

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 $\{3; 3,1; 3,14; 3,141; \dots\}$.

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/~fwim/fermat/wilesEnglish.html, 2016.

C. McLarty, *The large structures of Grothendieck founded on finite order arithmetic*, prépublication arXiv:1102.1773, 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