

de nombreuses avancées ont été réalisées. Par exemple, en 2010, Manjul Bhargava, de l'université de Princeton, et son doctorant Arul Shankar ont démontré un théorème qui confirme qu'une majorité des courbes elliptiques vérifient BSD. Manjul Bhargava a reçu la médaille Fields en 2014, notamment pour ce résultat.

La conjecture de Satō-Tate, qui remonte aussi au début des années 1960, a une histoire un peu similaire à BSD. De quoi s'agit-il ? Si p est un nombre premier, on peut considérer la courbe elliptique $y^2 \equiv x^3 + ax + b \pmod{p}$. Ici a et b sont des entiers fixés, x et y sont des entiers positifs variables, plus petits que p , et la notation signifie que la différence entre les deux côtés est un multiple de p . La conjecture de Satō-Tate est une prédiction qualitative à propos de la variation du nombre (toujours fini) de solutions lorsque l'on fait varier p (voir la figure ci-contre). Mikio Satō et John Tate auraient trouvé la conjecture indépendamment, le premier en étudiant les données produites par ordinateur et le second par un raisonnement théorique. En 2006 (puis dans une version plus généralisée en 2011), des collègues et moi-même avons prouvé cette conjecture. Mais même avant sa démonstration, la conjecture de Satō-Tate avait inspiré toute une série de conjectures plus générales, dont celles de Katz et Sarnak qui relient (entre autres) les distributions des nombres premiers à la théorie des matrices aléatoires. Ces conjectures ne sont toujours pas démontrées, mais elles aussi ont été confirmées numériquement par ordinateur.

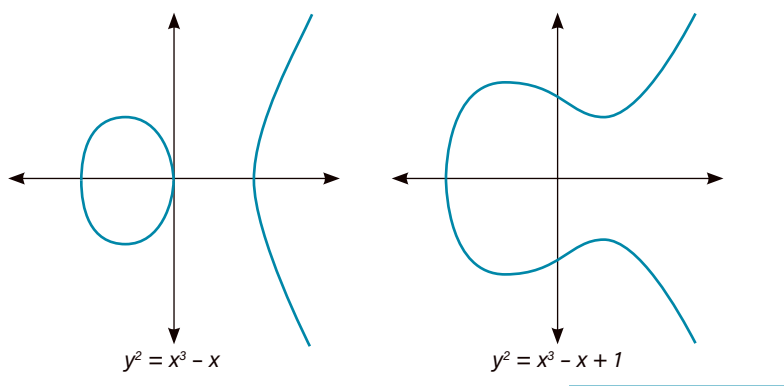
Pour les mathématiciens, l'utilisation des ordinateurs pour le calcul rapide n'a pas soulevé de controverse particulière. Il n'y a pas eu davantage de polémique quand les machines ont rendu possible pour la première fois la visualisation des solutions de systèmes d'équations avec un comportement complexe. Bien au contraire, c'est l'essor de ces nouvelles technologies qui a ouvert la voie à certaines branches des mathématiques connues familièrement sous le nom de «théorie du chaos». Cette dernière combine des méthodes théoriques et l'étude empirique d'images numériques. C'est par exemple grâce à des simulations numériques que les constantes de Feigenbaum, qui apparaissent dans les diagrammes de bifurcation en théorie du chaos (voir la figure page 34), ont été estimées.

Pour exploiter pleinement et le plus simplement possible les capacités des ordinateurs, de nombreux logiciels de calcul symbolique (Macysma, Mathematica, Maple, SageMath, etc.) ont été développés. Ces programmes manipulent des expressions algébriques complexes ou tracent facilement des courbes et autres graphiques. Ils font aujourd'hui partie des outils du chercheur en mathématiques.

Dès les premiers ordinateurs, l'enthousiasme pour ces machines a été grandissant. En 1958, les Américains Alan Newell et

LES COURBES ELLIPTIQUES

Ces courbes algébriques sont représentées dans le plan par une équation cubique. Elles ont essentiellement deux formes possibles (voir les deux exemples ci-dessous). Elles tirent leur nom de leur association aux intégrales elliptiques, utilisées pour calculer des longueurs d'arc dans des ellipses. Ces objets interviennent dans diverses conjectures en théorie des nombres, celle de Shimura-Taniyama-Weil (dont la démonstration par Andrew Wiles a mené au théorème de Fermat), de Birch et Swinnerton-Dyer, de Satō-Tate, etc. Elles sont également exploitées dans certaines techniques de cryptographie.



Herbert Simon ont prédit que, en dix ans, les ordinateurs numériques allaient atteindre quatre étapes cruciales, sur la voie vers un «monde où la puissance et la rapidité intellectuelles [des humains] seraient dépassées par l'intelligence des machines». Une de ces étapes était «la découverte et la preuve d'un nouveau théorème mathématique important». Les mathématiques ont donc été identifiées très tôt comme un territoire à explorer pour l'intelligence artificielle, dont Newell et Simon ont été deux des pionniers.

UNE POLÉMIQUE HAUTE EN COULEUR

Cet enthousiasme a cependant pris une autre tournure en 1976, lorsque Kenneth Appel et Wolfgang Haken ont annoncé leur démonstration du théorème des quatre couleurs (TQC). Le théorème, conjecturé au XIX^e siècle, affirme qu'il est possible de colorier n'importe quelle carte géographique avec quatre couleurs distinctes, de telle sorte que deux pays qui partagent une frontière n'ont jamais la même couleur. Pendant plus de cent ans, le problème a fasciné les débutants et les amateurs autant que les mathématiciens professionnels. Dans leur démonstration, Appel et Haken ont réduit le problème à une collection finie, mais très grande, d'éventuels contre-exemples, qu'il restait à éliminer. Mener cette stratégie à la main était impraticable (et l'est toujours), mais l'ordinateur était capable d'examiner tous les cas un par un et ainsi de faire aboutir la démonstration.

Mais s'agit-il vraiment d'une démonstration? Pour certains, l'utilisation de l'ordinateur comme aide n'était pas un problème alors que, pour d'autres, elle ne permettait pas de s'assurer à 100% que la preuve était fiable. Dès l'annonce de la démonstration d'Appel et Haken, cette frontière entre les deux camps a été tracée et a, depuis, à peine bougé. Les désaccords sur le statut de cette preuve ont été si vifs qu'ils

La place des machines en mathématiques n'est pas une question de compétition

ont attiré l'attention des sociologues et des philosophes, qui n'ont pas hésité à désigner l'événement comme un moment charnière pour l'épistémologie. De nombreux mathématiciens ont accueilli favorablement ces nouvelles méthodes. Selon le sociologue Donald MacKenzie, ils «ont accepté la partie mécanisée de l'analyse par Appel et Haken comme presque certainement correcte, et ils ont focalisé leurs doutes sur le raisonnement humain complexe impliqué dans la démonstration». Mais l'absence d'une preuve traditionnelle a aussi suscité une grande insatisfaction. «Nous sommes encore loin d'avoir une bonne démonstration du théorème des quatre couleurs, a notamment dit le mathématicien américain Paul Halmos. En effet, la preuve actuelle dépend d'un oracle, et je dis: à bas les Oracles! Ils ne sont pas les mathématiques.»

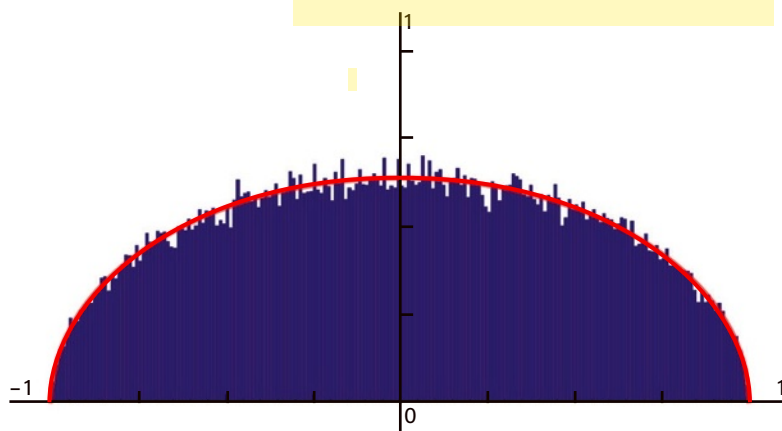
Pour la majorité des mathématiciens, leur travail de recherche, quand il vise à démontrer un théorème, consiste moins à confirmer sa validité qu'à comprendre pourquoi il est vrai. Dans l'un de ses livres, David Ruelle rapporte l'avis de son collègue Pierre Deligne à ce sujet: «Ce qui l'intéressait personnellement, c'étaient les résultats qu'il pouvait lui-même, et tout seul, comprendre dans leur intégralité. Cela exclut d'une part les résultats prouvés avec l'aide d'un ordinateur, d'autre part les résultats dont la démonstration... est tellement longue qu'elle dépasse les possibilités de vérification par un seul mathématicien.»

Une des réticences à l'égard des machines souvent mises en avant est le degré de confiance

qu'il est possible d'accorder aux résultats d'un système informatique qui interviennent dans une preuve. Les erreurs sont légion dans les preuves humaines, mais en principe elles sont détectables par d'autres êtres humains. Ceci est impossible avec la preuve d'Appel et Haken, qui a nécessité plus de mille heures de calcul en temps d'ordinateur. La question de la fiabilité a été au cœur d'une autre démonstration, qui constitue un autre événement majeur dans l'histoire des preuves faites à l'aide des ordinateurs. Sur le présentoir d'un primeur, les oranges sont presque toujours empilées de la même façon: chaque étage est un réseau hexagonal avec les oranges de l'étage suivant placées dans le milieu de chaque hexagone. La conjecture de Kepler (qui porte son nom car l'astronome Johannes Kepler la mentionne en 1611) dit, de façon plus formelle, que c'est la configuration la plus optimale pour empiler des sphères, celle qui laisse le minimum d'espace vide. En 1998, Thomas Hales, alors à l'université du Michigan, et son doctorant Samuel Ferguson ont annoncé avoir résolu le problème. Comme dans la preuve du théorème des quatre couleurs, Thomas Hales y est parvenu en ramenant le problème à une série finie de calculs, qui ont été exécutés sur un ordinateur.

UNE PREUVE INVÉRIFIABLE

Thomas Hales a soumis son article à la revue prestigieuse *Annals of Mathematics*. Quatre années plus tard, Gábor Fejes Tóth, le rapporteur principal chargé d'examiner le manuscrit, a envoyé son rapport. Il a affirmé être convaincu à 99% de l'exactitude de la preuve, sans pouvoir la certifier complètement. Une situation sans précédent dans l'histoire des mathématiques. Robert MacPherson, membre de l'institut des études avancées de Princeton

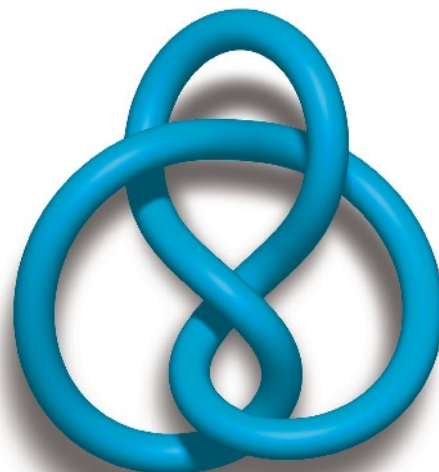


La conjecture de Satō-Tate est un énoncé statistique qui s'intéresse au nombre de solutions d'une courbe elliptique sur un corps fini à p éléments, où p est un nombre premier. Dit autrement, on peut considérer la courbe elliptique $y^2 \equiv x^3 + ax + b \pmod{p}$. Ici a et b sont des entiers fixés, x et y sont des entiers positifs variables, plus petits que p . La notation signifie que la différence entre les deux côtés est un multiple de p . Grâce aux calculs par ordinateur, il a été possible d'identifier la distribution du nombre de solutions en fonction de p , ce qui a permis à Mikio Satō d'énoncer la conjecture. John Tate y est parvenu par un raisonnement théorique.

UNE IA QUI DÉCOUVRE DES CONJECTURES

Depuis quelques années, l'intelligence artificielle joue un rôle croissant en sciences. Les chercheurs utilisent de tels algorithmes pour identifier des tumeurs sur des images médicales, pour reconstruire des cascades de désintégration au sein de collisionneurs de particules, etc. En décembre 2021, la société DeepMind, filiale de Google, a présenté son nouveau programme d'apprentissage profond – un type d'intelligence artificielle qui repose sur un réseau de neurones configuré lors d'une phase d'apprentissage menée sur une vaste collection d'exemples. Ce programme est capable de trouver et de formuler des conjectures mathématiques. Spécialiste de l'intelligence artificielle, DeepMind s'est notamment fait connaître grâce à AlphaGo, son logiciel capable de battre les champions au jeu de go, ou AlphaFold, qui détermine la structure tridimensionnelle de protéines à partir de leur séquence linéaire d'acides aminés. En mathématiques, une façon de découvrir de nouvelles conjectures consiste à étudier quelques exemples, y observer des motifs, c'est-à-dire des relations entre différents paramètres. Le mathématicien généralise alors l'intuition forgée sur un nombre restreint

de cas et prouve que la conjecture est vraie. Dans cet exercice qui nécessite de mobiliser toutes les capacités créatrices du chercheur, l'ordinateur a depuis longtemps sa place. En facilitant les calculs ou la représentation, la machine fournit les indices que l'humain traduit en conjecture. Le projet de DeepMind va plus loin. Son équipe et quelques mathématiciens se sont penchés sur la théorie des nœuds. Cette branche de la topologie s'intéresse aux entrelacements d'un « bout de ficelle » fermé. Il existe une infinité de nœuds. Les mathématiciens ont défini des « invariants », des fonctions qui prennent des valeurs différentes selon les nœuds et permettent de les caractériser. Certains de ces invariants sont de nature algébrique (décrits par des polynômes) et d'autres sont de nature géométrique. En s'appuyant sur une vaste base de données de millions de nœuds (tous contenant jusqu'à seize croisements), le logiciel de DeepMind a établi une conjecture reliant pour une famille de nœuds certains invariants algébriques et certains invariants géométriques. Marc Lackenby et András Juhász, de l'université d'Oxford et membres de l'équipe, ont ensuite démontré la conjecture.



L'équipe de DeepMind a également formulé une conjecture sur les groupes de symétries en utilisant une stratégie similaire, c'est-à-dire en cherchant des motifs dans une vaste base de données. Cette méthode pourrait se généraliser à différents domaines des mathématiques (ou de la biologie, de la physique, etc.), mais certains problèmes semblent difficiles à aborder par ce biais.

SEAN BAILLY
journaliste à *Pour la Science*

et alors éditeur de la revue, a conclu : « Les rapporteurs n'ont pas été en mesure de certifier l'exactitude de la preuve et ne seront pas capables de la certifier dans le futur, parce qu'ils n'ont plus d'énergie pour se consacrer au problème. Ce n'est pas ce que j'espérais. »

Comment se sortir de cette situation où des démonstrations semblent justes mais sont impossibles à vérifier ? Quand il est devenu clair que sa preuve ne pouvait pas être validée par le système habituel d'examen par les pairs (des humains), Thomas Hales a eu recours à la vérification formelle. Après une immersion rapide dans les techniques inventées par les informaticiens, le mathématicien a annoncé en 2003 la création du projet *Flyspeck*, avec l'objectif de réécrire sa preuve dans un langage symbolique pour produire une vérification mécanique. Il avait prévu que la formalisation prendrait vingt ans de travail, mais l'accueil de son projet a été si enthousiaste que l'équipe *Flyspeck*, qui comptait alors vingt-deux membres, a atteint son objectif dès 2014.

Thomas Hales n'a pas été le seul à s'intéresser sérieusement à la formalisation. En 2005, Georges Gonthier et Benjamin Werner, d'Inria,

ont formalisé le théorème des quatre couleurs avec le système Coq. En 2007, l'équipe de Jeremy Avigad, de l'université Carnegie-Mellon, à Pittsburgh, a formalisé le théorème des nombres premiers en utilisant l'assistant de preuve Isabelle. Dans le cadre du projet *Flyspeck*, Thomas Hales a aussi formalisé le théorème de Jordan qui dit que, dans le plan, une courbe fermée simple sépare l'espace en deux parties, et dont la preuve étonnamment subtile avait résisté aux mathématiciens du XIX^e siècle pendant des décennies. Plus récemment, Thomas Hales s'est tourné vers Lean, l'assistant de preuve développé par Microsoft, qui est de plus en plus adopté sur le plan international, en particulier par le projet *Xena*, mené par le spécialiste de la théorie des nombres Kevin Buzzard, de l'Imperial College, à Londres.

La formalisation des preuves est désormais une branche reconnue des mathématiques. Pour les experts de ce domaine, l'objectif est surtout de rendre la formalisation facile d'accès pour intégrer sa pratique dans les usages courants du mathématicien.

Pour certains chercheurs, l'arrivée de la formalisation représente un tournant dans leur