

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.

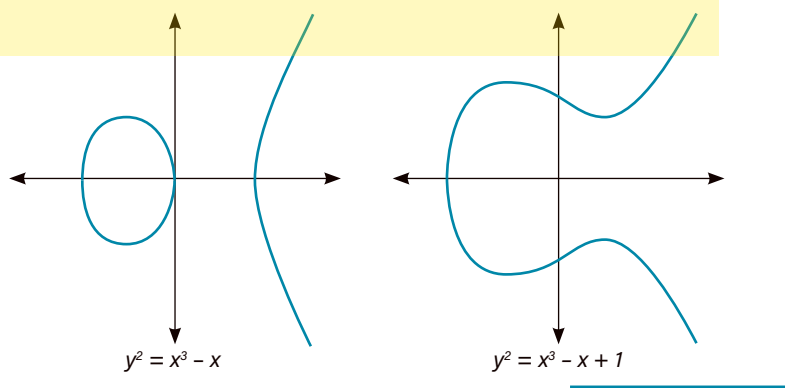
Pour les mathématiciens, l'utilisation des ordinateurs pour le calcul rapide n'a pas soulevé de controverse particulière. Il n'y a pas eu davantage de polémique quand les machines ont rendu possible pour la première fois la visualisation des solutions de systèmes d'équations avec un comportement complexe.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