

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 $x \rightarrow f(x)$ 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 inaccessible 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

dieck, Pierre Deligne, Gerd Faltings) utilisent aussi l'existence d'univers de Grothendieck.

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

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

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 Grothen-

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



HARVEY FRIEDMAN

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]. »

[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