lorsqu'on se restreint à la droite réelle, la singularité constitue une barrière infranchissable; mais dans le plan, on peut simplement la contourner.

RELIER ZETA 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: $\Gamma(n) = n! = n(n-1)(n-2) \dots 2 \cdot 1$.

Pour tous les nombres complexes distincts de $0, -1, -2, -3$, etc., la fonction gamma prend des valeurs finies. Grâce aux techniques de la

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 $0 \leq t \leq 50$. Quand la partie réelle $\text{Re}(s)$ 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 $\text{Re}(s)=1/2$, de tels passages par le point $\zeta=0$ ne se produisent pas dans le domaine – conformément à l'hypothèse de Riemann.



théorie des fonctions, Riemann obtint la relation suivante entre les fonctions zêta et gamma:

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

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 un «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 $s=0, -2, -4, \dots$ une valeur infinie. Mais si l'on choisit pour l'une de ces valeurs ($s=-2n$ pour un entier naturel n), le membre de droite de l'équation

UNE FORMULE REMARQUABLE

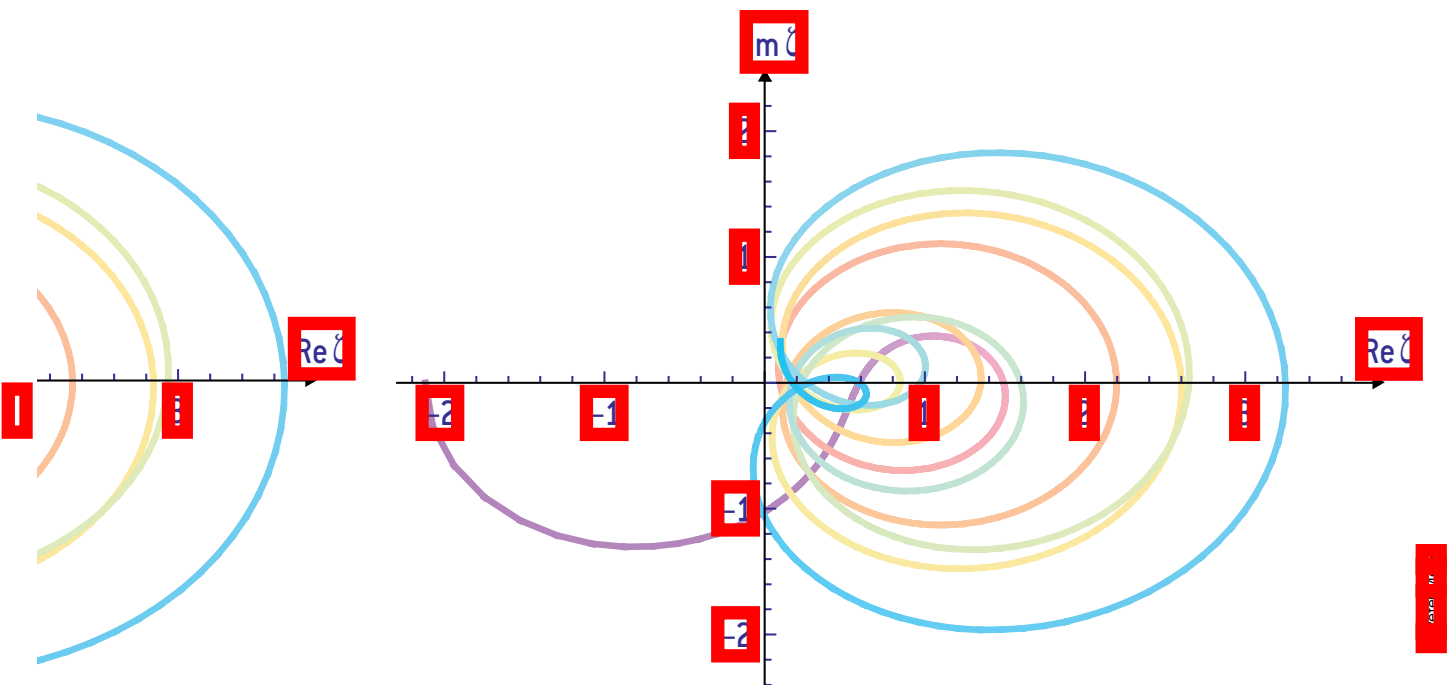
Leonhard Euler a obtenu la formule $1+1/2^2+1/3^2+1/4^2+1/5^2+\dots=\pi^2/6$ en représentant non pas la fonction zêta $\zeta(s)$, mais la fonction $(\sin x)/x$, de deux façons: d'une part comme une somme infinie, d'autre part comme un produit infini. Des multiplications et transformations habiles le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

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

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 $B_0=1, B_1=-1/2, B_2=1/6, B_3=-1/30, B_4=1/42$; pour les nombres impairs $j \geq 3$, on a $B_j=0$. Une formule simple analogue pour les valeurs de la fonction $\zeta(s)$ 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:

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

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.



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 on le verra, aucune 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:

$$N(T) = \frac{T}{2\pi} \left(\pi \left(\frac{T}{2\pi} \right) + o\left(\frac{T}{2\pi}\right) \right)$$

Le terme d'erreur

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 $\pi(x) \approx x/\ln x$, formule qu'il avait plus tard raffinée en $\pi(x) \approx \text{li}(x)$, où $\text{li}(x)$ est le «logarithme intégral», défini par $\text{li}(x) = \int_2^x \frac{du}{\ln u}$. Le signe $\approx$ signifie ici «à un terme correctif près, qui est petit par rapport à $\text{li}(x)$ 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: $\zeta(s) = a_0 + a_1 s + a_2 s^2 + \dots + a_n s^n$

Un polynôme a coefficients a_i complexes et le 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 $a(1-s/s_1)(1-s/s_2)\dots(1-s/s_n)$, 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 $(1-s/p)$, où p parcourt les zéros non triviaux, avec quelques ingrédients supplémentaires :

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

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

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 resource for the aficionado and virtuoso alike*, Springer, 2008.

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 les « formules de traces » qui présentent une

LA FONCTION GAMMA

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

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

Des théorèmes classiques du calcul intégral donnent :

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

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 Jonathan 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

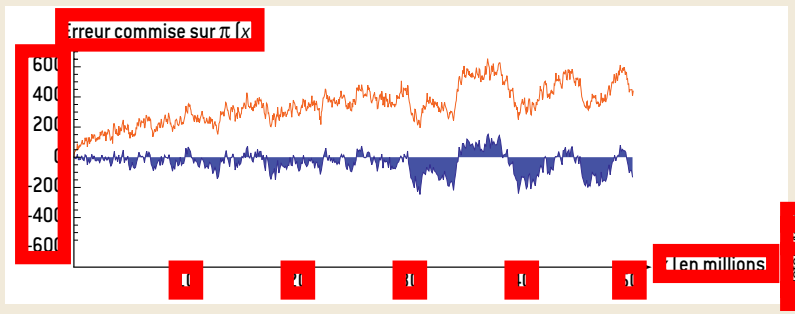
On montre même qu'il existe une infinité de nombres t vérifiant cette approximation pour une fonction f et un nombre ϵ donnés. En quelque sorte, la fonction zêta contient donc dans ses valeurs des informations sur toutes ces fonctions f . Un peu comme s'il s'agissait d'un atlas contenant toutes les cartes 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 $\pi(x)$

$$\pi(x) \sim \sum_{p \leq x} \frac{1}{p} = \text{li}(x) - \sum_{\rho} \text{li}(x^{1-\rho}) - \int_{-\infty}^{\infty} \frac{t}{(t^2-1)\ln t} dt$$

Cette formule relative au nombre $\pi(x)$ de nombres premiers inférieurs à x est valable pour tout $x \geq 2$ 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.



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 fautive, 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 $\text{Re}(s)=1/2$.

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'UQAM 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.

L

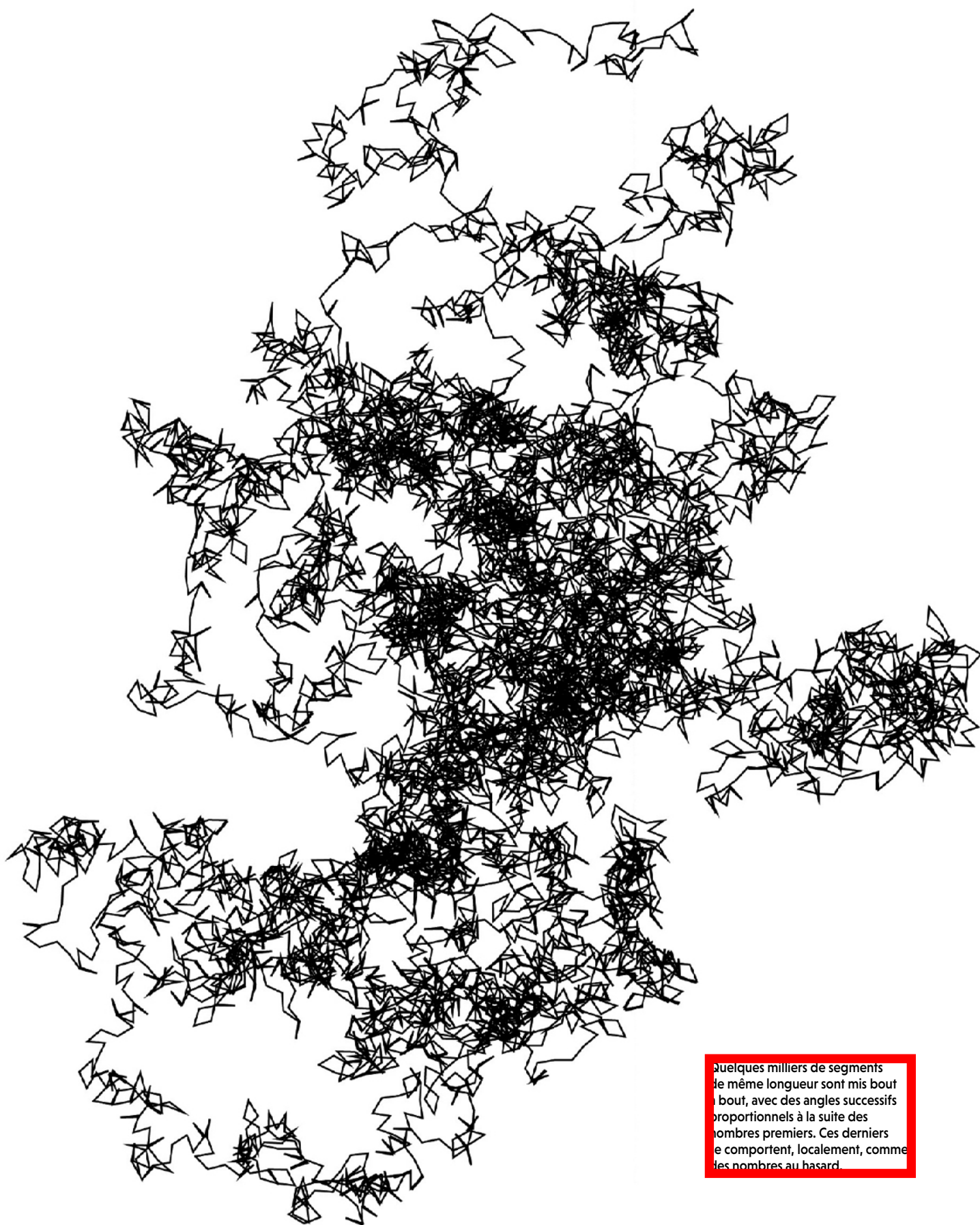
Le 7 décembre 2018, un record a été battu, celui du plus grand nombre premier connu. $2^{82589933} - 1$, qui comporte près de 25 millions de chiffres en écriture décimale. On doit cette performance (la vérification est en cours) au *Gimps*, le *Great Internet Mersenne Prime Search*. Ce projet, fondé 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 : $\varphi(n) = n^2 + n + 41$. 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 les nombres au hasard.

$$n^6 - 5n^5 + 1493n^4 - 1027n^3 + 100471n^2 - 11971n - 57347$$

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

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

une formule qui peut donner un nombre arbitraire de nombres premiers. Si $A = 1,30637/788,38630806904686144926...$ alors $[A^{3^n}]$ donne une suite arbitraire de nombres tous premiers. Ici $[]$ 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 8^e terme a déjà 762 chiffres, et le 20^e environ six milliards!

En 1951, le Britannique Edward Wright en proposait une autre, si $g_n = \alpha = 1,928/800...$ et $g_{n+1} = 781$ alors $10^{g_n} - 1 = 2 \times 10^{g_n} - 1$ est toujours premier. Les nombres premiers consécutifs sont uniquement représentés par α . La suite obtenue est 3, 13, 16381... le 4^e terme a plus de 4932 chiffres et personne n'a osé calculer le 5^e.

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?

LE TABLEAU DE CHASSE

Le «tableau de chasse» ci-contre récapitule les 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'Eratosthène, du nom d'un mathématicien grec du III^e 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'Eratosthène, 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

| Auteurs | Année | Commentaire | Efficacité | Nombres calculés |
|-------------------------------|-------------|---|--|---|
| Eratosthène | -276 à -194 | Crible d'exclusion | Pratique | Infini calculable |
| Mersenne | 1536 | Nombres premiers de la forme $2^p - 1$ | Pratique, exact | 1 |
| Fermat | 1640 | Petit théorème de Fermat | Produit des premiers probables, rapide | Infini calculable |
| Lehmer | 1917 | Polynôme du second degré | Pratique | 11 |
| Mill | 1924 | Double exponentielle | Pratique | Moins de 11 |
| Wright | 1951 | Super exponentielle | Pratique | Moins de 4 |
| Mills | vers 1780 | Formule qui donne n | Théorique | Très peu |
| Jones, Sato, Wada et Wien | 1976 | Polynôme de degré 25 à 26 | Théorique | Très peu |
| John H. Conway | 1988 | Fractale | Théorique | Très peu |
| Rowland | 2000 | Récurrance | Théorique | Très peu |
| F. Dress et B. Landreau | 2010 | Polynôme de degré 6 | Pratique | 1 |
| Jean-Pierre Perichon et al. | 2011 | 16 premiers en progression arithmétique | Pratique | 16 |
| Tomás Oliveira e Silva et al. | 2019 | Programme Primesieve: crible d'Eratosthène optimisé | Le plus rapide connu | Infini calculable (mais dépendant de la taille de p) |

Marin Mersenne (1588-1648),
ou *Marinus Mersenius*,
appartenait à l'ordre

A black and white portrait of a man, likely a religious figure, wearing a dark robe and holding a book. The image is framed by a thick red border.

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, 7332733... 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 $c=0.265588372943143390897129$

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

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

OEIS: <https://oeis.org>

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 $a_0 = 2$: $a_n = 2, 3, 7, 43, 1807, 3263443, 1065005695807, \dots$ Tous ne sont pas des nombres premiers ($1807 = 13 \times 139$), mais étonnamment, la somme des inverses de ces termes $1/2 + 1/3 + 1/7 + 1/43 + 1/1807 + 1/3263443 \dots$ 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» [1]. La réponse est oui.

Avec $a = 1.61814180932426$, $p_2, a_n = 2, 3, 7, 43, 811, 3277913, 10744710357637 \dots$ La croissance est bien inférieure à celle de la formule de Mills et *a fortiori* à celle de Wright. Chaque terme a_n environne deux fois la taille du précédent, ce qui conduit tout de même à $a = 9.838 \times 10^{1667}$.

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 $a_0 = 43,80468771580293481\dots$ 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: $S_n = 113, 367, 1607, 10177, 102217, \dots$

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 $a_0 = 100000000000000000000000000009,3\overline{221074776345\dots}$, 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
48 972 469 000 420 009 426 555 707 142 502 303 667 155 036 417 849 654 050 1...

2
3
5
11
17
23
31
37
41
43
47
53
59
67
71
73
79
83
89
97
101
103
107
113
127
137
139
149
151
157
163
167
173
179
181
187
191
193
197
199
211
223
227
229
233
239
241
251
257
263
269
271
277
281
283
293
307
311
313
317
331
337
347
349
353
359
367
373
379
383
389
397
401
409
419
421
431
433
439
443
449
457
461
463
467
473
479
487
491
499
503
509
521
523
527
533
541
547
557
563
569
577
581
583
587
593
599
601
607
613
617
619
623
629
631
637
641
643
647
653
659
661
667
671
673
677
683
687
691
697
701
709
713
719
727
733
739
743
749
757
761
763
767
773
781
787
791
793
797
803
809
811
817
821
823
827
829
833
837
839
843
847
853
857
859
863
867
871
877
881
883
887
893
897
901
907
911
913
917
919
923
929
931
937
941
943
947
953
959
961
967
971
973
977
983
987
991
993
997
1009
1013
1017
1021
1023
1027
1031
1033
1037
1039
1043
1047
1049
1053
1057
1061
1063
1067
1069
1073
1077
1081
1083
1087
1091
1093
1097
1103
1107
1113
1117
1121
1123
1127
1129
1133
1137
1143
1147
1151
1153
1157
1163
1167
1171
1173
1177
1181
1183
1187
1193
1197
1201
1203
1207
1213
1217
1223
1229
1231
1237
1241
1243
1247
1249
1253
1257
1259
1261
1267
1271
1273
1277
1283
1287
1291
1293
1297
1301
1303
1307
1309
1313
1317
1321
1323
1327
1329
1331
1333
1337
1339
1343
1347
1349
1353
1357
1359
1361
1363
1367
1369
1373
1377
1381
1383
1387
1391
1393
1397
1403
1407
1411
1413
1417
1421
1423
1427
1429
1433
1437
1439
1443
1447
1451
1453
1457
1459
1463
1467
1469
1473
1477
1481
1483
1487
1493
1497
1501
1503
1507
1511
1513
1517
1519
1523
1527
1529
1531
1533
1537
1539
1543
1547
1549
1553
1557
1559
1561
1563
1567
1569
1573
1577
1581
1583
1587
1591
1593
1597
1601
1603
1607
1609
1613
1617
1621
1623
1627
1629
1631
1633
1637
1639
1643
1647
1649
1653
1657
1659
1661
1663
1667
1669
1673
1677
1681
1683
1687
1691
1693
1697
1701
1703
1707
1709
1713
1717
1721
1723
1727
1729
1731
1733
1737
1739
1743
1747
1749
1753
1757
1759
1761
1763
1767
1769
1773
1777
1781
1783
1787
1791
1793
1797
1801
1803
1807
1809
1813
1817
1821
1823
1827
1829
1831
1833
1837
1839
1843
1847
1849
1853
1857
1859
1861
1863
1867
1869
1873
1877
1881
1883
1887
1891
1893
1897
1901
1903
1907
1909
1913
1917
1921
1923
1927
1929
1931
1933
1937
1939
1943
1947
1949
1953
1957
1959
1961
1963
1967
1969
1973
1977
1981
1983
1987
1991
1993
1997
2003
2009
2011
2013
2017
2019
2021
2023
2027
2029
2031
2033
2037
2039
2043
2047
2049
2053
2057
2059
2061
2063
2067
2069
2073
2077
2081
2083
2087
2091
2093
2097
2101
2103
2107
2109
2113
2117
2121
2123
2127
2129
2131
2133
2137
2139
2143
2147
2149
2153
2157
2159
2161
2163
2167
2169
2173
2177
2181
2183
2187
2191
2193
2197
2201
2203
2207
2209
2213
2217
2221
2223
2227
2229
2231
2233
2237
2239
2243
2247
2249
2253
2257
2259
2261
2263
2267
2269
2273
2277
2281
2283
2287
2291
2293
2297
2301
2303
2307
2309
2313
2317
2321
2323
2327
2329
2331
2333
2337
2339
2343
2347
2349
2353
2357
2359
2361
2363
2367
2369
2373
2377
2381
2383
2387
2391
2393
2397
2401
2403
2407
2409
2413
2417
2421
2423
2427
2429
2431
2433
2437
2439
2443
2447
2449
2453
2457
2459
2461
2463
2467
2469
2473
2477
2481
2483
2487
2491
2493
2497
2501
2503
2507
2509
2513
2517
2521
2523
2527
2529
2531
2533
2537
2539
2543
2547
2549
2553
2557
2559
2561
2563
2567
2569
2573
2577
2581
2583
2587
2591
2593
2597
2601
2603
2607
2609
2613
2617
2621
2623
2627
2629
2631
2633
2637
2639
2643
2647
2649
2653
2657
2659
2661
2663
2667
2669
2673
2677
2681
2683
2687
2691
2693
2697
2701
2703
2707
2709
2713
2717
2721
2723
2727
2729
2731
2733
2737
2739
2743
2747
2749
2753
2757
2759
2761
2763
2767
2769
2773
2777
2781
2783
2787
2791
2793
2797
2801
2803
2807
2809
2813
2817
2821
2823
2827
2829
2831
2833
2837
2839
2843
2847
2849
2853
2857
2859
2861
2863
2867
2869
2873
2877
2881
2883
2887
2891
2893
2897
2901
2903
2907
2909
2913
2917
2921
2923
2927
2929
2931
2933
2937
2939
2943
2947
2949
2953
2957
2959
2961
2963
2967
2969
2973
2977
2981
2983
2987
2991
2993
2997
3001
3003
3007
3009
3013
3017
3021
3023
3027
3029
3031
3033
3037
3039
3043
3047
3049
3053
3057
3059
3061
3063
3067
3069
3073
3077
3081
3083
3087
3091
3093
3097
3101
3103
3107
3109
3113
3117
3121
3123
3127
3129
3131
3133
3137
3139
3143
3147
3149
3153
3157
3159
3161
3163
3167
3169
3173
3177
3181
3183
3187
3191
3193
3197
3201
3203
3207
3209
3213
3217
3221
3223
3227
3229
3231
3233
3237
3239
3243
3247
3249
3253
3257
3259
3261
3263
3267
3269
3273
3277
3281
3283
3287
3291
3293
3297
3301
3303
3307
3309
3313
3317
3321
3323
3327
3329
3331
3333
3337
3339
3343
3347
3349
3353
3357
3359
3361
3363
3367
3369
3373
3377
3381
3383
3387
3391
3393
3397
3401
3403
3407
3409
3413
3417
3421
3423
3427
3429
3431
3433
3437
3439
3443
3447
3449
3453
3457
3459
3461
3463
3467
3469
3473
3477
3481
3483
3487
3491
3493
3497
3501
3503
3507
3509
3513
3517
3521
3523
3527
3529
3531
3533
3537
3539
3543
3547
3549
3553
3557
3559
3561
3563
3567
3569
3573
3577
3581
3583
3587
3591
3593
3597
3601
3603
3607
3609
3613
3617
3621
3623
3627
3629
3631
3633
3637
3639
3643
3647
3649
3653
3657
3659
3661
3663
3667
3669
3673
3677
3681
3683
3687
3691
3693
3697
3701
3703
3707
3709
3713
3717
3721
3723
3727
3729
3731
3733
3737
3739
3743
3747
3749
3753
3757
3759
3761
3763
3767
3769
3773
3777
3781
3783
3787
3791
3793
3797
3801
3803
3807
3809
3813
3817
3821
3823
3827
3829
3831
3833
3837
3839
3843
3847
3849
3853
3857
3859
3861
3863
3867
3869
3873
3877
3881
3883
3887
3891
3893
3897
3901
3903
3907
3909
3913
3917
3921
3923
3927
3929
3931
3933
3937
3939
3943
3947
3949
3953
3957
3959
3961
3963
3967
3969
3973
3977
3981
3983
3987
3991
3993
3997
4001
4003
4007
4009
4013
4017
4021
4023
4027
4029
4031
4033
4037
4039
4043
4047
4049
4053
4057
4059
4061
4063
4067
4069
4073
4077
4081
4083
4087
4091
4093
4097
4101
4103
4107
4109
4113
4117
4121
4123
4127
4129
4131
4133
4137
4139
4143
4147
4149
4153
4157
4159
4161
4163
4167
4169
4173
4177
4181
4183
4187
4191
4193
4197
4201
4203
4207
4209
4213
4217
4221
4223
4227
4229
4231
4233
4237
4239
4243
4247
4249
4253
4257
4259
4261
4263
4267
4269
4273
4277
4281
4283
4287
4291
4293
4297
4301
4303
4307
4309
4313
4317
4321
4323
4327
4329
4331
4333
4337
4339
4343
4347
4349
4353
4357
4359
4361
4363
4367
4369
4373
4377
4381
4383
4387
4391
4393
4397
4401
4403
4407
4409
4413
4417
4421
4423
4427
4429
4431
4433
4437
4439
4443
4447
4449
4453
4457
4459
4461
4463
4467
4469
4473
4477
4481
4483
4487
4491
4493
4497
4501
4503
4507
4509
4513
4517
4521
4523
4527
4529
4531
4533
4537
4539
4543
4547
4549
4553
4557
4559
4561
4563
4567
4569
4573
4577
4581
4583
4587
4591
4593
4597
4601
4603
4607
4609
4613
4617
4621
4623
4627
4629
4631
4633
4637
4639
4643
4647
4649
4653
4657
4659
4661
4663
4667
4669
4673
4677
4681
4683
4687
4691
4693
4697
4701
4703
4707
4709
4713
4717
4721
4723
4727
4729
4731
4733
4737
4739
4743
4747
4749
4753
4757
4759
4761
4763
4767
4769
4773
4777
4781
4783
4787
4791
4793
4797
4801
4803
4807
4809
4813
4817
4821
4823
4827
4829
4831
4833
4837
4839
4843
4847
4849
4853
4857
4859
4861
4863
4867
4869
4873
4877
4881
4883
4887
4891
4893
4897
4901
4903
4907
4909
4913
4917
4921
4923
4927
4929
4931
4933
4937
4939
4943
4947
4949
4953
4957
4959
4961
4963
4967
4969
4973
4977
4981
4983
4987
4991
4993
4997
5001
5003
5007
5009
5013
5017
5021
5023
5027
5029
5031
5033
5037
5039
5043
5047
5049
5053
5057
5059
5061
5063
5067
5069
5073
5077
5081
5083
5087
5091
5093
5097
5101
5103
5107
5109
5113
5117
5121
5123
5127
5129
5131
5133
5137
5139
5143
5147
5149
5153
5157
5159
5161
5163
5167
5169
5173
5177
5181
5183
5187
5191
5193
5197
5201
5203
5207
5209
5213
5217
5221
5223
5227
5229
5231
5233
5237
5239
5243
5247
5249
5253
5257
5259
5261
5263
5267
5269
5273
5277
5281
5283
5287
5291
5293
5297
5301
5303
5307
5309
5313
5317
5321
5323
5327
5329
5331
5333
5337
5339
5343
5347
5349
5353
5357
5359
5361
5363
5367
5369
5373
5377
5381
5383
5387
5391
5393
5397
5401
5403
5407
5409
5413
5417
5421
5423
5427
5429
5431
5433
5437
5439
5443
5447
5449
5453
5457
5459
5461
5463
5467
5469
5473
5477
5481
5483
5487
5491
5493
5497
5501
5503
5507
5509
5513
5517
5521
5523
5527
5529
5531
5533
5537
5539
5543
5547
5549
5553
5557
5559
5561
5563
5567
5569
5573
5577
5581
5583
5587
5591
5593
5597
5601
5603
5607
5609
5613
5617
5621
5623
5627
5629
5631
5633
5637
5639
5643
5647
5649
5653
5657
5659
5661
5663
5667
5669
5673
5677
5681
5683
5687
5691
5693
5697
5701
5703
5707
5709
5713
5717
5721
5723
5727
5729
5731
5733
5737
5739
5743
5747
5749
5753
5757
5759
5761
5763
5767
5769
5773
5777
5781
5783
5787
5791
5793
5797
5801
5803
5807
5809
5813
5817
5821
5823
5827
5829
5831
5833
5837
5839
5843
5847
5849
5853
5857
5859
5861
5863
5867
5869
5873
5877
5881
5883
5887
5891
5893
5897
5901
5903
5907
5909
5913
5917
5921
5923
5927
5929
5931
5933
5937
5939
5943
5947
5949
5953
5957
5959
5961
5963
5967
5969
5973
5977
5981
5983
5987
5991
5993
5997
6001
6003
6007
6009
6013
6017
6021
6023
6027
6029
6031
6033
6037
6039
6043
6047
6049
6053
6057
6059
6061
6063
6067
6069
6073
6077
6081
6083
6087
6091
6093
6097
6101
6103
6107
6109
6113
6117
6121
6123
6127
6129
6131
6133
6137
6139
6143
6147
6149
6153
6157
6159
6161
6163
6167
6169
6173
6177
6181
6183
6187
6191
6193
6197
6201
6203
6207
6209
6213
6217
6221
6223
6227
6229
6231
6233
6237
6239
6243
6247
6249
6253
6257
6259
6261
6263
6267
6269
6273
6277
6281
6283
6287
6291
6293
6297
6301
6303
6307
6309
6313
6317
6321
6323
6327
6329
6331
6333
6337
6339
6343
6347
6349
6353
6357
6359
6361
6363
6367
6369
6373
6377
6381
6383
6387
6391
6393
6397
6401
6403
6407
6409
6413
6417
6421
6423
6427
6429
6431
6433
6437
6439
6443
6447
6449
6453
6457
6459
6461
6463
6467
6469
6473
6477
6481
6483
6487
6491
6493
6497
6501
6503
6507
6509
6513
6517
6521
6523
6527
6529
6531
6533
6537
6539
6543
6547
6549
6553
6557
6559
6561
6563
6567
6569
6573
6577
6581
6583
6587
6591
6593
6597
6601
6603
6607
6609
6613
6617
6621
6623
6627
6629
6631
6633
6637
6639
6643
6647
6649
6653
6657
6659
6661
6663
6667
6669
6673
6677
6681
6683
6687
6691
6693
6697
6701
6703
6707
6709
6713
6717
6721
6723
6727
6729
6731
6733
6737
6739
6743
6747
6749
6753
6757
6759
6761
6763
6767
6769
6773
6777
6781
6783
6787
6791
6793
6797
6801
6803
6807
6809
6813
6817
6821
6823
6827
6829
6831
6833
6837
6839
6843
6847
6849
6853
6857
6859
6861
6863
6867
6869
6873
6877
6881
6883
6887
6891
6893
6897
6901
6903
6907
6909
6913
6917
6921
6923
6927
6929
6931
6933
6937
6939
6943
6947
6949
6953
6957
6959
6961
6963
6967
6969
6

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



ENIGME 5

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

ENIGME 6

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

ENIGME 7

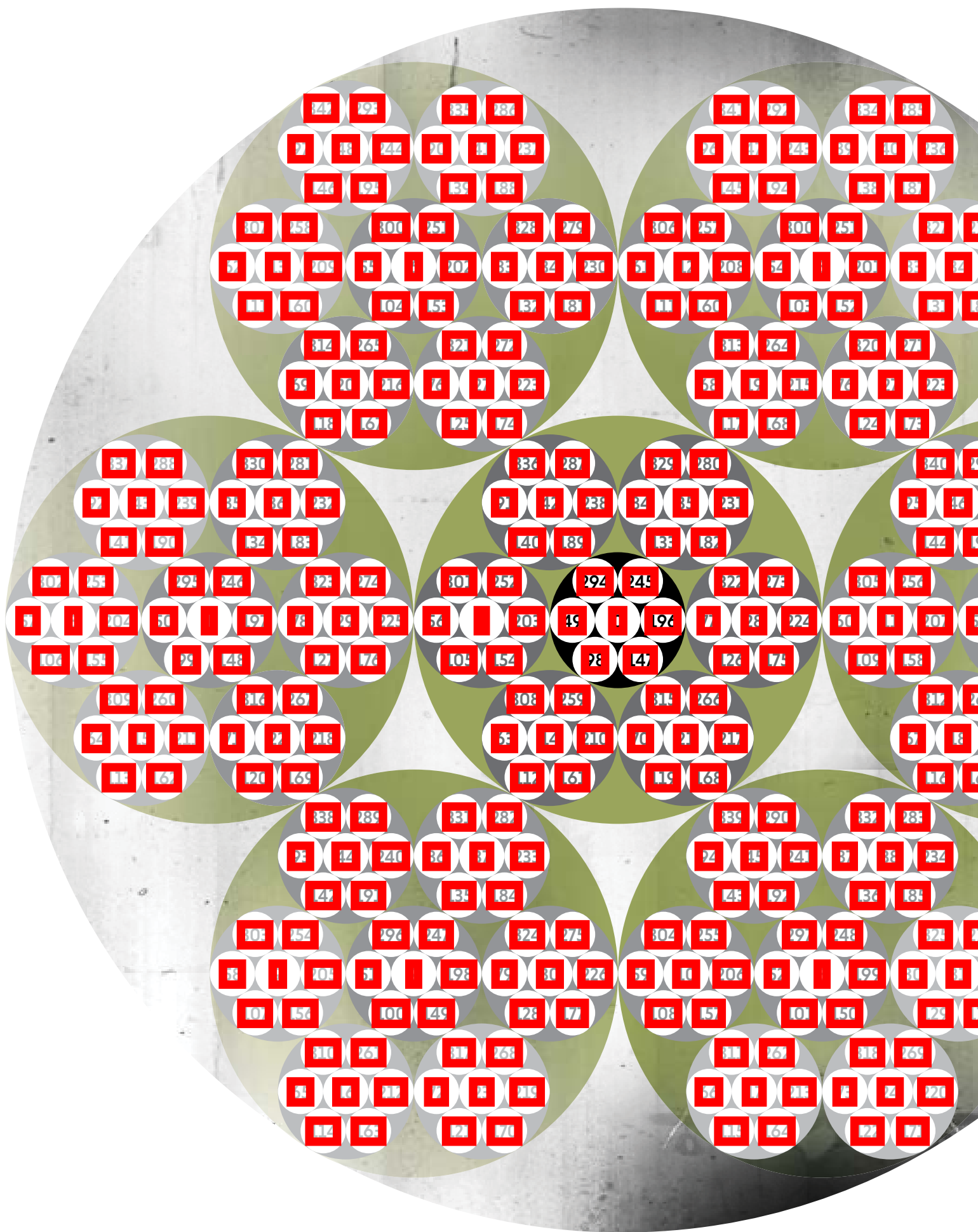
Quel est le plus grand nombre qu'on puisse obtenir en multipliant des nombres entiers positifs dont la somme vaut 8?

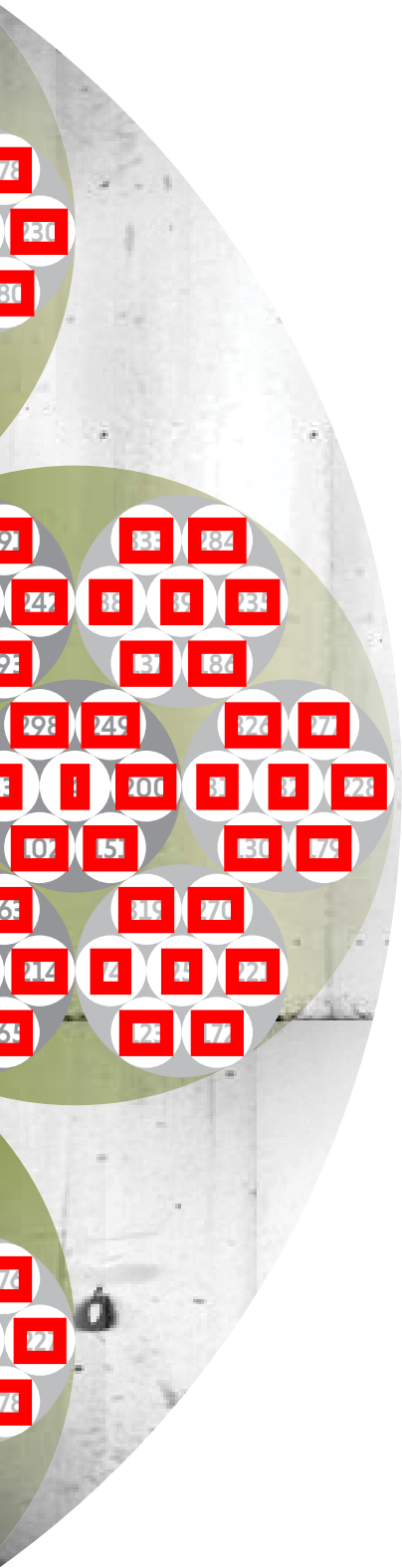
ENIGME 8

Si douze nombres strictement positifs $a_1 \leq a_2 \leq \dots \leq a_{12}$ 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 $\frac{a_{12}}{a_1}$?

ENIGME 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?





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 ardues 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 de 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 $7 \times 7 \times 7 + 7$, $n \times 7 \times 7 + 14$...



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

LESSSENTIEL

Peter Scholze, mathématicien allemand, à peine 30 ans, a reçu la médaille Fields en 2018.

Il a été récompensé totalement pour

es espaces perfectoides, les 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'AUTEUR



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.

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!»

A 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 perfectoides – 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.»



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>

E

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,

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'ARITHMETIQUE

Peter Scholze a commencé à apprendre seules 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*, 64^e 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.

A 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.»

A 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 étonnantes 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.

A 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.»

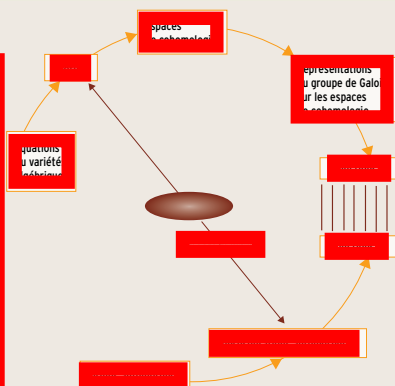
Peter Scholze a commencé ses recherches en géométrie arithmétique, où des outils de géométrie aident à approcher les solutions entières d'équations polynomiales (par exemple, $y^2 + 3y = 5$), qui n'impliquent que des nombres entiers, des variables et des exposants.

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 p -adiques offrent un moyen naturel d'étudier

LE PROGRAMME DE LANGLANDS

Une part substantielle des recherches menées ces dernières décennies en

algèbre 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 les «fonctions L», fonctions qui contiennent les 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 pour quoi 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.

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 seniors. 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 préférerait 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'appropriier 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 v et a , dans la plupart des cas, v est un carré

JE N'AI JAMAIS

VRAIMENT APPRIS

LES CHOSES

BASIQUES.

JE LES AI

ASSIMILÉES EN

M'INTÉRESSANT

A D'AUTRES

NOTIONS

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)

$$3 \times 10^2 + 4 \times 10^1 + 7 \times 10^0.$$

En fait, on peut identifier tout nombre réel avec la suite de ses chiffres: $a_n a_{n-1} \dots a_1 a_0 a_{-1} a_{-2} a_{-3} \dots$ est essentiellement identique à: $a_n \times 10^n + a_{n-1} \times 10^{n-1} \dots a_1 \times 10 + a_0 + a_{-1} \times 10^{-1} + a_{-2} \times 10^{-2} + a_{-3} \times 10^{-3} \dots$ Les chiffres a_i 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: $a_1, a_2, a_3 \dots$. C'est différent avec les nombres réels qui peuvent nécessiter une infinité de coefficients à indice négatif. Par exemple, $\pi = 3,14159$ s'écrit: $3 \times 10^0 + 1 \times 10^{-1} + 4 \times 10^{-2} + 1 \times 10^{-3} + 5 \times 10^{-4} + 9 \times 10^{-5} \dots$

où $a_0 = 3, a_1 = 1, a_2 = 4, a_3 = 1, a_4 = 5, a_5 = 9 \dots$

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 $\dots 4444+1=0$, 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^2 -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 à 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 $f(z) = a_0 + a_1 z + a_2 z^2 + a_3 z^3 \dots$ 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 $a_2 = 3$.

« s'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. »

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. »

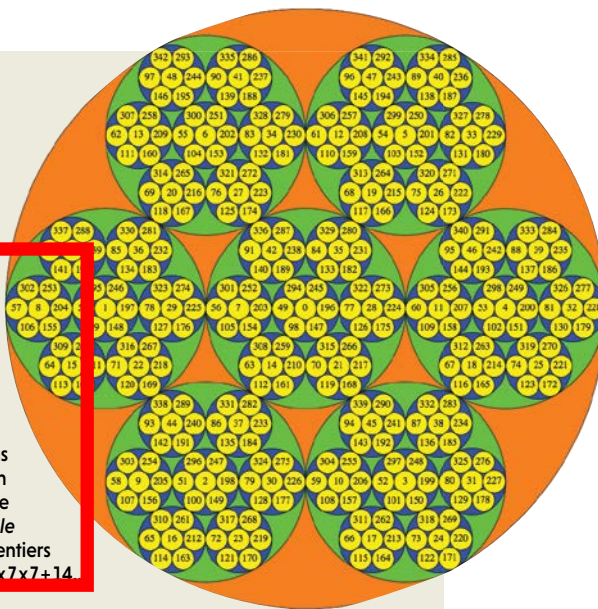
Pour autant, il ne souhaite pas tellement s'étendre sur cette passion. Quand on lui demande s'il était fait pour devenir mathématicien, il dément: « C'est une idée bien trop philosophique. » Plutôt secret, il n'est pas très à l'aise avec sa célébrité. En 2016, il est devenu le plus jeune lauréat du prix 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 900 000 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 abordent », explique Bhargav Bhatt.

Selon lui, quand Peter Scholze s'intéresse à son 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'appréhender 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. » ■

Les nombres ℓ -adiques (ici, les $7 \times 7 \times 7 = 43$ 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 $7 = 49$, entourés (dans le disque vert central) des entiers de la forme $nx7 \times 7 + 7$, $nx7 \times 7 + 14$.



Les fonctions de cette classe (dites méromorphes) sont complètement décrites par la suite de leurs coefficients

$$a_{-n}, a_{-(n-1)}, \dots, a_{-1}, a_0, a_1, a_2, \dots$$

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 $0, 1, \dots, p-1$, 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 POPPE (SPEKTRUM DER WISSENSCHAFT)
TRADUIT PAR NILS BERGLUND, DE L'INSTITUT
DENIS-POISSON, À L'UNIVERSITÉ D'ORLÉANS

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 ζ de Riemann, en inventant des méthodes radicalement nouvelles.

Il explore aujourd'hui les liens nichés au cœur du programme de Langlands, qui relie théorie des nombres, géométrie et analyse.

L'AUTEUR



ERICA KLARREICH, docteure en mathématiques à 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 !



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>

P

ur 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.

Coincidence. 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



ses «conjectures d'une portée surprenante». Ses idées sont «une vaste expansion de l'imagination», confirme Michael Harris, mathématicien à l'université Columbia.

Akshay Venkatesh, à Princeton

UN GENIE DANS LA TOURMENTE

Toutefois, alors qu'Akshay Venkatesh était encore étudiant, au tournant des années 2000, le mythe du génie a failli faire dérailler sa carrière. Sa précocité (il avait intégré l'université à 13 ans) était pourtant de bon augure. Mais à son arrivée à Princeton à l'âge de 17 ans, en tant qu'étudiant de master, Akshay Venkatesh fut surpris par «le grand nombre de personnes douées pour apprendre ou résoudre des problèmes rapidement, des caractéristiques que l'on attribue l'ordinaire ou aux seuls mathématiciens».

Avec ses voies sinueuses et ses impasses, la recherche en mathématiques était très différente de ce à quoi excellait l'étudiant Akshay Venkatesh, lorsqu'il s'agissait de s'atteler à des problèmes bien circonscrits et aux conclusions déjà connues. Habitué à faire partie des meilleurs, il trouvait ses travaux médiocres. Discrètement, il a alors commencé à réfléchir à une échappatoire, acceptant même un travail d'été dans la *start-up* de son oncle, spécialisée dans le *machine learning*.

Une proposition exceptionnelle se présente alors : un poste prestigieux d'enseignant «C. L. E. Moore» à l'Institut de technologie du Massachusetts, à Cambridge. De toute évidence, on l'avait fortement recommandé, mais pourquoi ? Alors qu'il l'interrogeait à ce sujet, Jordan Ellenberg, un ami et collègue du mathématicien,

lui a répondu : « Parfois, les gens voient en toi les choses que tu ne vois pas. » Akshay Venkatesh a été profondément marqué par ces mots.

Aujourd'hui, à 37 ans, Akshay Venkatesh semble avoir oublié ses hésitations et a acquis l'aisance de quelqu'un parfaitement en harmonie avec ses choix de vie. Mais cela lui a pris de nombreuses années pour voir ce que d'autres mathématiciens voyaient en lui depuis longtemps.

La plupart des mathématiciens ont des difficultés à décrire l'éventail complet des contributions mathématiques d'Akshay Venkatesh. Il a construit des ponts entre la théorie des nombres et des champs plus éloignés comme la topologie algébrique et les systèmes dynamiques. Il est connu pour arriver dans un domaine, le transformer, puis passer à autre chose.

« On dit toujours qu'il n'y plus de mathématicien universel, parce que ce serait trop difficile », explique Emmanuel Kowalski, de l'École polytechnique fédérale de Zurich, en Suisse. Mais, selon lui, l'esprit d'Akshay Venkatesh « peut réfléchir sur tous les sujets ».

UNE LONGUE MATURATION

Akshay Venkatesh est prêt à tout pour cacher son passé de prodige. « Je vous paierai pour ne rien en mentionner, plaisante-t-il. Je laisserais bien volontiers cette histoire derrière moi, c'est un peu comme si j'étais la star d'un spectacle de monstres. »

Toutefois, en grandissant à Perth, en Australie, où ses parents se sont installés après avoir quitté New Delhi quand il avait deux ans, Akshay Venkatesh ne se sentait pas « monstrueux ». Il décrit son enfance comme une « vie de banlieue assez normale », remplie de livres (essentiellement de science-fiction) et d'amitié. Il a participé aux Olympiades de mathématiques et de physique – les plus importantes compétitions internationales pour lycéens – et a remporté des médailles dans les deux matières, respectivement à 11 et 12 ans. Mais il accorde plus de valeur aux amitiés forgées à cette époque qu'à ses succès. « Avec du recul, je ne suis pas fan de ces concours », concède-t-il. Je pense que si les mathématiciens ne faisaient vraiment que ça, je n'apprécierais pas d'en être un. »

Les mathématiques sont un domaine relativement simple où l'on peut progresser rapidement, car elles ne nécessitent pas une grande expérience de la vie. Après son diplôme de mathématiques de premier cycle (avec la meilleure mention possible), à l'université d'Australie Occidentale, à Perth, à l'âge de 16 ans, Akshay Venkatesh a poursuivi sur sa lancée en deuxième et troisième cycles sans trop y réfléchir. Mais il

Lorsqu'il se sentait découragé, Akshay Venkatesh se plongeait dans des manuels de mathématiques

ne voit aucune forme de prédestination dans son choix. « J'aurais été tout aussi heureux en faisant autre chose », déclare-t-il.

À l'université de Princeton, tout le monde, excepté lui, s'est rapidement rendu compte de son talent. Tony Wirth, son colocataire de l'époque, se rappelle que, lorsqu'il lui a montré son manuel d'informatique théorique, Akshay Venkatesh en a instantanément compris les concepts fondamentaux. « Vous savez que vous avez à faire à un grand esprit lorsqu'il peut comprendre en profondeur un nouveau domaine en seulement quelques minutes. »

Quand Akshay Venkatesh a rendu visite à son directeur de thèse, Peter Sarnak, pour lui demander des références bibliographiques, ce dernier a décidé de le mettre à l'essai avec un livre sur la théorie de la représentation des groupes semi-simples, un sujet ardu en début de parcours. Peter Sarnak s'attendait à ce que l'adolescent revienne rapidement demander quelque chose de plus simple. Mais il se rappelle que, un mois plus tard, « il s'est présenté dans mon bureau pour m'expliquer ce qu'il avait lu, et il était clair pour moi que, en plus d'avoir compris son sujet, il en avait une intuition extraordinaire. »

Akshay Venkatesh « a toujours eu des idées remarquables », se rappelle Peter Sarnak, qui travaille désormais lui aussi à l'Institut d'études avancées. « De toute évidence, ce n'était qu'une question de temps avant qu'il se mette à raisonner de manière iconoclaste. »

Intérieurement, toutefois, Akshay Venkatesh luttait. « Je n'ai pas le sentiment d'avoir été heureux lorsque j'étudiais », concède-t-il. Il se sentait troublé, car l'une des idées majeures de sa thèse avait été suggérée par son directeur, Peter Sarnak, même si cela n'était pas rare. « Je n'avais pas l'impression d'avoir apporté quoi que ce soit d'original, se rappelle-t-il. Je pense qu'en sortant de ce cycle d'études, je ne m'estimais pas apte à faire de la recherche. »

Lorsqu'il se sentait découragé, Akshay Venkatesh se plongeait dans des manuels de mathématiques, souvent sur des sujets éloignés de son propre domaine. « C'est ce qui m'a toujours donné la force de continuer, même quand mes propres travaux n'aboutissaient pas. Je lis quelque chose d'inconnu et je me dis "ça, c'est vraiment merveilleux" ».

Tout au long de ses années d'études, il a absorbé de grandes quantités de mathématiques. Ce n'était pas une stratégie, mais il en résulte une vue d'ensemble qui lui permet maintenant de découvrir des relations que d'autres mathématiciens ont manquées.

Avec le temps, Akshay Venkatesh a compris que ses difficultés prenaient leurs

racines dans le fait qu'il ignorait quel genre de mathématicien il était. Contrairement à d'autres, qui travaillent intensément sur un projet et le terminent en quelques mois ou en une année, il s'est rendu compte que ses idées se développaient plus lentement, sur de longues durées. «Je me rendais compte que des idées anciennes revenaient après avoir mûri, parce qu'entre-temps j'avais découvert d'autres notions, explique-t-il. Je ne me serais jamais décrit comme une personne patiente, mais c'est ainsi.»

L'ESSENCE DES CHOSES

N'ayant pas encore eu cette prise de conscience à sa sortie de doctorat en 2002, Akshay Venkatesh avait hâte de faire ses preuves. Une collaboration avec Jordan Ellenberg lui en a alors donné l'opportunité. Ensemble, ils se sont mis à compter les «extensions du corps des nombres», la plus simple étant construite par l'addition aux nombres rationnels d'une poignée de nombres irrationnels satisfaisant certaines équations polynomiales. Ces systèmes de nombres «deviennent un peu irrationnels, mais pas trop», explique Jordan Ellenberg, désormais professeur à l'université du Wisconsin, à Madison.

Il existe une infinité d'extensions du corps des nombres, mais il y a un moyen naturel de mesurer la complexité de chacune d'elles, et

il s'agit alors de compter combien de ces extensions se trouvent en dessous de chaque niveau de complexité. Akshay Venkatesh et Jordan Ellenberg ont déterminé une nouvelle limite supérieure à ces chiffres, laquelle a amélioré considérablement la technique, qui n'avait pas changé depuis des décennies. Selon Akshay Venkatesh, ce projet «était psychologiquement très important». «On s'est attaqué à ce problème par nous-mêmes et nous avons beaucoup progressé.»

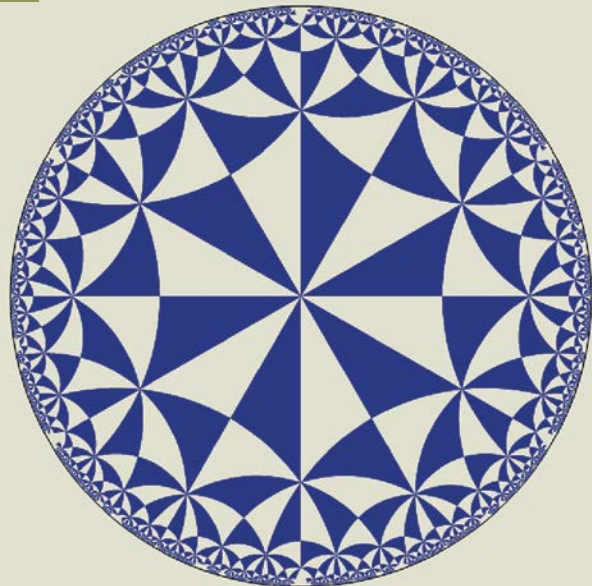
À l'origine, les deux amis se sont intéressés au problème en utilisant de nouveaux outils mathématiques dont ils avaient entendu parler lors d'une conférence. Mais, tandis qu'ils travaillaient à améliorer leur preuve, ils se sont rendu compte qu'ils avaient simplifié tous les nouveaux outils.

«Cela correspond tout à fait à ce que je reconnais aujourd'hui comme étant très caractéristique d'Akshay», explique Jordan Ellenberg. La première version, plus technique, de leur article a permis de prouver leur théorème. Mais pour Akshay Venkatesh, «la question n'est pas tant de savoir si vous avez répondu à la question ou prouvé le théorème. Il s'agit de savoir si on a vraiment compris de quoi il retourne.»

Outre Jordan Ellenberg, de nombreux mathématiciens sont frappés par la capacité d'Akshay Venkatesh à distiller les idées jusqu'à

LA SUBCONVEXITÉ

En 1859, le mathématicien Allemand Bernhard Riemann a défini la fonction zêta (une fonction de nombres complexes s de la forme $a + bi$, où $i^2 = -1$) qui s'exprime ainsi : $1/2^s + 1/3^s + 1/5^s + 1/7^s + \dots$. Les «valeurs triviales» de cette fonction (les valeurs qui annulent la fonction) sont placées le long d'une droite (une ligne critique) correspondant aux nombres complexes pour lesquels $\sigma = 1/2$. Les fonctions L sont des généralisations de la fonction zêta de Riemann où les numérateurs 1 sont remplacés par une séquence de nombres complexes. La subconvexité est liée à la taille de ces fonctions L, plus précisément à la limite supérieure de cette taille le long d'une ligne critique. Akshay Venkatesh explique avoir compris les fonctions L grâce à la géométrie hyperbolique dont un modèle en deux dimensions est le disque de Poincaré (voir la figure ci-contre), sources d'inspiration de l'artiste néerlandais Maurits Cornelis Escher. On observe que la somme des angles des triangles qui pavent le plan est, en géométrie hyperbolique, inférieure à 180° . Akshay Venkatesh étudie ces pavés grâce aux formes automorphes, des versions généralisées de fonctions périodiques, par exemple sinusoïdales. Elles relèvent de l'analyse harmonique où l'on s'intéresse, entre autres, aux... billards parfaits. En s'intéressant à la trajectoire d'une boule sur un billard ayant la forme d'un triangle hyperbolique, on tisse des liens inattendus entre géométrie et théorie des nombres. Ce sont ces liens que Akshay Venkatesh explore.



Le disque de Poincaré est une représentation en deux dimensions de la géométrie hyperbolique. La somme des angles d'un triangle y est inférieure à 180° .

leur essence. «Lorsqu'il a terminé, sa preuve se retrouve souvent dans tous les manuels», explique Peter Sarnak.

«Il n'est pas rare, en mathématiques, que des personnes viennent m'expliquer la bonne façon de raisonner à propos d'une notion, explique Frank Calegari, de l'université de Chicago. Mais Akshay est l'une des seules personnes à l'avoir fait pour mes propres travaux.»

Peu après ses résultats sur les extensions du corps des nombres, Akshay Venkatesh a obtenu son premier «fait d'armes», le problème de la subconvexité (voir l'encadré page précédente). Il concerne les généralisations de la fonction zêta de Riemann (voir *L'hypothèse qui valait un million*, par P. Meier, page 68), nommées fonctions L. En 1859, Bernhard Riemann a proposé que les valeurs pour lesquelles une certaine fonction zêta s'annulent aideraient à comprendre la répartition des nombres premiers. Mais personne n'est parvenu à le prouver. L'hypothèse de Riemann, qui a des centaines d'implications en dehors de la distribution des nombres premiers, est l'un des problèmes les plus importants en mathématiques.

Chaque fonction L a sa propre version de l'hypothèse de Riemann, toutes aussi difficiles à prouver que la version princeps. Pendant des décennies, les mathématiciens ont donc cherché à les contourner pour prouver directement certaines de leurs conséquences. L'une des plus importantes a trait à la subconvexité, un problème lié à la taille des fonctions L. À la clé, des informations sur les nombres entiers, par exemple sur les façons dont un grand nombre donné peut être écrit sous la forme de la somme de trois carrés parfaits.

Avant que Akshay Venkatesh ne se tourne vers les fonctions L, les solutions de subconvexité relevaient du cas par cas et faisaient souvent l'objet de longs articles techniques, explique Emmanuel Kowalski. Mais en 2004, Akshay Venkatesh a envoyé le premier jet d'un long papier à Philippe Michel, un spécialiste de la subconvexité aujourd'hui à l'École polytechnique fédérale de Lausanne. Dans son article, Akshay Venkatesh utilise des idées issues des systèmes dynamiques pour résoudre le problème de la subconvexité de façon bien plus générale que ce qui avait été accompli auparavant. «La méthode était complètement nouvelle, explique Philippe Michel. Ce fut un choc.»

Akshay Venkatesh et Philippe Michel ont fait équipe à l'occasion d'une seconde publication, basée sur cette nouvelle approche. Les deux papiers, avec d'autres, «ont fait de lui l'un des leaders mondiaux en théorie et en dynamique des nombres», estime Peter Sarnak.

Collaborer avec Akshay Venkatesh pourrait paraître intimidant, étant donné sa grande connaissance et la profondeur de ses idées. Ce

n'est pas le cas. «Il est très fort techniquement, mais on n'est pas écrasé en discutant avec lui», déclare Yiannis Sakellaridis, de l'Université Rutgers, à Newark. On parle simplement de l'essence des choses.»

Lorsque j'ai rencontré Akshay Venkatesh, nous nous sommes promenés de son bureau jusqu'au jardin d'enfants de l'institut pour récupérer sa plus jeune fille, Tuli, puis nous nous sommes rendus à leur appartement. Tara, l'aînée, nous a rejoints peu après. Il était seul à la maison, car sa femme, Sarah Paden, qui termine sa thèse en musicologie à l'université de Princeton, était à une réunion.

Akshay Venkatesh est toujours un grand lecteur. Ces temps-ci, il relit *Guerre et Paix*. L'écriture est aussi exceptionnelle que dans son souvenir, mais elle «est parsemée de passages didactiques que je trouve plus ennuyeux maintenant», dit-il.

DU CAFE, MAIS PAS TROP

Sarah Paden décrit son mari comme quelqu'un de casanier: «La routine, les habitudes et son foyer sont des réconforts pour lui». Ils lui offrent la liberté dont il a besoin, estime-t-elle, pour être plus audacieux dans le monde des mathématiques. «J'ai le sentiment qu'il n'est pas le même dans son travail qu'à la maison.»

La simplicité de la vie à Princeton en fait un environnement idéal pour Akshay Venkatesh. Il y a du café – l'un de ses petits plaisirs – au bout du couloir et à la cafétéria. Cependant, il s'astreint à ne pas en abuser. Son bureau dispose d'un luxe rare: un deuxième tableau noir, couvert de pense-bêtes («visa pour le Brésil», «chapitre XIII») et de formules mathématiques.

Akshay Venkatesh est à la fois surpris d'avoir remporté la médaille Fields et anxieux quant à l'exposition subite de sa carrière qu'elle implique. Étudiant, il s'était penché sur les travaux de nombreux lauréats qui l'ont précédé, se rappelle-t-il. «C'est difficile d'imaginer que j'en fais désormais partie.» Il ne sait pas quoi penser des prix en général, puisqu'ils contribuent à renforcer le mythe du génie solitaire. «Et j'en ai sûrement reçu plus que nécessaire», estime-t-il.

Il était particulièrement surpris de remporter la médaille Fields parce qu'une grande partie de ses travaux récents ne sont que des conjectures. Or la récompense est habituellement décernée à des personnes qui ont résolu de grands problèmes. «Mon travail n'est pas de cette nature», explique-t-il.

Ce sont ses travaux récents et hautement spéculatifs qui le rendent le plus heureux. Ils concernent le programme de Langlands, un vaste réseau de connexions entre théorie des nombres, géométrie et analyse. Au cœur de ce programme se trouve un lien – encore flou – entre des formes qui apparaissent dans deux contextes différents. D'un côté, on trouve

BIBLIOGRAPHIE

P. SCHOLZE, On torsion in the cohomology of locally symmetric varieties, *Annals of Mathematics*, vol. 182, pp. 945-1066, 2015.

A. VENKATESH, Sparse equidistribution problems, period bounds and subconvexity, *Annals of Mathematics*, vol. 172, pp. 989-1094, 2010.

P. MICHEL ET A. VENKATESH, The subconvexity problem for GL₂, *Publications mathématiques de l'IHÉS*, vol. 111, pp. 171-271, 2010.



les « motifs », des formes reliées aux ensembles de solutions des équations polynomiales (de la même façon qu'un cercle représente les solutions à l'équation $x^2 + y^2 = 1$).

Akshay Venkatesh, dans le parc de l'Institut d'études avancées, à Princeton, avec un café, son pêché mignon.

PAVES ET TORSION

De l'autre, des formes obtenues par le collage des côtés d'un « pavé », comme le tore l'est à partir d'un carré. Cependant, les « pavés » requis par le programme de Langlands sont moins simples et évoquent plus les compositions d'Escher. L'une des correspondances de ce type est au cœur de la preuve du dernier théorème de Fermat, fournie en 1994 par Andrew Wiles (voir *Le tombeur de Fermat* par G. Giorello, page 98).

Parfois, les pavés collés ont subi une torsion indétectable par les méthodes classiques du programme de Langlands. Quand Akshay Venkatesh entend parler de cette torsion, il est « convaincu qu'il y a quelque chose d'important à découvrir ». En 2009, Akshay Venkatesh et Nicolas Bergeron de l'université Pierre-et-Marie-Curie, à Paris, ont montré que la torsion est fréquente dans les pavés collés prévus dans les correspondances de Langlands.

Étonnamment, un des principaux résultats de Peter Scholze, autre médaillé Fields de la même « promotion » que Akshay Venkatesh (voir *L'oracle de l'arithmétique*, par E. Klarreich, page 84), a été de montrer que des classes de telles torsions sont justement associées à des « motifs », au sens décrit précédemment.

Ces dernières années, avec des collègues, Akshay Venkatesh a exploré d'autres caractéristiques de ces torsions, « mathématiquement plus profondes, mais moins visibles ». « Le programme de Langlands fourni une sorte de dictionnaire pour passer d'un objet à l'autre, déclare Frank Calegari. Akshay nous dit qu'il y a quelque chose d'encore plus précis. » Pour le moment, Akshay Venkatesh n'a prouvé qu'une infime partie de ses conjectures globales. « Mais au moins j'arrive à mieux voir ce qui devrait être vrai », dit-il.

Ce genre d'investigation, qui s'apparente à l'exploration d'un paysage flou, constitue ce qui lui convient le mieux. Plus tôt dans sa carrière, lorsqu'il ressentait le besoin d'impressionner les autres, il travaillait sur des problèmes déjà formalisés, le laissant en partie insatisfait. Il a depuis découvert la sensation d'être sur la piste de « quelque chose d'intéressant qui n'a pas encore été exploré, ou quelque chose d'anormal qui n'a pas beaucoup de sens ».

A Princeton, Akshay Venkatesh et Yiannis Sakellaridis ont travaillé sur deux problèmes distinctes: l'une concernant les fonctions L et l'autre étant une extension des travaux récents d'Akshay Venkatesh sur le programme de Langlands. Étrangement, ces deux thèmes semblent converger vers une même question. «C'est un très bon signe estime-t-il. Je ne sais pas exactement où cela va nous mener. Mais quelque chose nous attend au bout de ce chemin, c'est certain.» À suivre donc! ■

CÉDRIC
VILLANI

« Il y a un roman derrière le grand théorème de Fermat »

Pourquoi l'énoncé de Fermat, qui est simple et anodin en apparence, a-t-il acquis une telle célébrité ?

Cédric Villani : Il y a tout d'abord le contraste entre le côté élémentaire de cet énoncé du XVII^e siècle et la difficulté extrême de sa preuve que moi-même, par exemple, serais incapable de comprendre en détail sans avoir fait trois ou quatre années d'études préalables. L'énoncé de Fermat (quel que soit l'entier n supérieur à 2, il n'existe pas d'entiers positifs a , b et c tels que $a^n + b^n = c^n$) a attiré une multitude de mathématiciens amateurs, qui rêvaient de pouvoir entrer dans l'histoire en trouvant, un peu sur un coup de chance, une preuve. C'est encore le cas aujourd'hui, avec des gens persuadés qu'il existe une démonstration beaucoup plus simple que celle d'Andrew Wiles. Et au fil des siècles, plusieurs mathématiciens éminents ont, au détour de

BIO EXPRESS

1973

Naissance à Brive-la-Gaillarde, en Corrèze.

2009

Directeur de l'institut Henri-Poincaré

2010

Lauréat de la médaille Fields

2017

Député (LREM) de l'Essonne.

eurs travaux, prouvé le théorème de Fermat pour des valeurs particulières de l'exposant n . Un autre élément d'attrait est l'anecdote historique avec, en particulier, l'erreur ou le bluff de Fermat qui, dans la marge d'un livre, a écrit avoir découvert une démonstration merveilleuse, mais trop longue pour figurer dans cette marge. Il y a un roman derrière le grand théorème de Fermat, et il est haut en couleur !

Le « grand théorème de Fermat » est-il important pour la théorie des nombres ?

Cédric Villani : En soi, non. Ce théorème a ici et là quelques conséquences, mais les méthodes développées pour le démontrer sont de loin plus importantes

que le résultat lui-même. Et c'est une histoire qui a été pleine de rebondissements au cours des dernières décennies.

Dans les années 1980, Andrew Wiles, qui était fasciné depuis son enfance par la conjecture de Fermat, a compris que certains développements dans le domaine où il faisait ses recherches (la géométrie algébrique) lui permettraient peut-être d'élaborer une démonstration. Il a alors travaillé en secret durant des années, avant d'annoncer lors d'un séminaire en 1993 y être parvenu. Mais sa preuve comportait une erreur, et il a fallu l'aide de son ancien étudiant Richard Taylor pour la réviser et l'achever en 1995, dans une course de vitesse pour ne pas se faire doubler par quelqu'un d'autre.

Les méthodes mobilisées pour ce théorème continuent d'ailleurs de bouger, afin de réécrire la preuve et mieux relier l'énoncé de Fermat à d'autres sujets. Tout cela touche des domaines parmi les plus prestigieux des mathématiques, ceux qui font le plus rêver – la théorie des nombres, la géométrie algébrique, champs où l'activité est intense et où l'école française a d'ailleurs une forte expertise.

Pouvez-vous donner une idée de la démarche suivie par Andrew Wiles ?

Cédric Villani : Depuis 1986, on savait, à la suite de divers travaux, que la conjecture de Fermat pouvait être vue comme un cas particulier d'un énoncé plus vaste et plus technique, la conjecture de Shimura-Taniyama-Weil. Cette « conjecture STW », datant des années 1960, prédisait une sorte de dictionnaire, de correspondance, entre les « courbes elliptiques » – des courbes (qui ne sont pas des ellipses...) définies par des équations algébriques du troisième degré à coefficients entiers, et dont on ne considère que les points à coordonnées rationnelles – et des fonctions particulières, les « fonctions modulaires ». Or on peut associer une certaine courbe elliptique à l'équation de Fermat et on a montré que si cette équation avait des solutions en nombres entiers, alors la courbe elliptique correspondante ne vérifierait pas la conjecture STW. Par conséquent, si la conjecture STW est vraie, il s'ensuit que l'équation de Fermat n'a pas de solutions en nombres entiers et le grand théorème de Fermat serait ainsi prouvé. Andrew Wiles a donc entrepris de démontrer la conjecture STW.

C'est ce qu'il a réussi à faire ?

Cédric Villani : Presque. Andrew Wiles a réussi à démontrer une partie importante de la conjecture STW, qui suffisait à prouver la conjecture de Fermat. La conjecture STW complète a été démontrée plus tard, en 1999, par Christophe Breuil, Brian Conrad, Fred Diamond et Richard Taylor. Cette conjecture est d'ailleurs une brique d'un édifice plus vaste qu'on appelle le programme ou la correspondance de Langlands.

**Andrew Wiles
était fasciné depuis
son enfance par
la conjecture de Fermat.
Il a alors travaillé
en secret durant des
années avant d'annoncer
son résultat**

De quoi s'agit-il ?

Cédric Villani : C'est un ensemble d'idées et de conjectures complexes qui ont été esquissées à la fin des années 1960 par le mathématicien canadien Robert Langlands. Ce programme établit des ponts, ou des correspondances, entre la théorie des nombres et d'autres parties des mathématiques (géométrie algébrique, théorie des groupes, etc.). Il continue à occuper aujourd'hui de nombreux chercheurs brillants, parmi lesquels Laurent Lafforgue (médaillé Fields en 2002), Christophe Breuil, Ngô Bao Châu (médaillé Fields en 2010)...

Est-il fréquent que la preuve d'un énoncé élémentaire comme celui de Fermat nécessite des mathématiques de très haut niveau ?

Cédric Villani : Oui, j'y ai moi-même été confronté à plusieurs reprises au cours de ma carrière, dans mes travaux sur la stabilité des gaz et des plasmas. Avec mes collègues, nous nous sommes souvent retrouvés avec des preuves plutôt vertigineuses pour des énoncés qui étaient en eux-mêmes peu compliqués. Le cœur de la preuve peut être assez simple, mais c'est l'enrobage technique qui est très élaboré. Ce qu'on préfère, c'est quand l'idée centrale est à la fois simple et inattendue ; mais ce n'est pas toujours le cas ! ■

Propos recueillis par Maurice Mashaa

A full-page portrait of Andrew Wiles, an elderly man with glasses, wearing a grey tweed jacket over a red V-neck sweater and a patterned tie. He is standing outdoors in front of a modern building with large glass windows. The background is slightly blurred.

Le tombeur de Fermat

Le dernier théorème de Fermat ne fut démontré qu'en 1995, par Andrew Wiles, plus de 360 ans après sa première formulation. Une épopée riche en rebondissements et en détours.

L'ESSENTIEL

► Dans les années 1630, Pierre de Fermat affirma: « Soit n un entier supérieur ou égal à 3. L'équation $x^n + y^n = z^n$ n'a pas de solutions entières non nulles. »

► Plusieurs mathématiciens ont progressé vers la démonstration, parfois au prix de gros efforts intellectuels, mais la preuve définitive n'arriva qu'en 1995.

► Elle passe par des avancées récentes en géométrie arithmétique et notamment dans l'étude des courbes elliptiques et la démonstration de la conjecture de Shimura-Taniyama-Weil.

► Le résultat est important car il repose sur les méthodes employées, les théories déployées que par les questions soulevées.

LES AUTEURS



GIULIO GIORELLO et CORRADO SINIGAGLIA sont professeurs à l'université de Milan, en Italie.



Andrew Wiles Building

Mathematical Institute

CCTV operates in this building

No Smoking

It is against the law to smoke in these premises

Andrew Wiles devant le bâtiment qui porte désormais son nom, à l'université d'Oxford

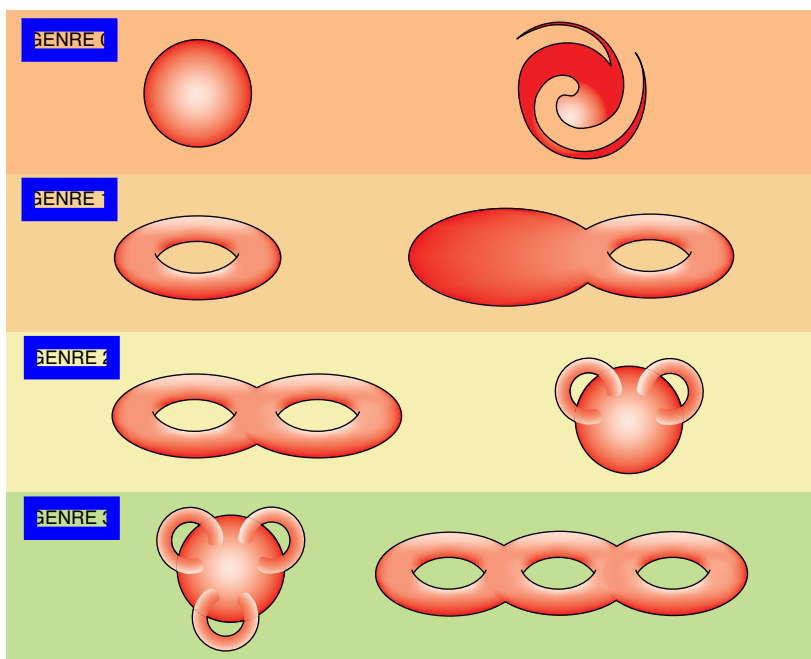
S

Star Trek, Doctor Who, Les Simpson... ces trois séries ont en commun d'avoir mis à l'honneur lors d'au moins un épisode l'un des plus célèbres théorèmes mathématiques. Quel rôle a-t-il joué dans une telle

recupération populaire? Le dernier théorème de Fermat, selon lequel $x^n + y^n = z^n$ n'admet pas de solution quel que soit $n > 2$. L'énoncé est simple, la démonstration, beaucoup moins.

Tout commence en 1637 quand Pierre de Fermat, magistrat et mathématicien, note dans la marge de son édition des *Arithmétiques*, de Diophante: «Au contraire, il est impossible de partager soit un cube en deux cubes, soit un bicarré en deux bicarrés, soit en général une puissance quelconque supérieure au carré en deux puissances de même degré: j'en ai découvert une démonstration véritablement

Dans le corps $\mathbb{C}$ des nombres complexes, l'équation de Fermat engendre une surface fermée et orientable, caractérisée par son genre, c'est-à-dire le nombre de trous qu'elle possède. Deux surfaces qui présentent le même nombre de trous ont topologiquement équivalentes: elles sont de genre égal. Si deux surfaces ont le même genre, on passe de l'une à l'autre à l'aide d'une succession de transformations continues comme les déformations d'une surface en caoutchouc.



merveilleuse que cette marge est trop étroite pour contenir.» On peut douter qu'il l'ait vraiment démontré, car ce n'est qu'en 1995 qu'un autre mathématicien, l'anglais Andrew Wiles, a pu en venir à bout à l'aide d'outils mathématiques très complexes. Ce fut l'épilogue d'une longue histoire riche en détours et en rebondissements.

Remontons le cours de l'histoire, et revenons au début du XIX^e siècle. À cette époque, les mathématiciens savent qu'il suffit de prouver le théorème pour les nombres premiers pour qu'il soit valide quel que soit n . Grâce à Ernst Kummer (1810-1893), ils savent en outre que le théorème est vrai pour les nombres premiers p qu'il a qualifiés de «réguliers» (une certaine propriété liée aux racines du polynôme $x^p - 1$ doit être vérifiée), et qu'il suffit donc de le démontrer pour les nombres premiers «irréguliers».

Toutefois, deux problèmes persistent. D'abord, il n'est pas facile de déterminer si un nombre premier est «régulier». Kummer a trouvé un critère permettant de déduire cette caractéristique, mais plus le nombre premier est grand, plus ce critère est lourd à déterminer. Il s'en est toutefois servi pour démontrer le théorème de Fermat pour tous les nombres premiers réguliers inférieurs à 100. Il est en revanche difficile d'aller plus loin à la main.

Ensuite, Kummer espérait qu'une infinité de nombres p étaient réguliers, faisant de ceux qui ne le sont pas des exceptions. Or, en 1915, le mathématicien danois Johan Jensen montre qu'il existe une infinité de nombres irréguliers.

UNE GOUTTE DANS L'OCEAN

Avec l'avènement de l'informatique, le seuil des nombres premiers réguliers connus croît progressivement: les recherches sur ordinateur montrent que la plupart des nombres premiers inférieurs à un certain seuil sont réguliers et que ces exceptions jouissent d'une propriété supplémentaire, une sorte de régularité faible qui fait que le théorème de Fermat s'applique aussi à ces entiers. Cela réduit d'autant le nombre de cas à traiter au-dessous d'un certain seuil pour démontrer la validité du théorème de Fermat sous ce seuil. Ainsi, en 1983, le théorème est vérifié pour n inférieur à 1 million, puis, en 1992, pour n inférieur à 4 millions.

Ces imposants résultats ne sont cependant qu'une goutte dans l'océan infini des nombres, et le problème de la démonstration du théorème dans sa généralité reste entier.

LA THÉORIE DES GROUPES DE GALOIS

En 1831, un mathématicien français d'une vingtaine d'années, Evariste Galois (1811-1832), soumet à l'Académie

des équations algébriques. Son manuscrit est refusé, qualifié d'inintelligible par ses examinateurs Lacroix et Poisson. Le jeune homme décède un an plus tard au cours d'un duel. Ses travaux ne seront redécouverts que dans les années 1840, par Joseph Liouville, qui les publie en 1846 dans son propre journal, intitulé *Journal de mathématiques pures et appliquées*. La théorie de Galois deviendra un élément incontournable des mathématiques modernes. De quoi s'agit-il ?

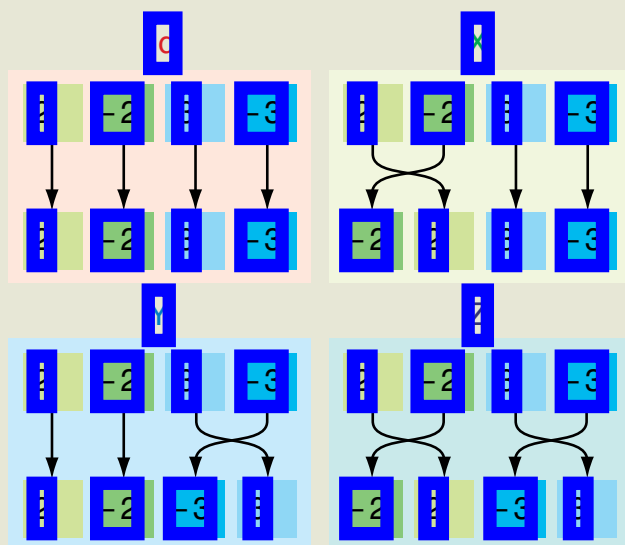
Galois a élaboré une théorie pour déterminer si une équation polynomiale de degré n à coefficients rationnels est résoluble par radicaux, c'est-à-dire à l'aide de ses coefficients et d'un nombre fini d'opérations classiques (addition, soustraction, multiplication, division et extraction de racines). Pour cela, il a associé à chaque équation un objet, qui constitue une « carte génétique » de l'équation. Cet objet est un groupe, le « groupe de l'équation » aujourd'hui baptisé « groupe de Galois ». Galois sait que si une fonction des solutions d'une équation est invariable quand on permute les solutions qu'elle renferme, elle s'exprime rationnellement à l'aide des coefficients de l'équation. Par exemple, la fonction $V(x_1, x_2) = x_1 + x_2$, où x_1 et x_2 sont les solutions de l'équation du second degré $x^2 + px + q = 0$, est invariante par les permutations du groupe S_2 , ensemble des permutations de deux éléments. Ces permutations sont l'identité, et la transposition qui échange x_1 et x_2 . Pour Galois, un groupe (fini) est un ensemble où la composition de deux éléments est un élément du groupe. Cette notion n'est pas si éloignée de la conception moderne du mot groupe (voir l'encadré page suivante). La fonction V

s'exprime donc rationnellement à l'aide des deux coefficients p et q de l'équation. Ici, le calcul est simple : $V(x_1, x_2) = (x_1 + x_2)^2 - 2x_1x_2$, avec $x_1 + x_2 = -p$ et $x_1x_2 = q$. Galois étend ce résultat et démontre que toute fonction des solutions d'une équation, invariable par certaines permutations de ces solutions, mais pas toutes, s'exprime rationnellement en fonction des coefficients de l'équation. Il démontre ensuite que les permutations des racines d'une équation qui conservent les relations rationnelles entre ces racines constituent un groupe, le groupe de Galois. Enfin, il démontre qu'à toute équation algébrique, on peut associer un tel groupe. Galois a ainsi établi une correspondance entre une fonction déterminable rationnellement et les permutations du groupe de l'équation. C'est cette correspondance entre fonctions et groupes finis, adaptée aux courbes elliptiques et aux fonctions modulaires, que Wiles utilise dans la démonstration de la conjecture de Shimura-Taniyama-Weil. Plus précisément, il utilise la correspondance entre le groupe de Galois absolu $G_{\mathbb{Q}}$ et des sous-ensembles de points des courbes elliptiques et des fonctions modulaires (voir l'encadré page 103). Le groupe de Galois absolu réunit toutes les « cartes génétiques » des équations polynomiales à coefficients rationnels : un élément de $G_{\mathbb{Q}}$ détermine ainsi sur chaque équation une permutation particulière des racines.



Evariste Galois, mathématicien malheureux (1811-1832)

Norbert Verdier, IUT de Cachan



| | | | |
|---|---|---|---|
| I | X | Y | Z |
| I | X | Y | Z |
| X | I | Z | Y |
| Y | Z | I | X |
| Z | Y | X | I |

L'ensemble des permutations Id, X, Y, Z constitue un groupe de l'équation $x^4 - 5x^2 + 6 = 0$, car la composition de deux éléments donne un élément de l'ensemble. Les quatre racines de l'équation sont $\pm\sqrt{2}$ et $\pm\sqrt{3}$ car l'équation s'écrit $(x^2 - 2)(x^2 - 3) = 0$. En outre, en examinant la table d'opération du groupe, on remarque que l'ensemble $\{\text{Id}, X\}$ est aussi un groupe : c'est un sous-groupe du groupe $\{\text{Id}, X, Y, Z\}$.

LA NOTION MODERNE DE GROUPE

La structure de groupe est centrale dans les branches les plus variées des mathématiques (groupes de Lie, géométrie algébrique, topologie).

On dit qu'un ensemble E est un **groupe** si, pour toute loi de composition interne $\times$ sur E , on a :
 - **Associativité** : $(x \times y) \times z = x \times (y \times z)$ pour tous x, y, z de l'ensemble.
 - Il existe un **élément neutre** u (unité) de l'ensemble tel que $u \times x = x \times u = x$ pour tout élément x , et chaque élément x possède un **inverse** x' dans l'ensemble tel que $x \times x' = x' \times x = u$.
 Enfin, le groupe est **commutatif** si pour tout couple (x, y) , on a $x \times y = y \times x$. Il est aisé de vérifier que l'ensemble $\mathbb{Z}$ des entiers relatifs (ayant un signe) forme un groupe commutatif pour la loi de composition « addition » ; l'élément neutre est $u=0$ et l'inverse de x est l'entier $-x$. En revanche, l'ensemble $\mathbb{N}$ des entiers naturels muni de la loi de composition « + » n'est pas un groupe. Cette notion abstraite de groupe fut introduite par l'Anglais Arthur Cayley en 1854.

Retour au début du xx^e siècle. L'examen de l'équation (1) $x^n + y^n = z^n$ montre que, pour n'importe quel n (y compris 2), lui trouver des solutions entières est équivalent à chercher des solutions rationnelles à l'équation (2) : $x^n + y^n = 1$.

Quel est l'intérêt de ce décalage ? Il est avantageux de travailler sur l'équation (2) dans le corps $\mathbb{Q}$ des nombres rationnels plutôt que sur (1) dans l'anneau $\mathbb{Z}$ des entiers, car cette équation se prête à une interprétation géométrique immédiate. Ainsi, pour $n=2$, l'équation (2) devient (3) $x^2 + y^2 = 1$, qui représente l'équation d'un cercle de rayon unité et de centre l'origine du plan. Dans ce cas, déterminer les triplets d'entiers vérifiant $x^2 + y^2 = z^2$ (les triplets pythagoriciens) revient à chercher les points du cercle dont les deux coordonnées sont rationnelles, ce qui est plutôt facile.

Pour $n > 2$ en revanche, les courbes associées à l'équation (2) sont plus compliquées qu'un simple cercle, comme on peut déjà le voir pour $n=3$. L'énigme de Fermat devient un cas particulier du problème général de la recherche des solutions rationnelles (c'est-à-dire dans $\mathbb{Q}$) de n'importe quelle équation polynomiale à deux inconnues x, y . En termes géométriques, cela revient à déterminer les points de coordonnées rationnelles sur les courbes réelles associées à ces équations.

DES COURBES AUX SURFACES

L'intuition qui se révélera gagnante (esquissée par Euler) consiste à immerger $\mathbb{Q}$ non dans le corps $\mathbb{R}$ des nombres réels, mais dans celui des nombres complexes, $\mathbb{C}$. De cette façon, on associe non plus des courbes aux équations (2), mais des surfaces fermées et orientables nommées surfaces de Riemann. Ces surfaces furent

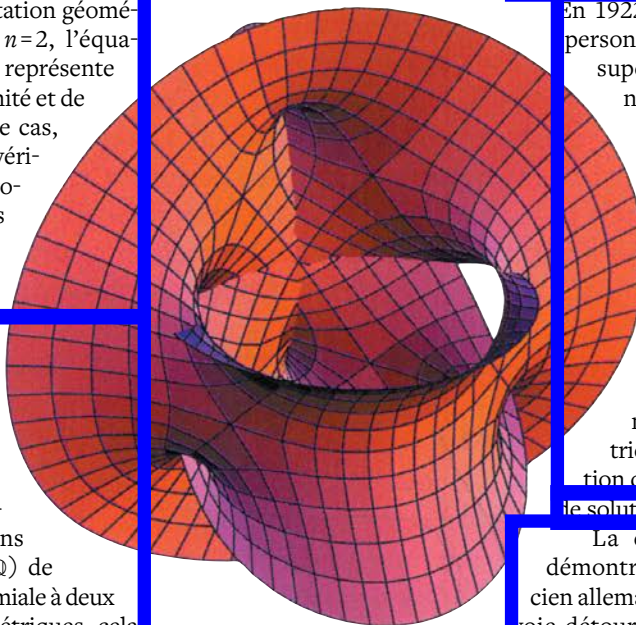
classifiées au xix^e siècle : une surface fermée, orientable et lisse est équivalente, du point de vue topologique, à une sphère avec un certain nombre d'anses (voir la figure page 100). Le nombre d'anses est le genre de la surface. Lorsque la surface est associée à une équation algébrique, le genre est aussi appelé genre de l'équation. Plus le genre est élevé, plus la géométrie de la surface est compliquée et plus il est difficile de trouver les points rationnels de celle-ci. Pour l'équation (2), le genre est donné par la formule $(n-1)(n-2)/2$.

Quand le genre est nul ($n=1$ ou 2), notre problème est simple. Comme nous l'avons vu dans le cas de l'équation (3), si l'équation admet une solution rationnelle, alors elle en admet un nombre infini (il existe bien sûr des équations de genre nul qui n'admettent aucune solution rationnelle, par exemple $x^2 + y^2 = -1$). L'affaire se complique dès lors qu'on considère une équation de genre 1 (c'est-à-dire pour $n=3$). Comme dans le cas précédent, une surface peut ne pas avoir de points rationnels. Mais si elle en a, alors ils sont en nombre fini ou, s'ils sont en nombre infini, ils peuvent être obtenus de manière canonique à partir d'un nombre fini de points rationnels appelés **générateurs**, comme le démontra le mathématicien anglais Louis Mordell.

En 1922, le même Mordell constate que personne n'a trouvé de courbe de genre supérieur ou égal à 2 possédant un nombre infini de points à coordonnées rationnelles. Il fait de cette constatation empirique une conjecture : aucune équation de genre supérieur ou égal à deux ne peut avoir un nombre infini de solutions « génératrices ». Dans notre contexte, la conjecture de Mordell implique que pour n supérieur ou égal à quatre, l'équation (2) a au plus un nombre fini de solutions « génératrices » et, par conséquent, que l'équation de Fermat a au plus un nombre fini de solutions primitives.

La conjecture de Mordell ne fut démontrée qu'en 1983 par le mathématicien allemand Gerd Faltings, au moyen d'une voie détournée. Qu'on en juge. En 1962, le mathématicien Igor Chafarevich avait proposé la conjecture suivante, qui prit ensuite son nom : sous certaines conditions, on peut reconstruire les solutions entières (c'est-à-dire dans $\mathbb{Z}$) d'une équation à partir de l'étude de cette équation modulo p , pour divers nombres premiers p .

En 1968, A. N. Parshin démontra que la conjecture de Chafarevich impliquait celle de Mordell. Et en 1983, Faltings s'attaqua avec succès à la conjecture de Chafarevich, prouvant comme corollaire celle de Mordell ! La



Surface engendrée par l'équation de Fermat $x^3 + y^3 = 1$ quand x et y sont les variables complexes.

COURBES ELLIPTIQUES ET LOI DE GROUPE

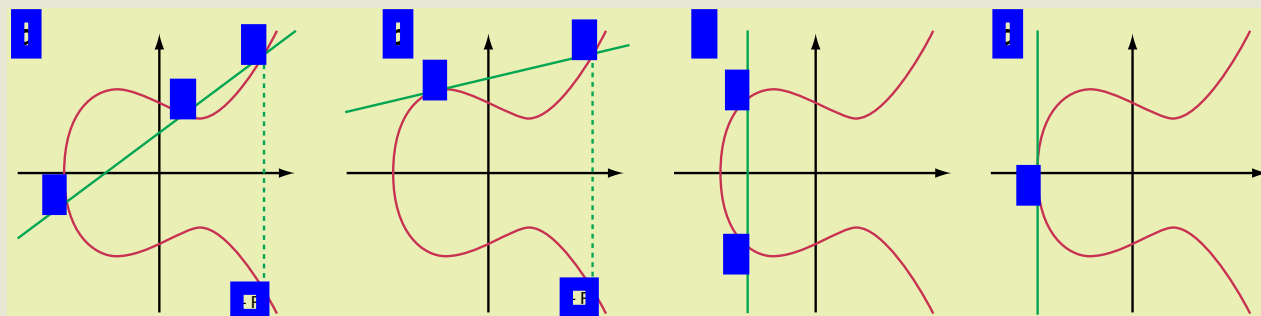
Les courbes elliptiques sont un des outils clés de la démonstration du théorème de Fermat par Andrew Wiles. Voyons de plus près leurs caractéristiques. Une courbe elliptique E est une courbe de

a, b, c, d et e sont des entiers. Une telle équation définit une courbe de genre 1 si elle n'a pas de points singuliers, c'est-à-dire si les dérivées partielles par rapport à x et à y de l'équation ne s'annulent pas en même temps (ce qui impose une condition sur les coefficients). Un point de la courbe E est n'importe quel couple de nombres complexes vérifiant l'équation associée. Si certains points ont des coordonnées réelles (respectivement rationnels), on dit qu'ils ont des coordonnées réelles (rationnelles). Une propriété cruciale des courbes elliptiques est la suivante : l'ensemble de leurs points forme un groupe commutatif, et il en est de même pour l'ensemble de leurs points réels et celui de leurs points rationnels. En d'autres termes, l'« addition » ou la « soustraction » de deux points de la courbe donne un point de la courbe. Qu'est-ce que l'addition de deux points ? Considérons par exemple la courbe elliptique d'équation : $y^2 = x^3 - x - 1$, et deux points distincts P et Q sur cette courbe (voir la figure). La droite qui les joint recoupe en général la courbe en un troisième point R . On définit la somme des points P et Q comme étant le point symétrique de R par rapport à l'axe des abscisses. Si $P = Q$, on utilise la tangente à la courbe : le point $P + P = 2P$ est le point symétrique par rapport à l'axe des abscisses du point d'intersection de la tangente en P avec la courbe. L'opposé d'un point P , noté $-P$, est le symétrique de P par rapport à l'axe des abscisses. Et l'élément

neutre du groupe commutatif est le point ∞ , point de rencontre des verticales à l'infini. Ainsi, la somme de P et de son opposé est bien nulle, puisque la droite qui joint ces points est verticale. Autre propriété importante des courbes elliptiques : elles présentent des points de torsion, c'est-à-dire des points dont un multiple entier est nul. Pour un entier $n > 2$, l'ensemble $E[n]$ des points à coordonnées complexes de la courbe E dont le n -ième multiple est 0 (les points de n -torsion), associés au point ∞ , l'élément neutre, constitue un groupe commutatif d'ordre n .

On montre, à partir de l'expression des coordonnées de la somme de plusieurs points, que les abscisses x des points de $E[n]$ vérifient une équation polynomiale à coefficients rationnels. Or, par définition, le groupe de Galois absolu conserve les relations algébriques, en particulier l'équation vérifiée par les abscisses des points de $E[n]$, et celle vérifiée par leurs ordonnées – l'équation de E . Par conséquent, il permute les points de $E[n]$ entre eux. C'est grâce à cette propriété que l'on peut établir une correspondance entre le groupe $E[n]$ et le groupe de Galois absolu. On a ainsi construit une représentation galoisienne des courbes elliptiques. Andrew Wiles démontra la conjecture de Shimura-Taniyama-Weil en établissant une correspondance similaire entre le groupe de Galois absolu et les fonctions modulaires, et en montrant que ces deux représentations galoisiennes sont isomorphes.

Catherine Goldstein, institut de mathématiques de Jussieu-Paris-Rive-gauche.



Différents cas d'addition de points P et Q sur la courbe elliptique d'équation $y^2 = x^3 - x - 1$, représentée dans le plan réel. Quand P et Q sont distincts, $P + Q = -R$ (a). Quand $P = Q$, $P + P = -R$ (b). Quand P et Q ont la même abscisse (c), leur somme est égale au point ∞ (là où les droites verticales se rencontrent à l'infini). Quand P et Q sont confondus en un point de tangente verticale, $P + P$ vaut le point ∞ (d).

La démonstration de Faltings exploite la résolution, due à Pierre Deligne en 1978, de la conjecture de Weil. André Weil avait proposé en 1949 un analogue pour les corps finis de la célèbre hypothèse de Riemann, formulée à l'origine pour le corps $\mathbb{C}$ des nombres complexes (voir *L'hypothèse qui valait un million*, par P. Meier, page 68).

DETOUR PAR LE JAPON

Ainsi aucune équation du type (2) ne peut avoir un nombre infini de solutions génératrices pour $n > 2$. Peu après, en 1985, en utilisant le résultat de Faltings, Andrew Granville et Roger Heath-Brown démontrèrent que le nombre de solutions des équations (2), s'il en existe, est une fonction décroissante de l'entier n . Ce point

ne résout cependant pas l'énigme de Fermat. Il suffit en effet d'une seule solution rationnelle de l'équation (2) pour obtenir une solution entière de l'équation (1) et donc un nombre infini de solutions de celle-ci.

La solution de l'énigme de Fermat fut finalement l'œuvre d'un descendant de la vieille Angleterre émigré aux États-Unis, Andrew Wiles. Le chemin tortueux de la découverte passa par le Japon tumultueux de l'après-guerre. Revenons au cas $n=2$ du théorème, exprimé au moyen de l'équation (3) : $x^2 + y^2 = 1$. On peut paramétriser x et y par respectivement des fonctions cosinus et sinus, qui satisfont la relation : (4) $\cos^2 \alpha + \sin^2 \alpha = 1$.

Résoudre l'équation de Fermat pour $n=2$, c'est-à-dire déterminer les triplets de Pythagore.

revient donc à trouver un angle α dont le sinus et le cosinus sont des rationnels. En 1955, le japonais Yutaka Taniyama énonça une conjecture qui généralisait cette idée aux courbes elliptiques définies sur $\mathbb{Q}$. Ces courbes, ainsi nommées parce qu'elles interviennent dans la rectification d'un segment d'ellipse, sont les courbes de genre 1 dont l'équation peut se ramener à une expression du type : $y^2 + axy + by = x^3 + cx^2 + dx + e$, où a, b, c, d et e sont des entiers (voir l'encadré page précédente). Taniyama conjectura que ces courbes peuvent être paramétrisées par certaines fonctions dites modulaires qui généralisent les fonctions trigonométriques. On retrouva Taniyama, âgé d'à peine 31 ans, mort dans son appartement le matin du 17 novembre 1958. Dans une lettre laissée sur son bureau, il confiait son intention de mettre fin à ses jours.

Précisée par André Weil en 1968 et reprise en 1971 par un autre Japonais, Goro Shimura, cette conjecture prit le nom de «conjecture de Shimura-Taniyama-Weil». Pour le mathématicien japonais, elle est inspirée par l'idée de la beauté intrinsèque des mathématiques. Quel lien existe-t-il entre cette conjecture et le dernier théorème de Fermat ?

En 1985, l'Allemand Gerhard Frey propose l'associer la courbe elliptique d'équation (5) : $y^2 = x(x+a^n)(x-b^n)$ à un triplet de Fermat (a, b, c) , c'est-à-dire un triplet vérifiant l'équation (6) : $a^n + b^n = c^n$ (en supposant qu'il en existe pour un quelconque n).

L'équation (5) est belle, mais infidèle : selon Frey, cette courbe représenterait un contre-exemple de la conjecture de Shimura-Taniyama-Weil. Il serait impossible de la paramétriser avec des fonctions modulaires. La conjecture de Frey (connue sous le nom de «conjecture epsilon») est une métaconjecture, c'est-à-dire une conjecture selon laquelle si une autre conjecture est vraie (la conjecture de Shimura-Taniyama-Weil) alors le théorème de Fermat l'est aussi.

Un an plus tard, l'Américain Kenneth Ribet démontre que la courbe de Frey n'est pas paramétrisable par des fonctions modulaires. Pour résoudre l'énigme de Fermat, il «suffit» donc à présent de démontrer la prémisse de la conjecture epsilon, c'est-à-dire la conjecture de Shimura-Taniyama-Weil.

LA FIN HEUREUSE D'UNE EPOPEE

On pourrait penser que l'énigme n'a été que simplement déplacée, mais, comme Andrew Wiles le souligne en 1993, travailler sur les courbes elliptiques modulaires, objets géométriques sur lesquels on sait déjà beaucoup et on espère en savoir encore plus, est bien différent de travailler avec les propriétés des nombres, que Fermat qualifiait de fugitives.

La preuve de Wiles s'insère dans ce contexte précis. En premier lieu, il restreint

l'analyse de la conjecture de Shimura-Taniyama-Weil en se limitant à la classe des courbes elliptiques dites semi-stables, classe à laquelle appartient la courbe d'équation (5).

La grande intuition de Wiles consiste à faire appel à un outil fondamental des mathématiques, la théorie des groupes de Galois (voir l'encadré page 101). Au XIX^e siècle, le jeune Évariste Galois a établi une correspondance entre les fonctions rationnelles des solutions d'une équation et le groupe des permutations de ces solutions. L'avantage de cette traduction est qu'un groupe est souvent une structure engendrée par un ensemble fini d'éléments. Wiles propose de comparer les représentations de Galois correspondant aux courbes elliptiques semi-stables avec celles correspondant aux fonctions modulaires.

UN TROU DANS LA DÉMONSTRATION

En 1993, au cours d'une rencontre à l'Institut de mathématiques de Cambridge, en Angleterre, il annonce y être parvenu. Mais quelques mois plus tard, en décembre, il reconnaît que sa démonstration présente un «trou». Rentré à Princeton, il se met au travail pour corriger la faille. En octobre 1994, il annonce en être venu à bout en collaboration avec un ex-étudiant de Cambridge, Richard Taylor.

En mai 1995, un long texte de Wiles, intitulé «Modular elliptic curves and Fermat's last theorem» («Les courbes elliptiques modulaires et le dernier théorème de Fermat») et contenant le cœur de son raisonnement, paraît dans la revue *Annals of Mathematics*, suivi d'un autre article écrit en collaboration avec Richard Taylor, «Ring theoretic properties of certain Hecke algebras» («Les propriétés théoriques annulaires de certaines algèbres de Hecke»), qui apporte la solution du point critique. Finalement, en 1999, Taylor, avec Brian Conrad, Christophe Breuil et Fred Diamond complètent le travail de Wiles en montrant que la conjecture de Shimura-Taniyama-Weil est aussi valide pour les courbes elliptiques non semi-stables.

Le dernier théorème de Fermat, qui découle de la conjecture de Shimura-Taniyama-Weil, est enfin démontré. L'épopée séculaire, commencée dans une marge trop étroite, est close. Comme l'écrivit François Rabelais (1494-1553), mieux vaut conclure les controverses par des signes que par des déclamations lorsqu'on recourt à des arguments si compliqués que les paroles humaines ne peuvent suffire à les exposer correctement. C'est pourquoi, après tant d'épisodes personnels bizarres ou dramatiques, la résolution de l'énigme de Fermat confirme le mot du mathématicien américain Hans Lewy : «L'histoire des mathématiques n'est ni tragique ni comique, mais épique.» ■

BIOGRAPHIE

J. VERDIER, Galois : le mathématicien maudit, Belin-Pour la Science, 2011.

R. TAYLOR et A. WILES, Ring-Theoretic Properties of Certain Hecke Algebras, *Annals of Mathematics*, vol. 141, pp. 553-572, 1995.

A. WILES, Modular Elliptic Curves and Fermat's Last Theorem, *Annals of Mathematics*, vol. 141, pp. 443-551, 1995.

C. GOLDSTEIN, Autour du théorème de Fermat, *Unémosyme* n° 7, pp. 34-61, 1994.

Des nombres et des énigmes

Les dernières énigmes préparées
par Ana Retchman et Sébastien Kerniviner

Solutions page 106

Ana
Retchman



Sébastien
Kerniviner



ENIGME 10

Trouver le plus petit
nombre divisible
par 999 qui ne contienne
pas de 9 parmi
ses chiffres

ENIGME 12

Si p et $p^2 + 8$ sont
des nombres premiers,
quelle est la valeur
de $p^3 + 4$?

ENIGME 11

Calculer la somme
de tous les nombres
palindromes
à 3 chiffres.

ENIGME 13

Combien de chiffres
a le plus petit nombre entier
qui se termine par 2 tel que
si on déplace le chiffre 2
en tête du nombre on obtient
un nombre deux fois
plus grand?

ENIGME 14

Écrire le nombre
2019 sous la forme
d'une somme
de cinq nombres
entiers au cube.

Réponses et solutions

Réponse 1: $N=8$

Solution. On dira que deux nombres sont *cotassés* lorsque chacun d'eux, ainsi que leur somme, sont coloriés d'une même couleur. En coloriant les nombres de $[1, 8]$ ainsi: $\{1, 2, 4, 8\}$ en rouge et $\{3, 5, 6, 7\}$ en bleu, on vérifie que la somme de deux nombres d'une même couleur n'est jamais de la même couleur. Le nombre cherché est donc au moins égal à 8. En revanche, comme $9=8+1=3+6$, il est illusoire de chercher à «prolonger» ce coloriage à $[1, 9]$ sans avoir de nombres cotassés.

Et cette impossibilité est générale, quel que soit le coloriage en deux couleurs. Démontrons-le.

Prenons un coloriage quelconque des nombres de $[1, 9]$ en deux couleurs. Parmi les cinq nombres $\{5, 6, 7, 8, 9\}$, au moins trois sont de la même couleur; appelons S cette couleur et a, b et c les trois nombres rangés ainsi: $5 \leq a < b < c \leq 9$. Définissons aussi $b' = c - a$, $c' = b - a$ et $a' = c - b$. On vérifie que b' et c' sont dans l'intervalle $[1, 4]$ et on calcule $b' - c' = (c - a) - (b - a) = c - b$. Si b' est colorié en S alors b' et a sont cotassés. De même pour c' . Sinon, b' et c' ne sont pas coloriés en S et si $a' = b' - c'$ n'est pas, lui non plus, colorié en S alors c' et a' sont cotassés et sinon $a' = b - c$ est colorié en S donc a' et b sont cotassés. Conclusion: Quel que soit le coloriage, dans tous les cas, on a trouvé deux nombres cotassés. Le nombre maximum recherché doit donc être strictement plus petit que 9. Nous avons vu qu'il doit aussi être au moins égal à 8: c'est donc 8. Il s'agit du nombre de Schur faible $WS(2)$ décrits page 38.

Réponse 2: 55

Solution. Appelons R_n le nombre de randonnées allant de 1 à un entier n . La dernière étape avant d'atteindre n , peut être un ajout de 2 provenant de $n-2$ (il y en a R_{n-2}) ou bien un ajout de 1 provenant de $n-1$ (il y en a R_{n-1}) donc $R_n = R_{n-1} + R_{n-2}$. Comme $R_2 = 1$ et $R_3 = 2$, (R_n) est la suite de Fibonacci. Par conséquent, $R_1 = F_{10} = 55$. Le nombre de randonnées cherché est 55.

Réponse 3: 1, 2, 3, 6, 12, 24, 48, 96, 192 et 384

Solution. Voici une possibilité pour cette liste de dix entiers positifs. Commençons par les deux premiers entiers positifs, 1 et 2. Le nombre suivant sera $1+2=3$, le quatrième sera $1+2+3=6$, le cinquième sera $1+2+3+6=12$. Nous observons que par construction, la somme est maintenant toujours divisible par tous ses termes puisque chaque nouvel élément est le double du précédent.

Continuons ce procédé jusqu'à obtenir le dixième élément de la liste, qui sera 384. Ainsi 1, 2, 3, 6, 12, 24, 48, 96, 192, 384 est une liste recherchée, chaque élément divisant la somme totale, ici 768. D'une façon générale, pour construire une telle liste, il faut la commencer avec un nombre entier positif a et son double $2a$.

Réponse 4: $r=1$

Solution. Ecrivons le nombre r sous la forme d'une fraction irréductible $r=a/b$: les nombres a et b sont alors deux entiers naturels premiers entre eux. On a alors $r+1/r = (a^2+b^2)/ab$. Si ce nombre est un entier, le dénominateur ab doit diviser le numérateur a^2+b^2 . Ainsi, a divise a^2+b^2 , donc il doit diviser b^2 . Comme a et b sont premiers entre eux, cela entraîne $a=1$. De manière analogue, on montre que $b=1$. Cela entraîne $r=1$. Comme réciproquement 1 est clairement solution, on voit que $r=1$ est l'unique nombre rationnel positif répondant à la question.

Réponse 5: $(x, y) = (2, 5)$ et $(3, 7)$

Solution. Dès que $x \geq 5$, le dernier chiffre de $x!$ est un 0, donc le dernier chiffre de $x!+3$ est un 3 et celui de $6 \times (x!+3)$ est un 8. Or, le dernier chiffre d'un nombre au carré comme y^2 est 0, 1, 4, 5, 6 ou 9, donc le dernier chiffre de y^2+5 est 0, 1, 4, 5, 6 ou 9, mais pas 8. Cela montre que le cas $x \geq 5$ est impossible. Il ne reste qu'à examiner les cas suivants.

Si $x=1$ alors $6 \times (x!+3)$ vaut 24. Comme 19 n'est pas le carré d'un nombre entier, cela ne correspond pas à une solution.

Si $x=2$ alors $6 \times (x!+3)$ vaut 30. Comme $25=5^2$, cela correspond à la solution $(x, y) = (2, 5)$.

Si $x=3$ alors $6 \times (x!+3)$ vaut 54. Comme $49=7^2$, cela correspond à la solution $(x, y) = (3, 7)$.

Si $x=4$ alors $6 \times (x!+3)$ vaut 162. Comme 157 n'est pas le carré d'un nombre entier, cela ne correspond pas à une solution.

Les seules solutions sont donc $(x, y) = (2, 5)$ et $(3, 7)$.

Réponse 6: 32 916

Solution. La décomposition en facteurs premiers de 156 est $2^2 \times 3 \times 13$. Donc $32a1b$ doit être divisible par 4, par 3 et par 13. Pour que ce nombre soit divisible par 4, il faut que le nombre formé par ses deux derniers chiffres (en l'occurrence $1b$) soit divisible par 4. On en déduit $b=2$ ou $b=6$.

Si $b=2$, alors pour que le nombre soit divisible par 3, il faut que a soit égal à 1 ou 4 ou 7, car la somme des chiffres du nombre $32a12$ doit être divisible par 3. Cependant, aucun des nombres alors obtenus n'est divisible par 13.

Si $b=6$, alors pour que le nombre soit divisible par 3, il faut que a soit égal à 0 ou 3 ou 6 ou 9. On obtient alors les nombres: 32016, 32316, 32616 et 32916. Le seul divisible par 13 est 32916.

Réponse 7: 18

Solution. Remarquons d'abord que l'ensemble de nombres cherché contient au maximum huit nombres, tous inférieurs ou égaux à 8. Pour que le produit de ces nombres soit le plus grand possible, il faut que ces nombres soient différents de 1. Ainsi les

différentes possibilités sont: $2+6$; $2+3+3$; $2+2+2+2$; $3+5$; $2+2+4$; $4+4$.

On voit alors que le plus grand produit est $18=2 \times 3 \times 3$.

Réponse 8: 144

Solution. Pour trois nombres a, b, c , si $0 < a < b < c$ et si $c < a+b$ alors il existe un triangle dont les côtés ont pour longueurs a, b et c . Par l'hypothèse faite sur les a_i et comme les valeurs de a_i sont en ordre croissant, on a: $a_1+a_2 \leq a_3$; $a_2+a_3 \leq a_4$; $a_3+a_4 \leq a_5$...

$$a_{10}+a_{11} \leq a_{12}.$$

En combinant les deux premières inégalités, on obtient:

$$a_1+2a_2 \leq a_4.$$

Puis, en ajoutant la première inégalité, on obtient: $2a_1+3a_2 \leq a_5$.

En sommant ces deux dernières inégalités, on obtient:

$$3a_1+5a_2 \leq a_6.$$

On continue ainsi jusqu'à obtenir le terme a_{12} . Remarquons qu'au fur et à mesure, de la même façon que dans la suite de Fibonacci, le coefficient devant a_1 est obtenu en sommant les deux coefficients précédents. Les coefficients devant a_2 se comportent de la même manière. Ainsi, la dernière inégalité sera: $55a_1+89a_2 \leq a_{12}$.

Comme $a_2 \geq a_1$, on a nécessairement $144a_1 \leq a_{12}$ et donc $a_{12}/a_1 \geq 144$.

Il est de plus possible d'atteindre cette valeur en considérant la suite de Fibonacci $a_1=a_2=1$, $a_3=2$, $a_4=3$, $a_5=5$... $a_{12}=144$. Finalement, la valeur recherchée est 144.

Réponse 9: 25 et 100

Solution. Notons z et w les deux nombres. On a donc $z+w=125=4z+w/4$. Par conséquent:

$$4z+4w=16z+w, 3w=12z, w=4z \text{ et donc } 5z=125.$$

On en déduit $z=25$ et $w=100$.

Réponse 10: 111888

Solution. Notons a ce nombre. On a donc:

$$a=999 \times b = (1000-1)b = 1000b-b.$$

Si le nombre b avait un ou deux chiffres, alors le chiffre des centaines de $1000b-b$ serait un 9. Par conséquent b est constitué d'au moins trois chiffres. D'autre part, b ne peut pas se terminer par 0 puisque si c'était le cas, on pourrait trouver un nombre strictement plus petit et ne contenant pas de 9 (simplement en divisant par 10). De plus, le chiffre des dizaines ne peut pas non plus être 0, car sinon, celui de a serait un 9. Enfin b ne peut pas se terminer par un 1 car sinon a se terminerait par un 9. Ainsi le nombre minimum pour b est 112. Dans ce cas, $a=999 \times 112=111888$ ne contient pas de 9.

Réponse 11: 49500

Solution. A chaque nombre palindrome aba avec ses chiffres $a \neq 0$ et $b \neq 0$, on associe le palindrome $(10-a)(10-b)(10-a)$. La somme de aba et de $(10-a)(10-b)(10-a)$ est:

$$(100a+10b+a) + (100(10-a) + 10(10-b) + (10-a)),$$

$$\text{soit } 10(100+10+1) = 1110.$$

Il y a $9 \times 9 = 81$ nombres palindromes avec $a \neq 0$ et $b \neq 0$. La somme de ces 81 nombres vaut donc $(81 \times 1110)/2 = 44955$, où l'on divise par deux, car on compte chaque nombre deux fois dans la somme. Il reste à ajouter la somme de tous les nombres palindromes de la forme $a0a$ avec $a \neq 0$: $909+808+\dots+101 = 4545$.

Donc la somme de tous les nombres palindromes à 3 chiffres est $44955+4545=49500$.

Réponse 12: 3

Solution. Au premier abord, on peut penser que p peut prendre beaucoup de valeurs, et donc qu'il y a de nombreuses solutions. L'énoncé de l'énigme laisse pourtant entendre qu'il n'y a qu'une valeur de p premier pour laquelle p^2+8 aussi est premier. La valeur $p=2$ donne $p^2+8=12$ qui n'est pas premier, et la valeur $p=3$ donne $p^2+8=17$ qui est bien premier. Nous allons montrer que pour toute autre valeur de p , le nombre p^2+8 n'est pas premier.

Si p est un nombre premier différent de 3, alors p est de la forme $3n+1$ ou $3n-1$, pour un certain entier n . On va alors écrire $p=3n \pm 1$ et avec cette écriture on calcule:

$$p^2+8 = (3n \pm 1)^2 + 8 = 9n^2 \pm 6n + 9.$$

Ce dernier nombre est toujours divisible par 3 et strictement supérieur à 3, donc il n'est pas premier. Par conséquent, on a nécessairement $p=3$. Ainsi $p^3+4=31$ (qui est premier).

Réponse 13: 18 chiffres

Solution. Notons a le nombre initial dont l'écriture se termine par 2 et b le nombre obtenu en déplaçant ce 2 en premier chiffre. Par hypothèse, $2a=b$ et a se termine par 2, donc b se termine par 4. Donc a se termine par 42 par conséquent b se termine par 84. Alors a se termine par 842 donc b par 684 (ici on ne peut pas dire que b se termine par 1684). En continuant on voit que a se termine par 6842, et donc b par 3684, et de proche en proche on obtient que a se termine par 105263157894736842.

A ce moment, la multiplication par 2 montre que b commence par 105263157894736842 $\times 2 = 210526315789473684$.

Comme ce nombre est obtenu justement en déplaçant le 2 final de a , on voit que ce choix de a fait l'affaire, et que tout autre a doit se terminer ainsi. Enfin le nombre 105263157894736842 a 18 chiffres.

Réponse 14: 2019=113+73+73+13+13

Solution. Il est assez facile d'écrire 2019 comme somme de sept cubes, puisque $2000=10^3+10^3$, et donc:

$$2019=10^3+10^3+2^3+2^3+1^3+1^3+1^3.$$

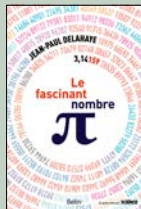
Par contre pour réaliser 2019 comme somme de cinq cubes, il faut utiliser des nombres plus grands que 10. Puisque $13^3=2197$, on doit nécessairement utiliser un 11^3 ou un 12^3 . Avec 11^3 , on trouve $11^3+7^3+7^3+1^3+1^3=1331+343+343+1+1=2019$.

POUR D'AUTRES ENIGMES

A. Rechtman Bulajich,
Calendrier mathématique, Presses
universitaires de Grenoble, 2019.

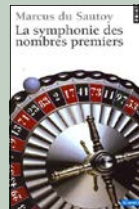


PUG



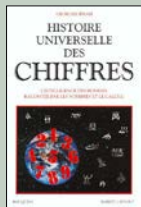
Le Fascinant Nombre π
JEAN-PAUL DELAHAYE
BELIN, 2018
384 PAGES. 22 EUROS

Le nombre π est une star incontournable. Omniprésente en mathématiques et en physique comme dans la culture populaire. Et c'est à juste titre! On a très tôt cherché à l'appivoiser. La quadrature du cercle a suscité bien des efforts, même après que l'on a prouvé son impossibilité. Et sur l'océan des décimales de π se défient aujourd'hui d'étranges navigateurs, faisant appel tant à l'informatique qu'aux mathématiques. Ce livre retrace l'histoire de son exploration, en insistant sur les épisodes les plus récents qui nous font percevoir tout le mystère de ce nombre: plus on connaît π , plus il se dérobe.



La Symphonie des nombres premiers
MARCUS DU SAUTOY
SEUIL, POINTS SCIENCE, 2001
496 PAGES. 11.20 EUROS

Depuis Pythagore et Euclide, une petite musique insistante empêche les mathématiciens de dormir. Les nombres premiers et de leur étrange distribution dans la suite des nombres «normaux». Pour raconter les péripéties d'une recherche séculaire et expliquer ses enjeux, l'auteur campe les grands héros de l'histoire – Riemann, le «Wagner» des mathématiques, Hilbert, virtuose incomparable, ou Ramanujan, jeune prodige indien –, et explicite également les mille applications potentielles d'une recherche qui ne peut plus fondamentale.



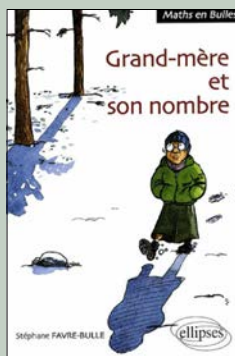
Histoire universelle des chiffres (T. 1 & 2)
GEORGES IFRAH
ROBERT LAFFONT, 1994
1056 ET 1024 PAGES. 28 EUROS PAR TOME

Des années durant, l'auteur s'est plongé dans une quête aussi folle que celle de la Grèce pour comprendre d'où viennent les chiffres. De ses recherches, il a tiré un ouvrage exceptionnel, une encyclopédie qui raconte en termes accessibles toute l'histoire des chiffres et apporte de nouvelles lumières, non seulement à l'épopée du calcul (des cailloux à l'ordinateur), mais encore à des domaines aussi éloignés que l'histoire des religions et des mystiques. Outre les Égyptiens, les Babyloniens, les Juifs, les Mayas, on découvre aussi la civilisation indienne à qui l'on doit l'invention capitale de notre zéro.



Le Dernier Théorème de Fermat
SIMON SINGH
PLURIEL, 2011
312 PAGES. 8.10 EUROS

Pierre Fermat, au XVII^e siècle, s'était contenté d'indiquer dans une marge : « Je n'ai pas le temps de démontrer que $x^n + y^n = z^n$ n'a pas de solution merveilleuse, mais la place me manque pour la développer. » Ce théorème allait devenir la quête ultime du monde mathématique. Les plus puissants esprits de tous les siècles et de toutes les nations tentèrent de venir à bout de cette équation jusqu'à ce que, en 1993, un jeune Anglais, Andrew Wiles, parvienne enfin à la résoudre, devant le regard ébahi de la communauté scientifique. Une épopée qui met en scène les intelligences les plus brillantes.



Grand-mère et son nombre
STÉPHANE FAVRE-BULLE
ELLIPSES, 2008
96 PAGES. 14.20 EUROS

Faire défiler dans sa tête les nombres entiers naturels (1, 2, 3, 4...) est un jeu d'enfant! Pourtant, il a fallu des millénaires pour que l'on puisse utiliser ces nombres d'une manière aussi simple: 2+3 ou 10-5 ou 2x3. Et 11 et $\sqrt{2}$? Sont-ils apparus beaucoup plus tard? Sont-ils si différents? Sont-ils si difficiles à approcher? Lionel ne s'était jamais posé toutes ces questions en arrivant chez sa grand-mère pour le week-end. Mais une mamie mathématicienne aime raconter des histoires parsemées de chiffres... Et elle devient vite passionnante lorsqu'elle parle de son monde fabuleux!

RENDEZ-VOUS

P. 110

REBONDISSEMENTS

DES ACTUALITÉS SUR
DES SUJETS ABORDÉS
DANS LES HORS-SÉRIES PRÉCÉDENTES



P. 114

DONNÉES À VOIR

DES INFORMATIONS
SE COMPRENNENT MIEUX
LORSQU'ELLES SONT MISES EN IMAGES



P. 116

LES INCONTOURNABLES

DES LIVRES, DES EXPOSITIONS,
DES SITES INTERNET, DES VIDÉOS,
DES PODCASTS... À NE PAS MANQUER



P. 118

SPÉCIMEN

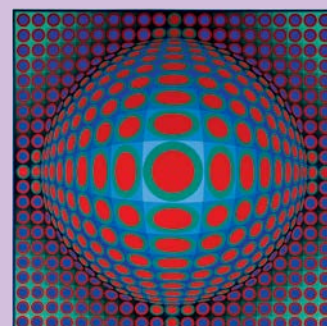
UN ANIMAL ÉTONNANT CHOISI
PARMI CEUX PRÉSENTÉS SUR
LE BLOG «BEST OF BESTIOLES»



P. 120

ART & SCIENCE

COMMENT UN ŒIL SCIENTIFIQUE
OFFRE UN ÉCLAIRAGE INÉDIT
SUR UNE ŒUVRE D'ART



HORS-SÉRIE N° 101 : VÉGÉTAL

Une restauration rapide, mais dans le désordre

La nature reprend ses droits quand des terres déboisées ne sont plus exploitées. Une forêt, dite secondaire, se réinstalle. Mais à quel rythme ? Et dans quelle mesure ressemble-t-elle à une forêt primaire ?

Les arbres nous procurent à nous humains, quantité de bienfaits détaillés dans le *Hors-Série* n° 101 : « La révolution végétale », et pourtant, on ne cesse de les décimer. Essentiellement sous les coups de la conquête de terres agricoles, la déforestation va bon train. Mais que se passe-t-il après, une fois que l'exploitation cesse et que les terres prises sur la forêt sont « relâchées », rendues à la nature ? C'est ce qu'ont voulu savoir Danaë Rozendaal, de l'université de Wageningen, aux Pays-Bas.

Pour ce faire, ils ont inventorié les espèces d'arbres dans quelque 1800 zones de forêt secondaire tropicale d'âges variés à travers 10 pays d'Amérique centrale et du Sud et les ont comparées avec celles présentes en forêt primaire. Rappelons que ces dernières hébergent l'essentiel (96%) de la biodiversité planétaire en termes d'arbres, avec quelque 53 000 espèces. Or elles disparaissent peu à peu : aujourd'hui, les forêts secondaires représentent 28% des terres en Amérique latine.

Qu'ont observé les chercheurs ? La biodiversité en termes de nombre d'espèces revient vite et retrouve les niveaux de la forêt primaire en cinq décennies (le taux de

récupération est de 80% en 20 ans). Cependant, la composition initiale en espèces (déduite de l'étude des forêts primaires voisines) et leurs proportions relatives ne reviennent qu'après plusieurs siècles. C'est notamment le cas lorsque certaines espèces ont disparu localement. Après 20 ans, seuls 34% de la composition originale sont retrouvés. En d'autres termes, après un épisode de déforestation, une forêt diversifiée revient vite, mais ce n'est plus la même qu'auparavant.

Selon l'un des auteurs de l'étude, la récupération rapide de la biodiversité est plutôt une bonne nouvelle. Toutefois, des actions ciblées de réintroduction d'espèces particulières seront nécessaires pour garantir leur préservation sur le long terme. De même, la protection de forêts primaires est indispensable au reboisement. Un message important pour respecter le Défi de Bonn (Bonn Challenge) visant, à l'initiative de l'UICN, le reboisement de 150 millions d'hectares de terres dégradées d'ici à 2020 et 350 millions d'hectares d'ici à 2030.

D. ROZENDAAL ET AL., SCIENCE ADVANCES, VOL. 5, N° 3, ART. EAAL13114, 2019

Après un épisode de déforestation, une forêt primaire récupère assez vite, mais un peu dans le désordre



Réparer la mémoire

La mémoire est fragile. Le *Hors-Série* n° 102 :

« La mémoire » le montrait. Elle est notamment perturbée lors d'une dépression, du vieillissement... Comment y remédier ? Étienne Sibille, de l'université de Toronto, au Canada, et ses collègues proposent de cibler les anomalies des récepteurs GABA qu'ils ont reliées aux dysfonctionnements de la mémoire. Pour ce faire, ils ont conçu de nouvelles molécules, dérivées de benzodiazépines (une classe d'antidépresseurs), qui contrecarreraient ces dommages des récepteurs GABA. Les premiers essais précliniques sont encourageants. Si l'efficacité est confirmée, ces molécules pourraient également être utiles dans les premiers stades de la maladie d'Alzheimer où l'on détecte les mêmes anomalies.

E. PREVOT ET AL., MOLECULAR NEUROPSYCHIATRY, RÉPUBLICATION 2019

Vitamines contre cancer

Parmi les nouvelles pistes de traitement, les vitamines ont été étudiées dans le *Hors-Série* n° 99 : « Cancer. L'arsenal des nouvelles thérapies », les thérapies à base de cellules souches sont de plus en plus courantes, notamment contre les cancers du sang (lymphomes, leucémies...). Cependant, on doit veiller à stimuler la production de cellules sanguines pour pallier les effets négatifs du traitement. L'équipe d'Olaia Naveiras, de l'EPFL, a montré qu'un dérivé de la vitamine B3 serait particulièrement indiqué pour cette tâche. Pourquoi ? Parce que ce composé favoriserait l'élimination des mitochondries « stressées » et leur remplacement.

N. VANNINI ET AL., CELL STEM CELL, VOL. 24, PP. 405-418, 2019

La musique nuit gravement à la créativité

Les vertus de la musique sur le cerveau sont nombreuses, plusieurs articles du *Hors-Série* n° 100: «Good vibrations» en ont apporté la preuve. Stress atténué, émotions contrôlées, dépression écartée... Une opinion bien partagée veut qu'en écoutant de la musique nous soyons également plus créatifs. Emma Threadgold, de l'université du Lancashire central, à Preston, en Grande-Bretagne, et ses collègues ont voulu en avoir le cœur net.

Ils ont étudié l'effet d'un fond musical sur les performances d'individus dans plusieurs tâches sollicitant la créativité. Par exemple, il s'agissait de trouver un mot qui, ajouté à trois autres, en forme autant de nouveaux. Ainsi, quel mot peut-on accoler à «feuille», «manteau» et «monnaie»? Trois ambiances ont été testées: musique instrumentale, musique et paroles dans une langue étrangère, ainsi que musique et paroles dans une langue connue. Dans tous les cas, les résultats ont montré un effet négatif du fond sonore sur les exercices à accomplir par rapport à un environnement silencieux. Même des chansons améliorant l'humeur (dans la troisième ambiance) nuisent aux performances.

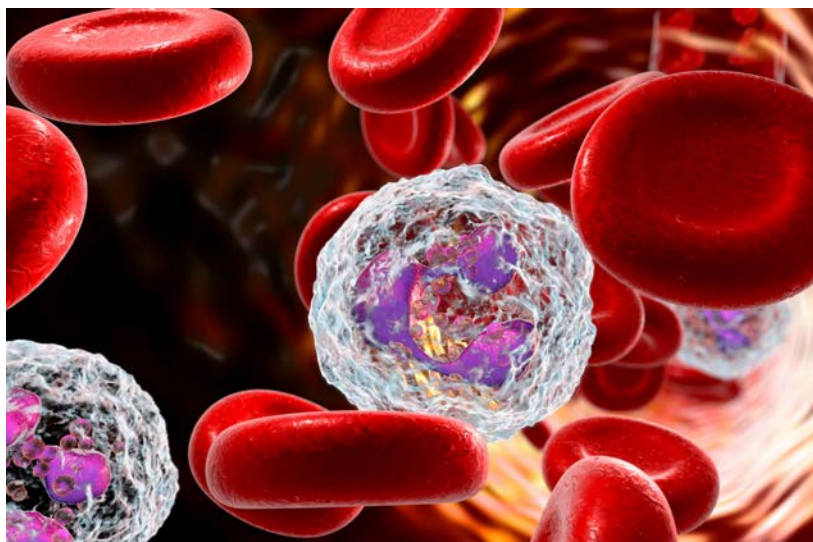
Etonnamment, un fond sonore reproduisant celui d'une bibliothèque (feutré, mais réel) n'avait en revanche pas d'influence. Si vous voulez profiter au maximum de votre créativité, vous savez désormais ce qu'il vous reste à faire.

P.S. Dans le silence, vous auriez trouvé «porte», qui donne «portefeuille», «porte-manteau» et «porte-monnaie».

E. THREADGOLD ET AL., *APPLIED COGNITIVE PSYCHOLOGY*, PRÉPUBLICATION 2019

Se coller pour mieux décoller

Les neutrophiles, des globules blancs, joueraient un rôle important dans le développement de métastases. Une découverte importante pour d'éventuels médicaments.



Les neutrophiles, une catégorie de globules blancs, participent au processus métastatique

Une des conséquences dramatiques du développement d'un cancer

est la dissémination de cellules tumorales, prologue au développement de métastases, un phénomène décrit dans le *Hors-Série* n° 99: «Cancer. L'arsenal des nouvelles thérapies». Les mécanismes en jeu sont mal connus. Aussi les résultats de Barbara Maria Szczerba, de l'université de Bâle, en Suisse, et de ses collègues sont-ils importants.

Pour qu'un cancer devienne invasif, des cellules tumorales doivent se détacher de la tumeur initiale, circuler dans le corps et notamment le sang, un environnement hostile. En étudiant des patients atteints d'un cancer du poumon à un stade avancé et des souris modèles, les biologistes ont découvert des cellules tumorales circulantes associées à des neutrophiles (via une protéine VCAM1), une catégorie de globules blancs spécialisés dans l'élimination de bactéries ou de cellules infectées.

Les neutrophiles sont plus qu'un moyen de transport. En effet, des cellules tumorales prélevées dans ces complexes et réinjectées, seules, dans des souris saines, déclenchent plus de tumeurs que des cellules tumorales qui n'ont pas été associées à des neutrophiles. Cette observation, et d'autres, montre le rôle actif des neutrophiles. Pour quelles raisons?

Les neutrophiles associés à des cellules tumorales produisent des molécules inflammatoires (les interleukines IL-1 β et IL-6) qui favorisent le pouvoir métastatique des cellules cancéreuses (elles sont dotées des récepteurs adéquats). Elles sont «dopées» et prêtes à proliférer. Une mutation particulière, celle du gène *TLE1* favoriserait l'adhésion des cellules tumorales aux neutrophiles.

L'ensemble de ces résultats offrent des pistes pour mieux repérer les cancers sujets à métastases, voire des cibles pour empêcher cette évolution.

B. SZCZERBA ET AL., *NATURE*, VOL. 566, PP. 553-557, 2019

HORS-SÉRIE N° 102 : MÉMOIRE

Un modèle pour la dynamique d'Alzheimer

Comment évoluent les structures cérébrales dans le cas de la maladie d'Alzheimer? Un modèle, élaboré grâce à plus de 4 000 IRM, répond.

La maladie d'Alzheimer, qui touche de plus en plus de monde, est de mieux en mieux comprise, le *Hors-Série n° 102* : «Les mutations de notre mémoire» s'en faisait l'écho. Par exemple, on sait précisément comment différentes zones du cerveau s'atrophient chez les malades. Cependant, les connaissances sur l'évolution de ces anomalies, et la dynamique de leur divergence par rapport à des sujets sains, manquaient. Pour combler ce manque, Pierrick Coupé, du Laboratoire bordelais de recherche en informatique, Gwenaëlle Catheline de l'École pratique des hautes études et leurs collègues espagnols ont analysé 4329 IRM de sujets sains et malades grâce à la plateforme volBrain. Cette plateforme gratuite analyse automatiquement les IRM (plus de 120 000 au monde) de manière entière.

Grâce au très grand nombre d'échantillons, les chercheurs ont créé un modèle qui reproduit à l'échelle de toute une vie l'évolution et la dynamique du cerveau. Le modèle de cerveau normal, de référence, est fondé sur 2944 sujets sains âgés de quelques mois à 94 ans. Le modèle pathologique moyen a été établi à

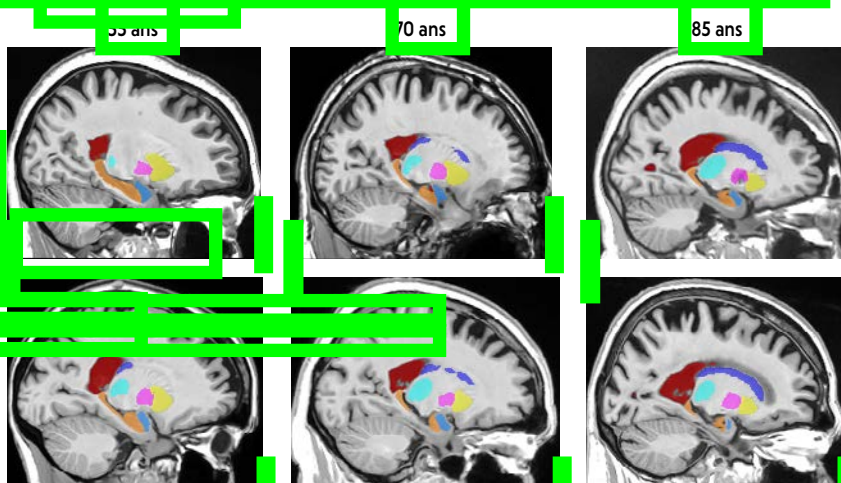
partir des IRM de 1385 sujets malades âgés de plus de 55 ans et de 1877 jeunes sujets sains. Que constate-t-on?

Dans le cas de la maladie d'Alzheimer, l'hippocampe s'atrophie de façon plus marquée que chez les sujets sains avant l'âge de 40 ans. C'est ensuite au tour de l'amygdale : sa taille diminue plus vite chez les malades que chez les sujets sains. Ces deux structures du système limbique impliquées dans la mémoire sont les deux plus touchées par la maladie d'Alzheimer. La matière blanche, la matière grise, le thalamus, les noyaux caudé et accumbens... suivent des évolutions similaires dans les deux catégories d'individus étudiés.

Qu'en est-il des ventricules latéraux (des cavités à l'intérieur du cerveau) dont la dilatation est souvent considérée comme un marqueur de la maladie d'Alzheimer? Selon les modèles obtenus, ils s'élargissent précocement chez les malades, mais de façon similaire chez les deux groupes au-delà de 60 ans. L'examen de ces structures serait donc d'un intérêt limité à des âges avancés.

PIERRE COUPÉ ET AL., SCIENTIFIC REPORTS, 9, ART. 3998, 2019

Les atrophies de l'hippocampe (en orange) et de l'amygdale (en rouge) sont plus précoces et plus prononcées chez des sujets malades (en bas) que chez des sujets sains (en haut). De même, l'élargissement des ventricules latéraux (en vert) apparaît plus tôt.



Communier en musique

La musique nous enveloppe au plus profond

Plonger, les articles du *Hors-Série n° 100* : «Good vibrations» le démontraient bien. C'est particulièrement vrai lors d'un concert où le public semble vibrer à l'unisson. Mais de quelle façon cela se traduit-il dans notre cerveau? Jens Madsen, du City College, à New York, aux États-Unis, et ses collègues ont montré que, chez 20 individus écoutant de la musique classique en même temps, les ondes cérébrales se synchronisent et montrent de fortes similarités. Une simple distraction suffisait à écarter l'un des volontaires de l'harmonie générale.

J. MADSEN ET AL., SCIENTIFIC REPORTS, PRÉPUBLICATION, 2019

Des mixotrophes partout

Dans le *Hors-Série n° 101* : «La révolution

mixotrophes, ces étonnants et méconnus organismes planctoniques mi-animal, mi-végétal. Avec cette double casquette, ils bouleversent ce que l'on pensait savoir du cycle du carbone dans les océans. Il importe donc d'en savoir un peu plus sur ces mixotrophes. Les travaux d'une équipe (Sorbonne Université, CNRS, MNHN et CEA) emmenée par Émile Faure vont dans ce sens. À partir des données recueillies par l'expédition Tara Oceans entre 2009 et 2013, ils ont identifié 33 lignées taxonomiques appartenant aux quatre groupes fonctionnels distincts de ces organismes. La mixotrophie est vraiment ubiquitaire et tous les groupes ont approximativement la même distribution. Cependant, certaines lignées sont des aires géographiques plus délimitées : c'est particulièrement le cas pour celles de l'un des groupes.

E. FAURE ET AL., THE ISME JOURNAL, PRÉPUBLICATION, 2019

1 AN

**ABONNEZ-VOUS À
POUR LA
SCIENCE**

SCIENCE

2 FORMULES AU CHOIX

FORMULE BASIQUE

FORMULE INTÉGRALE

| | | |
|--|---|---|
| Le magazine papier (12 numéros par an) | ✓ | ✓ |
| Le hors-série papier (4 numéros par an) | ✓ | ✓ |
| L'accès en ligne illimité à purlascience.fr | | ✓ |
| L'édition numérique du magazine (12 numéros par an) | | ✓ |
| L'édition numérique du hors-série (4 numéros par an) | | ✓ |
| L'accès aux archives numériques depuis 1996 | | ✓ |

VOTRE TARIF D'ABONNEMENT

79€

Au lieu de ~~114,40€~~

31 %

99€

Au lieu de ~~174,40€~~

43 %

BULLETIN D'ABONNEMENT

À renvoyer accompagné de votre règlement à :

Pour la Science – Service abonnements – 19 rue de l'Industrie – BP 90055 – 67402 Illkirch Cedex – email: pourlascience@abopress.fr

☒

OUI, je m'abonne pour 1 an à

POUR LA SCIENCE

☐

le choisis ma formule (merci de cocher)

☐

**FORMULE PAPIER
HORS SÉRIE**

12 n° du magazine papier
4 Hors-série papier

79€

114.40€

1 an

☐

**FORMULE
INTÉGRALE**

12 n° du magazine papier
4 Hors-série papier
Accès illimité aux contenus en ligne

19€

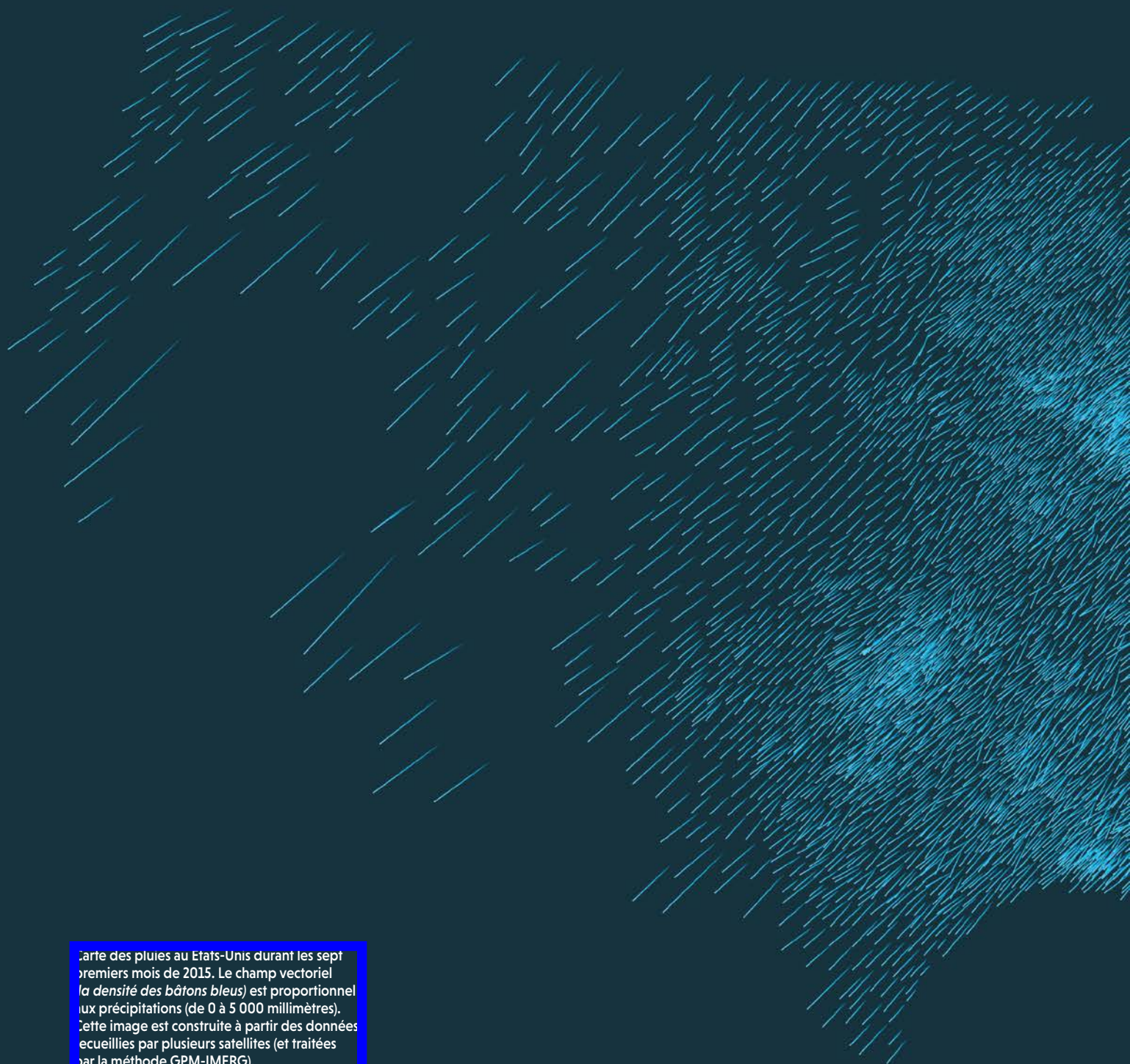
4.40€

1 an

[illegible]

réduction par rapport au prix de vente en kiosque et l'accès aux archives numériques. Durée d'abonnement : 1 an. Délai de livraison : dans le mois suivant enregistrement de votre règlement. Offre valable jusqu'au 31/12/2019 en France métropolitaine uniquement. Pour un abonnement à l'étranger, merci de consulter notre site <https://boutique.pourlascience.fr>. Photos non contractuelles.

Les informations que nous collectons dans ce bulletin d'abonnement 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, de 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@pouirlascience.fr.



Carte des pluies au Etats-Unis durant les sept premiers mois de 2015. Le champ vectoriel (la densité des bâtons bleus) est proportionnel aux précipitations (de 0 à 5 000 millimètres). Cette image est construite à partir des données recueillies par plusieurs satellites (et traitées par la méthode GPM-IMERG).

Où est passé l'Ananas express ?

Le climat se dérègle, les précipitations sont perturbées, les épisodes de sécheresse s'abattent sur l'ouest des États-Unis alors qu'à l'est, les inondations se succèdent...

Une datavisualisation rend compte de ce fort contraste, en partie imputable à l'absence du Pineapple express, une rivière atmosphérique chargée de pluies

Le réchauffement planétaire se traduit par des bouleversements notamment dans le régime climatique. Et les États-Unis de Donald Trump ne sont pas épargnés. Pour s'en convaincre, il suffit d'aller à... Milan, en Italie, où a lieu la 22^e triennale, au Palazzo dell'Arte, sur le thème de «La nature cassée». Dans le pavillon français, intitulé *De la pensée au visible*, on peut y voir notamment les travaux de David Bihanic, designer et maître de conférences à l'université Panthéon-Sorbonne, sur les pluies qui ont trappé, ou non, les États-Unis, durant les sept premiers mois de 2015 (*ci-contre*). Que peut-on voir sur cette datavisualisation animée fondée sur les données de la Nasa et de l'Agence spatiale japonaise (Jaxa) ?

Incontestablement, le pays est marqué par un fort contraste pluviométrique. Le long d'un couloir nord-sud, au centre-est (Kentucky, Illinois, Idaho, Louisiane, Texas...), les pluies ont été abondantes (les traits bleus sont nombreux et denses). De fait, les inondations, en mai 2015, ont fait des centaines de victimes, obligeant les autorités de plusieurs États à déclarer l'état d'urgence. Les dégâts se comptent en milliards de dollars.

A l'inverse, l'ouest, et plus particulièrement la Californie, a subi une grave sécheresse. En conditions normales, les États occidentaux (Californie, mais aussi Nevada, Nouveau-Mexique...) et le nord du Mexique profitent d'une «rivière atmosphérique» (un corridor où l'humidité se concentre), qui se déplace de Hawaï, dans l'océan Pacifique, jusqu'au-dessus des terres de la côte ouest de l'Amérique du Nord : cette rivière atmosphérique est le Pineapple express (l'Ananas express, du nom du fruit emblématique de Hawaï).

Mais depuis 2012, le Californie accumule un déficit en précipitations d'environ 500 millimètres, soit l'équivalent d'un an de pluie ! Un système de hautes pressions atmosphériques au-dessus de l'est de l'océan Pacifique empêcherait le Pineapple express d'arroser l'ouest des États-Unis. Un événement El Niño pourrait renverser la situation, mais à quel prix ? On ne se rend pas compte du pouvoir de l'ananas ! ■

Pavillon français de la XXII^e triennale de Milan
jusqu'au 1^{er} septembre 2019 : <https://www.triennale.org>

À LIRE



En attendant les robots
Enquête sur le travail du clic
ANTONIO A. CASILLI

SEUIL, 2019
400 PAGES, 24 EUROS

L'intelligence artificielle, de fait toujours plus performante, est soupçonnée de pouvoir un jour remplacer les humains dans de nombreuses tâches. Le travail tel que nous le connaissons est-il appelé à disparaître? À changer en tout cas, et l'on peut d'ores et déjà constater les conséquences de l'essor du numérique sur le quotidien de nombreux humains devenus des petites mains d'une intelligence pas vraiment « artificielle ». C'est ce que fait Antonio Casilli, enseignant chercheur à Télécom ParisTech, et chercheur associé à l'École des hautes études en sciences sociales, dans son dernier ouvrage. Il a enquêté sur les différents aspects peu reluisants du *digital labor* en suivant les « travailleurs du clic ». Nous, d'abord, qui utilisons gratuitement les réseaux sociaux, les données personnelles et de contenus créatifs. Ceux ensuite qui, rivés à des écrans chez eux ou dans des « fermes à clic », font vivre les plateformes les plus célèbres : par exemple, YouTube, Facebook et les autres se développent parce que des centaines de millions de personnes (aux Philippines, au Pakistan, en Roumanie...) trient des textes, annotent des vidéos retranscrivent des documents scannés... Pour ces « tâcherons » du clic, comme les appelle l'auteur de façon provocante, le travail est fastidieux, répétitif, précaire. Selon Antonio A. Casilli, l'automatisation, aujourd'hui, ce n'est pas remplacer des humains par des robots, mais par d'autres humains, moins bien payés. Un nouveau prolétariat invisible. Pensez-vous la prochaine fois qu'Amazon ou un site touristique vous font des suggestions. Les humains vont-ils remplacer les robots?

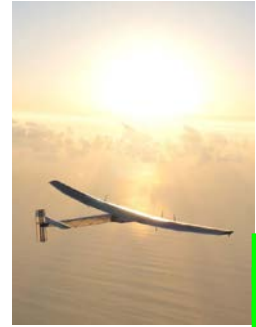


La prodigieuse histoire
du nom des éléments
PIERRE AVENAS

EDP SCIENCES, 2019
272 PAGES, 19 EUROS

Cette année, le tableau périodique des éléments chimiques de Mendeleïev a fait le thème de l'année 2019. Pierre Avenas propose d'explorer cette classification par le biais de l'étymologie et de l'origine des noms des différents éléments. Par exemple, d'où vient le nom « cobalt »? Eh bien il dérive des *kobolds*, petites divinités du folklore germanique qui étaient soupçonnées de causer des accidents dans les mines et de voler les minerais précieux, comme l'argent. Ces lutins les remplaçaient par d'autres matériaux de moins grande valeur nommés *kobolt* ou *kobalt*. Or le cobalt que l'on connaît a été découvert dans des résidus miniers... L'auteur va bien au-delà des éléments chimiques simples et conte les histoires des noms d'éléments dans tous les sens du terme, qu'ils soient de la nature (la terre, l'eau, plantes et animaux...), constitutifs du vivant (l'ADN, les protéines, les oligoéléments...) ou des matériaux (métaux, polymères...). Cet ouvrage reprend des articles de la rubrique « Clins d'œil étymologiques » qui paraissent tous les mois dans *L'Actualité Chimique* depuis 2013. Un moyen de faire de la chimie en amusant, et de rencontrer un petit Nicolas, un garçon vraiment nickel...

À VISITER



Sur les traces
de *Solar Impulse*

L'Exposition Futuroscope à Poitiers, « Habitude de l'avenir », a emboité le pas de l'astronaute Thomas Pesquet en 2018, le parc dédié en 2019 deux manifestations à l'avion solaire *Solar Impulse*. D'abord, le documentaire *Planet Power*, de Pascal Vuong et Ronan Chapalain, nous entraîne dans les pas des Suisses Bertrand Piccard et André Borschberg, qui ont conçu et piloté à tour de rôle l'engin autour du monde. Élu meilleur documentaire 3D aux *Lumières Awards*, à Los Angeles, en janvier 2019, le film invite également à découvrir les grands inventeurs qui ont fait l'histoire de l'électricité, de la première étincelle créée par la main de l'homme aux plus grandes centrales. Le message est clair: le Soleil peut nous aider à sauvegarder notre planète et par là même rendre notre avenir meilleur. Ensuite, l'exposition *L'Oiseau solaire* et *L'Oiseau des mers* donne à voir cinquante-six photographies grand format présentées en plein air. Par ces images, Francis Demange raconte lui aussi l'odyssée de *Solar Impulse*, et il la rapproche de celle de l'hydroptère, le trimaran d'Alain Thébault qui « vole » au-dessus des flots. Deux aventures humaines et scientifiques.

Le site de *Planet Power*:
<http://bit.ly/PP-Solar>
Le site du Futuroscope:
<https://www.futuroscope.com/>

AVOIR

La Lune, en gros plan

Andrew McCarthy, installé à Half Moon Bay, en Californie, l'informaticien, est aussi astronome amateur. À partir d'un télescope Orion SkyQuest XT10, de deux appareils photos numériques et de quelques logiciels dédiés, comme Photoshop, il a rassemblé 10 000 clichés de la Lune en une seule image. Avec ses 81 mégapixels, elle permet d'observer tous les plus fins détails de notre satellite. N'espérez tout de même pas voir *Chang'e-4*, l'atterrisseur chinois qui, de toute façon, n'est posé sur la face cachée. Le photographe propose beaucoup d'autres clichés du même acabit sur son site: <http://bit.ly/Redd-AJMC>

ILLUSTRATION: REDD/AMC

À ÉCOUTER

Vive les ARN !

Connaissez-vous les ARN ? Jusqu'à récemment, on les considérait comme de simples intermédiaires entre la majesté l'ADN et les protéines, l'ARN a été pendant des décennies dédaigné. La situation a changé depuis que l'on a découvert les multiples rôles que ces molécules ont dans les cellules. Les biologistes s'intéressent de près à des brins d'ARN particuliers, les ARN interférents, qui peuvent inhiber, temporairement, certains gènes. Annick Harel-Bellan (CNRS) et Florence Cabon (Inserm), invitées de Nicolas Martin, sur France Culture, dans son émission *La Méthode scientifique* réhabilitent ces molécules. Avec raison, car leurs applications thérapeutiques sont nombreuses contre le cancer, les virus...

ILLUSTRATION: S. B. / GETTY IMAGES



PHOTO: GETTY IMAGES

À VISITER

Le médusarium

Approcher au plus près plusieurs dizaines d'espèces de méduses, sans vous faire piquer. De quoi vous réconcilier avec ces animaux extraordinaires !

Les méduses hantent les mers depuis des centaines de millions d'années. Elles sont parmi les premiers organismes pluricellulaires qui ont peuplé notre planète. Elles devraient fasciner le plus grand nombre, et pourtant, leur réputation n'est pas bonne. De fait, elles sont synonymes de piqûres, de pullulations, de gélification des mers... Cette image négative changera après une visite au médusarium de l'aquarium de Paris, dans les jardins de Trocadéro.

Cet établissement présente depuis peu 24 bassins, où 45 espèces (de quelques millimètres à 50 centimètres) évoluent, par roulement, révélant une diversité de formes et de couleurs étonnante. C'est une des plus importantes collections de méduses au monde, qui s'est constituée grâce aux nombreux échanges avec l'aquarium de Kamo, à Tsuruoka, dans le nord du Japon. L'expertise nippone ne s'arrête pas là. Pour concevoir le « bar à méduses », où les visiteurs observent d'en haut des méduses évoluant dans quatre bassins formant un cercle, les équipes de l'aquarium de Paris sont allées jusqu'à Otsuki, sur les pentes du mont Fuji, pour travailler avec un artisan japonais, inventeur du système.

Comment entretenir de telles populations ? En maîtrisant les cycles de reproduction. Chaque espèce est placée dans une eau à la composition en nutriments et en sels minéraux adaptée aux stades de croissance. Pour chaque bassin de présentation dont les paramètres de salinité, de température, de courant... sont rigoureusement contrôlés, on compte cinq bassins installés en laboratoire, dont une partie est visible par le public.

Le ballet offert est hypnotique, et l'on se laisse emporter par les pulsations des ombrelles et les ondulations des filaments. L'intérêt des méduses va bien au-delà. L'exposition montre également comment ces animaux sont les sentinelles du climat et sensibilise le public aux grands défis qui affectent les océans. Le réchauffement, la pollution, la surpêche favorisent la prolifération des méduses. « Les eaux de la mer Noire et de la Baltique sont d'ores et déjà devenues des soupes de méduses », constate Jacqueline Goy, spécialiste des méduses. Si l'on ne fait rien – et le premier pas est une prise de conscience – nous pourrions observer à loisir les méduses engorger le littoral et nos plages préférées. Nous n'aurons rien d'autre à faire, car la baignade sera interdite. Alors, mieux vaut les voir dans des bassins !

Le médusarium de l'aquarium de Paris: 5, avenue Albert-de-Mun, 75116 Paris. <http://www.cineaquarium.com/index.php/fr/medusarium>





L'oryx, bon sang mais c'est bien sûr !

Vivre dans les milieux désertiques n'est pas une sinécure et nécessite de bonnes adaptations. La physiologie économe en eau du dromadaire *Camelus dromedarius* est un exemple bien connu. Mais ce n'est pas le seul. Ursula Windberger, de l'université de Vienne, en Autriche, et ses collègues en ont exploré une autre, chez le dromadaire, mais aussi chez l'oryx algazelle *Oryx capensis*, deux animaux qu'ils ont comparés à des moutons sud-africains et des vaches de race africaine Nguni. Leur attention s'est portée sur le sang de ces animaux et notamment sur les propriétés des globules rouges.

Les oryx se distinguent des autres espèces animales étudiées par des globules rouges qui s'aggrègent et se déforment peu. Les biologistes y voient le signe de membranes cellulaires fortifiées qui résisteraient alors mieux aux variations osmotiques du plasma, inévitables durant les cycles d'hydratation et de déshydratation. Ainsi équipé, l'oryx peut faire face aux rigueurs du désert, garder son... sang-froid. ■

U. Windberger et al., *Clin. Hemorheol. Microcirc.*, vol. 69(4), pp. 533-543, 2018

Cette photographie est extraite du blog *Best of Bestioles* : <http://bit.ly/PLS-BOI>

Du petit carré à l'Univers en entier

Victor Vasarely a cherché à traduire la totalité de l'Univers, et des lois qui y règnent, notamment grâce à une approche combinatoire de la peinture.

C

ouvertures de *Vogue* à *Scientific American* en passant par la collection *Tel* de Gallimard, pochette du disque *Space Oddity* de David Bowie, logo de Renault... rarement œuvre d'art aura autant irrigué la vie quotidienne. C'est celle du peintre d'origine hongroise Victor Vasarely (1906-1997), «père de l'art optique», un art qui exploite les failles de la vision à travers les jeux optiques. Il fait l'objet d'une rétrospective au centre Pompidou, à Paris, qui réunit plus de trois cents œuvres. C'est l'occasion d'explorer les facettes scientifiques de sa production à travers une œuvre emblématique, *Vega 222*, réalisée à la fin des années 1960 (voir ci-contre).

D'abord, les ronds dans des carrés renvoient à l'approche combinatoire, qu'a adoptée Vasarely pour de nombreuses créations. Inspiré par les travaux du théoricien des couleurs Wilhelm Ostwald, par ailleurs Prix Nobel de chimie en 1909, il a élaboré un alphabet pictural en guise de palette, un réservoir de formes-couleurs (des unités plastiques) : des chiffres codent les couleurs pures, d'autres les gammes nuancées et d'autres encore, couplés à des lettres pour les formes (ronds, carrés...). Il peut alors jouer avec les permutations et ce qui s'apparente à des algorithmes pour ses compositions. Les études préparatoires ressemblent à des matrices où chaque

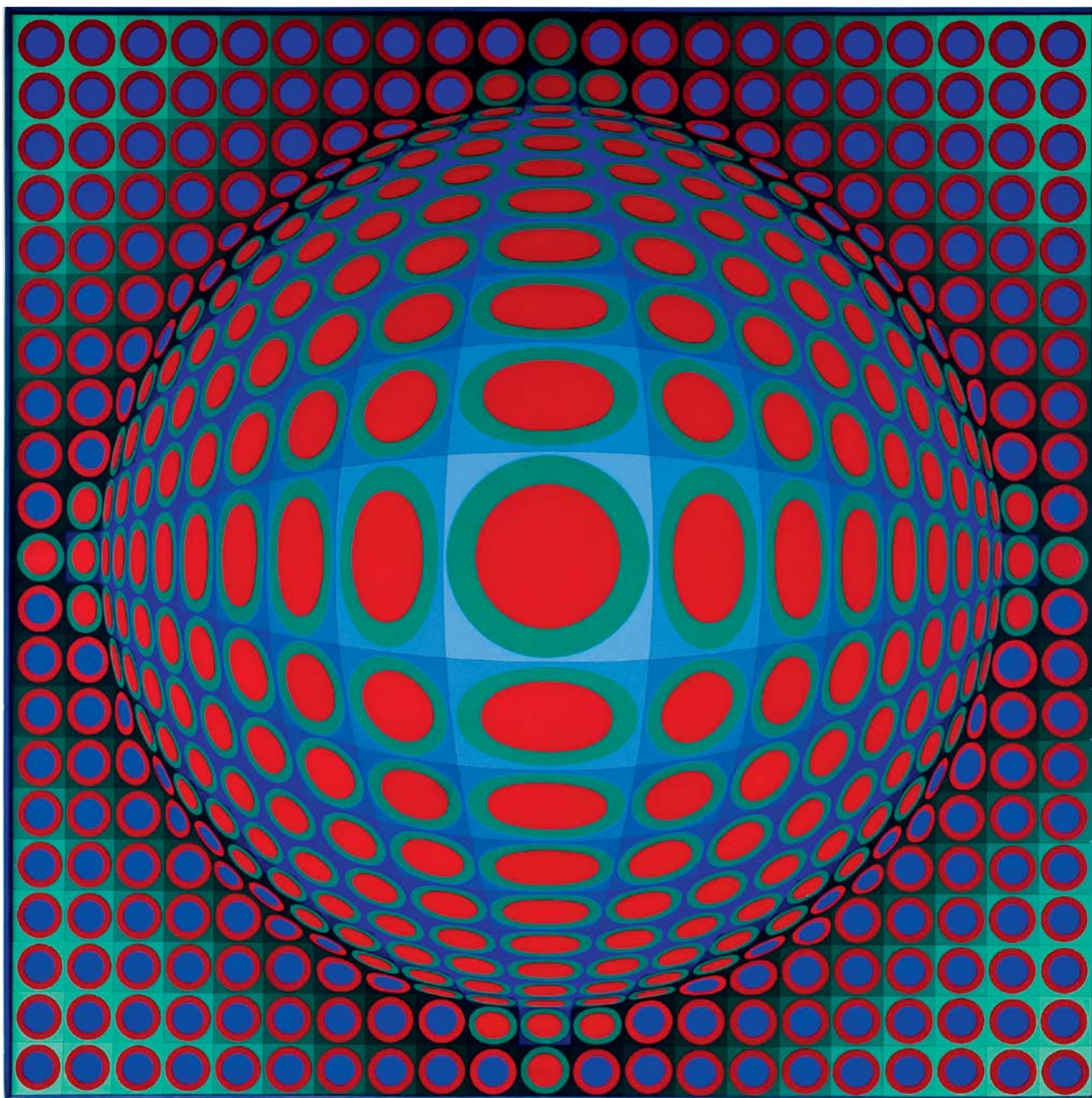
case contient des chiffres et des lettres indiquant, par exemple, un rond bleu dans un carré vert.

L'autre aspect scientifique qui transparaît dans la dilation au centre de *Vega 222* est l'ordre physique voire cosmologique. Vega est en effet l'un des noms de l'étoile la plus brillante de la constellation de la Lyre.

Grand lecteur de Niels Bohr, Werner Heisenberg... Vasarely voyait dans la science le seul langage commun véritable de l'humanité. À la suite des travaux du physicien Louis de Broglie, il distinguait dans son œuvre deux pôles : les ondes et les corpuscules. Et l'on peut percevoir dans *Vega 222* une déformation de l'espace-temps par de la matière-énergie sur une trame corpusculaire. Selon Vasarely, les unités plastiques sont comparables aux atomes d'hydrogène, l'élément fondamental et le plus abondant de l'Univers.

De son propre aveu, l'artiste souhaitait donner corps aux «mondes qui, jusqu'ici, ont échappé à l'investigation des sens : monde de la biochimie, de l'onde, des champs, de la relativité.» Visiter l'exposition, c'est donc explorer l'Univers! ■

«Vasarely, le partage des formes», jusqu'au 6 mai 2019, au centre Pompidou, à Paris.



© 2019 L'ÉDITIONS L'ÉCLAIR

Vega 222, ou comment
espace-temps est déformé
par la matière-énergie

PROCHAIN HORS-SÉRIE
en kiosque le 10 juillet 2019



Les océans

TERRE PROMISE DE L'HUMANITÉ

Les mers et les océans couvrent plus de 70 % de la planète et l'on en sait si peu. Quelle biodiversité abritent-ils, notamment dans les zones extrêmes ? Quelles ressources ont-ils encore à offrir ? Comment influent-ils sur le climat et atténuent-ils le réchauffement ? Les océans sont un nouveau continent à explorer, et à protéger. Embarkement dans le prochain numéro

Découvrez notre hors-série numérique

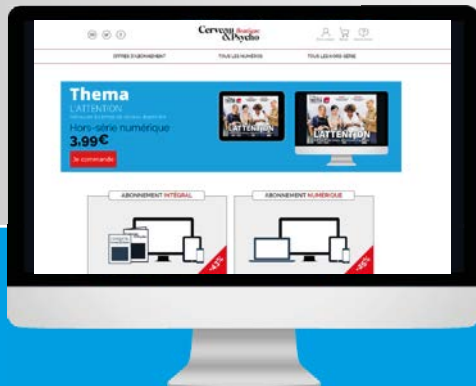
L'ATTENTION

**RETROUVEZ DU TEMPS
DE CERVEAU DISPONIBLE**

3,99 €



80 pages de lecture
pour tout savoir sur le sujet

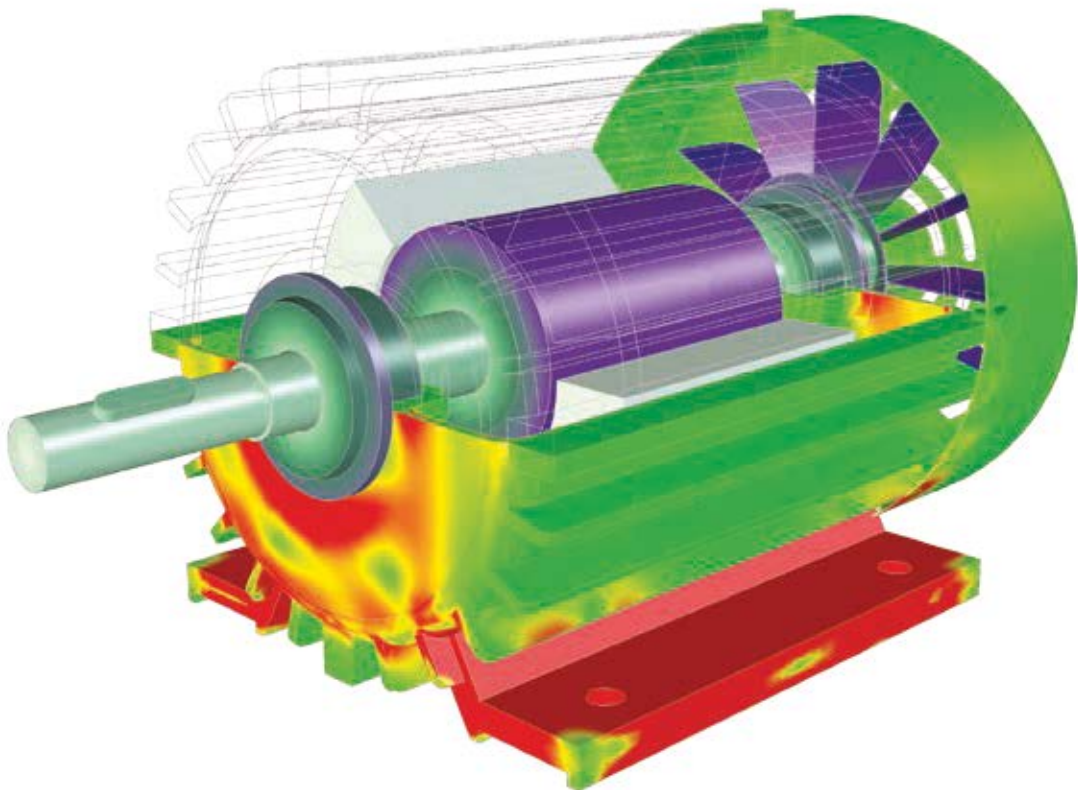


Les *Thema* sont une nouvelle collection de hors-séries numériques. Chaque *Thema* contient une sélection des meilleurs articles publiés dans *Cerveau & Psycho* sur une thématique.

- 1 Commandez le *Thema* sur **boutique.cerveauetpsycho.fr**
- 2 Rendez-vous sur votre compte client, dans la rubrique **Ma bibliothèque numérique**
- 3 **Téléchargez le PDF** directement depuis votre tablette, téléphone ou ordinateur
- 4 Bonne lecture !

Rendez-vous sur
boutique.cerveauetpsycho.fr

Inventé au 19^{ième} siècle. Optimisé pour aujourd'hui.



Distribution des contraintes de von Mises dans le carter d'un moteur à induction avec prise en compte des effets électromécaniques.

Au 19^{ème} siècle, deux scientifiques ont inventé séparément le moteur à induction AC. Aujourd'hui, c'est un composant commun en robotique. Comment y sommes nous arrivé, et comment les ingénieurs d'aujourd'hui peuvent-ils continuer d'améliorer ces moteurs?

Le logiciel COMSOL Multiphysics® est utilisé pour simuler des produits, des systèmes et des procédés dans tous les domaines de l'ingénierie, de la fabrication et de la recherche. Découvrez comment l'appliquer pour vos designs.

comsol.blog/induction-motor