Mathématiques et informatique

L'informatique a totalement transformé le paysage des mathématiques. Les liens à double sens entre les deux disciplines sont de plus en plus intenses et riches.

> PAR JEAN-PAUL DELAHAYE, UNIVERSITÉ DES SCIENCES ET TECHNOLOGIES DE LILLE, LABORATOIRE D'INFORMATIQUE FONDAMENTALE DE LILLE, UMR-CNRS 8022, À VILLENEUVE-D'ASCQ

L'informatique connaît depuis plus d'un demi-siècle une évolution rapide qui a suscité une réflexion d'une extrême fécondité. Cela a conduit soit à utiliser des théories mathématiques existantes, qui se sont alors enrichies (l'arithmétique, la théorie des graphes, la théorie de l'information), soit à créer de nouveaux domaines mathématiques (par exemple, la théorie de la complexité liée à la théorie de la calculabilité). Une nouvelle sensibilité mathématique est née de l'usage des ordinateurs et des problèmes qu'ils posent à l'esprit théoricien. Si tout remonte à la décennie 1930 avec les travaux de l'Autrichien Kurt Gödel, du Britannique Alan Turing et de l'Américain Alonso Church sur la notion d'algorithme, cette sensibilité mathématique nouvelle a connu un essor considérable au cours des dernières décennies. À côté des mathématiques du continu, ces mathématiques du discret, du calcul et de l'information se sont épanouies, et l'on est très loin d'en avoir parcouru ne serait-ce que les allées principales.

Organiser des milliards de calculs ?

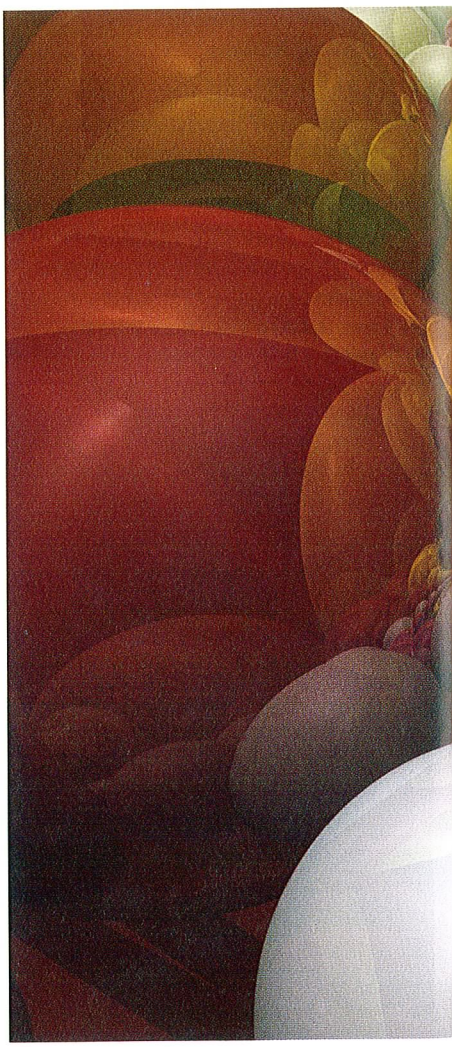
Donner des ordres précis aux ordinateurs afin qu'ils fassent ce qu'on attend d'eux s'appelle « écrire des programmes ». Les mathématiciens conçoivent depuis toujours de telles méthodes de calcul, mais, en pratique, la règle implicite était qu'on utilise les algorithmes en opérant à la main quelques dizaines ou quelques centaines d'opérations élémentaires. Lorsque des machines capables de réaliser des millions, puis des milliards de calculs sans erreur furent disponibles, on découvrit que toute une science nouvelle, l'algorithmique, devait se développer et que cette science était d'essence mathématique. Commander des calculateurs automatiques n'est ni simple ni évident, et des méthodes au premier regard satisfaisantes se révèlent vaines dans le monde des ordinateurs. La résolution de systèmes d'équations linéaires par les formules du Suisse Gabriel Cramer (qui expriment les solutions comme des rapports de déterminants) ne permet pas de traiter des systèmes de taille 30, alors que d'autres méthodes iront bien au-delà. Les ordinateurs, quels qu'ils soient, butent sur des limites, et c'est à cette évidence qu'est confronté celui qui écrit des programmes et qui ne peut donc jamais raisonner en se disant que la puissance de la machine suppléera le manque d'analyse préalable.

LES ORDINATEURS BUTENT SUR DES LIMITES

La règle véritable est donc celle-ci : plus une machine est puissante, plus il y a de travail mathématique initial à produire pour la faire fonctionner correctement et en maîtriser la marche.

Un problème aussi simple que la multiplication des nombres entiers conduit au développement de méthodes complexes et délicates quand on doit manipuler des nombres de grandes tailles possédant plusieurs milliers, millions ou même milliards de chiffres. On a été étonné en s'apercevant que sur une question aussi élémentaire des progrès étaient possibles. Pourtant, dans la décennie 1970, des méthodes ont été mises au point, qui permettent de multiplier deux nombres de n chiffres en un temps proportionnel à $n \times ln(n) \times ln(ln(n))$. En pratique, cela est presque équivalent à un temps proportionnel à n et bien plus rapide que les méthodes classiques tirées des procédures pratiquées à la main depuis des millénaires qui, elles, demandent un

Une spirale de Doyle. Certaines structures géométriques complexes ne sont « visualisables » qu'à l'aide de programmes informatiques qui aident à les comprendre.



temps de travail proportionnel à n^2 ou n^3. Ce qu'il est possible de faire avec le bon algorithme de multiplication contemporain, sans lui et en ne comptant que sur la loi de Moore (qui prédit un doublement de la puissance des ordinateurs tous les 18 mois environ), il faudrait attendre 2050 ou plus pour y parvenir.

Des avancées surprenantes. Grâce à cette algorithmique sans cesse revisitée, complétée et perfectionnée, ainsi qu'aux progrès de l'électronique, on a pu progresser dans le calcul des constantes mathématiques et arriver à obtenir plusieurs milliards de décimales des principales d'entre elles (π, e, $\sqrt{2}$, le nombre d'or, etc.). Ces progrès se sont parfois accompagnés de surprises, comme la découverte par une équipe canadienne, en 1995, d'une nouvelle formule pour le calcul de π et d'une méthode exploitant cette formule, qui permet d'obtenir les chiffres binaires de π indépendamment les uns des autres.

Cet exploit théorique a été transformé en exploit pratique par Colin Percival qui, en septembre 2000, a obtenu une petite tranche de chiffres binaires autour du 10^{15e} chiffre binaire de π. Une telle performance semblait hors de portée pour des siècles. Ainsi, un bon algorithme rend possible ce qui, sans lui, ne l'est pas.

Comme autres conséquences de cette maîtrise algorithmique des calculs arithmétiques avec des nombres de grande taille, il faut citer la découverte de nombres premiers records : un nombre premier de deux millions de chiffres en 1999 et, récemment, un nombre de plus de 10 millions de chiffres. Là encore, la découverte des tests probabilistes de primalité (qui indiquent sans certitude absolue, mais avec un risque d'erreur infinitésimal, qu'un nombre entier est premier) fut une surprise théorique, par ailleurs d'une grande utilité en cryptographie.

UNE VISION NOUVELLE DES OBJETS ABSTRAITS

Au-delà des exploits informatiques parfois anecdotiques, c'est toute la science de l'organisation des calculs qui progresse et atteint la maturité, tissant des liens profonds avec les mathématiques et changeant parfois radicalement les points de vue. Des livres d'arithmétique d'un genre nouveau sont apparus dans lesquels les concepts introduits sont systématiquement associés à des outils algorithmiques permettant de les manipuler réellement avec un ordinateur. Les mathématiques sont nécessaires à la maîtrise des ordinateurs et contribuent en profondeur à leur compréhension, mais, en retour, les ordinateurs conduisent à pratiquer les mathématiques de manière différente et donnent une vision nouvelle des objets abstraits que la machine manipule mieux que l'esprit humain et avec une sûreté incomparable.

Des liens de plus en plus étroits. Ce n'est pas seulement l'arithmétique, mais une partie importante des mathématiques qui est concernée par les progrès de l'algorithmique. Le calcul formel (l'ordinateur calcule non plus seulement avec des nombres, mais aussi avec des symboles, des fonctions, des équations, etc.) s'est considérablement développé. Cependant, les rapports entre l'informatique et les mathématiques ne s'arrêtent pas là. Il faut citer notamment :

– l'analyse numérique, qui permet de résoudre des systèmes d'équations de grande taille ;

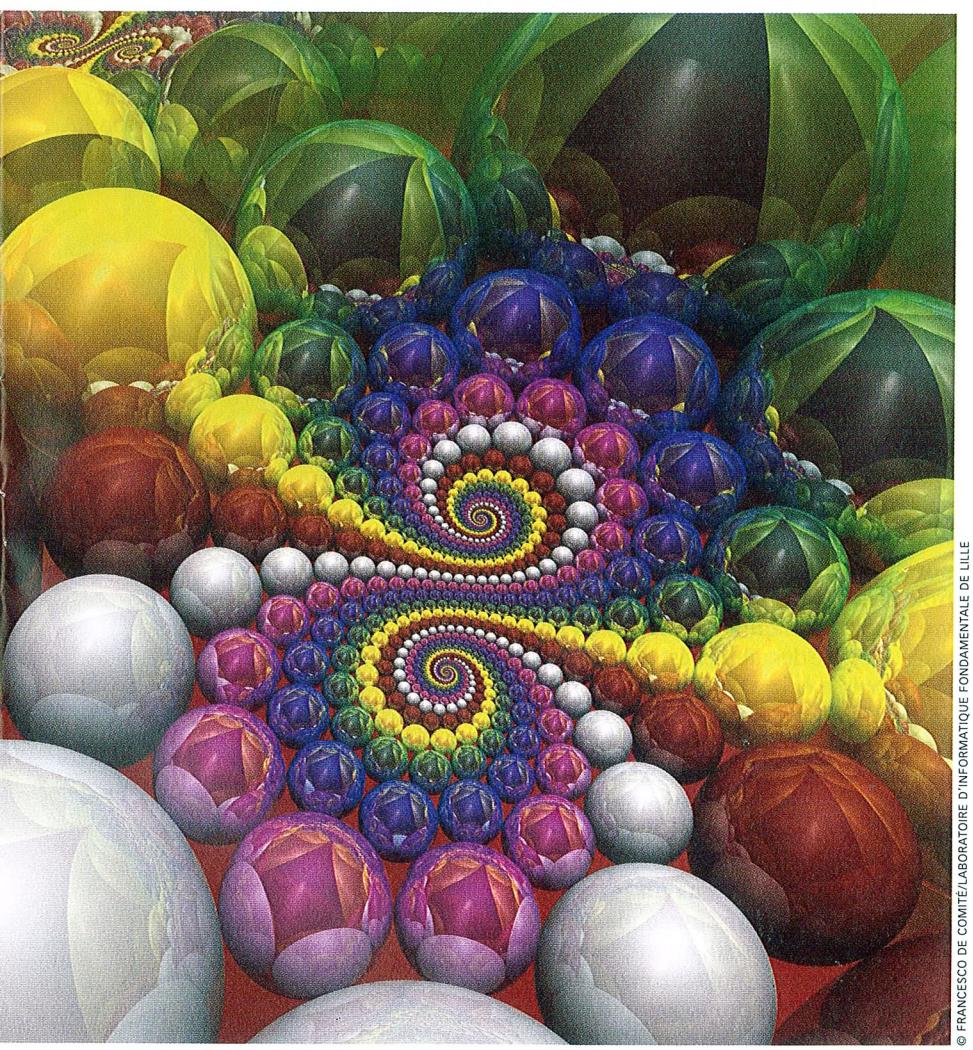
– la logique mathématique et ses extensions, utilisées en intelligence artificielle, dans le domaine des bases de données, pour la mise au point de méthodes de démonstration automatique et la certification de programmes ;

– la modélisation et la simulation qui, à l'aide de graphes et d'une grande variété de structures discrètes, permettent la reproduction dans l'ordinateur d'objets et de systèmes complexes provenant de la physique, de l'économie et de la biologie ;

– la sécurité informatique et la cryptographie, qui créent tout un ensemble de problèmes nouveaux, souvent rattachés à l'arithmétique ;

– l'étude des réseaux, qui suscite de nouvelles idées mathématiques.

L'avenir verra sans doute les liens entre l'informatique et les mathématiques se consolider et se resserrer encore. Il est devenu clair, aujourd'hui, que les deux sciences sont sœurs et que leur développement en synergie rend chaque jour plus profondes et intenses les relations qui les unissent. ●



© FRANCESCO DE COMITÉ/LABORATOIRE D'INFORMATIQUE FONDAMENTALE DE LILLE

SAVOIR +

- DEHORNOY Patrick. *Complexité et décidabilité.* Bâle : Birkhauser, 2000 (coll. Mathématiques et applications).
- DELAHAYE Jean-Paul. *Complexités : aux limites des mathématiques et de l'informatique.* Paris : Belin/Pour la science, 2006.