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 $e = \exp(1) = 2{,}718\,281\,828\,459\ldots$: 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.

© Domaine public

PIERRE DE FERMAT

© Audun Braastad (www.abelprize.no)

ANDREW WILES, EN 2016

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.

Si l'énoncé de Fermat est indécidable, alors il est vrai !

Une question naturelle se pose à propos des énoncés arithmétiques E tels que celui affirmant que tout nombre pair à partir de 4 est somme de deux nombres premiers (conjecture de Goldbach) ou l'énoncé du théorème de Fermat : « Se peut-il que E soit indécidable, c'est-à-dire que ni E ni sa négation, non(E), ne soient démontrables ? »

La question, posée dans l'absolu, n'a pas de sens. Il n'y a pas de notion de démonstration dans l'absolu, mais seulement des notions relatives à des systèmes formels comme PEANO, ZFC ou INAC évoqués dans l'article. Il faut donc reformuler la question et se demander par exemple : Est-il possible que le système PEANO ne puisse démontrer ni E, ni non(E) ? Autrement dit : E est-il un indécidable de PEANO ?

On connaît des indécidables de PEANO (par exemple l'énoncé qui affirme que PEANO est non contradictoire). La question n'est donc pas absurde et c'est d'ailleurs cette question qui est posée par les recherches évoquées dans l'article à propos du théorème de Fermat. La plupart des mathématiciens pensent que l'énoncé de Fermat n'est sans doute pas un indécidable de PEANO, bien qu'aujourd'hui ce ne soit pas démontré.

Cependant, si, en utilisant par exemple les moyens de ZFC (ou INAC), on démontrait que l'énoncé de Fermat est indécidable dans PEANO, alors on disposerait automatiquement d'une nouvelle preuve du théorème de Fermat dans la théorie qui aurait prouvé l'indécidabilité.

En effet, PEANO a la propriété que tous les énoncés élémentaires du type « $3+7=10$ », « $2^3+3^3\neq5^3$ », « 13 est un nombre premier » sont démontrables dans PEANO quand ils sont vrais. PEANO ne passe à côté d'aucune démonstration pour des vérités arithmétiques aussi élémentaires.

La preuve dans ZFC (ou dans INAC) de l'indécidabilité dans PEANO du théorème de Fermat démontrerait, pour chaque quadruplet d'entiers n, x, y, z avec $n>2$ et x, y, z non nuls, que PEANO n'établit pas $x^n+y^n=z^n$ (dans le cas contraire, PEANO fournirait un contre-exemple à l'énoncé de Fermat, lequel serait donc décidable), donc que PEANO démontrerait que $x^n+y^n\neq z^n$ (puisque PEANO ne manque aucun énoncé de cette forme). En simplifiant un peu : si l'énoncé de Fermat est indécidable, alors il est vrai.

La même propriété est vraie pour la conjecture de Goldbach. Celui qui démontrerait qu'elle est indécidable dans PEANO en utilisant les moyens d'un système formel F, démontrerait du même coup la conjecture de Goldbach dans le système F. Il ne serait donc pas très malin, face à la difficulté qu'on a à établir la conjecture de Goldbach, de se mettre à rechercher la preuve que la conjecture est indécidable dans PEANO. L'indécidabilité de ce type d'énoncés E dans PEANO est une affirmation plus difficile à prouver que E lui-même.

On adoptera par exemple l'axiome des « cardinaux fortement inaccessibles » qui autorise certaines formes d'ensemble de tous les ensembles et autres grosses collections. Notons INAC un tel système. Si l'on admet qu'il est non contradictoire, alors on sait démontrer que ZFC l'est aussi, alors que l'inverse est impossible.

Quand on passe de PEANO à ZFC puis à INAC, on accepte l'existence d'objets de plus en plus nombreux et gros, mais le monde mathématique supposé devient aussi plus difficilement contrôlable, et on peut même, au-delà d'un certain point (qui varie selon la sensibilité de chacun), considérer ces mondes mathématiques surabondants comme illusoires. Qu'il puisse exister des entités abstraites telles que les entiers est facile à accepter. Pour les nombres réels et leurs décimales qui se prolongent à l'infini, c'est un peu plus difficile, et certains physiciens considèrent ces nombres comme des fictions commodes sans contrepartie dans le monde réel. Passer au niveau supérieur avec INAC devient un peu déraisonnable, même si les mathématiciens réussissent à penser et à démontrer des choses dans ces univers follement étendus.

Ces trois points de repère, PEANO, ZFC, INAC, ne sont que des échelons d'une série plus riche de systèmes formels envisagés par les mathématiciens et les logiciens.

Ontologie risquée

Un système formel décrit un ensemble de possibilités de manipulations de formules qui donnent à l'arrivée les théorèmes. Il ne faut pas qu'il permette de démontrer une formule absurde du type $0=1$, qui serait en contradiction avec la formule $0\neq1$ (le système serait alors incohérent, « inconsistant » ou contradictoire). En effet, dès qu'on a une contradiction, tout devient vrai et tout devient faux à la fois : plus rien n'a de sens. Passer d'un système faible (par exemple PEANO) à un système plus puissant fait prendre des risques, puisqu'on accroît l'ensemble des énoncés que l'on peut démontrer.

On sait aussi que prouver qu'on ne prend pas de risques (de rencontrer une contradiction qui détruirait tout) est impossible ou nécessairement insatisfaisant. En effet, l'une des conséquences des théorèmes d'incomplétude de Gödel est que, pour démontrer qu'un système est non contradictoire, on doit se placer dans un système plus puissant (donc plus risqué !). S'élever dans la puissance des systèmes formels fait prendre des risques de non-sens.

Ainsi, lorsqu'on s'intéresse à des énoncés sur les entiers, il est souhaitable de ne pas s'aventurer à utiliser des objets infinis, ou, ce qui revient au même, il faut rester sagement dans PEANO ou un système formel sans infini plus faible encore.

Le travail consistant à reprendre des preuves aux hypothèses ontologiques fortes pour les reconstruire dans des mondes mathématiques plus élémentaires, éventuellement sans infini, est donc un objectif raisonnable et, s'il est atteint, utile. En mathématiques, on a d'ailleurs toujours considéré que minimiser les hypothèses d'un résultat, c'est obtenir un meilleur résultat et une multitude de travaux publiés dans les revues professionnelles consistent à se débarrasser d'hypothèses qu'on a cru un moment nécessaires et qui se révèlent inutiles avec la nouvelle preuve.

Le célèbre théorème des nombres premiers qui donne leur densité et dont on dispose aujourd'hui de preuves formelles a été démontré dans un premier temps en utilisant des notions liées aux fonctions de variables complexes qui n'entrent pas dans PEANO. Les preuves de Jacques Hadamard et de Charles-Jean de La Vallée Poussin (1896) ont été reprises par Paul Erdős et Atle Selberg en 1948. Ils ont su en donner une version dite élémentaire ; en simplifiant un peu, ils ont transformé la preuve donnée initialement dans ZFC en une preuve donnée dans PEANO.

Personne n'a contesté que cette formulation de la preuve initiale dans un univers réduit était mathématiquement intéressante et Atle Selberg a obtenu une médaille Fields en 1950 en partie grâce à ce résultat. Se préoccuper du problème de ce qu'exige vraiment la preuve du grand théorème de Fermat est sans le moindre doute une authentique préoccupation mathématique.

Or, et c'est là le problème, la preuve formulée par Andrew Wiles utilise des notions et des résultats qui ne sont pas confinés à l'arithmétique de PEANO. Qui plus est, certains résultats dus en particulier à Alexandre Grothendieck et utilisés par Andrew Wiles ne prennent sens et n'ont été établis que dans des systèmes plus puissants que ZFC.

La démonstration publiée par Andrew Wiles en 1995 utilise des méthodes de géométrie algébrique. Cette discipline a connu des avancées considérables grâce aux travaux de Grothendieck, mort en 2014 après une vie de rebelle (*voir* Pour la Science *n° 467, septembre 2016*). On y considère des équations algébriques et l'ensemble de leurs solutions

Les univers d'Alexandre Grothendieck

Pour formuler et démontrer le théorème de Fermat, Andrew Wiles a utilisé des notions mathématiques (parfois seulement implicitement, en reprenant des résultats démontrés avant lui) qui n'ont de sens que dans une théorie logique (un système formel) plus puissante que celle des entiers. La théorie logique utilisée est même plus puissante que la pourtant très puissante théorie des ensembles de Zermelo-Fraenkel avec axiome du choix (ZFC), qui suffit à la plus grande partie des mathématiques.

La théorie utilisée par Andrew Wiles postule l'existence des « univers de Grothendieck », des ensembles U munis d'une relation d'appartenance « être dans » ayant les propriétés suivantes :

– si x est dans U, et que y est dans x, alors y est dans U (axiome de transitivité) ;

– si x et y sont dans U, alors la paire $\{x, y\}$ est dans U (axiome de la paire) ;

– si x est dans U, alors l'ensemble des sous-ensembles de x est aussi dans U (axiome de l'ensemble des parties) ;

– si $x \to f(x)$ est une fonction telle que x et chaque $f(x)$ sont dans U, alors la réunion de tous les $f(x)$ est aussi dans U (axiome de la réunion).

L'existence de ces univers ne peut pas être démontrée en utilisant seulement des raisonnements de ZFC, il faut ajouter à ZFC un axiome qui affirme l'existence d'ensembles très grands :

– plus grands que $\mathbb{N}$, l'ensemble des entiers ;

– plus grands que $P(\mathbb{N})$, l'ensemble des parties de $\mathbb{N}$;

– plus grands que l'ensemble $P(P(\mathbb{N}))$ des parties de $P(\mathbb{N})$, etc.

L'axiome d'existence de cardinaux fortement inaccessibles INAC bien connus des logiciens est équivalent à l'existence d'univers de Grothendieck. Cet axiome (contrairement à l'axiome du choix, ou à l'hypothèse du continu) a un effet sur les démonstrations concernant les entiers : certaines propriétés démontrables en l'utilisant et concernant exclusivement les entiers ne sont pas démontrables sans lui. La question de savoir si l'énoncé du théorème de Fermat est une telle propriété n'est pas évidente. Peu de mathématiciens envisagent que ce théorème exige vraiment d'utiliser INAC, mais prouver proprement qu'on peut se passer de INAC pour démontrer l'énoncé de Fermat n'est pas facile. Notons aussi qu'une partie importante des résultats forts de géométrie algébrique (dus à Grothendieck, Pierre Deligne, Gerd Faltings) utilisent aussi l'existence d'univers de Grothendieck.

Pour comprendre ce qui est simple, il faut s'élever dans d'extravagants mondes infinis

Il est remarquable que la démonstration de résultats dont l'énoncé est compréhensible par tout le monde (comme celui de Fermat) et qui ne concernent que les entiers semble dépendre de l'existence d'infinis bien au-delà de tout ce que peut imaginer un être humain (à l'exception d'un logicien !). Si nous réussissons à prouver ces résultats sans utiliser ces univers extraordinaires de Grothendieck, alors cela se fera très certainement en compliquant les démonstrations et en les rendant moins naturelles, donc en procédant à l'opposé de tout ce que Grothendieck a toujours souhaité faire. Pour comprendre ce qui est simple, il faut s'élever dans d'extravagants mondes infinis.

La grande conjecture de Harvey Friedman

Harvey Friedman est un mathématicien de l'université d'État de l'Ohio, aux États-Unis. Aujourd'hui à la retraite, il conserve une activité productive hors du commun. Il est mentionné dans le *Livre Guinness des records* comme ayant été, à 18 ans, le plus jeune enseignant de tous les temps à donner un cours à l'université Stanford.

S'intéressant aux fondements des mathématiques, il recherche des énoncés les plus concrets possible dont la preuve exige l'emploi d'axiomes stipulant l'existence de très grands ensembles infinis (axiomes de grands cardinaux). Il réussit assez bien, mais les énoncés de ce type qu'il découvre restent abstraits et jamais aussi simples que le théorème de Fermat. Ce qu'il trouve confirme cependant le bien-fondé des travaux de Colin McLarty visant à prouver que le théorème de Fermat n'exige pas d'axiomes forts sur l'infini.

Harvey Friedman semble penser que la distinction entre « concret et assez simple » et « très simple » dépend de la nécessité d'utiliser des axiomes affirmant l'existence de grands ensembles. Dans le cas du théorème de Fermat, il conjecture qu'il doit pouvoir se démontrer en utilisant des systèmes d'axiomes très faibles n'utilisant pas l'infini. Il a énoncé ce qu'on nomme aujourd'hui « la grande conjecture de Friedman », selon laquelle tous les théorèmes d'arithmétique qui intéressent spontanément les mathématiciens (donc à l'exclusion des résultats de logique, ou des énoncés construits artificiellement afin qu'ils exigent des axiomes forts) sont démontrables en utilisant un système où l'infini ne joue aucun rôle direct. S'il a raison, il faudra comprendre pourquoi ce qui intéresse les mathématiciens reste dans un secteur limité de complexité et définir avec précision ce secteur. Harvey Friedman exprime son point de vue ainsi : « Le défi le plus intéressant concernant les fondements des mathématiques est de trouver des énoncés portant sur les entiers et dont la démonstration dépende de manière incontournable des univers [de Grothendieck]. »

HARVEY FRIEDMAN

(ce sont des objets géométriques : par exemple, l'équation $x^2 + y^2 = 1$ définit un cercle), et on raisonne globalement sur ces structures.

Malheureusement, les travaux de Grothendieck sortent du cadre usuel de la théorie des ensembles telle que ZFC la formalise, car les outils que ce mathématicien de génie a introduits et manipulés sont d'une abstraction extrême qui exige par exemple qu'on parle sans contrainte d'objets tels que la collection de tous les groupes.

Un axiome aujourd'hui bien étudié sur lequel s'appuie Grothendieck affirme l'existence de ce qu'il appelle des « univers » *(voir l'encadré page 81)*. Cet axiome lui permet de manipuler dans ses démonstrations non seulement les entiers eux-mêmes, mais aussi les ensembles d'entiers, et les ensembles de tels ensembles d'entiers, et toute une hiérarchie de structures d'une abstraction inhabituelle en mathématiques. Cette théorie des catégories dont Grothendieck fait un usage systématique pour ses raisonnements ne se trouve à l'aise qu'en postulant ces « univers » dont les logiciens savent depuis longtemps qu'on ne peut en démontrer l'existence dans le cadre de ZFC. En clair, puisque Andrew Wiles s'appuie sur ces résultats postulant l'existence des cardinaux fortement inaccessibles, sa preuve n'a de sens que dans une théorie très forte qui semble être INAC.

« Tout le monde voit que c'est là une méthode précipitée et grossière », commente Colin McLarty, de l'université de Cleveland. Ce dernier est professeur de philosophie, mais très compétent en mathématiques et en logique : il a régulièrement publié dans les meilleures revues de ces disciplines et il est membre du « Grothendieck Circle » qui travaille à rendre accessible sur Internet les travaux de Grothendieck.

Prouver avec moins

Il s'est ainsi attaqué à la question : peut-on faire baisser le niveau des hypothèses implicites de la démonstration de Wiles ? Dit autrement, peut-on la faire reposer sur des formalismes plus faibles que INAC, ou même que ZFC ?

Colin McLarty précise que « Les grands cardinaux en tant que tels n'étaient ni intéressants ni problématiques pour Grothendieck [...]. Pour lui, ils n'étaient que des moyens légitimes pour accéder à quelque chose d'autre. Il voulait organiser l'arithmétique et ses calculs dans un monde conceptuel géométrique. Il a trouvé un moyen de le faire avec la cohomologie [une méthode algébrique abstraite] et l'a utilisée pour concevoir des outils de calcul qui, auparavant, avaient échappé aux meilleurs mathématiciens tentant de résoudre les conjectures de Weil [démontrées en 1974 par Pierre Deligne en utilisant les outils créés par Grothendieck]. Il a ainsi posé les bases de la géométrie algébrique moderne. [...] Sa cohomologie s'appuie sur les univers, mais des fondements plus faibles devraient suffire même si y recourir entraîne la perte d'une certaine élégance conceptuelle. [...] Il n'y a aucune absurdité à considérer les univers inutiles en principe, et utiles en pratique. »

Colin McLarty expose une méthode pour construire une preuve du grand théorème de Fermat entièrement dans ZFC. Pour l'essentiel, elle consiste à utiliser des théories des ensembles prudentes, comme celle proposée par John von Neumann, Paul Bernays et Kurt Gödel (notée NBG). Ces théories autorisent la manipulation de gros

ensembles en ne les assimilant pas à de simples ensembles : il y a donc deux types de collections différentes. Bien qu'un peu compliquées et parfois jugées artificielles, ces théories permettent, dans un système équivalent en force à ZFC, de faire ce que les univers de Grothendieck font. On a donc, moyennant quelques complications, et sans prendre les risques liés à INAC, un monde mathématique autorisant la démonstration du théorème de Fermat.

Une autre méthode proposée récemment par Colin McLarty, fondée sur l'étude de ce qui est vraiment indispensable de ZFC pour disposer des théories arithmétiques de Grothendieck, permet en théorie de formaliser la preuve dans un système d'une force comprise entre celle de PEANO et celle de ZFC. Mais ce n'est pas encore pleinement satisfaisant. Une autre approche, esquissée par Angus Macintyre, permettrait de démontrer le théorème de Fermat dans PEANO, soit mieux que ce que propose McLarty. Son idée est que les objets du monde continu utilisés dans la démonstration peuvent être obtenus comme des limites d'objets définissables à partir des entiers. Un nombre réel, par exemple, est la limite des nombres décimaux correspondant à ses chiffres pris progressivement : ainsi, π est la limite de (3 ; 3,1 ; 3,14 ; 3,141 ; ...).

En procédant systématiquement par cette méthode, on doit pouvoir ramener la preuve d'Andrew Wiles et toutes celles antérieures dont il a besoin dans son travail à des mathématiques entièrement situées dans PEANO. Il ne suffit pas de le dire, il faut le faire et ce très soigneusement. Angus Macintyre a proposé quelques détails dans un texte d'une dizaine de pages sur la façon de mettre en œuvre sa méthode, et il semble avoir convaincu plusieurs spécialistes que ces réductions fonctionnent. Mais le travail définitif reste à faire pour être certain qu'aucun obstacle inattendu ne s'interpose.

On le voit, on n'a pas fini de travailler sur la démonstration d'Andrew Wiles et sur les théories de Grothendieck.

Notons pour finir qu'il existe des systèmes plus faibles que PEANO, en particulier le système EFA (pour *Exponential Functional Arithmetics*), où l'on n'autorise les raisonnements par récurrence que pour une classe limitée de formules simples. Le système EFA semble d'ailleurs la vraie limite pour démontrer le théorème de Fermat.

On sait en effet qu'en allant plus bas, les systèmes qu'on définit naturellement pour l'arithmétique ne permettent pas tous de démontrer ce théorème. Une autre raison pour s'intéresser à EFA est une conjecture proposée par un mathématicien respecté, selon laquelle EFA suffirait pour l'essentiel des résultats arithmétiques vraiment intéressants. La « grande conjecture de Harvey Friedman » affirme ainsi que tous les résultats d'arithmétique dont on trouve la démonstration dans la revue *Annals of Mathematics* (où a été publiée la preuve d'Andrew Wiles) sont démontrables dans EFA.

EFA, système ultime ?

La formulation de cette conjecture est un peu étrange, puisqu'elle n'envisage qu'une classe d'énoncés définie par les publications d'une revue, ce qui n'est pas très mathématique et variera dans le temps quand de nouveaux articles seront publiés. L'idée est cependant claire : on sait, en utilisant des méthodes logiques ou de la théorie de Ramsey, construire des formules d'arithmétique non démontrables dans EFA et même dans PEANO, mais démontrables dans des systèmes plus forts. Pas question donc d'affirmer que tout résultat arithmétique se démontre dans EFA. Cependant, la revue *Annals of Mathematics,* qui est une revue de mathématiques pures, ne publie pas ce type de résultats jugés artificiels. Ce qu'elle publie est limité au cœur des mathématiques. Et selon la grande conjecture de Harvey Friedman, cela n'exige jamais plus que EFA.

Avant de savoir si Harvey Friedman a raison et comment caractériser précisément les choix de la revue *Annals of Mathematics*, il faudra mieux comprendre les hypothèses implicites des théories de Grothendieck, les démonstrations comme celles d'Andrew Wiles et la mise en forme des réductions esquissées aujourd'hui. Ce chemin sera riche en leçons et utile pour produire des preuves vérifiables par ordinateur de ce domaine mathématique qu'à l'heure actuelle on ne sait pas formaliser explicitement. ■

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).

Dernier ouvrage paru : *Mathématiques et mystères*, une intrigante sélection de ses chroniques parues dans *Pour la Science* (Belin, 2016).

BIBLIOGRAPHIE

P. Glivický et V. Kala, **Fermat's Last Theorem and Catalan's conjecture in weak exponential arithmetics**, prépublication arXiv:1602.03580, 2016.

W. Hesselink, **Computer verification of Wiles' proof of Fermat's Last Theorem**, www.cs.rug.nl/ffwim/fermat/wilesEnglish.html, 2016.

C. McLarty, **The large structures of Grothendieck founded on finite order arithmetic**, prépublication arXiv:1102.1723, 2014.

A. Macintyre, **The impact of Gödel's incompleteness theorems on mathematics**, dans *Kurt Gödel and the Foundations of Mathematics*, pp. 3-25, Cambridge Univ. Press, 2011.

J.-P. Delahaye, **Du rêve à la réalité des preuves**, *Pour la Science* n° 402, pp. 90-95, avril 2011.

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