LOGIQUE & CALCUL

Les longues démonstrations sont-elles vérifiables ?

En mathématiques, certaines démonstrations font plusieurs centaines de pages, voire plus. Comment s'assurer qu'elles sont dépourvues de toute erreur ? L'ordinateur devient dans ce domaine un précieux assistant.

Jean-Paul DELAHAYE

À l'école ou au lycée, une démonstration d'une page nous semblait longue et difficile. Ceux qui ont poursuivi des études scientifiques ont étudié des démonstrations de plusieurs pages. Les mathématiciens connaissent tous des exemples de démonstrations dépassant la dizaine de pages, comme celle indiquant que la densité de nombres premiers autour de l'entier n est de l'ordre de $1/\ln(n)$, pour n grand.

Plusieurs questions se posent au sujet de tels raisonnements mathématiques de grande taille. Existe-t-il une limite à la longueur des preuves que proposent les mathématiciens sans utiliser de machines ? Quelles sont les preuves les plus longues aujourd'hui ? Est-il raisonnable de leur accorder notre confiance ? Que changent les ordinateurs ? Quelle est la valeur d'une preuve informatique si longue qu'aucun humain ne pourra jamais la vérifier ? Les ordinateurs aident-ils à garantir la justesse des preuves ?

En 1935, Maurice Lecat publiait à Bruxelles un étrange livre intitulé *Erreurs de mathématiciens, des origines à nos jours.* Il y recensait 500 erreurs commises par 350 mathématiciens, parmi lesquels Cauchy, Chasles, Euler et Gauss. Il expliquait : « En général, plus grand est un mathématicien, plus il est fécond et plus lourd est son casier. Il n'y a pas là matière à scandale. Si l'œuvre s'étend, par exemple, sur une soixantaine de forts *in-quarto*, comme c'est le cas pour Euler, on conçoit que quelques inadvertances aient pu être commises. Ainsi que l'a écrit Goethe, ″Il est trop facile à ceux qui ne proposent rien d'intelligent de ne point se tromper″. »

Le théorème géant, une preuve en 15 000 pages

Si l'on envisageait une mise à jour de l'ouvrage, plusieurs tomes seraient sans doute nécessaires, le nombre de publications mathématiques ayant explosé depuis 1935. Comme les longues démonstrations sont davantage susceptibles de contenir des erreurs, on doit se demander si, au-delà d'une certaine taille, il est encore possible qu'une démonstration soit juste.

La démonstration du théorème de classification des groupes finis simples, un théorème d'algèbre qui énumère la totalité des possibilités pour les structures élémentaires de groupes, est un cas extrême. On la considéra achevée vers 1980. On évalua alors qu'elle occupait 15 000 pages dispersées dans plus de 500 articles publiés par plus de 100 auteurs différents. Le résultat a été qualifié de « théorème géant » (*voir l'article de Daniel Gorenstein dans Pour la Science de février 1986*). Comme aucun mathématicien ne prétend l'avoir lue et comprise entièrement, la démonstration est jugée fragile.

Alma Steingart, une anthropologue et historienne des sciences du MIT, fait remarquer que la démonstration s'appuie sur l'existence d'une étroite communauté de chercheurs qui en dispose collectivement, sans qu'elle soit disponible aux non-spécialistes du sujet. En conséquence, la preuve du théorème est menacée d'oubli, comme les savoir-faire des artisans quand l'industrie les étouffe. Pour Alma Steingart, « les articles qui constituent la démonstration sont si éparpillés que personne, en dehors des théoriciens des groupes, ne sait comment les regrouper et les assembler ».

Daniel Gorenstein, coordinateur lors de l'élaboration de cette démonstration éclatée, disait lui-même : « Profondément enterrée dans les pages poussiéreuses de journaux oubliés, elle sera progressivement perdue pour le monde vivant des mathématiciens. » Plusieurs chercheurs, dont Jean-Pierre Serre, médaillé Fields et lauréat du prix Abel, ont exprimé des doutes sur la

Exemples de longues démonstrations

Les longues démonstrations ne sont pas rares en mathématiques, mais certaines le sont tellement qu'on a du mal à imaginer comment elles sont conçues. Voici, en plus des cas mentionnés dans l'article, quelques exemples de longues démonstrations.

POLYGONE À 65 537 CÔTÉS

Le mathématicien allemand Johann Hermes (1846-1912) publia en 1894 les détails de la construction à la règle et au compas d'un polygone régulier à 65 537 côtés. L'existence d'une telle construction résulte du théorème de Gauss-Wantzel qui énonce une condition nécessaire et suffisante sur n (n est le produit de nombres premiers de Fermat distincts – c'est-à-dire de la forme $2^{2^n}+1$ – et d'une puissance de 2) pour que le polygone régulier à n côtés soit constructible à la règle et au compas. Le procédé de Hermes s'étale sur 200 pages. La mise au point de cette démonstration lui demanda plus de dix années. Le nombre 65 537 est le cinquième nombre premier de Fermat.

DÉCOMPOSITION PRIMAIRE

La démonstration en 1905 par le mathématicien et joueur d'échecs allemand Emanuel Lasker (1868-1941) du théorème de « décomposition primaire » recouvre une centaine de pages. Celui qui fut champion du monde d'échecs pendant 27 ans (un record) proposait une généralisation du théorème de décomposition des nombres entiers en produits de nombres premiers. Aujourd'hui, grâce aux progrès de l'algèbre, on démontre ce théorème en quelques dizaines de lignes.

LES QUATRE COULEURS

Le théorème des quatre couleurs indique que toute carte tracée sur un plan se colorie avec quatre couleurs sans que deux pays voisins aient la même couleur. La première démonstration par Kenneth Appel et Wolfgang Haken, en 1974, comportait 139 pages sans compter de longs calculs menés par ordinateur et réalisés à part. Depuis, la preuve a été un peu simplifiée et surtout, elle a été entièrement formalisée en 2005 par Georges Gonthier et son équipe, ce qui en assure la justesse. Aucune preuve écrite suffisamment courte pour être humainement vérifiable n'existe de ce théorème, dont l'énoncé est compréhensible par un enfant de quatre ans.

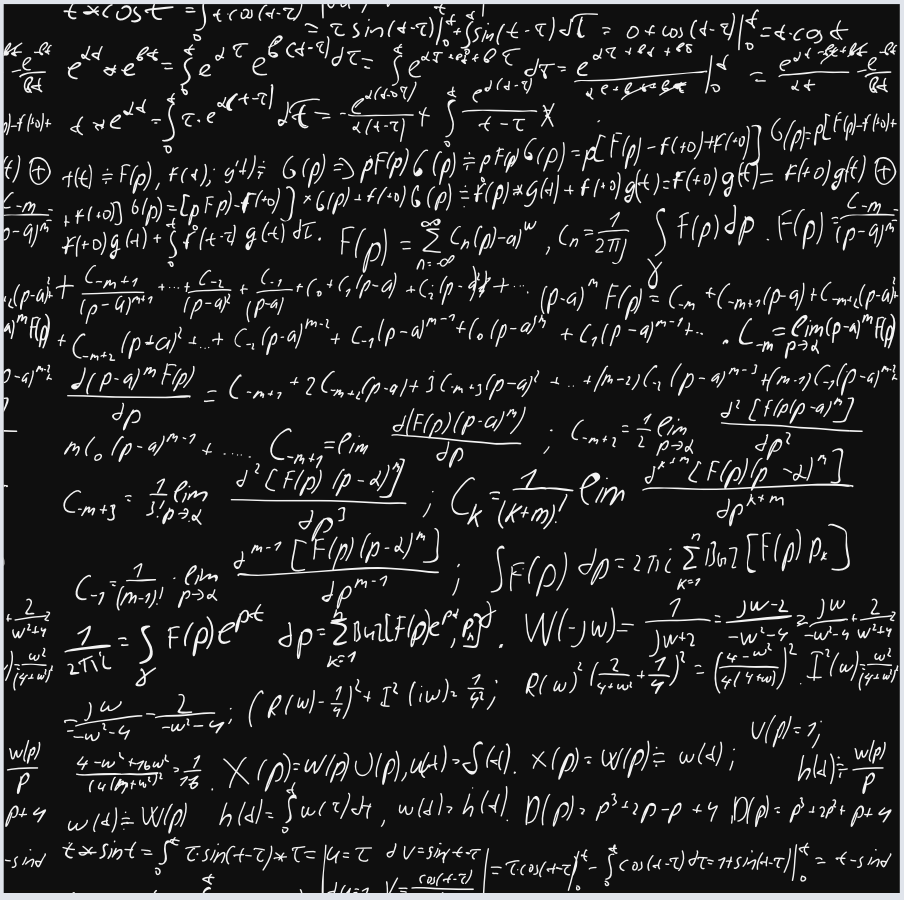
LE GRAND THÉORÈME DE FERMAT

En 1995, le Britannique Andrew Wiles démontra le théorème de Fermat affirmant qu'il n'existe aucun quadruplet d'entiers positifs a, b, c, n tel que $a^n + b^n = c^n$ avec $n > 2$. La démonstration publiée en 1995 dans *Annals of Mathematics* repose sur un grand nombre de résultats préliminaires et occupe pourtant 108 pages. Cette démonstration n'a pas encore été formalisée.

CONJECTURES DE LANGLANDS

En 2000, le Français Laurent Lafforgues établit un résultat démontrant une partie des conjectures de Robert Langlands formulées en 1967, conjectures qui établissent un lien entre arithmétique et théorie des groupes. Ce travail de plus de 600 pages valut à Laurent Lafforgues la médaille Fields en 2002. Là encore, ces preuves n'ont pas à ce jour de formalisation.

Pour d'autres exemples de longues démonstrations, voir : http://fr.wikipedia.org/wiki/Longueur_d'une_démonstration.



preuve. D'ailleurs, en 2008, Koichiro Harada et Ronald Solomon identifièrent une erreur qui, par chance, fut corrigée. Comment être certain qu'il n'en subsiste pas d'autres ?

Des mathématiciens ont réuni des morceaux de la démonstration et entrepris de la simplifier pour rédiger une démonstration de « seconde génération ». On évalue qu'elle sera longue de 5 000 pages. Six volumes ont déjà été publiés et l'on en attend autant. Une preuve de troisième génération est envisagée. Dans d'autres domaines des mathématiques, on a trouvé des théorèmes ayant des démonstrations très longues, et leur nombre se multiplie.

Depuis quelques années, grâce au réseau Internet, le travail collaboratif en mathématiques engendre la mise au point de preuves de plus en plus complexes : de nombreux mathématiciens dispersés dans le monde travaillent sur un même sujet, se corrigent et perfectionnent certaines idées et techniques prometteuses jusqu'à en tirer le maximum.

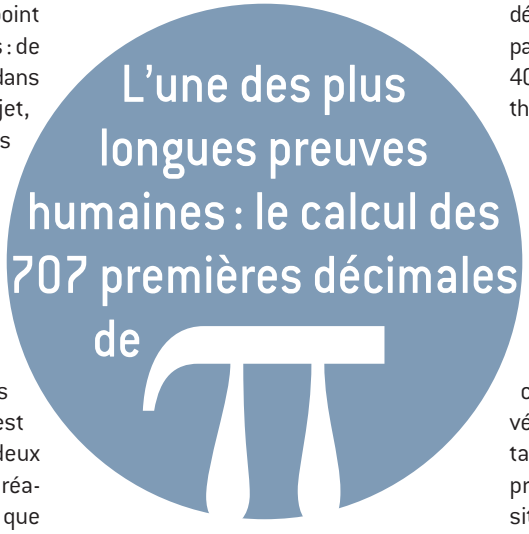
Le site *Polymath* (http://polymathprojects.org/) est un point de rencontre et de coordination pour de tels projets. Le projet 8 traite de l'écart entre nombres premiers consécutifs, et a récemment été l'objet de progrès spectaculaires. La question est : quel est le plus petit écart possible entre deux nombres premiers consécutifs qui est réalisé une infinité de fois ? On conjecture que la réponse est 2 et qu'il y a donc une infinité de nombres premiers jumeaux, tels 11 et 13, ou 17 et 19.

Une méthode introduite par le Chinois Yitang Zhang en 2013 a permis de prouver (en 53 pages) qu'il existe une infinité de couples de nombres premiers dont l'écart est inférieur à 70 000 000. Après de considérables efforts et plusieurs dizaines d'étapes de perfectionnement, les participants au projet *Polymath,* conduit par Terence Tao, réussirent à établir le résultat pour 4 680 au lieu de 70 000 000. L'article collectif signé *D. H. J. Polymath* présentant la démonstration occupe 165 pages. Depuis, d'autres progrès ont eu lieu et conduit à la borne 246, démontrée dans un nouvel article collectif plus court… de 80 pages.

Un autre domaine où les preuves sont très longues est la théorie des graphes. Par exemple, le théorème des mineurs *(voir « Une propriété cachée des graphes », Pour la Science d'avril 2008)* exige une démonstration de 500 pages. Tout cela est impressionnant et pourtant il existe des démonstrations bien plus longues depuis longtemps.

Calculer, c'est démontrer

En effet, il n'est pas absurde d'assimiler « calcul » et « démonstration ». Calculer, en respectant les règles et en détaillant chaque étape, que par exemple 2^{10} vaut 1 024, c'est démontrer que $2^{10} = 1\,024$.



À l'inverse, quand on écrit soigneusement toutes les étapes d'une démonstration, on opère une sorte de calcul.

Pour qui accepte ce point de vue, adopté en logique mathématique, la démonstration de William Shanks (1812-1882) figure parmi les plus longues démonstrations menées exclusivement à la main. Ce Britannique détermina 707 décimales du nombre π et il les publia en 1876. Son calcul l'a occupé plus d'une dizaine d'années et a exigé, pour écrire les opérations, plusieurs milliers de feuilles de papier. Malheureusement, le « théorème de Shanks » est faux à partir de la 528e décimale, ce dont on ne s'aperçut que 70 ans plus tard par un calcul mobilisant cette fois des machines à calculer mécaniques de bureau. Le long délai écoulé avant que l'on s'aperçoive de l'erreur prouve l'exploit de Shanks. En ne considérant que les 527 premières décimales de π, il serait juste et charitable de considérer que Shanks a démontré un vrai théorème dont la preuve a été très longue, et qui est peut-être la plus longue de toutes les preuves menées par un humain sans l'aide de machine.

Aujourd'hui, le record de calcul des décimales de π est 13 300 000 000 000 (il date d'octobre 2014), et la longueur de la preuve associée à ce nouveau record dépasse largement les 15 000 pages du théorème de classification des groupes finis simples. Écrire le résultat, ce qui est beaucoup court que le détail du calcul, à raison de 2 000 caractères par page, nécessiterait six milliards de pages, 400 000 fois plus que les 15 000 pages du théorème géant !

La démonstration du théorème selon lequel aucun sudoku 9×9 ne comportant que 16 données initiales n'a de solution unique (*voir cette rubrique dans Pour la Science de janvier 2015*) a été obtenue par un énorme calcul : il a duré plus d'un an et a mis en œuvre un puissant dispositif de machines. Comme dans le calcul de π, il faut refaire le calcul pour vérifier le résultat, car les détails des résultats intermédiaires qui constitueraient la preuve n'ont pas été conservés. Étrange situation : la preuve est si longue qu'on en confie la réalisation à des machines, mais on ne cherche même pas à en préserver un exemplaire !

Notons que la résolution de certains problèmes, tels que la factorisation d'un grand entier, exige beaucoup de calculs, mais que la vérification du résultat est courte. Dans un tel cas, même en assimilant calculs et démonstrations, il n'est pas vrai qu'on a affaire à une longue démonstration : pour prouver que l'entier a se factorise en bc, qu'importe qu'on ait passé des jours ou des mois à trouver b et c, il suffit de calculer le produit bc et de vérifier que le résultat est a.

Certains contestent qu'un calcul soit une démonstration et refuseront donc de considérer que le théorème du sudoku minimal ou celui donnant les décimales de π

a nécessité une longue démonstration. Mais un exemple récent montre que la question est délicate, et qu'il y a des situations où rien ne permet de distinguer calculs et démonstrations.

En 1930, le Hongrois Paul Erdős conjectura que, de toute suite infinie $x_1, x_2, ..., x_n, ...$ formée de +1 et de –1, on peut extraire une sous-suite de la forme $x_d, x_{2d}, x_{3d}, ..., x_{kd}$ (les indices constituent une suite arithmétique) dont la somme des éléments est, en valeur absolue, supérieure à 2 :

$|x_d + x_{2d} + x_{3d} + ... + x_{kd}| > 2$.

L'idée est qu'il est impossible d'équilibrer les +1 et les –1 simultanément pour toutes les sous-suites « d'indice arithmétique » et que l'on sort inévitablement de l'intervalle [–2, +2] pour certaines suites extraites. Erdős conjectura le résultat aussi avec +3 et –3 au lieu de +2 et –2, et même avec +*K* et –*K* à la place de +2 et –2 pour tout entier *K*. Ce problème est dénommé en anglais problème de la *Discrepancy* (écart). Nous noterons *Discrep* (*K*) la conjecture correspondant à l'entier *K*. Le seul cas facile est *Discrep* (1) qu'on peut traiter à la main (voir https://www.youtube.com/watch?v=pFHsrCNtJu4).

Il se peut que *Discrep* (*K*) soit vraie pour tous les entiers *K*, ou qu'elle soit vraie pour tous les entiers jusqu'à une certaine valeur maximale à partir de laquelle la conjecture devient fausse. Nul ne le sait !

Le problème est resté irrésolu pendant 80 ans, y compris dans sa version élémentaire *Discrep* (2). La question est un problème majeur de la théorie combinatoire des nombres. Un projet *Polymath* s'est intéressé à la conjecture et a conduit Boris Konev et Alexei Lisitsa, de l'Université de Liverpool, à le résoudre en février 2014... d'une façon très surprenante.

Un cheminement logique

Ces chercheurs ont traduit le problème en un ensemble de formules logiques du calcul des propositions et ont demandé à un programme capable de traiter ce type de formules de s'y attaquer.

Soyons plus précis : Boris Konev et Alexei Lisitza ont écrit sous la forme d'une énigme logique la recherche d'une suite de longueur 1 161 telle que toutes les sous-suites considérées (celles dont les indices forment une suite arithmétique *d*, 2*d*, ... *kd*) ont une somme qui reste comprise entre –2 et +2. Une recherche précédente leur avait montré que pour 1 160, une telle suite existe *(voir la figure page ??)*. Le programme a prouvé qu'il n'existe pas de solution de longueur 1161, donc qu'*a fortiori* il n'en existe pas de longueur infinie, ce qui établit *Discrep* (2).En langage de mathématicien, le programme a montré que le problème logique posé est insatisfiable. L'important est qu'un tel programme mène à une démonstration par l'absurde en utilisant des pas de raisonnement du type :

Si (A ou non-B) et (A ou B), alors A.

Non seulement le programme fournit la réponse « Non, le problème logique n'a pas de solution », mais il produit un « certificat de non-satisfiabilité » qui est une écriture détaillée des étapes du raisonnement. Un tel certificat peut être confié à un programme indépendant de celui qui l'a trouvé. Cela a d'ailleurs été fait, et l'on

Où William Shanks s'était-il trompé ?

William Shanks (1812-1882) a mené seul l'un des calculs les plus fous jamais entrepris : déterminer à la main la valeur du nombre π avec une précision de 707 chiffres après la virgule. On peut considérer son calcul comme une sorte de démonstration mathématique géante.

Les 707 décimales du résultat ont été utilisées lors de la création de la salle π du Palais de la découverte en 1937... et corrigées quand on a compris que Shanks s'était trompé.

Afin d'avoir une idée du travail accompli par Shanks, voici, avec une précision de cinq chiffres après la virgule, ce que donne l'utilisation de sa méthode en prenant trois termes du développement en série de la fonction Arctan *x* :

$\pi \approx 4\,(4\,\text{Arctan}\,1/5 - \text{Arctan}\,1/239)$;

$\text{Arctan}\,x \approx x - x^3/3 + x^5/5$;

$\text{Arctan}\,1/5 \approx 0{,}20000 - 0{,}00267 + 0{,}00006 = 0{,}1973$;

$\text{Arctan}\,1/239 \approx 0{,}00418 - 0{,}00000 + 0{,}00000 = 0{,}00418$;

$\pi \approx 4\,(4 \times 0{,}1973 - 4 \times 0{,}00418) = 3{,}14152$.

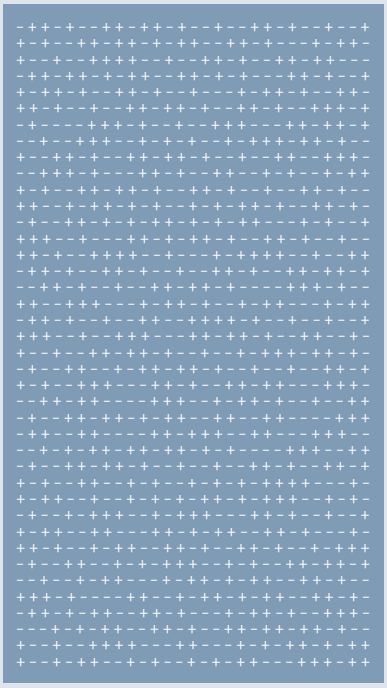
Pour arriver à son résultat, Shanks dut évaluer non pas trois termes, mais plus de 400. Le résultat qu'il trouva est faux à partir de la 528e décimale. Une analyse rétrospective indique qu'il omit de recopier un zéro en position 530 du terme 248 du calcul de Arctan (1/5). La rectification de cette erreur permet en effet de corriger 39 chiffres du résultat de Shanks. Cependant, cela n'explique pas tout et d'autres inattentions se sont glissées dans ses opérations *(voir l'article de B. Hayes,* Pencil, paper and pi, *American Scientist, vol. 102/5, pp. 342-345, sept.-oct. 2014)*.

On peut aussi se tromper dès la première décimale, comme l'illustre ce raisonnement/calcul erroné (cherchez l'erreur !) :

$x = (\pi + 3)/2 \Rightarrow 2x = \pi + 3 \Rightarrow$
$2x\,(\pi - 3) = (\pi + 3)\,(\pi - 3) \Rightarrow$
$2\pi x - 6x = \pi^2 - 9 \Rightarrow$
$9 - 6x = \pi^2 - 2\pi x \Rightarrow$
$9 - 6x + x^2 = \pi^2 - 2\pi x + x^2 \Rightarrow$
$(3 - x)^2 = (\pi - x)^2 \Rightarrow 3 - x = \pi - x$
$\Rightarrow \pi = 3$.

Une démonstration vraiment très longue

La suite ci-contre de 1160 symboles « + » et « – », disposée en 40 lignes de 29 symboles, a une remarquable propriété d'équilibre. Si l'on en retire des termes régulièrement espacés, par exemple ceux en positions 3, 6, 9, 12, 15, 18, 21, alors l'écart entre le nombre de « + » et le nombre de « – » sera toujours inférieur ou égal à 2. Cette propriété d'équilibre est vérifiée pour toutes les suites correspondant à des positions du type *p*, 2*p*, 3*p*, ..., *kp*.



En particulier, pour $p = 1$ et $k = 1160$, on vérifie qu'il y a 581 « + » et 579 « – », et pour $p = 2$, $k = 10$ on trouve cinq « + » et cinq « – » bien disposés. Plus remarquable et difficile à démontrer : il n'existe aucune suite infinie de signes « + » et « – » ayant la même propriété.

Cette affirmation est la conjecture *Discrepancy* de Paul Erdős pour $K = 2$. Erdős la formula il y a 80 ans pour K quelconque ($K \geq 1$) et promit 500 dollars à qui la démontrerait. Seul le cas particulier $K = 2$ vient d'être démontré, à l'aide d'un ordinateur ; ce dernier a mené un raisonnement par l'absurde conduisant à la conclusion qu'une suite de longueur 1161 au plus ne pouvait avoir la propriété d'équilibre attendue. La première démonstration produite par l'ordinateur occupait 13 milliards de caractères, soit 13 000 ouvrages d'un million de caractères. C'est sans doute la plus longue démonstration jamais proposée en mathématiques. Le fichier la contenant a été confié à un programme indépendant de celui qui l'a trouvé, et a confirmé que la démonstration est correcte. Bien évidemment, jamais aucun humain ne sera capable d'effectuer seul un tel contrôle. La démonstration trouvée grâce au travail de Boris Konev et Alexei Lisitsa, de l'Université de Liverpool, n'a pas été imprimée et la publication qui décrit comment la conjecture de Erdős a été démontrée n'occupe que huit pages. La preuve de 13 gigaoctets, ce qui est autant que toute l'encyclopédie *Wikipedia*, n'a même pas pu être mise en ligne. On s'évertue à la simplifier ; les chercheurs ont réussi à obtenir une preuve plus concise... de 850 millions de caractères qui, elle aussi, a été contrôlée par un programme indépendant.

Beaucoup de mathématiciens pensent aujourd'hui qu'une preuve obtenue avec l'aide d'un ordinateur et soumise à des tests de confirmation (comme cela a été le cas ici) a bien moins de risques de receler une erreur qu'une preuve que seuls des mathématiciens ont vérifiée.

a donc une confirmation informatique indépendante que la démonstration de *Discrep* (2) est juste. Ici, les machines raisonnent et se surveillent les unes les autres pour limiter le risque d'erreur.

Pour autant, pas question de publier la preuve dans un livre ou un journal. En effet, la taille de la démonstration est de 13 gigaoctets, soit 13 milliards de caractères, ou 13 millions de pages de 1 000 caractères, qui occuperaient 13 000 ouvrages de 1 000 pages si l'on avait la folie de l'imprimer. On a évoqué une preuve « *Wikipédia-longue* », puisque le texte de la démonstration de *Discrep* (2) occuperait autant d'espace que tous les articles proposés par *Wikipédia*. On évalue par exemple à 2 000 volumes la taille de l'encyclopédie *Wikipedia* en langue anglaise. Depuis sa découverte en février 2014, la preuve a pu être simplifiée un peu : aujourd'hui, on dispose d'une démonstration de 850 millions de caractères (soit 850 ouvrages de 1 000 pages, chaque page ayant 1 000 caractères).

Bien sûr, et personne ne le conteste, la preuve est ici moins variée que celle du théorème de classification des groupes finis simples. Elle est longue et difficile, mais est assez répétitive dans son principe : une immense armée de mathématiciens courageux et organisés pourrait en entreprendre le contrôle. Pour la classification des groupes, la preuve fait intervenir des raisonnements touchant des domaines variés et subtils, et il est beaucoup plus difficile d'organiser la vérification ou de raccourcir la longueur de la démonstration.

L'écriture d'une preuve n'utilisant qu'un nombre fini de règles bien identifiées de raisonnement (sa formalisation) est pour l'instant trop difficile pour le théorème de classification des groupes finis simples. Pourtant, c'est sans doute le seul moyen à terme d'avoir une certitude de sa justesse.

Des assistants de preuve

Au contraire de la conjecture *Discrep* (2), la diversité des méthodes et techniques utilisées dans la démonstration du théorème de classification est telle qu'il est inconcevable qu'un programme produise seul cette formalisation. Aussi a-t-on développé des outils nommés *assistants de preuve (voir « Du rêve à la réalité des preuves », rubrique d'avril 2011)*, lesquels aident à la mise au point de telles formalisations en dialoguant avec un mathématicien qui connaît et comprend la preuve à contrôler.

L'une des étapes de la démonstration du théorème de classification des groupes finis simples est la démonstration du théorème de Feit-Thompson qui affirme que tout groupe fini simple ayant un nombre impair d'éléments est résoluble. Un groupe résoluble peut s'obtenir à partir de groupes plus simples, comme un nombre composé s'obtient comme produit de nombres premiers. Ce théorème, conjecturé en 1911 par l'Anglais William Burnside, a été démontré en 255 pages par Walter Feit et Griggs Thompson en 1963, aux États-Unis.

La vérification du théorème de classification des groupes finis simples exige que l'on vérifie le théorème de Feit-Thompson. Or la meilleure vérification possible consiste à en produire une formalisation qui, comme pour la conjecture d'Erdős relative à $K = 2$, sera mécaniquement contrôlable.

Une preuve formelle grâce à *Coq*

Cela a été fait récemment par une équipe de l'Inria, en France. En utilisant le logiciel *Coq* (un assistant de preuves ayant déjà servi à formaliser la preuve du théorème des quatre couleurs), Georges Gonthier et ses collègues ont démontré formellement le théorème de Feit-Thompson. Une partie du théorème de classification des groupes finis simples est ainsi validée.

L'intérêt de ce travail, qui a exigé six années d'efforts, est qu'il a obligé à formaliser en *Coq* de nombreux résultats de base d'algèbre, ce qui permettra désormais d'attaquer plus facilement toutes sortes de problèmes… dont, un jour peut-être, le théorème géant lui-même. Il ne faut cependant pas espérer que cela soit rapide : avant une formalisation à l'aide de *Coq*, il faudra que la démonstration de seconde, voire de troisième, génération soit disponible. Nous n'y sommes pas !

Dans le cas du théorème de Feit-Thompson, Georges Gonthier et ses collègues précisent : « Notre développement comporte 150 000 lignes de schémas de preuves, environ 4 000 définitions et plus de 13 000 théorèmes intermédiaires. Les 250 pages de la preuve existante et servant de base ont été traduites en 40 000 lignes de formalisations, ce qui correspond à une multiplication par environ 4 ou 5 de la longueur du texte informel. Durant la formalisation, nous avons dû corriger et réécrire certains arguments du texte que nous suivions, mais le plus long travail pour l'aboutissement du projet a été de mettre au point les bibliothèques mathématiques de base. »

Situation retournée

Nous sommes loin de l'époque où l'utilisation d'un ordinateur pour une démonstration ou une partie de démonstration heurtait certains philosophes. Quand on utilise l'ordinateur, on met en place des procédures de contrôle nombreuses et rigoureuses, entraînant en particulier la possibilité d'opérer une vérification par un système indépendant de celui qui trouve la preuve ou aide à l'écrire. Il en résulte qu'il n'y a plus aucune raison de refuser l'aide de l'ordinateur. C'est même lui qui, seul, donne accès à certaines questions.

La situation s'est en quelque sorte retournée : le raisonnement humain ne contrôle pas le raisonnement de la machine, c'est l'inverse. L'aboutissement en 2014 du projet de formalisation de la preuve du théorème de Hales (qui résout la conjecture de Kepler sur l'empilement de sphères le plus dense) est un autre exemple majeur de vérification par l'ordinateur d'une preuve dont on ne parvenait pas à être certain de l'exactitude.

Armés de ces outils, les mathématiciens peuvent aborder des questions qu'il leur était inconcevable de traiter auparavant. L'ordinateur n'est plus regardé avec méfiance. Il ne faut pas confondre ce qu'il démontre ou calcule sans précaution (que ce soit un élément partiel de raisonnement, ou un résultat complet) avec ce qu'il calcule et démontre en fournissant sous la forme de fichiers informatiques des « certificats » autorisant des contrôles indépendants *a posteriori*. Un calcul, même par ordinateur, est parfois faux, nous le savons bien : des outils de vérification doivent donc toujours accompagner les résultats prétendument démontrés par l'informatique. Quand c'est le cas, la certitude devient presque parfaite. ■

L'AUTEUR

J.-P. DELAHAYE est professeur émérite à l'Université de Lille et chercheur au Centre de recherche en informatique, signal et automatique de Lille (CRISTAL).

BIBLIOGRAPHIE

B. Konev et A. Lisitsa, **A SAT attack on the Erdős discrepancy conjecture**, *Theory and Applications of Satisfiability Testing - SAT 2014*, pp. 219-226, Springer, 2014.

D. H. J. Polymath, **The « bounded gaps between primes » Polymath project – a retrospective**, http://arxiv.org/abs/1409.8361, sept. 2014.

G. Gonthier *et al.*, **A machine-checked proof of the odd order theorem**, *4th Conference on Interactive Theorem Proving*, Springer, LNCS 7998, pp.163-179, 2013.

Références supplémentaires sur www.pourlascience.fr

Retrouvez la rubrique Logique & calcul sur www.pourlascience.fr