

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.