théorie de la complexité de Kolmogorov a apportés, on remarque ceux-ci.

1) Une nouvelle compréhension du sens des théorèmes d'incomplétude de Gödel : les propositions indécidables (ni elles, ni leur négation ne sont démontrables) dans une théorie donnée doivent leur existence au fait que le contenu en information de la théorie (qu'on mesure par la complexité de Kolmogorov des axiomes de la théorie) limite son pouvoir de preuve : l'incomplétude est un problème de contenu en information des théories, ce qui n'apparaissait pas clairement dans les travaux antérieurs des logiciens.

2) Une conception objective de l'entropie physique : l'entropie physique, lorsqu'on la définit traditionnellement, comporte une composante subjective (elle semble dépendre de l'observateur, ce qui est gênant) qu'évite la définition proposée par le physicien W. Zurek, définition fondée sur la prise en compte de la complexité de Kolmogorov des informations mémorisée par l'observateur.

3) Le nombre *Oméga* de Chaitin est le seul nombre réel qu'on peut définir précisément et dont on peut montrer qu'il est équiréparti dans toutes les bases (en base 10, par exemple, son écriture comporte autant de 0 que de 1, que de 2, etc.), ce qui éclaire à nouveau les phénomènes d'incomplétude et d'indécidabilité algorithmique et rassure sur la cohérence de la théorie de la mesure (laquelle indique qu'il existe des nombres équirépartis, mais ne propose aucune méthode pour en définir).

4) Une nouvelle compréhension du problème de l'induction scientifique (que le philosophe Hume considérait comme impossible et qui fut à l'origine des travaux de K. Popper), de la règle de Bayes et du principe du rasoir d'Ockam (qui indique que, dans une explication, il faut éviter autant qu'on le peut de multiplier les entités et les concepts) et des mises en relation précises de toutes ces notions.

5) La proposition par Charles Bennett d'une distinction mathématique entre complexité aléatoire et complexité organisée (utilisant la complexité de Kolmogorov), distinction qui semble essentielle pour expliquer la complexification des structures de l'Univers au cours du temps qui passe (évolution stellaire, évolution du vivant, etc.).

LA QUESTION DE L'UTILITÉ DES RÉSULTATS DIFFICILES

L'énumération pourrait se poursuivre, mais nous allons nous arrêter sur une des applications toute récente de la théorie de la complexité à l'étude d'un problème d'épistémologie des sciences : est-ce que les résultats mathématiquement difficiles sont ceux qui ont le plus de chances d'être utiles dans les applications ou, au contraire, un résultat mathématiquement difficile est-il toujours condamné à avoir peu d'incidences concrètes?

Bien sûr, tous les mathématiciens souhaitent et tentent de défendre l'idée que démontrer des résultats difficiles est important et très utile. Bien sûr aussi, personne ne conteste que les théories abstraites, les résultats complexes ou très longs à démontrer sont souvent d'une grande beauté et constituent des accomplissements humains remarquables. De même, personne ne met en doute que la compréhension profonde du monde physique ou mathématique nécessite des concepts et des théories qui peuvent être d'une grande abstraction et vraiment très difficiles. On disait à un moment (ce qui est sans doute exagéré) que seul Einstein comprenait la théorie de la relativité, dont l'utilité est incontestable.

Ce dont il s'agit ici c'est seulement la question de savoir si les résultats difficiles parce que longs à démontrer sont utiles, sans prendre en compte la difficulté de la compréhension, qui est un autre problème (chacun sait d'ailleurs que certains résultats de démonstration simple sont difficiles à comprendre).

Il faut reconnaître que les résultats incontestablement difficiles n'ont que peu d'applications concrètes précises. Inversement, les théorèmes les plus utiles des mathématiques semblent être tous assez simples à prouver. Citons quelques exemples confirmant cette remarque, que le mathématicien J. Hartmanis a récemment développée.

FACILE ET TRÈS UTILE, OU DIFFICILE MAIS INUTILE?

Rares sont ceux qui prétendent qu'on trouvera une application concrète au théorème de Fermat (il n'existe pas de solution entière de l'équation $x^n + y^n = z^n$, pour n supérieur à 2), dont on chercha la démonstration pendant des siècles avant de la trouver, il y a six ans, à l'aide d'un raisonnement d'une extrême difficulté, à la fois long et faisant usage de concepts d'une grande abstraction. Aujourd'hui le théorème de Fermat est l'exemple type d'un résultat mathématique difficile, mais sans utilité concrète.

Parmi les résultats difficiles des mathématiques, il y a le fameux théorème de raréfaction des nombres premiers, qui indique que la proportion de nombres premiers parmi les entiers proches de n est environ $1/\ln(n)$. Longtemps recherchée, la preuve de ce théorème fut découverte en 1896 par Jacques Hadamard et Charles de La Vallée-Poussin. Cette preuve, longue et complexe, a été très soigneusement étudiée. Des variantes évitant le recours aux concepts abstraits, dont il semblait étrange que la preuve fasse usage, ont été mises au point, mais ces variantes élémentaires, dans leurs concepts, sont toujours longues et complexes. On peut donc dire, sans risque de se tromper, que ce résultat fait bien partie de la classe des résultats complexes à démontrer. Pourtant son utilité pratique semble réduite, et je crois qu'aucun commerçant, assureur, chimiste ou physicien ne trouvera jamais la moindre utilité à ce théorème : même s'il aide à la conception de certains algorithmes, il n'est jamais utile pour en garantir le bon fonctionnement.

Les résultats d'arithmétique qui sont les plus utiles, par exemple en cryptographie, sont tous d'une relative simplicité et, par exemple, les résultats qui justifient l'algorithme *RSA* (voir *La cryptographie RSA vingt ans après*, *Pour la*

3. Les théorèmes mathématiques utiles sont faciles à démontrer

On a constaté que les résultats mathématiques les plus utiles sont souvent relativement simples à démontrer, ce qui n'empêche pas qu'ils peuvent passer inaperçus durant des siècles. Le cas le plus étonnant est celui de la règle de calcul de Karatsuba, qui permet de réaliser des multiplications entre grands nombres plus rapidement que la méthode classique. Cette règle s'écrit :

$$(a + b \times 10^k)\,(c + d \times 10^k) = ac - [(a - b)\,(c - d) - ac - bd] \times 10^k + bd \times 10^{2k}$$

On peut la démontrer en classe de troisième. Cette identité, lorsqu'on multiplie deux entiers de longueur 2k, ramène le calcul à 3 multiplications entre entiers de taille k, ce qui fait gagner 25 pour cent du temps de calcul par rapport à l'identité classique à la base de la méthode usuelle :

$$(a + b \times 10^k)\,(c + d \times 10^k) = ac + (ad + bc) \times 10^k + bd \times 10^{2k}$$

Les additions sont plus nombreuses dans la formule de Karatsuba, mais elles sont d'un coût négligeable à côté des multiplications.

Directement sous cette forme ou sous des formes un peu plus élaborées (mais toujours faciles à démontrer), l'identité de Karatsuba est l'un des résultats le plus concrètement utiles des mathématiques, car de nombreux logiciels de calcul en font usage. Or elle est à la portée d'un élève de troisième...

Science, février 2000) sont élémentaires, comparés à ceux nécessaires au théorème de raréfaction des nombres premiers. Relevons en passant un paradoxe : les résultats pour le *RSA,* bien plus simples et utiles que le théorème de raréfaction des nombres premiers, ont pourtant été formulés et démontrés bien après : ce qui était difficile, ce n'était pas démontrer de le résultat clef du *RSA*, mais de le découvrir et d'en comprendre l'intérêt.

La règle de calcul de Karatsuba est exactement dans la même situation, mais d'une façon plus nette encore. Elle permet des multiplications rapides de grands nombres, et c'est l'un des résultats les plus utiles de toutes les mathématiques (à chaque seconde qui passe, elle est utilisée par des milliers d'ordinateurs). Pourtant cette règle est véritablement facile à prouver.

Inversement, de nombreux autres grands résultats mathématiques (classification des groupes simples, démonstration de la transcendance de π, théorèmes de Gödel, etc.), et dont les démonstrations sont longues, semblent d'une utilité pratique nulle.

De même, les grandes conjectures indémontrées (dont on peut penser qu'elles sont indémontrées parce qu'elles n'ont pas de démonstrations simples) ne paraissent pas avoir d'applications potentielles. Si l'on réussissait à établir qu'il y a une infinité de nombres premiers jumeaux (conjecture des nombres premiers jumeaux), ou que tout nombre pair est somme de deux nombres premiers (conjecture de Goldbach), ou que l'algorithme de Syracuse conduit toujours à 1 (conjecture de Syracuse), rien de concret n'en résulterait, aucune *start-up* n'en sortirait et, abstraction faite des récompenses offertes par des mécènes sensibles aux mystères des mathématiques et des positions universitaires auxquelles pourront prétendre les génies qui résoudront ces problèmes, ce sont de purs défis sans conséquences économiques ou matérielles attendues.

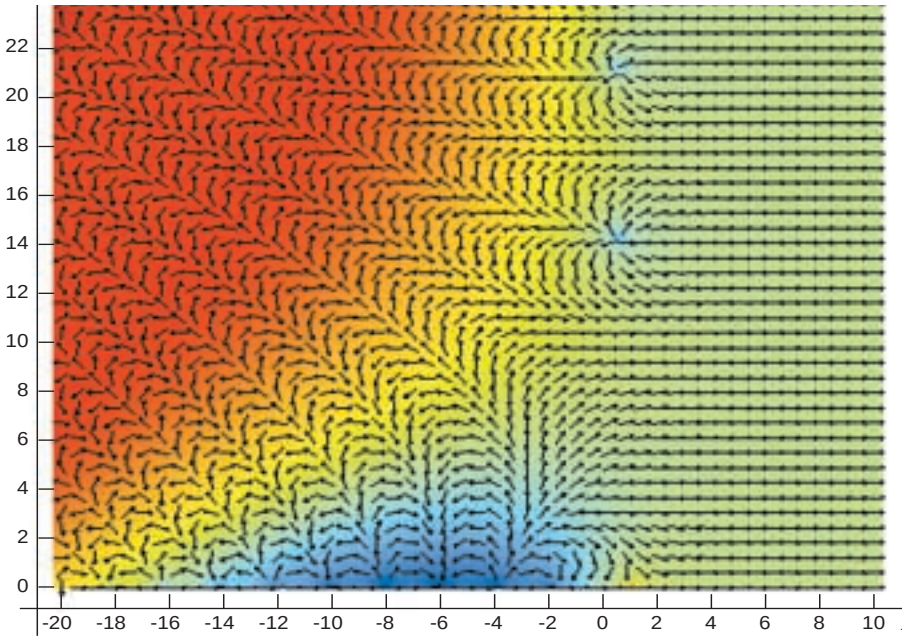
Les réflexions menées sur la célèbre conjecture *P = NP* (qui pourtant porte sur une question d'efficacité d'algorithmes) ont conduit le mathématicien J. Hartmanis à croire que sa solution (si on la trouve) ne changera concrètement pas grand-chose à la situation de l'informatique. Là encore, et même en informatique, on croit découvrir la confirmation que ce qui est difficile à prouver ne peut pas être concrètement utile.

Cette constatation ne doit pas nous décourager de faire des mathématiques, mais au contraire doit nous rassurer : si ce qui est utile est toujours assez facile à démontrer, c'est une raison de plus pour faire des mathématiques qui deviennent, pour ce qui est applicable, une science à la portée du plus grand nombre.

LA LOI DE L'INUTILITÉ DES PREUVES COMPLEXES

Les résultats mathématiques utiles semblent donc toujours simples, ou – ce qui revient au même – ce qui est mathématiquement complexe à démontrer apparaît toujours inutile sur le plan concret. Peut-on établir de telles affirmations générales et en apparence philosophiques? Oui, et c'est ce que viennent de faire Vladik Kreinovich et Luc Longpré, deux chercheurs de la théorie de la complexité. Ils ont prouvé que, si un résultat est potentiellement utile, alors il n'est pas possible qu'il possède une preuve complexe.

Le résultat technique est impossible à expliquer dans tous ses détails, mais



4. La conjecture de Riemann est-elle utile ?

Le théorème suivant est dû à G. Miller et E. Bach :

Si l'hypothèse de Riemann généralisée (une conjecture liée à la répartition des nombres premiers, qui stipule que les zéros de cette fonction, représentée ci-dessus, sont sur la droite d'abscisse 1/2) est vraie et si pour tout entier *a* entre 1 et $2.\ln^2(n)$ le nombre *n* est *a-fortement-probablement-premier*, alors, *n* est premier.

(Le nombre *n* est *a-fortement-probablement premier* si, après avoir écrit $n - 1 = 2^r q$ avec *q* impair, on constate que $a^q = 1 \bmod n$ ou que $a^{q\,2^i} = -1 \bmod n$ pour un entier $i = 0,1, ..., r - 1$.)

Considérons alors l'algorithme suivant :

Algorithme de Miller et Bach

• Pour tout $a = 2, 3,$ jusqu'à $2.\ln^2 (n)$, tester si *n* est *a-fortement-probablement premier ;*
• Dès que la réponse est non, répondre : *n* est composé ;
• Si la réponse a toujours été oui, répondre : *n* est premier.

Le résultat de Miller et Bach signifie que, si l'hypothèse de Riemann généralisée est vraie, cet algorithme ne se trompe jamais. Cet algorithme fonctionne en temps polynomial c'est-à-dire rapidement. Nous avons donc un algorithme rapide pour tester la primalité des nombres entiers (ce qui est incontestablement utile), mais la garantie de son bon fonctionnement n'est pas assurée, car l'hypothèse de Riemann généralisée reste non démontrée. Il semble donc que l'hypothèse de Riemann généralisée est un résultat à la fois difficile et utile concrètement : sa démonstration garantirait que l'algorithme de Miller et Bach fonctionne toujours.

Un théorème récent de Vladik Kreinovich et Luc Longpré indique que, malgré cette situation, l'hypothèse de Riemann généralisée n'est pas vraiment utile, car, en pratique, sans l'hypothèse de Riemann, on montre que, sauf pour des cas très rares, l'algorithme de Miller et Bach fonctionne correctement.

Leur théorème, dont le sens est plus général, signifie que, si un résultat ne possède que des démonstrations complexes, alors il ne peut être concrètement utile.