

Hilbert a été à l'initiative d'un programme nommé «le formalisme», dont le but était de rendre les mathématiques capables de vérifier l'exactitude de leur propre raisonnement. Hilbert avait observé qu'un énoncé mathématique pouvait être réécrit sous la forme d'une chaîne de symboles, et qu'une preuve était équivalente à une suite de transformations de ces chaînes selon les règles admises de la logique (comme dans le système de Bertrand Russell et Alfred Whitehead présenté dans leur livre *Principia Mathematica*). De la même manière qu'on peut calculer les solutions de certains types d'équations polynomiales, ou d'équations différentielles, à partir de la forme de l'équation en question, Hilbert a proposé que l'existence d'une preuve d'un théorème pouvait se déduire de la forme du théorème dans un langage symbolique adapté. De ce point de vue, le raisonnement mathématique était une sorte de calcul.

Cependant, en 1931, Kurt Gödel a semé le trouble et mis un point d'arrêt au programme de Hilbert en formulant ses deux célèbres théorèmes d'incomplétude. Il a montré que dans tout cadre axiomatique donné, certaines questions sont fondamentalement indécidables. Il n'est donc pas toujours possible de prouver qu'un énoncé est vrai ou faux. Les conséquences de ces théorèmes ont inspiré une décennie de réflexion intensive sur la nature du calcul et du raisonnement mathématique. Certains acteurs clés dans cette histoire, tels Alan Turing, Alonzo Church, et John von Neumann, ont alors jeté les bases de la théorie, et ensuite de la réalisation concrète des ordinateurs numériques.

Sans surprise, les mathématiciens ont très vite adopté les ordinateurs après leur mise au point. La capacité des premiers ordinateurs numériques à exécuter rapidement et avec précision des calculs a été exploitée dans de nombreux problèmes pratiques, dont le plus marquant, à cette époque, est la conception et le déploiement de la bombe à hydrogène.

Les performances du calcul numérique ont aussi été décisives pour la recherche théorique en mathématiques, en particulier dans le domaine de la théorie des nombres. Au milieu des années 1960, le mathématicien Peter Swinnerton-Dyer notait l'avantage que procureraient ces machines: «Avec l'invention des ordinateurs électroniques, les calculs qui auparavant auraient été hors de portée sont maintenant faisables aisément, à condition qu'ils soient assez répétitifs. Il doit y avoir beaucoup de branches de la théorie des nombres dans lesquelles le calcul intelligemment dirigé fournirait des résultats précieux.»

L'histoire des mathématiques est riche en exemples d'intuition forgée grâce à des calculs. Swinnerton-Dyer pensait à des résultats comme le théorème des nombres premiers, qui indique que la proportion de nombres premiers (des

nombres qui n'ont aucun diviseur en dehors de 1 et eux-mêmes) inférieurs à un entier donné n est environ $n/\ln(n)$, où $\ln$ est le logarithme naturel. Au XIX^e siècle, c'est en explorant à la main la répartition des nombres premiers que Adrien-Marie Legendre et surtout Carl Friedrich Gauss ont suggéré cette formule. Grâce à cette recherche empirique, et en s'appuyant sur des techniques d'analyse mathématique sur les séries infinies, Jacques Hadamard et Charles Jean de la Vallée-Poussin ont démontré le théorème des nombres premiers de façon indépendante la même année, en 1896.

Gauss, le fondateur d'une grande partie des mathématiques théoriques modernes, était fier de sa capacité exceptionnelle de calcul. Mais il n'aurait pas fait le poids face aux ordinateurs (même ceux relativement primitifs évoqués par Swinnerton-Dyer). Ces nouvelles machines produisent rapidement de vastes collections de données que les mathématiciens analysent pour y déceler des tendances et formuler des conjectures.

UNE CONJECTURE ASSISTÉE PAR ORDINATEUR

C'est de cette façon qu'au début des années 1960 Swinnerton-Dyer et son collègue Bryan Birch ont énoncé une conjecture qui porte leur nom (conjecture de Birch et Swinnerton-Dyer, BSD) et qui est encore aujourd'hui une des plus importantes en théorie des nombres. Pour arriver à cette proposition, les deux chercheurs ont mené un grand nombre de calculs sur l'ordinateur EDSAC de l'université de Cambridge. La conjecture concerne l'existence de solutions rationnelles pour les courbes elliptiques, des équations cubiques à deux variables, comme $y^2 = x^3 - Dx$, où D est un nombre rationnel (voir l'encadré page 30). De façon générale, ces équations sont les plus simples pour lesquelles les méthodes élémentaires sont incapables de déterminer *a priori* si le nombre de solutions rationnelles est fini (comme pour $D = 1$) ou infini (comme pour $D = 25$). La question est de nature algébrique; la conjecture BSD donne une réponse conjecturale et caractérise les solutions.

L'article de Swinnerton-Dyer fournit d'excellents arguments théoriques pour croire la conjecture BSD, qui depuis l'an 2000 est un des problèmes du millénaire de l'institut Clay (avec à la clé un prix de 1 million de dollars pour celui qui fournira une preuve). Le texte explique également comment des arguments heuristiques ont guidé la formulation de la conjecture et ses raffinements ultérieurs. Cette conjecture n'aurait probablement pas été acceptée aussi vite sans la présence des données numériques que seuls les ordinateurs pouvaient produire.

Ces machines ont largement contribué au dynamisme et à la fertilité de la recherche en théorie des nombres. Ainsi, si BSD résiste encore,

LES ESPACES VECTORIELS LIQUIDES DE PETER SCHOLZE

Dans un projet ambitieux pour construire un cadre axiomatique plus vaste que la topologie, Peter Scholze et Dustin Clausen ont présenté la preuve d'un théorème si complexe qu'ils ont demandé à un logiciel de la confirmer.

Peter Scholze a bâti sa réputation de brillant mathématicien en développant sa théorie des espaces perfectoides, décrits dans un article du magazine *Wired* comme étant à la fois « une classe de structures fractales » et une « construction enveloppante infinie », qui « permet de faire glisser certaines questions sur les polynômes [...] dans un univers mathématique différent où les calculs sont beaucoup plus simples ». Depuis que le jeune chercheur allemand a présenté cette théorie pour la première fois en 2011, ces espaces et les notions connexes qu'il a inventées avec ses collaborateurs ont servi à résoudre des problèmes difficiles de la théorie des nombres, tout en élargissant considérablement sa portée. Dans la continuité de ces travaux, Peter Scholze espère que les « espaces vectoriels liquides », qui font l'objet de ses travaux plus récents avec Dustin Clausen, fourniront une base à un univers mathématique qui permettra de réinterpréter l'analyse – au cœur du calcul infinitésimal, de la théorie du chaos, des équations de la physique mathématique, etc. – et la théorie des nombres.

La majorité des problèmes en théorie des nombres se résume souvent à des questions sur des polynômes, et plus précisément à la compréhension des solutions en nombres entiers aux équations polynomiales. Ces solutions se caractérisent par au moins deux types de propriétés : leur taille (au sens où 15 est plus grand que 12) et leur degré de divisibilité (au sens où 15 est divisible par 3). Un aspect essentiel des travaux dans ce domaine consiste à comprendre les interactions de ces deux propriétés.

Au cœur de la question de la taille des solutions polynomiales se cache la notion de continuité, qui a longtemps été difficile à saisir. Pour les philosophes présocratiques, la continuité ne pouvait être appréhendée que par l'intuition de processus infinis, ce qui entraînait en conflit avec la finitude de l'esprit. Zénon a résumé ce point avec son paradoxe de la flèche d'Achille qui ne peut atteindre sa cible, car elle parcourt la moitié du chemin, puis encore la moitié... Sous l'impulsion de Newton et Leibniz, l'analyse et le calcul infinitésimal ont apporté une réponse à ce paradoxe, en montrant qu'une série infinie peut converger. Au xx^e siècle, les espaces topologiques ont fourni un cadre axiomatique pour traiter les notions de limite et de continuité, où qu'elles se manifestent (théorie des nombres, analyse, mécanique quantique ou espaces perfectoides). Avec leur théorie des « mathématiques condensées » qui inclue les espaces vectoriels liquides, Dustin



Peter Scholze lors de la remise de sa médaille Fields, en 2018. Il est récompensé pour ses travaux à la frontière entre l'arithmétique et la géométrie.

Clausen et Peter Scholze espèrent construire un cadre encore plus général que la topologie. Dans ces espaces, les points forment des « structures fractales », ce que Peter Scholze nomme plutôt « un nuage de poussières ».

Peter Scholze et Dustin Clausen espèrent construire un cadre encore plus général que la topologie

À partir de ces nuages de poussières, les espaces perfectoides construisent une géométrie utile pour étudier la divisibilité des solutions des équations polynomiales. La divisibilité est une notion algébrique, qui se prête donc bien à la manipulation par les ordinateurs. Dès 2019, l'équipe de Kevin Buzzard a formalisé les espaces perfectoides avec l'assistant de preuve Lean. La taille, en revanche, est une notion géométrique. Avec leur récent théorème, Peter Scholze et Dustin Clausen espèrent que les aspects difficiles de l'analyse (et donc de la taille)

puissent être « mis dans une boîte noire » à l'aide des espaces vectoriels liquides, afin que les arguments de l'analyse puissent être rendus plus accessibles aux outils puissants des algébristes.

Peter Scholze considère qu'il s'agit de « son théorème le plus important à ce jour ». Il avait donc besoin d'avoir la garantie qu'il était correct. Or il lui semblait clair qu'aucun autre humain ne passerait en revue les détails de la démonstration. « La preuve n'est pas très amusante... », confie-t-il. C'est dans ce contexte qu'il a lancé le défi de « l'expérience du tenseur liquide » à l'équipe de Lean en décembre 2020. Ce projet reconnaît donc que les travaux humains peuvent bénéficier d'une confirmation au-delà de la simple preuve humaine, lorsqu'ils sont particulièrement délicats ; et que cette double vérification ultime est bien justifiée lorsque le théorème en jeu aurait des implications capitales.

Depuis le 5 juin 2021, Lean a formalisé la preuve et entériné la validité du théorème de Dustin Clausen et Peter Scholze. Le sort final du théorème, comme de tout autre théorème, dépendra de ce que les mathématiciens en feront. Et le fait que sa première preuve ait été formalisée ne sera probablement retenu que comme une note de bas de page.

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.

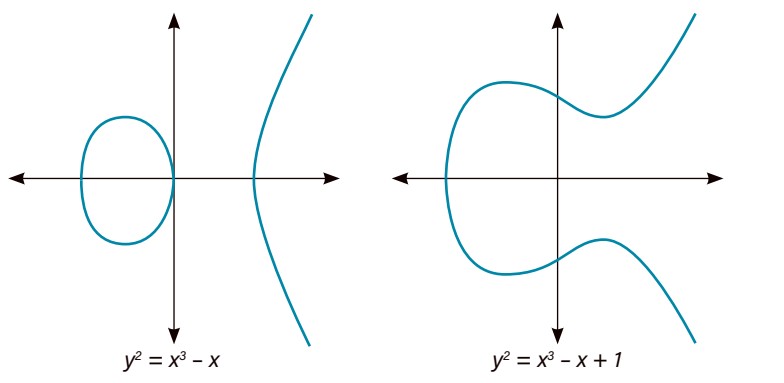
Pour les mathématiciens, l'utilisation des ordinateurs pour le calcul rapide n'a pas soulevé de controverse particulière. Il n'y a pas eu davantage de polémique quand les machines ont rendu possible pour la première fois la visualisation des solutions de systèmes d'équations avec un comportement complexe. 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.