PLS

Que reprochez-vous précisément à ce genre d'écrits ?

➜ **YVES GINGRAS :** Ces livres, qui se veulent être de la vulgarisation scientifique, sont destinés au grand public et jouissent de l'aura de leurs auteurs, dont le statut et la réputation scientifiques sont acquis. Les lecteurs leur accordent donc une forte crédibilité. Or ces auteurs outrepassent leur compétence scientifique en mettant en avant des conceptions religieuses ou mystiques qui sont étrangères à la science. Ils profitent de leur image de scientifiques pour diffuser leurs opinions personnelles. Leurs livres se veulent une présentation des découvertes de la science moderne, mais leurs titres et une partie de leur contenu suggèrent, en général de façon subtile et indirecte, des liens entre la science de pointe et la spiritualité, la solution des mystères de la vie et des origines de l'Univers. Ils jouent sur l'ambiguïté, sur la fibre du mystère, comme le fait *X-Files*, série télévisée où l'on navigue constamment entre la science et les croyances paranormales. C'est également flagrant avec les spéculations, invérifiables par définition, sur les « univers parallèles ».

PLS

De telles incursions hors de la science pourraient n'être qu'une simple stratégie commerciale de la part de l'auteur ou de son éditeur, pour mieux appâter les lecteurs…

➜ **YVES GINGRAS :** Quand seul le titre joue sur la corde mystique et pas le contenu, on peut croire que oui. Mais cela confirme la tendance à vouloir marier science et religion, ou du moins science et spiritualité, ce qui crée une confusion dangereuse. Et même dans cette situation, l'auteur a une responsabilité quant au choix du titre et ne peut se défausser sur son éditeur. Utiliser comme titre *The God Particle* comme l'a fait L. Lederman – ou comme l'ont fait de nombreux journaux et magazines à propos de la récente découverte au CERN du boson de Higgs – ne fait qu'entretenir la confusion entre ce qui relève de la science et ce qui relève de la spiritualité. Cela étant, l'usage stratégique des soi-disant liens entre science et religion ne se limite pas à faire mousser les ventes. Ainsi, L. Lederman avait plutôt un but politique en publiant en 1993 son ouvrage. Les physiciens américains cherchaient à l'époque des appuis publics pour convaincre leurs autorités de ne pas mettre fin à la construction du SSC, un collisionneur de particules gigantesque et coûteux qui devait permettre de découvrir le boson de Higgs, particule clef prédite par les théoriciens.

PLS

Les scientifiques qui jouent sur le registre mystique, mais qui n'ont pas de visée stratégique, sont-ils malgré tout suspects ?

➜ **YVES GINGRAS :** Chacun est libre de croire en ce qu'il veut, mais promouvoir ses convictions spirituelles en s'appuyant sur la science est, au mieux, une preuve de grande naïveté épistémologique de la part de personnalités censées être d'un haut niveau scientifique.

Il faut aussi remarquer que la vague de publication d'ouvrages de vulgarisation scientifique faisant l'amalgame entre science et religion ou mysticisme a été fortement encouragée par les activités de la fondation américaine *Templeton* créée en 1987. Ayant pour mission de promouvoir les liens entre science, théologie, spiritualité et religion, elle décerne notamment un prix annuel de plus de un million de dollars à une personnalité ayant fait « une contribution unique à une meilleure compréhension de Dieu et des réalités spirituelles ».

Or plusieurs scientifiques, qui ne sont nullement philosophes ou théologiens, ont obtenu ce prix. Le premier fut d'ailleurs P. Davies, physicien reconnu et auteur prolifique de livres où abondent les mots *Dieu*, *science*, *esprit*, *miracle*, etc. La stratégie de la fondation de donner l'impression que science et spiritualité sont compatibles est tellement évidente qu'il était possible (je l'ai fait !) de prédire que l'astrophysicien britannique Martin Rees l'obtiendrait, ce qui fut le cas en 2011. M. Rees fait partie de ceux qui ont surinterprété le soi-disant « principe anthropique » selon lequel les constantes de la nature sont précisément calibrées pour permettre l'apparition de l'homme. Or ce principe n'est qu'une tautologie, qui consiste à dire que si le monde avait été différent, nous ne serions pas là ! Au lieu d'expliquer qu'il n'y a là aucun mystère, on laisse planer l'idée qu'un créateur doit avoir fixé ces valeurs pour nous faire ensuite apparaître. Cela n'a rien de scientifique, mais c'est très attrayant pour les esprits qui cherchent à conforter leurs croyances religieuses ou spirituelles en se servant de la science.

PLS

Comment réagissent les autres scientifiques face à cette dérive ?

➜ **YVES GINGRAS :** Ils sont plutôt indulgents envers leurs confrères, comme si une forme de corporatisme leur soufflait que tout est bon pour promouvoir les sciences. J'ai été stupéfait de lire un compte rendu du livre *The Physics of Immortality* dans la revue hebdomadaire *Science,* qui était somme toute positif et ne disait mot de l'absurdité de prétendre démontrer l'immortalité de l'âme en invoquant des équations de la théorie quantique des champs – des équations présentes dans le livre simplement pour impressionner les lecteurs. Et je n'ai pas vu beaucoup de physiciens déconstruire le *Tao de la physique* ou critiquer les interprétations abusives du « principe anthropique ». Au lieu de se contenter de dénoncer les astrologues et autres charlatans évidents, ce qui est assez facile, les scientifiques rationalistes devraient rappeler à l'ordre ceux parmi leurs collègues qui mélangent les genres. N'oublions pas que les scientifiques, malgré certaines critiques, ont encore une forte crédibilité, dont doit découler une vraie responsabilité.

PLS

Quelle attitude devraient-ils adopter ?

➜ **YVES GINGRAS :** Il faut, selon moi, constamment rappeler la spécificité des sciences, dont les méthodes n'ont pas vocation à répondre à tout. L'honnêteté intellectuelle oblige à dire que l'on ne trouvera jamais Dieu dans un accélérateur de particules ! Et même quand l'objectif est juste de faire la promotion des sciences, il faut rester sur les rails. La fin ne justifie pas les moyens, même lorsqu'il s'agit de faire « aimer » les sciences. ■

Propos recueillis par Maurice Mashaal.

La conjecture

Gerhard Frey

Les décompositions en facteurs premiers de deux nombres entiers *A* et *B* sont reliées à celle de leur somme *C* par des lois profondes qui s'éclaircissent peu à peu.

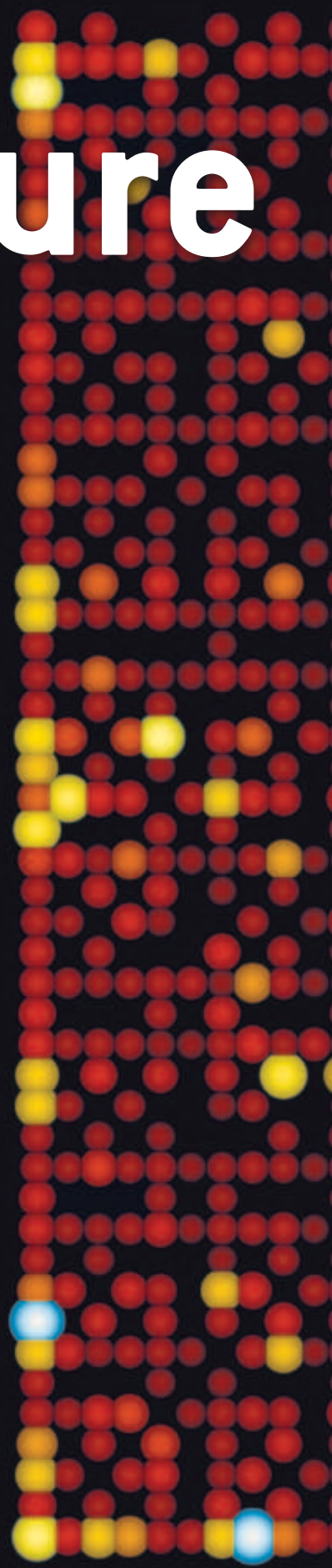
À première vue, la conjecture *ABC* semble être d'une trompeuse simplicité. Elle énonce une certaine propriété sur trois nombres entiers naturels *A*, *B* et *C* liés par la relation la plus simple possible : $A + B = C$. Ce qu'elle affirme exactement n'est pas évident. L'idée est que si les facteurs premiers de deux nombres *A* et *B* se répètent beaucoup, il y a peu de chance pour que ce soit aussi le cas pour leur somme.

La conjecture *ABC* a été énoncée en 1985 par Joseph Oesterlé, de l'Université Paris VI, et David Masser, de l'Université de Bâle, en Suisse. Malgré de solides indices en faveur de la validité de cette conjecture, aucune piste de démonstration ne semblait jusqu'ici très évidente, et la preuve paraissait encore éloignée. Cependant, cela pourrait avoir changé : un mathématicien reconnu de l'Université de Kyoto, Shinichi Mochizuki, affirme aujourd'hui avoir démontré la conjecture *ABC*. Ses pairs ont commencé à examiner sa démonstration, très longue et faisant appel à des outils nouveaux, mais il est trop tôt pour dire si son approche a été couronnée de succès.

La preuve de la conjecture *ABC* apporterait une solution à de nombreux problèmes importants de la théorie des nombres. En particulier, dans sa version forte, elle entraînerait la preuve du grand théorème de Fermat par une méthode différente de celle utilisée par Andrew Wiles et Richard Taylor en 1994.

La plupart des problèmes concernant les nombres entiers impliquent d'une façon ou d'une autre leurs facteurs premiers. Les nombres premiers sont les nombres qui ne sont divisibles que par eux-mêmes et par 1. La suite commence ainsi : 2, 3, 5, 7, 11, 13, 17… À première vue, la répartition des nombres premiers semble aléatoire. Y chercher une structure occupe les mathématiciens depuis des siècles. Le « théorème des nombres premiers » fournit cependant une estimation : le nombre de nombres premiers inférieurs à n croît comme $n / \ln(n)$ lorsque n devient grand.

D'après le théorème fondamental de l'arithmétique, chaque entier naturel se décompose de façon unique en un produit de nombres premiers (à l'ordre des facteurs près). Par exemple, $6\,936 = 2^3 \cdot 3 \cdot 17^2$

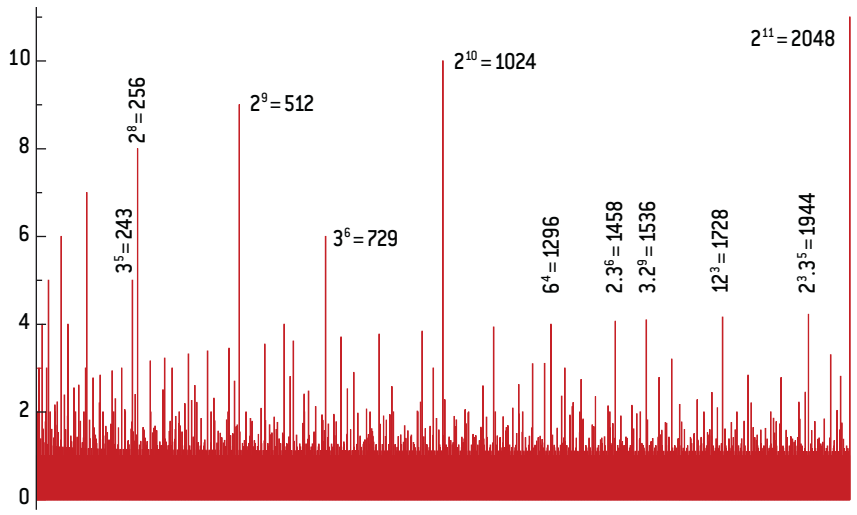


1. LA « RICHESSE » DES TRIPLETS *A*, *B*, *C* d'entiers où $C = A + B$ est représentée ici pour *A (en abscisse)* et *B (en ordonnée)* compris entre 2 et 50. La couleur et la taille des cercles indiquent la valeur de la richesse $\kappa(A, B, C)$ *(de 0,37, en rouge sombre, à 1,22, en blanc)*. Les lignes qui se dessinent suggèrent qu'en général, pour qu'un triplet d'entiers soit riche, il faut que l'un des membres le soit. On voit déjà dans cet échantillon modeste que la richesse se raréfie pour les grands nombres.

ABC

L'ESSENTIEL

- Tout nombre entier se décompose de façon unique en un produit de facteurs premiers.
- Les entiers formés de facteurs premiers portés à une puissance élevée sont qualifiés de « riches ». Ils sont assez rares.
- Il est encore plus rare que la somme de deux entiers riches soit encore riche. La conjecture *ABC* donne un sens précis à cet énoncé.
- Des théorèmes importants de la théorie des nombres, le théorème de Fermat notamment, découlent aisément de la conjecture *ABC*.
- La conjecture *ABC* semble vraie, mais sa démonstration se fait toujours attendre.



2. LA RICHESSE D'UN NOMBRE ENTIER *n*, notée δ(*n*), correspond à la puissance moyenne des facteurs premiers qui le composent. Ce graphique montre δ(*n*) pour les entiers compris entre 2 et 2 048. Les nombres les plus riches sont les « puissances pures » (comme 2^{11}), suivies de près par les nombres « puissants » (tous les facteurs premiers sont à la puissance 2 au moins). Le hasard semble régir cette distribution.

n'est divisible par aucun autre nombre premier que 2, 3 et 17.

La conjecture *ABC* porte sur les facteurs premiers des nombres entiers, et plus précisément sur leur diversité et leur fréquence. Un entier pris au hasard a en général peu de facteurs premiers, bien que certains soient présents plusieurs fois. Tout multiple de 9 contient par exemple deux fois au moins le facteur premier 3 (car $9 = 3^2$). Mais il est rare que la majorité des facteurs premiers apparaissent de nombreuses fois dans la décomposition. Les puissances pures, comme $67\,108\,864 = 2^{26}$, sont peu fréquentes, de même que les nombres « puissants », où chaque facteur premier apparaît avec un exposant au moins égal à 2 (comme dans $614\,810\,677 = 13^3 \cdot 23^4$). Si *A* et *B* sont deux nombres exceptionnels comportant des puissances élevées de leurs facteurs premiers, il faudrait que le diable s'en mêle pour que leur somme $A + B = C$ soit encore un entier exceptionnel. La conjecture *ABC* précise cet énoncé un peu flou.

Cette conjecture cache une particularité de la théorie des nombres. La structure additive des entiers naturels est particulièrement simple, et la structure multiplicative n'est guère plus compliquée. Mais les deux structures ne cohabitent pas bien : si on les combine, les choses se compliquent… et deviennent intéressantes. En d'autres termes, des propriétés de la somme $A + B$, du point de vue de la structure additive, dépendent de façon très régulière de celles de *A* et de *B*, mais du point de vue de la structure multiplicative, cette dépendance semble presque aléatoire. Le grand théorème de Fermat, selon lequel il n'existe pas d'entiers non nuls *a*, *b* et *c* vérifiant l'égalité $a^n + b^n = c^n$ pour $n > 2$, mélange ainsi addition et multiplication (sous forme de puissances), pour un résultat d'une redoutable complexité.

Richesse et pauvreté chez les nombres entiers

Mais revenons à la notion de nombre exceptionnel. On dit qu'un entier est « riche » si certains de ses facteurs premiers sont présents plusieurs fois dans la décomposition (c'est-à-dire avec une puissance supérieure ou égale à deux). On l'« appauvrit » en supprimant les facteurs premiers redondants pour ne conserver qu'un seul exemplaire de chaque. Cette version dépouillée d'un entier *n* est appelée son radical, noté Rad(*n*). Par exemple,

Rad (324) = Rad ($2^2 \cdot 3^4$) = $2 \cdot 3 = 6$;

Rad (424) = Rad ($2^3 \cdot 53$) = $2 \cdot 53 = 106$;

Rad (437) = Rad ($23 \cdot 19$) = $23 \cdot 19 = 437$.

Le radical d'un nombre est toujours inférieur ou égal à ce nombre. Les nombres premiers et ceux qui contiennent une seule fois chacun de leurs facteurs premiers sont « au seuil de pauvreté » : ils sont égaux à leur radical. À l'inverse, si chaque facteur premier de *n* est muni d'un exposant élevé, alors Rad (*n*) est beaucoup plus petit que *n*.

Pour quantifier la richesse d'un nombre, on lui associe sa « puissance moyenne » δ(*n*), définie par l'égalité $n = [\mathrm{Rad}(n)]^{\delta(n)}$. En passant au logarithme, on obtient une définition explicite :

$$\delta(n) = \frac{\log(n)}{\log(\mathrm{Rad}(n))}$$

Pour les exemples précédents, on a : $\delta(324) = \log(324)/\log(6) = 3{,}22629\ldots$; $\delta(424) = \log(424)/\log(106) = 1{,}29726\ldots$, et évidemment $\delta(437) = \log(437)/\log(437) = 1$.

Un petit programme suffit à calculer rapidement la valeur moyenne δ* de δ pour un ensemble de nombres. En tirant plusieurs fois au hasard 10 000 entiers entre un et un milliard, nous avons obtenu successivement les moyennes $\delta^* = 1{,}047519\ldots$, puis $\delta^* = 1{,}05267\ldots$, et $\delta^* = 1{,}04793\ldots$ Un tirage de 100 000 nombres au hasard sans limite de taille a donné $\delta^* = 1{,}049266\ldots$ Cela suggère qu'un nombre « moyen » ne vit que légèrement au-dessus du seuil de pauvreté. En règle générale, on s'attend à ce que la puissance moyenne ne dépasse pas 1,06.

Cette valeur moyenne suffit-elle à capturer la diversité des nombres entiers ? Évidemment, non. Il existe des cas isolés qui sont loin de toute valeur moyenne. Par exemple, dans l'intervalle allant de un à un milliard, on trouve le nombre richissime $67\,108\,864 = 2^{26}$, qui a une puissance moyenne $\delta = 26$. Et la richesse n'est pas bornée, puisqu'il existe des puissances de 2 avec un exposant aussi grand que l'on veut.

Cherchons le nombre le plus riche parmi 10 000 choisis au hasard dans l'intervalle précédent. Un premier essai donne $n = 692\,599\,663$, avec $\delta(n) = 3{,}831201\ldots$ Sa décomposition en facteurs premiers est $n = 7^7 \cdot 29^2$. Une deuxième tentative donne $n = 614\,810\,677 = 13^3 \cdot 23^4$, avec $\delta(n) = 3{,}55004\ldots$ Les nombres riches sont en général des nombres puissants. Par définition, la puissance moyenne des nombres puissants vaut au moins deux, donc la valeur maximale de δ pour un grand échantillon de nombres ne peut pas être inférieure à 2. En général, elle est nettement supérieure, comme le montrent les exemples.

Nos expériences numériques montrent en outre que les nombres puissants sont plus fréquents que les puissances pures (du type 2^{26}), ce que confirment des arguments – difficiles – de la théorie des nombres. Plus fréquents encore sont les nombres « presque puissants », c'est-à-dire puissants à un facteur près, petit par rapport à ce nombre (par exemple, 5 000 000 est presque puissant, car 5 est petit devant 1 000 000, très puissant). Eux aussi ont une

puissance moyenne δ qui est bien au-dessus de la moyenne des entiers.

Résumons les conclusions de ces expériences numériques. Le nombre moyen est pauvre : $\delta(n) \leq 1{,}06$. Les nombres riches, avec $\delta \geq 2$, sont rares, bien plus encore que les nombres premiers, mais ils sont plus fréquents que les puissances pures et leur richesse est en principe illimitée.

On ne peut pas dire grand-chose d'intéressant de plus sur la richesse d'un seul nombre. Il est peu probable que deux nombres choisis au hasard soient tous les deux riches. Mais, en reprenant l'idée évoquée précédemment de combiner les structures multiplicative et additive, posons-nous la question suivante : la somme de deux nombres assez riches est-elle riche elle aussi ?

Mesurer la puissance moyenne d'un triplet

Choisissons deux entiers A et B avec la seule restriction qu'ils soient premiers entre eux (sans facteurs premiers en commun). En posant $C = A + B$, on s'attend en fait à ce qu'au moins un des nombres A, B ou C se comporte comme un nombre moyen.

Si A est un nombre moyen, on s'attend à ce que $A \leq \mathrm{Rad}(A)^{1{,}06}$ ou, de façon équivalente, $\log(\mathrm{Rad}(A)) \geq \log(A)/1{,}06$. Si c'est vrai pour A, B et C, alors $\log(\mathrm{Rad}(A\cdot B\cdot C)) = \log(\mathrm{Rad}(A)) + \log(\mathrm{Rad}(B)) + \log(\mathrm{Rad}(C)) \geq [\log(A) + \log(B) + \log(C))]/1{,}06$ (comme A, B et donc C sont premiers entre eux, on a $\mathrm{Rad}(A\cdot B\cdot C) = \mathrm{Rad}(A)\cdot\mathrm{Rad}(B)\cdot\mathrm{Rad}(C)$).

Or pour des nombres entiers positifs, on a $A + B \leq A\cdot B + 1$, ce qui entraîne que $\log(C) \leq \log(A) + \log(B)$. En substituant cette inégalité dans la précédente, on obtient $\log(\mathrm{Rad}(A\cdot B\cdot C)) \geq 2\log(C)/1{,}06$. Autrement dit, on s'attend à ce que, en moyenne, $C \leq \mathrm{Rad}(A\cdot B\cdot C)^{0{,}53}$, ce qui peut être approximé par $\sqrt{(\mathrm{Rad}(A\cdot B\cdot C))}$.

Par analogie avec la puissance moyenne, qui quantifie la richesse d'un nombre, on introduit une mesure de la « richesse » d'un triplet : pour des entiers naturels A, B, C premiers entre eux qui vérifient $A + B = C$, on pose :

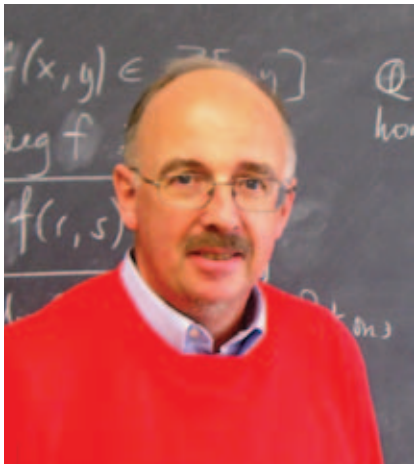
$$\kappa(A,B,C) = \frac{\log(C)}{\log(\mathrm{Rad}(A\cdot B\cdot C))}$$

$\kappa(A,B,C)$ est la puissance à laquelle il faut élever le radical de ABC pour retrouver C :

$$C = [\mathrm{Rad}(A\cdot B\cdot C)]^{\kappa(A,B,C)}.$$

Nous avons évalué cette mesure par des expériences numériques. En choisissant au hasard 10 000 triplets $(A, B, A + B = C)$ entre 1 et 10 milliards, nous avons obtenu une valeur moyenne $\kappa^*(A,B,C) = 0{,}3848\ldots$ C'est largement en dessous de la valeur 0,53 conjecturée précédemment. En fait, l'approximation de $A + B$ par AB est très grossière.

La valeur moyenne de $\kappa(A,B,C)$ ne livre cependant pas beaucoup d'informations. Déterminer une borne supérieure serait plus intéressant. Mais existe-t-elle ?



3. LA CONJECTURE *ABC* A ÉTÉ ÉNONCÉE en 1985 par David Masser, de l'Université de Bâle, en Suisse *(en haut)*, et Joseph Oesterlé, de l'Université de Paris VI *(en bas)*.

Commençons par essayer de construire des triplets A, B, C pour lesquels $\kappa(A,B,C)$ est assez grand. Pour cela, il est utile de prendre un nombre C riche, par exemple l'entier $614\,810\,677 = 13^3\cdot 23^4$ utilisé précédemment, et de l'écrire comme une somme de deux entiers A et B premiers entre eux. En choisissant 10 000 couples (A, B) au hasard qui vérifient ces conditions, nous avons obtenu $\kappa^*(A,B,C) = 0{,}70195$. C'est déjà bien plus que la valeur conjecturée 0,53, et ce pour un choix aléatoire.

En outre, il existe des triplets particuliers pour lesquels κ est encore plus grand. Par exemple, $\kappa(1\,365,\ 614\,797\,312,\ 614\,810\,677)$ est égal à 0,864135... Comment expliquer cela ? Les nombres $A = 13\,365 = 3^5\cdot 5\cdot 11$ et $B = 614\,797\,312 = 150\,097\cdot 2^{12}$ sont assez riches, et $C = 13^3\cdot 23^4$ l'est davantage. De plus, A est petit par rapport à C, ce qui en général signifie qu'il a peu de chances de contribuer au radical. Il est remarquable que notre exploration aléatoire ait trouvé cette solution.

À partir d'un tel triplet de nombres presque puissants, on peut construire une équation pour laquelle des facteurs du triplet sont une solution. Pour l'exemple précédent, on peut construire l'équation $55\,x^5 + 150\,097\,y^{12} = 23\,z^3$, qui a pour solution $x = 3$, $y = 2$ et $z = 299 = 13\cdot 23$.

On peut généraliser cet exemple trouvé par hasard : on se donne une équation de trois variables, on cherche autant de solutions que possible et l'on construit à partir de celles-ci des triplets de nombres riches. Voici deux types d'équations intéressantes.

D'après un résultat élémentaire de la théorie des nombres, l'équation $x^2 = 3y^2 + 1$ admet un nombre infini de solutions. Le couple (3 650 401, 2 107 560) en est une. Si on pose $A = 1$, $B = 3y^2$ et $C = x^2$, on obtient

$$\kappa(A,B,C) = \frac{\log(C)}{\log(\mathrm{Rad}(A\cdot B\cdot C))} = \frac{2\log(x)}{\log(\mathrm{Rad}(x\cdot 3\cdot y))}$$

Comme x et $3y$ sont premiers entre eux (sinon, un diviseur diviserait $x^2 - 3y^2 = 1$), on a $\mathrm{Rad}(x\cdot 3y) = \mathrm{Rad}(x)\ \mathrm{Rad}(3y)$. En outre, $\log(3y)$ et $\log(x)$ sont presque égaux pour x et y assez grands ; par conséquent, si l'on suppose que ceux-ci sont des nombres « moyens » dont la puissance moyenne δ vaut 1,06, on déduit que $\kappa(A,B,C) \approx 1{,}06$, soit $\kappa(A,B,C) \geq 1$. Pour les nombres cités en exemple, on trouve $\kappa(1,\ 13\,325\,427\,460\,800,\ 13\,325\,427\,460\,801) = 1{,}06843$. C'est en effet supérieur à 1, mais pas de beaucoup.

Le deuxième type d'équations donne des puissances κ encore plus grandes : il s'agit de $ax^3 + by^3 = cz^3$, où les coefficients a, b et c sont des entiers relatifs. Si une solution (x, y, z) comporte des termes négatifs, on peut toujours modifier l'équation pour n'avoir que des termes positifs. Si tous les monômes de l'équation sont positifs, on pose $A = ax^3$, $B = by^3$ et $C = cz^3$.

On connaît assez bien l'ensemble des solutions de ce type d'équations : elles appartiennent aux courbes elliptiques, des objets très étudiés en théorie des nombres et en géométrie algébrique. Parfois, ce type

Croissance polynomiale ou exponentielle

La croissance d'une fonction $f(x)$ quand x tend vers l'infini peut être similaire (entre autres) à celle d'un polynôme x^a ou à celle d'une exponentielle a^x (a fixé). Peu importe le comportement de $f(x)$ dans un intervalle fini, la croissance exponentielle devient tôt ou tard plus rapide que la croissance polynomiale.

Cette distinction est essentielle pour les calculs numériques. Un problème où le temps de calcul nécessaire croît de façon polynomiale en fonction de la variable étudiée (ou problème P) est considéré comme « facile » : il peut être résolu en un temps raisonnable. Si, en revanche, le nombre d'opérations croît exponentiellement avec la variable considérée (problème NP, pour *non polynomial*), le problème est considéré comme difficile et dépasse vite les capacités de calcul existantes. Une des sept « questions du millénaire » est de savoir si les problèmes NP peuvent se ramener à des problèmes P.

d'équation n'a aucune solution parmi les entiers naturels non nuls (par exemple, $x^3 + y^3 = z^3$ n'a pas de solutions, d'après le théorème de Fermat), parfois elles en ont une infinité.

Si les nombres x, y, z sont à peu près du même ordre de grandeur et sont très supérieurs aux coefficients a, b et c, alors on obtient, par une estimation analogue à la précédente, que $\kappa(A,B,C) \approx \delta(x)$ et que cette valeur est probablement inférieure à 1,06. Si, en revanche, x est beaucoup plus petit (de plusieurs ordres de grandeur) que y et z, on obtient $\kappa(A,B,C) \approx 3/2\ \delta(x)$.

Le triplet $(51^3, 5\cdot 49^3, 22\cdot 32^3)$ donne par exemple $\kappa(A,B,C) = 1{,}27509\ldots$, le triplet $(1, 17\cdot 7^3, 18^3)$ donne $\kappa = 1{,}31962\ldots$, et le triplet $(1, 5\cdot 2^4, 3\cdot 3^3)$ donne $\kappa = 1{,}29\ldots$

Le dernier exemple est particulièrement intéressant, car $81 = 3^4 = 5\cdot 2^4 + 1$ est une solution de l'équation $x^4 = 5y^4 + z^k$, où k est un entier aussi grand que l'on veut. Plus les exposants dans l'équation sont élevés (2 et 3 dans les exemples précédents), plus la valeur de $\kappa(A,B,C)$ que l'on peut obtenir est grande – si tant est que l'équation en question admette encore des solutions. Or il n'y en a pas beaucoup. Gerd Faltings, lauréat de la médaille Fields en 1986 pour sa démonstration de la conjecture de Mordell, a montré par celle-ci que l'équation $x^4 = 5y^4 + z^k$ n'a, pour chaque exposant $k \geq 4$, qu'un nombre fini de solutions dont les termes sont premiers entre eux. On pense même que l'ensemble des solutions pour tous k confondus est fini, c'est-à-dire que l'ensemble des triplets (x, y, z) premiers entre eux et pour lesquels il existe un entier $k \geq 4$ tel que $x^4 = 5y^4 + z^k$ est fini.

Résumons. Nos expériences numériques suggèrent qu'en moyenne, la puissance moyenne $\kappa(A,B,C)$ d'un triplet est d'environ 0,5 ; dans tous les cas étudiés, κ est inférieur à 2 ; pour de nombreux exemples, κ est supérieur à 1, et ces valeurs élevées sont intimement liées à des solutions d'équations polynomiales à trois variables.

La version forte de la conjecture *ABC*

Tous ces résultats expérimentaux permettent enfin de proposer – avec toute la prudence requise vis-à-vis de résultats empiriques – la conjecture suivante : la puissance moyenne $\kappa(A,B,C)$ des triplets (A,B,C), où A, B et C sont premiers entre eux et tels que $A + B = C$, est bornée, c'est-à-dire qu'il existe un nombre positif α tel que $\kappa(A,B,C) \leq \alpha$.

On peut exprimer la même chose sans faire référence aux quantités C et κ, qui dépendent de A et de B. Un peu de travail donne :

$$A + B \leq [\mathrm{Rad}(A\cdot B\cdot (A+B))]^{\alpha}$$

Plutôt que d'affirmer l'existence d'une telle borne α, on aurait préféré qu'elle soit calculable. Des algorithmes qui peuvent en principe déterminer cette valeur ont été mis au point ; mais en pratique, le temps de calcul prendrait des siècles, voire plus. On cherche toujours un algorithme effectif, c'est-à-dire qui pourrait livrer un résultat en un temps raisonnable, par exemple une semaine de calcul sur un ordinateur personnel.

TAILLER LE COSTUME IDÉAL
pour les entiers signifie couvrir tous les cas, mais avec une approximation aussi proche du corps que possible.

Même si l'on parvenait à démontrer la conjecture pour une très grande valeur de α, cela ne servirait pas à grand-chose : une approximation trop grossière ne dit plus grand-chose sur le comportement des triplets. La borne α doit être aussi petite que possible. D'après nos résultats empiriques, on serait tenté de choisir $\alpha = 1{,}4$. Malheureusement, dans certains cas, $\kappa(A,B,C)$ est supérieur à 1,4. Par ailleurs, dans la plupart des cas, $\kappa(A,B,C)$ est beaucoup plus petit. Cette borne est à la fois trop grande et trop petite.

Pour contourner ce problème, on introduit une deuxième constante. À la place de l'équation précédente, on pose :

$$A + B \leq d\,[\mathrm{Rad}(A\cdot B\cdot (A+B))]^{\alpha}$$

où d est une constante qui devrait être effective. En exprimant cette inégalité en fonction de κ, on obtient l'inégalité suivante :

$$\kappa(A,B,C) \leq \alpha + \frac{\log d}{\log(\mathrm{Rad}(A\cdot B\cdot C))}$$

À première vue, la conjecture initiale est si déformée qu'elle semble vidée de sa substance. Si un contre-exemple ne vérifie pas l'inégalité, on n'a qu'à choisir une valeur de d plus grande pour que l'inégalité soit satisfaite. Supposons que l'on ait cherché un contre-exemple parmi tous les nombres inférieurs à un milliard ; il suffit de prendre d supérieur au plus grand des nombres C testés, soit un milliard, pour que la conjecture soit vérifiée pour tout α, ce qui n'a aucun intérêt.

Mais cette première impression est trompeuse. On a montré que plus A, B et C sont grands, plus $\log(\mathrm{Rad}(A\cdot B\cdot C))$ devient grand, bien que plus lentement. Ainsi, le degré de liberté que nous offre la constante d devient négligeable lorsque les nombres considérés deviennent grands. Pour les nombres « très grands », seule la borne α compte.

Cependant, cette formulation contient encore trop de choix. Pour faire rentrer un contre-exemple dans le rang, on a le choix d'augmenter α ou d. Le but est pourtant de tailler, par un choix approprié de α et d, un « costume idéal » pour tous les entiers naturels : il devrait tout couvrir (aucun contre-exemple) et en même temps être aussi proche du corps que possible (l'approximation ne doit pas être trop large). Cela signifie que pour au moins quelques triplets, l'inégalité ci-dessus devrait être une égalité. En prenant α et d légèrement plus petits que ces valeurs bien ajustées, on pourrait trouver un contre-exemple. Diminuer α demanderait d'agrandir d et inversement.

La conjecture *ABC* dans la version énoncée par J. Oesterlé et D. Masser est encore plus forte que notre dernière version. Elle dit qu'il suffit de prendre α supérieur à 1, mais aussi proche de 1

que l'on veut. Tous les cas particuliers peuvent alors être englobés en choisissant une valeur appropriée de d. Il faut juste accepter que d devienne arbitrairement grand si α s'approche de 1. En termes précis, la conjecture *ABC* s'énonce ainsi :

Pour tout nombre réel $\varepsilon > 0$, il existe un nombre réel $d_\varepsilon > 0$ tel que, pour tous entiers naturels A, B et C premiers entre eux et tels que $A + B = C$, on ait :

$$C \leq d_\varepsilon [\mathrm{Rad}(A \cdot B \cdot C)]^{1+\varepsilon}$$

Autrement dit, en prenant le logarithme :

$$\kappa(A,B,C) \leq 1 + \varepsilon + \frac{\log(d_\varepsilon)}{\log(\mathrm{Rad}(A \cdot B \cdot C))}$$

où le terme d'erreur $\log(d_\varepsilon)$ dépend de ε.

Pourquoi ne pas choisir α égal à 1, voire moins ? Parce que l'on connaît certains contre-exemples (notamment de la forme $(A,B,C) = (1, 2^{p(p-1)} - 1, 2^{p(p-1)})$, où p est un nombre impair tel que $2^{p(p-1)} - 1$ est divisible par p^2). Par ailleurs, peut-on trouver un ε pour lequel on peut prendre $d_\varepsilon = 1$, ce qui correspond à notre première version de la conjecture ? Bien sûr, on cherche $\alpha = 1 + \varepsilon$ qui soit le plus petit possible.

La plus grande valeur connue pour $\kappa(A,B,C)$ est 1,6299117. Elle correspond au triplet $(2, 3^{10} \cdot 109, 23^5)$, solution de l'équation $x^5 - 109\,y^{10} = 2$, trouvée par Éric Reyssat, aujourd'hui à l'Université de Caen. Ayant testé tous les nombres jusqu'à 10^{20}, nous savons qu'au moins dans cet intervalle immense, il n'existe pas de contre-exemple (pour $d_\varepsilon = 1$) à la conjecture *ABC* avec $\alpha = 2$ (qui correspond à $\varepsilon = 1$), c'est-à-dire $\kappa(A,B,C) \leq 2$.

À la recherche des bons triplets

Depuis que la conjecture *ABC* a été énoncée, elle a suscité une recherche intense de triplets nécessitant de grandes constantes α et d, c'est-à-dire pour lesquels $\kappa(A,B,C)$ est grand. Ces exemples resserrent l'intervalle pour le choix de ε et d_ε, mais il y a aussi une part de compétition dans cette recherche des triplets les plus riches. C'est à qui mettra au point l'algorithme le plus rapide et le plus performant. On peut en outre espérer découvrir des équations intéressantes.

On dit que (A,B,C) est un « bon triplet » si $\kappa(A,B,C) > 1{,}4$. Ces triplets sont extrêmement rares. Dans la tranche des entiers allant jusqu'à 10^{20}, presque entièrement explorée, il n'y en a qu'environ 200.

Sur le modèle des projets participatifs de recherche de signaux extraterrestres ou d'étude du repliement des protéines, le projet ABC@home invite tous les internautes à participer à la recherche d'autres bons triplets en donnant un peu de temps de calcul de leur ordinateur, ou même en développant leur propre algorithme.

Outre son intérêt intrinsèque, la démonstration de la conjecture *ABC* entraînerait celle de nombreux problèmes de la théorie des nombres. C'est le cas notamment du redoutable théorème de Fermat, dont la conjecture *ABC* apporte une preuve – du moins pour n assez grand – d'une simplicité dérisoire.

Dans l'équation $x^n + y^n = z^n$, posons $A = x^n$, $B = y^n$, $C = z^n$. On donne d'abord une borne supérieure grossière pour $\mathrm{Rad}(ABC)$:

$$\mathrm{Rad}(ABC) = \mathrm{Rad}(x^n y^n z^n)$$
$$= \mathrm{Rad}(xyz) \leq xyz < z^3.$$

Cela donne une borne inférieure pour $\kappa(A,B,C)$: $\kappa(A,B,C) = \log(C)/\log(\mathrm{Rad}(ABC)) \geq \log(z^n)/\log(z^3) = n/3$.

Cette dernière quantité tend vers l'infini pour des exposants n élevés. Si par exemple $\kappa(A,B,C)$ était borné par 2, on aurait ainsi démontré que l'équation de Fermat n'a pas de solutions pour $n \geq 6$. Le théorème de Fermat étant prouvé depuis longtemps pour des petits exposants, cela suffirait pour boucler sa démonstration.

La validité de la conjecture *ABC* apporterait des démonstrations faciles et élégantes à d'autres poids lourds de la théorie des

■ L'AUTEUR

Gerhard FREY est professeur à l'Institut de mathématiques expérimentales de l'Université Duisburg-Essen, en Allemagne.

Le logarithme

Le logarithme (décimal) d'un nombre strictement positif X est le nombre $\log X$ tel que $X = 10^{\log X}$. La fonction logarithme transforme un produit en somme : $\log(ab) = \log(a) + \log(b)$, et $\log(a^n) = n \log(a)$. Par ailleurs, $\log 1 = 0$. On peut choisir une autre base que la base 10. Pour la base e = 2,718..., le logarithme est dit népérien et est noté ln.

	$\kappa > 1$	$\kappa > 1{,}05$	$\kappa > 1{,}1$	$\kappa > 1{,}2$	$\kappa > 1{,}3$	$\kappa > 1{,}4$
$C < 10^2$	6	4	4	2	0	0
$C < 10^3$	31	17	14	8	3	1
$C < 10^4$	120	74	50	22	8	3
$C < 10^5$	418	240	152	51	13	6
$C < 10^6$	1 268	667	379	102	29	11
$C < 10^7$	3 499	669	856	210	60	17
$C < 10^8$	8 987	3 869	1 801	384	98	25
$C < 10^9$	22 316	8 742	3 693	706	144	34
$C < 10^{10}$	51 677	18 233	7 035	1 159	218	51
$C < 10^{11}$	116 978	37 612	13 266	1 947	327	64
$C < 10^{12}$	252 856	73 714	23 773	3 028	455	74
$C < 10^{13}$	528 275	139 762	41 438	4 519	599	84
$C < 10^{14}$	1 075 319	258 168	70 047	6 665	769	98
$C < 10^{15}$	2 131 671	463 446	115 041	9 497	998	112
$C < 10^{16}$	4 119 410	812 499	184 727	13 118	1 232	126
$C < 10^{17}$	7 801 334	1 396 909	290 965	17 890	1 530	143
$C < 10^{18}$	14 482 065	2 352 105	449 194	24 013	1 843	160

4. LA LISTE DES « BONS » TRIPLETS. Ce tableau présente le nombre de valeurs de C dans certains intervalles *(lignes)* pour lesquelles il existe A et B premiers entre eux, avec $A + B = C$, tels que la richesse $\kappa(A,B,C)$ soit supérieure à une borne donnée *(colonnes)*.

nombres. Il s'agit en général de problèmes diophantiens, du nom du mathématicien du IIIe siècle Diophante d'Alexandrie. Ces problèmes font intervenir des équations polynomiales à coefficients entiers, dont on cherche les solutions parmi les nombres entiers (on parle d'équations diophantiennes). Une démonstration de la conjecture *ABC* fournirait en particulier une solution simple aux problèmes suivants :

– La conjecture de Catalan, selon laquelle l'équation $x^m - y^n = 1$ n'a qu'une seule solution parmi les entiers naturels : $3^2 - 2^3 = 1$. Elle a été démontrée en 2002 par le mathématicien roumain Preda Mihăilescu.

– La conjecture de Mordell, démontrée en 1983 par Gerd Faltings, affirme que chaque courbe dont le « genre » est plus grand que 1, définie par une équation polynomiale à coefficients rationnels, ne peut contenir qu'un nombre fini de points dont les coordonnées sont rationnelles (le genre peut être vu comme le nombre de fois où il est possible de couper la courbe sans obtenir deux morceaux séparés). Noam Elkies, de l'Université Harvard, a démontré en 1991 que la conjecture de Mordell est une conséquence de la conjecture *ABC*. Si la conjecture *ABC* était valable dans sa version la plus forte, cela prouverait non seulement l'existence de ces points rationnels, mais donnerait aussi un procédé effectif pour les déterminer.

– Un grand nombre de généralisations de ces problèmes. La preuve de la conjecture *ABC* entraînerait par exemple celle que chaque égalité (dite de Fermat) $ax^n + by^n = cz^n$ pour $n \geq 4$ (et a, b, c entiers relatifs) n'a qu'un nombre fini de solutions. Il en est de même pour l'équation de Catalan-Fermat $x^n + y^m = z^k$, si les exposants sont « grands », c'est-à-dire si $1/n + 1/m + 1/k < 1$.

Il reste qu'à ce jour, la conjecture *ABC* n'est pas démontrée – du moins tant que les affirmations de S. Mochizuki n'ont pas été vérifiées. Pourquoi serait-elle vraie ? Et quels sont les résultats intermédiaires atteints à ce stade ?

Comme on l'a vu, de nombreuses données numériques soutiennent la validité de la conjecture, mais elles n'aident en rien à la prouver. En mathématiques, on cherche à obtenir des énoncés qui ne concernent pas seulement un comportement moyen, mais qui sont valables dans tous les cas. Or la difficulté de la conjecture *ABC* vient des nombres exceptionnels qui échappent à la statistique.

Des pistes ténues vers une démonstration

En utilisant des méthodes de ce qu'on appelle la théorie des nombres transcendants, Cameron Stewart, Robert Tijdeman et Kunrui Yu ont pu montrer que le taux de croissance de C en fonction de Rad(ABC) est au plus exponentiel. D'après la conjecture *ABC*, cette croissance est polynomiale, avec un exposant égal au plus à 2 ou $1 + \varepsilon$, suivant la version de la conjecture. On sait donc au moins que la croissance de C n'est pas illimitée, mais cela est insuffisant pour des grandes valeurs de C. Et il semble hors de portée de gravir, avec les méthodes utilisées, la marche séparant la croissance exponentielle de la croissance polynomiale.

Une autre approche emprunte un chemin *a priori* paradoxal. En généralisant la conjecture *ABC*, donc en la rendant en quelque sorte plus difficile, on a l'espoir de faciliter la démonstration. La généralisation consiste à remplacer les nombres naturels usuels par des structures abstraites plus compliquées. Les propriétés des entiers naturels utilisées dans la conjecture sont la structure additive, la structure multiplicative et l'ordre total : deux entiers peuvent toujours être comparés, au sens que l'un est forcément plus petit ou égal à l'autre. Ces trois propriétés se retrouvent dans beaucoup d'autres structures mathématiques, par exemple :

– Les nombres rationnels, c'est-à-dire les fractions de la forme r/s, où r et s sont des entiers relatifs. On utilise l'addition et la multiplication usuelles, mais au lieu de l'ordre habituel, on ordonne ici les rationnels par leur « hauteur », c'est-à-dire le maximum entre le numérateur et le dénominateur de la fraction sous forme réduite (sans tenir compte du signe). La hauteur est en quelque sorte une mesure de la complexité d'un nombre rationnel.

– Les polynômes, c'est-à-dire des sommes de produits de puissances des variables et de constantes. L'ordre est donné par le degré du polynôme, la plus élevée des sommes des exposants d'un terme du polynôme.

– Les fonctions rationnelles, c'est-à-dire les fractions dont le numérateur et le dénominateur sont des polynômes.

– Les extensions algébriques des nombres rationnels (corps de nombres algébriques) et des fonctions rationnelles (corps de fonctions algébriques).

Il est possible de transposer la conjecture *ABC* pour ces structures ; le contexte devient ainsi plus clair. R. Mason et W. Stothers ont prouvé l'équivalent de la conjecture *ABC* pour les polynômes par des méthodes élémentaires en 1981, avant que la conjecture sur les entiers n'ait été énoncée. Et dans le cadre général des corps de fonctions, la relation avec les courbes elliptiques, qui avaient déjà joué un grand rôle dans la preuve du théorème de Fermat, devient évidente.

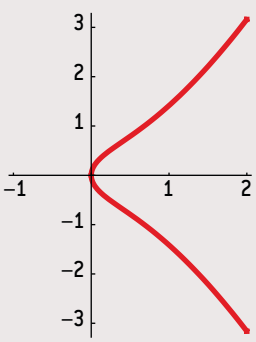
Considérons une courbe elliptique E. On peut définir trois nombres qui la caractérisent : son invariant modulaire, noté j_E, son discriminant, noté Δ_E, et sa hauteur, notée h_E *(voir l'encadré ci-contre)*. Le comportement de la courbe E est décrit par le radical du discriminant, aussi appelé conducteur de la courbe.

Lucien Szpiro, de l'Université de New York, a conjecturé qu'il existe un nombre k tel que pour toute courbe elliptique E, $\delta(|\Delta_E|) \leq k$ (la puissance moyenne du discriminant est bornée). Il est remarquable que L. Szpiro ait observé ce comportement dans le cas des corps de fonctions, et ait formulé un analogue pour le cas des corps de nombres.

Un lien intime avec les courbes elliptiques

Une courbe elliptique E *(ci-contre un exemple)* est l'ensemble des points de coordonnées (x, y) solutions d'une équation de la forme $y^2 = x^3 + ax + b$, où a et b sont des entiers tels que le « discriminant » $\Delta_E = 4a^3 - 27b^2$ soit non nul (cela garantit que la courbe n'ait pas de points singuliers).

On peut définir une hauteur de Faltings h_E pour une courbe elliptique E. Lorsque la courbe est « semi-stable », h_E est reliée à la hauteur du nombre $j_E = 12^3 \cdot 4a^3/\Delta_E$, nommé invariant modulaire.



La « conjecture sur la hauteur des courbes elliptiques », formulée par l'auteur, énonce que la hauteur h_E est bornée par une quantité qui dépend du radical du discriminant Δ_E ($h_E \leq k \log \mathrm{Rad}(|\Delta_E|)$). La conjecture *ABC* découle de celle sur les hauteurs.