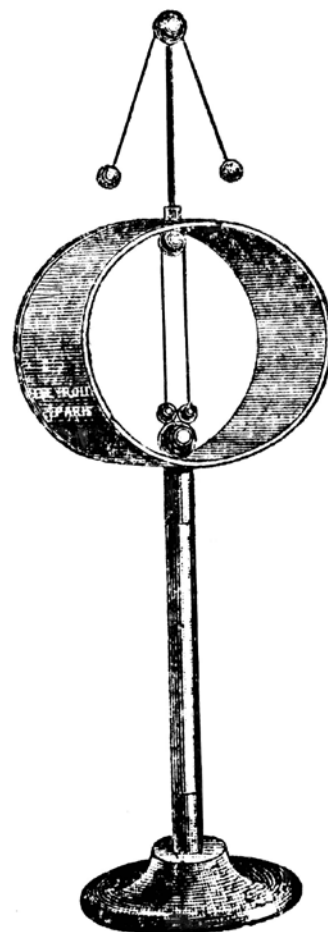




© F. Gires, Ivete Guez-de-Balzac, Angoulême

CYLINDRE OUVERT DE MASCART

Lors d'un orage, l'électricité atmosphérique reste à la surface des carrosseries métalliques des automobiles ou des avions, et les passagers sont protégés. C'est le même phénomène que met en évidence le dispositif imaginé par Eleuthère Mascart, professeur de physique au Collège de France, dans la seconde moitié du XIX^e siècle. Un cylindre creux conducteur en laiton est isolé sur un pied de bois. Dans son prolongement, une tige métallique, fixée sur le cylindre, porte deux pendules électriques (des billes en moelle de sureau suspendues à des fils de lin). Dans le cylindre, deux autres pendules sont en contact avec sa surface intérieure. Quand on électrise le cylindre, les pendules extérieurs divergent aussitôt, tandis que ceux à l'intérieur restent immobiles. On en conclut que seule la surface extérieure est chargée. Les charges électriques sur cette surface n'exercent aucune influence sur tout point à l'intérieur du conducteur, qui forme un écran électrique pour tout ce qu'il contient.

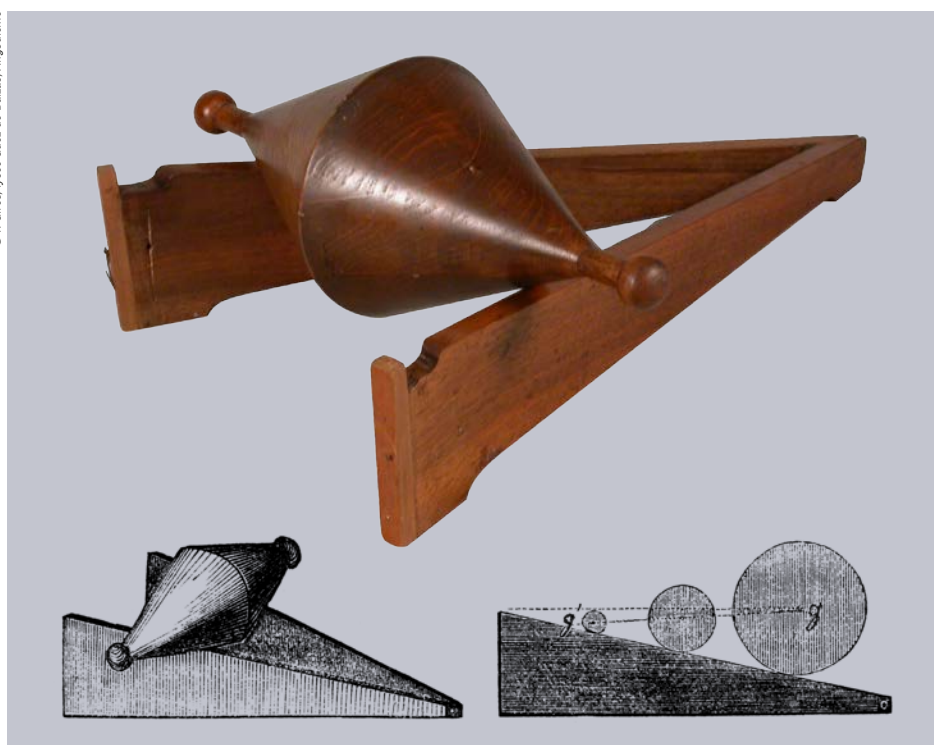


DOUBLE CÔNE DE NOLLET

« Il est beaucoup plus aisé de trouver de l'argent qu'un homme comme lui », disait Voltaire de l'abbé Jean Antoine Nollet, l'un des plus grands vulgarisateurs scientifiques européens du XVIII^e siècle. La démonstration du bicône est une des nombreuses expériences de physique décrites pour la première fois en France dans ses ouvrages. Elle illustre le fait que la stabilité d'un corps correspond à la position la plus basse de son centre de gravité, même si le mouvement qui conduit à cette position contredit l'intuition.

L'objet comporte un double cône et deux planchettes identiques formant un angle aigu entre elles. Les bords supérieurs des planchettes constituent une sorte de plan incliné. On pose le bicône sur la partie inférieure du plan incliné. Il « remonte » alors le plan en tournant, suivant ainsi un mouvement en apparence contraire à celui des corps pesants. Mais en mesurant l'altitude du centre de gravité g du bicône au cours de son mouvement, on constate qu'elle décroît. En d'autres termes, le centre de gravité descend bien quand le bicône remonte la pente, et la loi du mouvement des corps pesants est donc validée...

© F. Gires, Ivete Guez-de-Balzac, Angoulême



LOGIQUE & CALCUL

Quand considère-t-on qu'un théorème est définitivement prouvé ?

Renforcer la confiance qu'on a dans la démonstration d'un théorème difficile est possible. Il faudrait le faire pour le grand théorème de Fermat.

Jean-Paul DELAHAYE

Le « dernier théorème de Fermat » (ou « grand théorème de Fermat », ou « théorème de Fermat-Wiles ») affirme que si n est un entier supérieur à 2, alors il n'existe pas de triplets d'entiers positifs x, y, z tels que $x^n + y^n = z^n$. Il est considéré comme démontré depuis 1995. Andrew Wiles a d'ailleurs obtenu le prix Abel en 2016 pour sa contribution déterminante à la preuve de ce théorème.

Peu de gens comprennent le détail de la démonstration, dont la partie finale a été publiée par Andrew Wiles dans la prestigieuse revue *Annals of Mathematics*. Les experts compétents sont cependant tous d'accord pour dire qu'il n'y a aucune faille dans le raisonnement exposé. Depuis, plusieurs livres ont présenté aussi complètement que possible la démonstration. On peut avoir confiance : la preuve d'un théorème aussi célèbre est examinée en détail par une armée de mathématiciens intransigeants. La probabilité qu'il reste une erreur est infime.

Formaliser pour une meilleure garantie

Pourtant, les logiciens considèrent qu'on peut perfectionner la preuve et rendre le résultat plus sûr. Pourquoi ? Pour plus de certitude, il faudrait disposer d'une version formelle complète de la preuve, ou, ce qui revient au même, d'une version écrite de la preuve vérifiable par ordinateur. Les très longues preuves sont difficiles à formaliser,

car chaque pas d'un raisonnement formel, aussi infime ou évident soit-il, doit y être détaillé et se conformer à des règles fixées une fois pour toutes. Pas question dans une preuve formelle d'écrire « Le cas $n = 5$ se traite comme le cas $n = 3$ », ou les traditionnels « On vérifie aisément que... », « Laissé en exercice au lecteur » ou « Trivial ».

Les outils informatiques d'écriture des démonstrations formelles, nommés « assistants de preuve », permettent de construire progressivement et minutieusement ces preuves ultimes, et réduisent donc le risque d'erreur bien plus encore que les vérifications humaines. Mentionnons quelques théorèmes que l'on a ainsi réussi à formaliser.

– Le théorème des quatre carrés de Lagrange : tout entier positif s'écrit comme la somme de quatre carrés (par exemple, $23 = 9 + 9 + 4 + 1$).

– Le théorème fondamental de l'algèbre : un polynôme de degré n à coefficients complexes a exactement n racines (en comptant les multiplicités de celles-ci).

– Transcendance du nombre $e = \exp(1) = 2,718\ 281\ 828\ 459\dots$: e n'est la racine d'aucun polynôme à coefficients entiers.

– Le premier théorème d'incomplétude de Gödel : tout système formel non contradictoire pour l'arithmétique ou une théorie plus puissante permet d'exprimer des énoncés E qu'il ne peut pas démontrer, et dont il ne peut pas démontrer la négation, non(E).

– Le théorème des nombres premiers de Hadamard et de La Vallée Poussin : la

densité des nombres premiers autour de l'entier n est approximativement $1/\ln(n)$.

Notons aussi que les cas particuliers du théorème de Fermat-Wiles pour $n = 3$ et $n = 4$ ont été vérifiés par la méthode des assistants de preuve.

Reste que certaines preuves humaines sont trop complexes encore pour qu'on ait su les transformer en preuves informatiques. C'est le cas pour le grand théorème de Fermat. Il y a une raison profonde à cette difficulté de formalisation, qui est un sujet de préoccupation pour les logiciens lié à la façon dont un résultat mathématique prend du sens. Le programme de travail supplémentaire qu'ils mènent sur la preuve d'Andrew Wiles est une tentative utile de limiter les hypothèses implicites sur lesquelles la preuve aujourd'hui admise s'appuie, en même temps d'ailleurs qu'une approche pour aboutir à l'écriture d'une preuve formelle.

Notons que les assistants de preuve, qu'il ne faut pas confondre avec les outils de démonstration automatique (qui, eux, cherchent les démonstrations) ne font qu'aider le mathématicien : celui-ci reste aux commandes et propose les éléments organisant les démonstrations. Selon Wim Hesselink, spécialiste néerlandais du sujet, « Ces outils ne sont presque jamais capables de prouver seuls un théorème. Ils vérifient la validité des arguments que les humains leur présentent. »

Pour comprendre pourquoi travailler à améliorer et à reformuler la preuve

Le dernier théorème de Fermat

L'énoncé de ce théorème est simple : « Si n est un entier supérieur à 2, il n'existe pas d'entiers positifs (non nuls) x, y, z tels que $x^n + y^n = z^n$. Pour $n = 2$, il existe une infinité de tels triplets, par exemple (3, 4, 5) puisque $3^2 + 4^2 = 5^2$.

On pense que Fermat disposait de la démonstration pour $n = 4$.

Le cas $n = 3$ a été démontré par Leonhard Euler vers 1760. Le cas $n = 5$ a été prouvé par Adrien-Marie Legendre et Johann Dirichlet en 1825. Le théorème a été démontré jusqu'à $n = 36$ par Ernst Kummer en 1847. En 1976, Samuel Wagstaff publia une preuve du théorème de Fermat pour tous les entiers compris entre 3 et 1 million.

L'énoncé a été formulé par Pierre de Fermat dans une note écrite dans la marge d'un livre de Diophante, dont l'exemplaire est aujourd'hui perdu.

Plus de trois siècles ont été nécessaires pour qu'une preuve publiée soit reconnue correcte.

Elle est due, pour la partie finale, au mathématicien britannique Andrew Wiles qui en présenta une première version en 1993, et en compléta certaines insuffisances en 1994 avec l'aide de Richard Taylor. Le fait que Fermat ait écrit qu'il disposait d'une jolie preuve du théorème est aujourd'hui considéré comme très probablement dû à une erreur de sa part. C'est principalement par les idées et outils mis en œuvre pour démontrer le résultat qu'il est considéré comme mathématiquement très important.

La preuve repose, entre autres, sur des méthodes et

résultats d'Alexandre Grothendieck et Pierre Deligne. Elle est en définitive fondée sur des systèmes logiques puissants mettant en œuvre des objets mathématiques infinis allant bien au-delà des entiers.

Les logiciens s'interrogent aujourd'hui sur l'utilisation de ces objets à la fois très abstraits et logiquement plus risqués que les entiers. Ils tentent de formuler des preuves du théorème de Fermat qui n'utilisent que les entiers (donc jamais explicitement d'objets infinis).

Ils essaient même de se limiter à des raisonnements simples sur ces entiers tels qu'ils sont définis par le système formel EFA (voir page 83). Obtenir une preuve du théorème de Fermat vérifiable par ordinateur semble aujourd'hui encore hors de portée.



PIERRE DE FERMAT



ANDREW WILES, EN 2016

© Domaine public

© Audun Braastad (www.abelprix.no)

d'Andrew Wiles a un sens, revenons à la notion de système formel. Les progrès de la logique mathématique ont conduit, au début du XX^e siècle, à une situation étonnante et à vrai dire inattendue. On a réussi à identifier de manière parfaite les règles de raisonnement mises en œuvre en mathématiques, et à les exprimer de façon suffisamment précise pour que la vérification d'une démonstration, dont le mathématicien écrit chaque pas dans ce système de règles, soit faisable mécaniquement, c'est-à-dire sans intelligence. Aujourd'hui, bien sûr, ce « faisable mécaniquement » renvoie à des ordinateurs et des programmes informatiques.

Quand on s'intéresse aux nombres entiers, on tente de formaliser les raisonnements dans le système de l'arithmétique de Giuseppe Peano (qu'on notera PEANO) qui, en particulier, permet les raisonnements par récurrence. On envisage parfois des

systèmes plus faibles, c'est-à-dire disposant de moins de moyens de raisonnement.

Pour traiter d'ensembles infinis d'entiers, de nombres réels comportant une infinité de décimales, de fonctions continues et d'objets plus riches encore tels que des ensembles de fonctions ou des espaces de dimension infinie, on envisage divers systèmes formels.

Plusieurs systèmes formels

Le système le plus souvent retenu est celui de la théorie des ensembles, formalisé au début du XX^e siècle et noté ZFC pour « Zermelo-Fraenkel avec axiome du choix ». Il permet de manipuler directement des objets infinis qui n'existent pas dans PEANO, mais il est plus puissant pour une autre raison : supposer que ZFC est non contradictoire permet de démontrer que PEANO

est non contradictoire, alors que l'inverse est impossible.

Rarement, mais cela arrive, la théorie des ensembles usuelle ZFC n'est pas suffisante. Si, par exemple, on veut parler de toutes les fonctions, ou de tous les groupes et raisonner globalement sur leurs structures et les liens entre ce type de structures (c'est ce que fait la théorie des catégories), on rencontre une ennuyeuse difficulté. En effet, ni « L'ensemble de tous les ensembles », ni « L'ensemble de toutes les fonctions », ni « L'ensemble de tous les groupes », etc., ne sont des ensembles au sens de ZFC, qui ne connaît que les collections d'objets mathématiques de taille limitée. Exprimer les propriétés des grandes structures et les raisonnements qui les concernent exige alors des systèmes formels plus puissants. On utilisera par exemple ceux qu'on obtient à partir de ZFC en ajoutant des axiomes affirmant l'existence d'ensembles très grands.