

> 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 $2^{13} > 4^5$, 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: $\log(3)/\log(2) < p/q \leq \log(3 + 2 \times 10^{-19})/\log(2)$.

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: $I =]1,58496250072115618145, 1,58496250072115618155]$.

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

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

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

DURÉE LIBRE

43 %
de réduction *

Partie réservée au service abonnement. Ne rien inscrire.

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

les 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 ELIAHOU
Professeur à l'université
du Littoral Côte d'Opale,
à 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

ers 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. Giorello, page 98).

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 p) 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 des 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 donné permet parfois des progrès inattendus dans de 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.

À 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 $(a, b, a + b)$.

**À partir du
sixième nombre de
Schur, on en sait si peu
qu'on ne dispose même
pas de conjectures
quant à leurs valeurs
possibles !**

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

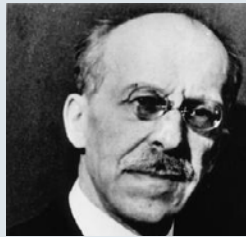
Avec une bonne dose de patience, on peut vérifier que pour ce coloriage, il n'existe aucun triplet $(a, b, a+b)$ monochromatique. Voici quelques triplets : $(1,3,4)$, $(1,5,6)$, $(3,5,8)$, $(2,7,9)$, $(4,6,10)$, $(9,10,19)$... L'inégalité $S(4) \geq 44$ est donc vérifiée.

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 ISSAÏ SCHUR ?

Issaï 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 $S(n)$: algorithme, complément, décomposition, inégalité, lemme, 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'anti-sémitisme 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.

© Konrad Jacobs, Erlangen

- 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...

44, 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

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 :

n	$(3^n - 1)/2$	$3 \times n! - 1$
2	4	5
3	13	17
4	40	71
5	121	359
6	364	2159
7	1093	15119
8	3280	120959

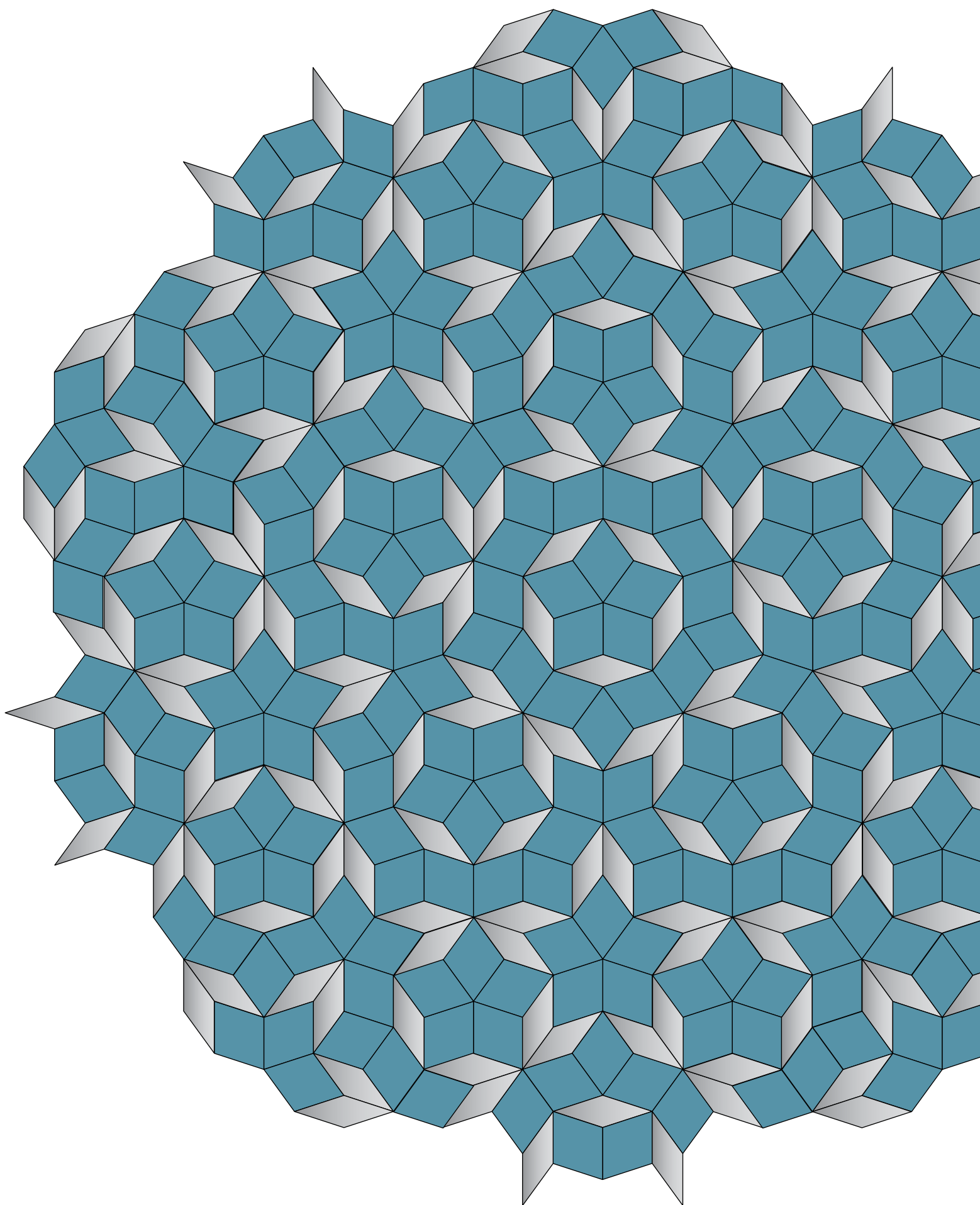
Par conséquent, l'incertitude concernant la valeur précise de $S(n)$ dans l'intervalle ainsi délimité croît elle aussi très vite en fonction de n , du moins en l'état actuel des connaissances.

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 l'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. ■

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

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



L'ESSENTIEL

- Le nombre d'or, ou φ , surgit souvent là où 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», ces nouveaux matériaux découverts récemment.

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

L'AUTEUR



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

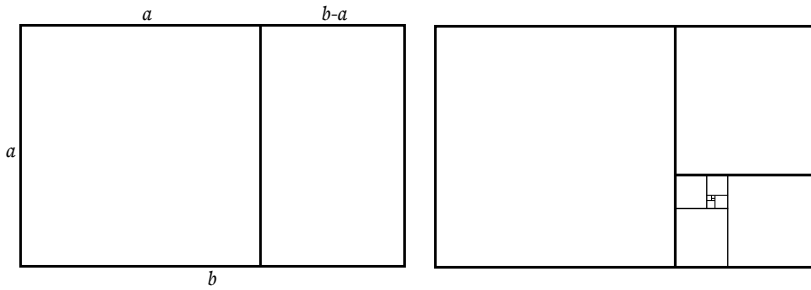
e nombre d'or, désigné par la lettre grecque φ (prononcée *fi*), fascine depuis plus de deux millénaires. Identifié dès l'Antiquité, par exemple par les pythagoriciens, on le retrouve à toutes les époques: dans les écrits du mathématicien perse Al-Khawarizmi au VIII^e siècle, dans *La divine proportion*,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

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 des 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.

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.

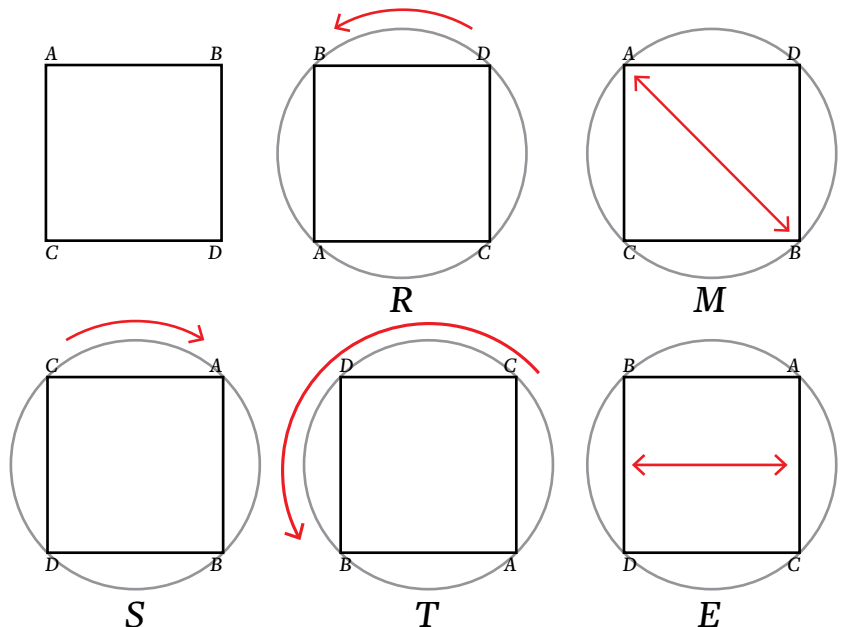
On peut donc fabriquer des symétries à partir de symétries déjà déterminées, simplement en prenant des inverses ou des composées de celles-ci, indépendamment de la nature géométrique du problème. On peut recommencer tant qu'on obtient de nouvelles symétries. Dans notre exemple, en partant de S et M ,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

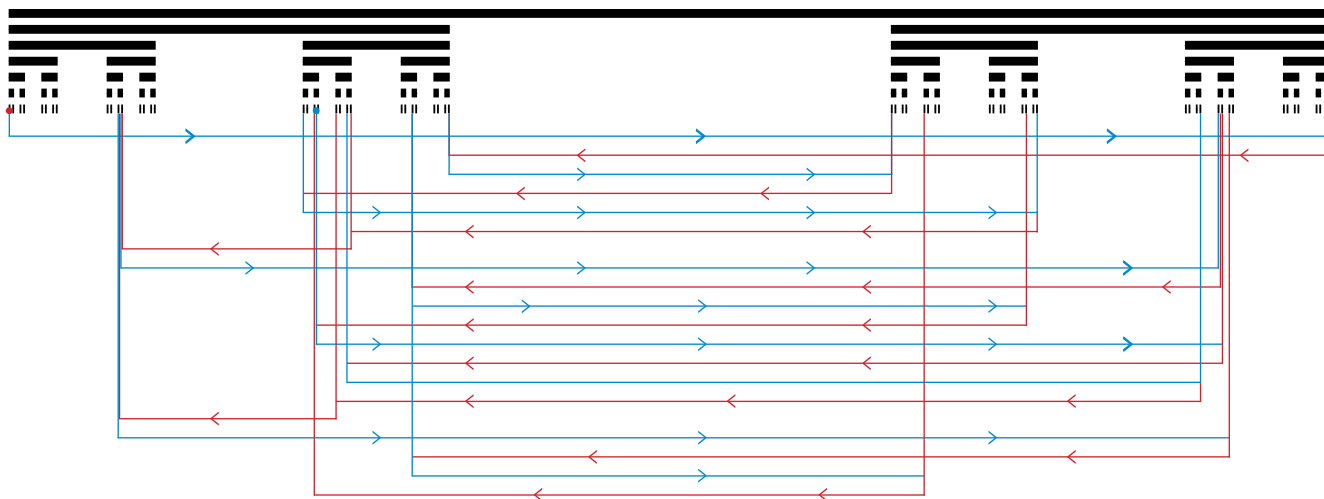
Cet ensemble est le groupe du carré, au sens mathématique du terme, engendré par S et M . Un groupe est un ensemble de transformations tel que l'inverse ou la composée de n'importe lequel de ses éléments est encore un élément de celui-ci.

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

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





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 les 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 : $\bar{S}$, $\bar{T}$, ST , TS , $\bar{S}\bar{T}$, $\bar{T}\bar{S}$, $S\bar{S}$, $S\bar{T}$, $T\bar{S}$, $T\bar{T}$, 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).

À 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 . À 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 $\bar{S}$ (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 par un de longueur 1. Si on part du segment $[0, \varphi]$, on obtient successivement par application répétée de T la figure ci-dessous.

À 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 pentagone régulier, le rapport de la longueur des diagonales sur la longueur des côtés est égal à φ . Cela se traduit par l'égalité $2 \cos(\pi/5) = \varphi$. De l'équation précédente, on peut également montrer que :

$$\varphi = 1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \dots}}}}}$$

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

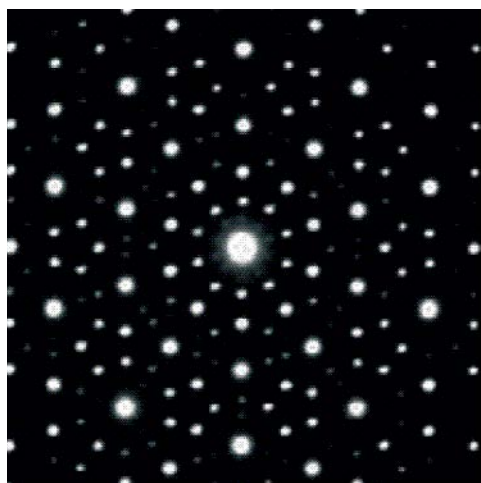
retrouve enfin dans le monde végétal. Les écailles des pommes de pin, les fleurons des tournesols et des marguerites, les feuilles le long d'une tige s'agencent en deux séries de spirales. Lorsqu'on les compte, on trouve deux nombres consécutifs de la suite de Fibonacci, et donc une approximation du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



© Clifford Pugliese/Shutterstock.com

- 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.



© P. Schechtman

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

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, pp. 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



ÉNIGME 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 !

ÉNIGME 2

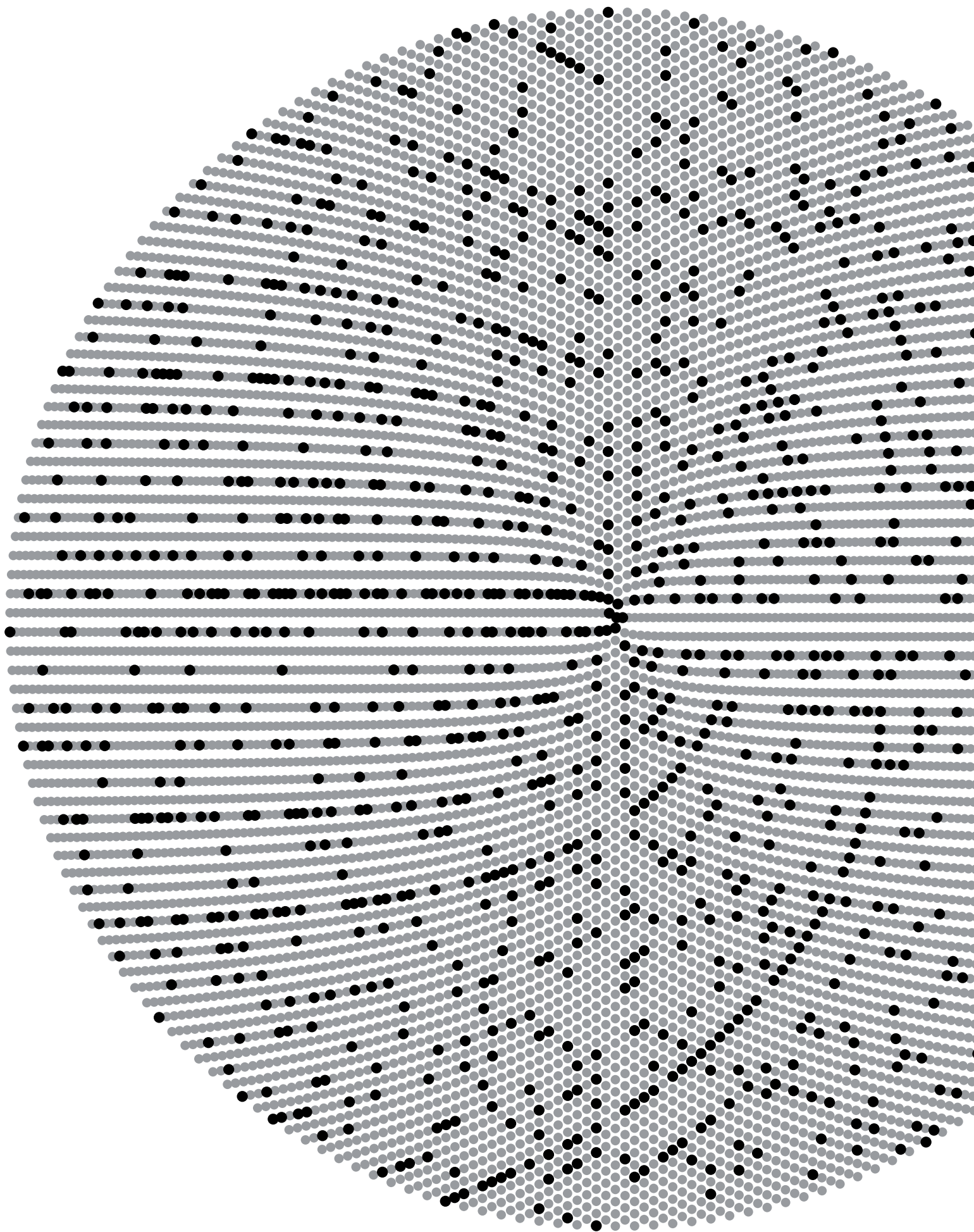
Combien y a-t-il de « randonnées » partant du nombre entier 1 et arrivant au nombre entier 10 en ajoutant successivement ou bien 1 ou bien 2 à chaque pas ?

ÉNIGME 3

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

ÉNIGME 4

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





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

L'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 les méthodes de chiffrement

pleinement homomorphe que les travaux de Craig Gentry ont rendues 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.

L'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

i 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 MÉTHODE TRÈS 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 $\mathbb{O}$) chargé de les sauvegarder. Pour connaître par exemple la moyenne de vos données ou de certaines d'entre elles, vous demandez à $\mathbb{O}$ de calculer la moyenne sur les données dont il dispose et ➤