© Sasha Maslov/Quanta magazine

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

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

PAVÉS 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 balisés, 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 ».

À Princeton, Akshay Venkatesh et Yiannis Sakellaridis ont travaillé sur deux problématiques 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 »

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.

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 XVIIe 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 leurs 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 (médaille Fields en 2002), Christophe Breuil, Ngô Bao Châu (médaille 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 Mashaal

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, tant par 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 devant le bâtiment qui porte désormais son nom, à l'université d'Oxford.

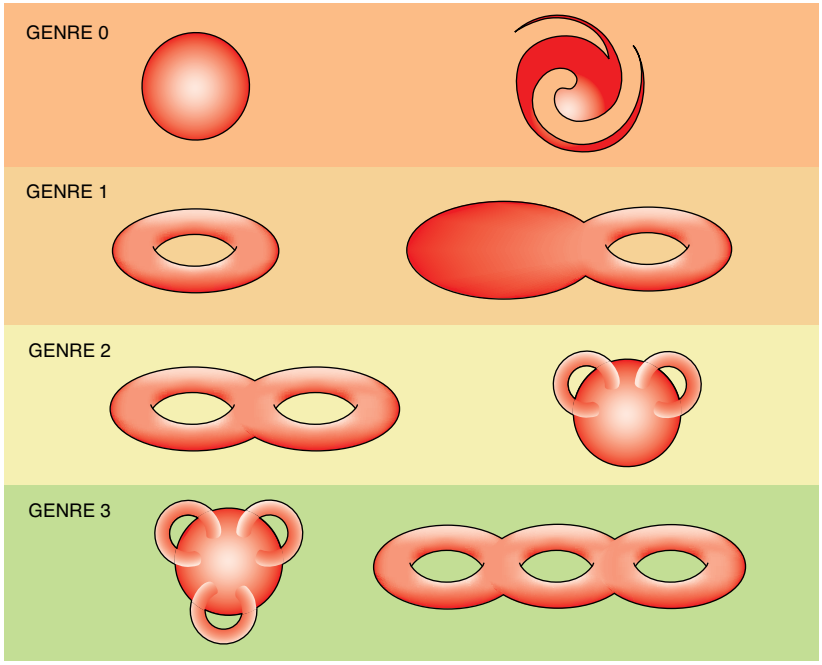
***Star Trek, Doctor Who, Les Simpsons*... ces trois séries ont en commun d'avoir mis à l'honneur lors d'au moins un épisode l'un des plus célèbres théorèmes mathématiques.** Quel résultat a-t-il mérité une telle récupération populaire? Le dernier théorème de Fermat, selon lequel $x^n+y^n=z^n$ n'admet 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 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 XIXe 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.



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 sont 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.

UNE GOUTTE DANS L'OCÉAN

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 les 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, Évariste Galois (1811-1832), soumet à l'Académie des sciences un manuscrit sur la résolution 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 $V(x_1, x_2)=x_1^2+x_2^2$, 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 $x_1x_2=q$.

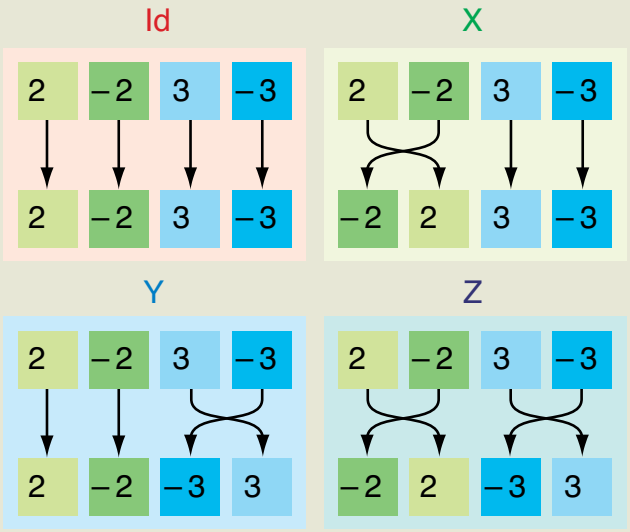
Galois étend ce résultat et démontre que toute fonction des solutions d'une équation, invariable par certaines permutations de ces solutions, mais pas toutes, s'exprime rationnellement en fonction des coefficients de l'équation.

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 sa 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.

Norbert Verdier, IUT de Cachan

Évariste Galois, mathématicien malheureux (1811-1832).



o	Id	X	Y	Z
Id	Id	X	Y	Z
X	X	Id	Z	Y
Y	Y	Z	Id	X
Z	Z	Y	X	Id

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 {Id, X} est aussi un groupe : c'est un sous-groupe du groupe {Id, X, Y, Z}.

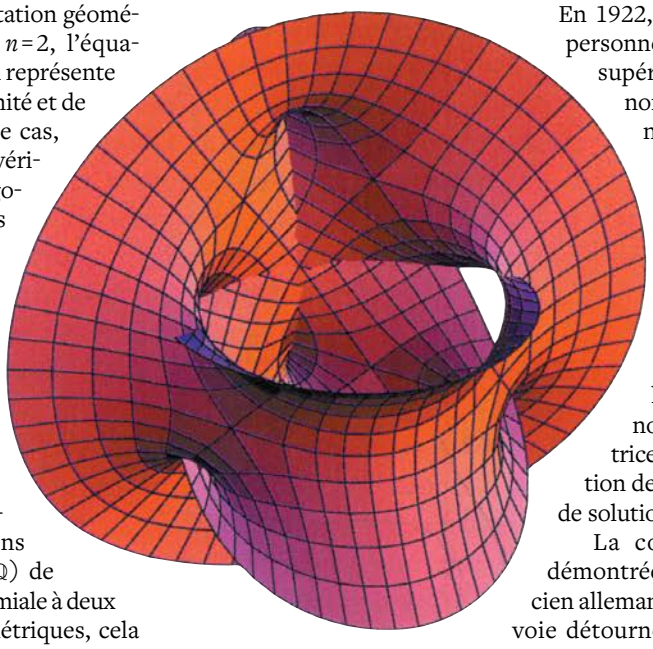
LA NOTION MODERNE DE GROUPE

La structure de groupe est centrale dans les branches les plus variées des mathématiques (groupes de Lie, géométrie algébrique, topologie algébrique et différentielle, théorie des nombres…). Un groupe est un ensemble d'éléments fermé pour une loi de composition $\times$ associative, c'est-à-dire que $(x \times y) \times z = x \times (y \times z)$ pour tous x, y, z de l'ensemble. En outre 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 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.



Surface engendrée par l'équation de Fermat $x^3+y^3=1$ quand x et y sont des variables complexes.

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.

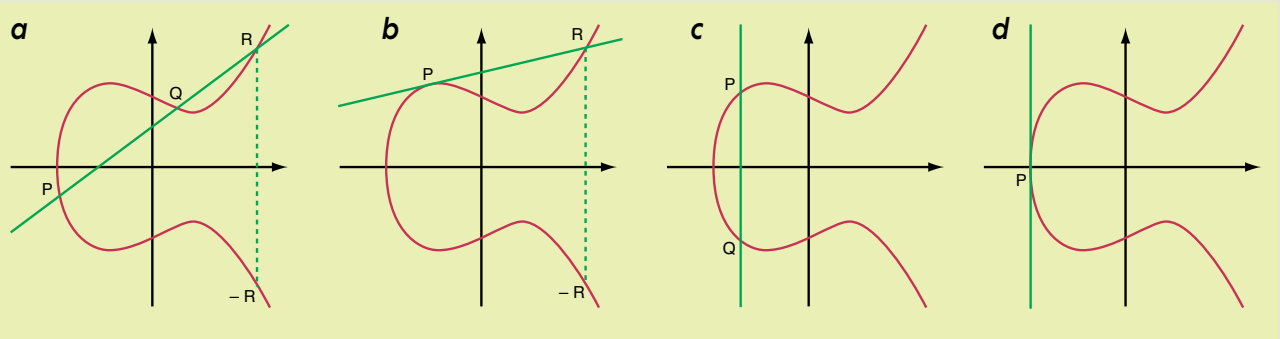
En 1968, A. N. Parshin démontra que la conjecture de Chafarevich impliquait celle de Mordell. Et en 1983, Faltings s'attaqua avec succès à la conjecture de Chafarevich, prouvant comme corollaire celle de Mordell ! La

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 genre 1 dont l'équation se ramène à : $y^2+axy+by=x^3+cx^2+dx+e$, où 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 sont réels (rationnels). 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 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 dit de n-torsion.

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*).

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*).

DÉTOUR 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 les 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 bonté intrinsèque des mathématiques. Quel lien existe-t-il entre cette conjecture et le dernier théorème de Fermat ?

En 1985, l'Allemand Gerhard Frey propose d'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 ÉPOPÉE

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 XIXe 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 elliptics 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 Hecker algebras » (« Les propriétés théoriques annulaires de certaines algèbres de Hecker »), 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

N. 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, *Mnémosyne* n° 7, pp. 34-61, 1994.

Des nombres et des énigmes

Les dernières énigmes préparées par Ana Retchman et Sébastien Kernivinen.

Solutions page 106.


Ana Retchman


Sébastien Kernivinen

ÉNIGME 10

Trouver le plus petit nombre divisible par 999 qui ne contienne pas de 9 parmi ses chiffres.

ÉNIGME 11

Calculer la somme de tous les nombres palindromes à 3 chiffres.

ÉNIGME 12

Si p et p^2+8 sont des nombres premiers, quelle est la valeur de p^3+4 ?

ÉNIGME 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 ?

ÉNIGME 14

Écrire le nombre 2 019 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. Écrivons 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: 32916

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 $18=2\times3\times3$.

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: $4z+4w=16z+w$, $3w=12z$, $w=4z$ 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, $a = 999\times112=111888$ ne contient pas de 9.

Réponse 11: 49500

Solution. À 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: $(100a+10b+a)+(100(10-a)+10(10-b)+(10-a))$, soit $10(100+10+1)=1110$.
Il y a $9\times9=81$ nombres palindromes avec $a \neq 0$ et $b \neq 0$. La somme de ces 81 nombres vaut donc $(81\times1110)/2=44955$, 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...+101 = 4545.
Donc la somme de tous les nombres palindromes à 3 chiffres est 44955+4545=49500.

Réponse 12: 31

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 $p=3n\pm1$ et avec cette écriture on calcule: $p^2+8=(3n\pm1)^2+8=9n^2\pm6n+9$:
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.
À ce moment, la multiplication par 2 montre que b commence par $105263157894736842\times2=210526315789473684$.
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 ÉNIGMES

A. Rechtman Bulajich, *Calendrier mathématique*, Presses universitaires de Grenoble, 2019.

PUG

À LIRE EN PLUS

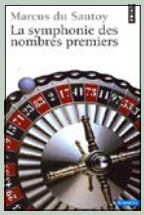
Le Fascinant Nombre π

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'apprivoiser. 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.



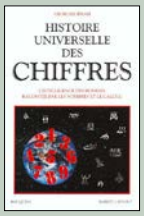
La Symphonie des nombres premiers

MARCUS DU SAUTOY

SEUIL, POINTS SCIENCE, 2007

(**496 PAGES, 11,20 EUROS**)

Depuis Pythagore et Euclide, une petite musique insistante empêche les mathématiciens de dormir : celle des 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 on 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 du Graal pour comprendre d'où venaient 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.

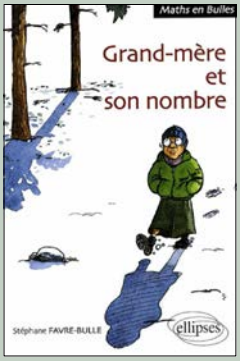
Le Dernier Théorème de Fermat

SIMON SINGH

PLURIEL, 2011

(**312 PAGES, 8,10 EUROS**)

Pierre Fermat, au XVII^e siècle, s'était contenté d'indiquer dans une marge : «$x^n+y^n=z^n$ impossible si $n>2$. J'ai trouvé une 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.



BANDE DESSINÉE

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 et écrire ces nombres d'une manière aussi simple ! Et 2/3 ou −45 ou 3,18 ? Et π ? Et √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