Preuves et cert

Depuis la parution des Éléments de mathématique *de Nicolas Bourbaki, l'ordinateur a fait son apparition dans l'univers mathématique. Il sert même dans des démonstrations qui sont trop longues et complexes pour qu'on les vérifie à la main. Cet avènement impose une remise en question de la notion de preuve.*

Jean-Paul Delahaye
Université des Sciences et Technologies de Lille

Démonstrations par l'ordinateur

En 1998, Thomas Hales proposa une démonstration de la conjecture de Kepler qui indique que la façon la plus dense de ranger des sphères dans l'espace est celle des empilements des boulets de canon[1] et conduit à une densité de $\pi/\sqrt{18}$. Malheureusement, une partie de la démonstration de Hales utilise des calculs informatiques, ce qui rend très difficile sa vérification pas à pas.

Empilements

Boulets de canon, oranges, clémentines ou autres, comment empiler des sphères de même rayon pour qu'elles occupent le moins d'espace possible?

La démonstration de Hales a été publiée dans le prestigieux journal *The Annals of Mathematics*. Un comité de douze experts présidé par le mathématicien Gabor Fejes Toth (spécialiste des problèmes d'empilements) a été chargé d'examiner la validité de la preuve. Ce comité, malgré quatre années d'un travail acharné, a indiqué qu'il n'était certain qu'à 99 pour cent de la validité de la démonstration. Le journal a donc publié la preuve avec cette réserve. Une telle situation ne s'était pas produite pour le grand théorème de Fermat, démontré par A. Wiles il y a bientôt une douzaine d'années, et dont les experts, après quelques aménagements du manuscrit initial, avaient accepté de garantir la validité de la preuve.

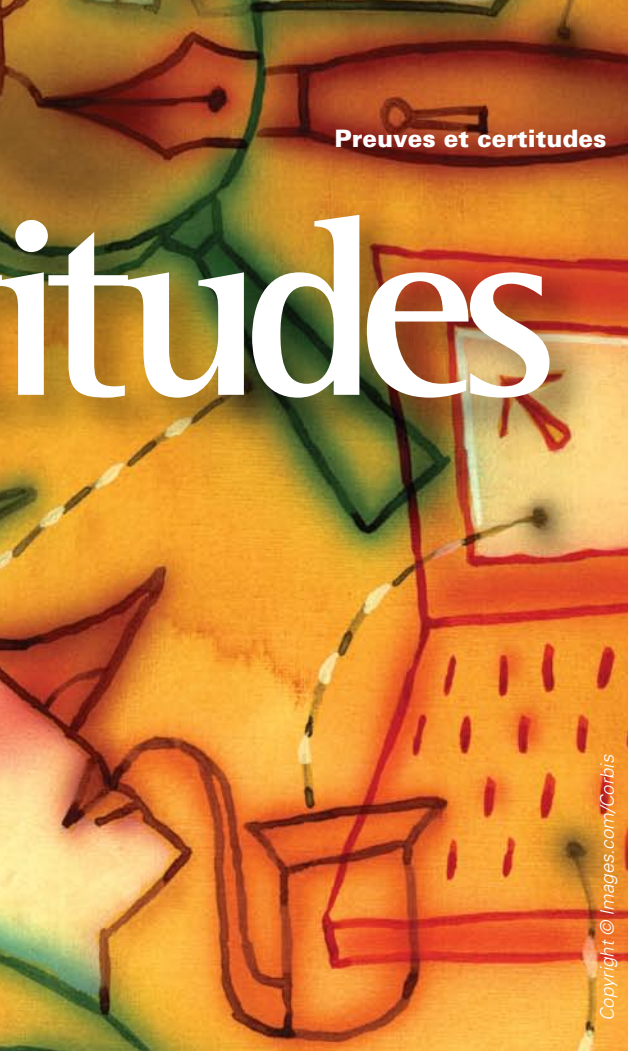
Conjecture de Kepler

Dans un problème comme celui de la densité des empilements, il y a un nombre élevé de cas particuliers à vérifier et c'est grâce à l'ordinateur que Thomas Hale est parvenu à faire ces vérifications sur plus de 5 000 cas de distribution des sphères dans l'espace.

Pour remédier à la situation nouvelle créée par la démonstration de Hales, un projet intitulé Flyspeck[2] a été engagé. Son but est de contrôler à l'aide de techniques informatiques chaque pas de la démonstration, ce qui revient à écrire explicitement une preuve formelle comme celles envisagées par Hilbert ou Bourbaki[3]. Le projet demandera 20 hommes-années de travail pour être mené à terme. Seules la longueur et la complication inhabituelles de la preuve de Hales rendent obligatoire l'utilisation de telles méthodes pour garantir une preuve et certains y voient une nouvelle ère pour les mathématiques.

1. *Voir l'article* Savez-vous empiler des oranges? *en page 20 de ce numéro.*
2. *http://www.lix.polytechnique.fr/~zumbeller/Flyspeck.html*
3. *Voir l'article* Preuves sans mots *en page 14 de ce numéro.*

Jean-Paul Delahaye • Université des Sciences et Technologies de Lille



Théorème des quatre couleurs

Le théorème des quatre couleurs affirme qu'il suffit de quatre couleurs pour colorier n'importe quelle carte découpée en régions connexes de sorte que deux régions adjacentes soient toujours de couleurs distinctes.

C'est en 1852 que Francis Guthrie, intéressé par le coloriage de la carte des régions d'Angleterre, a énoncé la conjecture des quatre couleurs.

En 1976, les Américains Kenneth Appel et Wolfgang Haken affirment avoir démontré le théorème des quatre couleurs. Leur démonstration partage la communauté scientifique : pour la première fois, en effet, la démonstration exige l'usage de l'ordinateur pour étudier les 1200 cas critiques. Le problème de la validation du théorème se trouve alors déplacé vers le problème de la validation :

- d'une part de l'algorithme d'exploration ;
- d'autre part de sa réalisation sous forme de programme.

Depuis 1976, l'algorithme d'Appel et Haken a été repris et simplifié par d'autres chercheurs.

Je voudrais insister sur un exemple plus net encore de l'intrusion brutale des ordinateurs en mathématiques. Le livre paru en 2003 de Steven Finch intitulé *Mathematical Constants* est une encyclopédie de 600 pages consacrée aux constantes mathématiques. Le livre s'intéresse bien sûr aux grandes vedettes que sont π et e, mais aussi à plusieurs centaines d'autres constantes rencontrées dans toutes sortes de domaines mathématiques. Il se termine par une table donnant la valeur approchée d'un millier de constantes. Les valeurs numériques citées aussi dans le texte de l'ouvrage et dans cette table doivent être vues comme des théorèmes, chacun de la forme :

La constante de Catalan, la somme de la série : 1−1/32+1/52−1/72... vaut 0,9159655941...

Ces centaines de théorèmes, qui constituent une part importante du contenu de l'ouvrage, ont, sauf quelques-uns, été démontrés à l'aide d'un ordinateur. Bien sûr, les étapes de ces démonstrations – ici des calculs, ne sont pas détaillées – dans l'ouvrage ni n'ont été contrôlées à la main[4].

Le livre de Finch contient donc plusieurs centaines de propositions dont les preuves reposent sur les ordinateurs. L'usage des preuves par ordinateur n'est donc pas rare et dans bien des cas n'émeut plus les mathématiciens. Ceux qui formulent des doutes sur l'acceptabilité des preuves mathématiques par ordinateur et qui soutiennent que seuls les théorèmes mathématiques provenant d'un travail humain, ou humainement vérifiable, doivent être considérés comme authentiquement prouvés, devraient aussi s'interroger sur ce cas.

Il semble ainsi que la notion de preuve acceptable évolue et qu'en pratique aujourd'hui elle tolère l'usage d'un calcul par ordinateur. Bien plus, dans certains cas, il semble que seul l'ordinateur pourra valider un résultat que les humains, trop faillibles, proposent. Cette acceptation de l'ordinateur pour fonder certaines certitudes mathématiques repose toujours sur la notion de preuve formalisée que Hilbert défendait. Cependant, d'autres pratiques récentes montrent que l'informatique remet en question plus profondément l'idée que seule une preuve classique et formalisable produit de la certitude mathématique.

4. Voir aussi le site de Simon Plouffe : http://www.lacim.uqam.ca/~plouffe/

Démonstrations probabilistes

Il arrive qu'une erreur se glisse dans une démonstration et qu'elle passe inaperçue pendant des décennies. Cela s'est produit pour le théorème des quatre couleurs dont aujourd'hui on ne connaît que des preuves utilisant l'ordinateur (voir encadré à la page 23). Aussi, la probabilité qu'une preuve un tant soit peu complexe soit fausse n'est jamais totalement nulle : donc, même au sens classique, une preuve peut n'apporter qu'une certitude forte et jamais absolue (faire vérifier la preuve par un ordinateur ne réduit pas le risque à zéro, car les mêmes erreurs de raisonnement peuvent être présentes dans les logiciels utilisés).

Il en résulte que si certaines vérités mathématiques étaient connues avec un risque d'erreur très faible, nous devrions les considérer comme aussi certaines que les théorèmes prouvés par des démonstrations classiques (avec ou sans ordinateurs). Il se trouve que, depuis 1975, le problème se pose vraiment, car des méthodes de preuves probabilistes ont été introduites par les mathématiciens M. Rabin et G. Miller pour établir qu'un nombre est premier. Ces méthodes permettent d'engendrer des nombres entiers dont on sera certain, par exemple à 99,9999999 pour cent, qu'ils sont premiers. Si un risque de $1/10^9$ vous paraît trop important, paramétrez votre méthode de preuve probabiliste pour qu'il soit de $1/10^{12}$ ou $1/10^{20}$, mais ne soyez pas trop exigeant et n'oubliez pas que, selon votre âge, la probabilité que vous avez de mourir dans la prochaine seconde varie entre $1/10^9$ et $1/10^{11}$. Or, aujourd'hui, malgré la découverte en 2002 d'un algorithme fonctionnant en temps polynomial pour prouver la primalité, les méthodes les plus efficaces pour établir qu'un nombre est premier sont probabilistes : ce sont donc elles qu'on utilise en cryptographie lorsqu'on a besoin de grands nombres premiers. En pratique donc, faisant fi des réticences des mathématiciens qui prétendent que seules les preuves traditionnelles produisent de la certitude, les cryptologues utilisent massivement les preuves probabilistes.

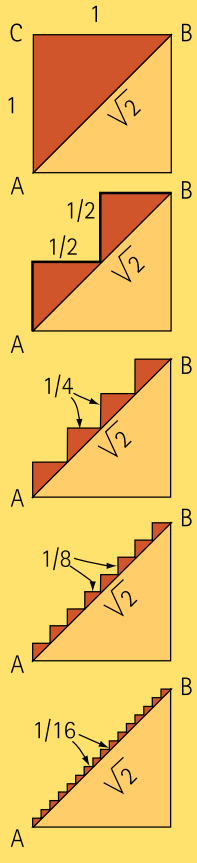
De plus, les logiciels de calcul symbolique (Maple, Mathematica, etc.) se servent de ces méthodes dès qu'on les interroge sur des nombres ayant beaucoup de chiffres. Toutefois, même lorsqu'une preuve est probabiliste, elle reste communicable : en transmettant les éléments à votre disposition qui vous ont persuadé qu'un certain nombre N est premier avec un risque P d'erreur, vous persuaderez votre interlocuteur que N est premier avec un risque P d'erreur.

Conviction incommunicable

Cette transmissibilité de la certitude — jugée essentielle par beaucoup de mathématiciens — n'est pas une règle absolue,

Vérification des preuves

La vérification des preuves par des « experts indépendants » est une composante importante de la construction du savoir mathématique.



Lorsque le raisonnement conduit à un paradoxe ou à une contradiction comme dans l'exemple qui suit, il est assez simple de conclure qu'il y a une faille dans le raisonnement, mais lorsque le raisonnement conduit à une conclusion que l'on croit vraie, il est important qu'une équipe d'experts indépendants vérifie la preuve.

On peut facilement illustrer qu'il faut se méfier des raisonnements sans mot, car ils ne donnent pas toujours des résultats valides. Considérons la première figure ci-contre représentant un carré de côté unitaire. La longueur de la diagonale AB est donc $\sqrt{2}$ alors que le parcours des arêtes ACB est de 2 unités. Supposons que l'on modifie ce parcours comme dans la deuxième figure. Le parcours des arêtes est toujours égal à 2 puisqu'il est constitué de quatre longueurs de 1/2. Si on double le nombre d'étapes comme à la troisième figure, on obtient 8 longueurs de 1/4 pour une longueur totale de deux unités. Or, après une infinité d'étapes, le parcours des arêtes devient visuellement la diagonale, ce qui semble démontrer que $\sqrt{2}=2$.

Il est manifeste qu'il y a une faille dans ce raisonnement visuel puisqu'on obtient un paradoxe. Il n'est pas toujours simple, cependant, de déceler la faille dans un raisonnement, surtout s'il ne donne pas un résultat paradoxal. La faille de ce raisonnement tient au fait qu'on admet, de façon erronée, que la limite des mesures de longueurs est forcément égale à la mesure de la limite de ces mêmes longueurs[5].

5. *Voir aussi* Solution au paradoxe précédent, *p. 31 de ce numéro.*

car un type de preuve, inventé il y a 20 ans par les trois mathématiciens O. Goldreich, S. Micali et C. Rackoff, conduit à des certitudes non partageables. Les preuves « sans transfert de connaissance »[6] permettent à quelqu'un d'acquérir la certitude qu'un énoncé mathématique E est vrai sans pourtant qu'il dispose d'aucune information communicable lui permettant de faire partager à un tiers sa conviction de la vérité de E.

Le principe général des preuves sans transfert de connaissance est le suivant:

- Alain dispose d'une information de type mathématique, par exemple qu'une carte est coloriable en utilisant trois couleurs seulement (ce qui n'est pas évident puisque le théorème déjà évoqué indique seulement que quatre couleurs suffisent).
- Alain dialogue avec Béatrice d'une telle façon qu'il la persuade qu'il connaît un coloriage à trois couleurs et donc qu'un tel coloriage existe bien. Pourtant, le dialogue ne permet pas à Béatrice d'acquérir la moindre information sur le coloriage détenu par Alain.
- Après l'échange, Béatrice se trouve donc dans la situation suivante : elle a la certitude que la carte est bien coloriable avec trois couleurs, mais ne sait pas faire un tel coloriage et elle ne peut communiquer sa certitude à personne.

Avec ce type de schéma — utilisé en cryptographie pour concevoir des protocoles d'authentification — on découvre donc qu'une certitude mathématique, comme celle de Béatrice, peut être incommunicable[7].

Démonstrations quantiques

L'idéal classique des démonstrations claires, sans risques, communicables et vérifiables par tous est bien loin. Cependant, le pire n'est peut-être pas atteint, car le calcul quantique pourrait dans l'avenir conduire à des situations encore plus étranges. Dans le cas du coloriage à trois couleurs, un personnage de l'histoire (Alain) possède une preuve communicable. Même si Béatrice a acquis la certitude du résultat sans prendre connaissance de la preuve classique, la preuve classique existe quelque part et quelqu'un la connaît.

Avec les preuves quantiques, tout cela pourrait bien changer. L'idée du calcul quantique est d'opérer simultanément un grand nombre de calculs en parallèle en exploitant les superpositions d'états que permet la mécanique quantique. Par nature, les étapes d'un calcul quantique ne sont pas accessibles : en prendre connaissance perturberait le déroulement du calcul et le fausserait. Si un résultat mathématique était démontré par un ordinateur quantique, il se pourrait donc qu'on ne dispose pas des étapes de calcul ayant conduit au résultat. Nous serions donc dans une situation où « quelque chose » aurait prouvé le résultat, nous l'aurait communiqué, mais sans rien nous transmettre des arguments ayant conduit à celui-ci. Comme dans le cas d'Alain et Béatrice, nous aurions la certitude de la validité d'un résultat (pour peu que notre machine soit fiable), mais ici ni Alain, ni personne ne détiendraient d'éléments tangibles constituant la preuve : nous aurions acquis une certitude mathématique sans que le moindre élément de preuve ne subsiste.

Une telle situation, envisagée récemment par C. Calude, E. Calude et S. Marcus, ne s'est pas encore produite, mais si un jour nous réussissons à mettre au point des ordinateurs quantiques et que nous les utilisons pour démontrer des résultats mathématiques, dans certains cas nous nous trouverons donc avec la certitude nue qu'un énoncé est vrai.

On le voit, tant que l'être humain n'a utilisé que le crayon et le papier pour faire des mathématiques, la notion de démonstration n'a pas posé de problèmes graves, même dans le cas des *preuves sans mots*[8] qui, par jeu, apparaissent imprécises et risquées. Depuis que les ordinateurs, quantiques ou non, sont entrés dans la danse, tout est devenu plus compliqué, et il semble qu'existent maintenant des certitudes mathématiques de natures différentes. L'homme, en s'aidant des systèmes matériels complexes pour explorer le monde abstrait, se trouve avec lui dans un rapport nouveau, plus riche et plus varié qu'auparavant.

6. *http://en.wikipedia.org./wiki/Zero-knowledge proof*
7. *Pour plus de détails sur ces persuasions non transmissibles, consulter le dossier de* Pour la science *sur* L'art du secret, la cryptographie*, publié en 2002.*
8. *Voir l'article* Preuves sans mots *en page 14 de ce numéro.*