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.

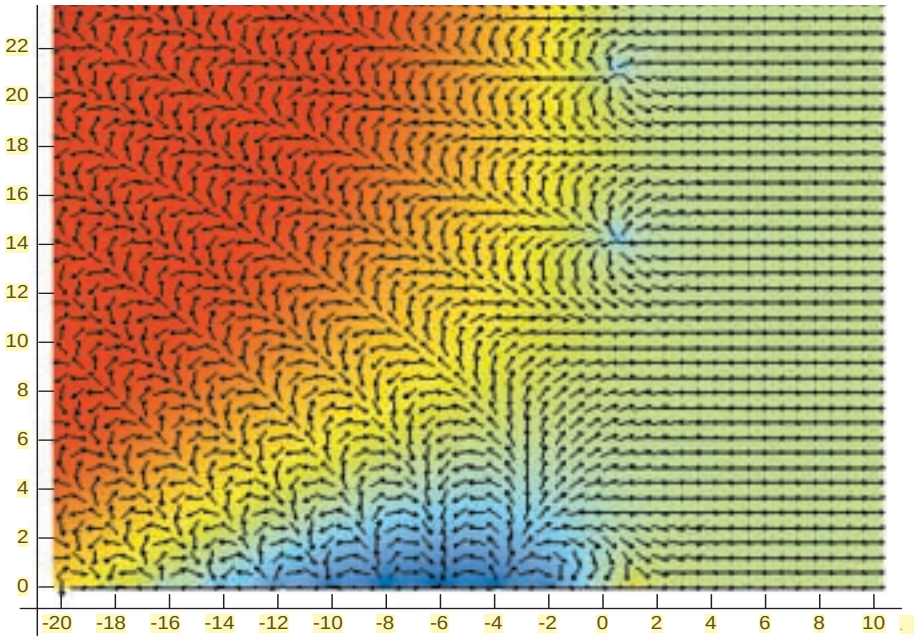
Les réflexions menées sur la célèbre conjecture *P* = *NP* (qui pourtant porte sur une question d'efficacité d'algorithmes) ont conduit le mathématicien J. Hartmanis à croire que sa solution (si on la trouve) ne changera concrètement pas grand-chose à la situation de l'informatique. Là encore, et même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

5. La loi de l'inutilité des preuves complexes

Vladik Kreinovich et Luc Longpré ont prouvé, en utilisant les concepts et méthodes de la théorie de la complexité, que :
– Si un résultat est potentiellement utile, alors il n'est pas possible qu'il possède une preuve complexe.
Leur travail a comporté plusieurs étapes.
– Formulation d'une définition mathématique de la notion de résultat potentiellement utile. Selon eux, un résultat est utile s'il permet de prouver le bon fonctionnement d'un algorithme et qu'on ne peut pas substituer à cet algorithme un algorithme probabiliste (c'est-à-dire fonctionnant avec un risque d'erreur aussi petit qu'on le souhaite) dont le bon fonctionnement soit simple à établir.
– Formulation d'une définition mathématique de la notion de preuve complexe. Leur définition prend en compte à la fois le nombre d'étapes élémentaires de raisonnement de la preuve et les possibilités de simplification dues à d'éventuelles parties répétitives. Pour eux, une preuve complexe est une preuve longue, et qui le reste même après exploitation des parties répétitives.
– Utilisation de la théorie de la complexité pour prouver leur affirmation.
Le résultat de Kreinovich et Longpré est un exemple récent provenant de la théorie de la complexité de résultats mathématiques ayant un contenu philosophique intéressant et inattendu. Il est probable qu'il déplaira aux mathématiciens qui aiment justifier leurs travaux, même les plus difficiles, en évoquant de possibles applications futures.

tentons tout de même de le présenter, il en vaut la peine.

Les deux chercheurs, pour arriver à leur résultat, ont d'abord donné une définition mathématique de la notion de résultat potentiellement utile.

Pour eux, un tel résultat est un énoncé *S*, qui permet d'établir une formule du type «pour tout *x*, *P(x)*», où *P(x)* est facilement vérifiable (par exemple, une formule du type «si la somme des chiffres de *x* est un multiple de 9, alors *x* est un multiple de 9»).

Leur définition est justifiée, car ce sont les résultats de ce type qui assurent que les méthodes algorithmiques fonctionnent correctement : algorithmes de codage, algorithmes de recherche dans une base de données, algorithmes de tri de données, algorithmes de calcul numérique, algorithmes de simulation, etc.

Ensuite les deux chercheurs définissent une preuve complexe d'une manière fine et subtile *(voir la figure 5)*.

Leur résultat, formulé avec plus de précision, est : si *S* n'a que des preuves complexes et permet de montrer que «pour tout *x P(x)*», alors pour la quasi-totalité des données de taille raisonnable (les seules qu'on rencontre en pratique) *P(x)* est vrai indépendamment de *S*. En quelques mots : si *S* est complexe, et que *S* = > (pour tout *x P(x)*) alors, sauf de manière exceptionnelle, on n'a pas besoin de *S* pour savoir que *P(x)* est vrai.

En très court, si *S* est complexe, alors ce n'est pas un résultat potentiellement utile.

Ce résultat s'applique en particulier à la conjecture de Riemann (un résultat qui concerne la répartition des nombres premiers et qui est considéré comme l'énoncé mathématique irrésolu le plus recherché des mathématiques aujourd'hui). Il a été prouvé par G. Miller et E. Bach que, si une forme généralisée de l'hypothèse de Riemann était vraie, alors il existait un algorithme efficace (l'algorithme de Miller et Bach) pour tester la primalité des nombres entiers en temps polynomial, c'est-à-dire efficacement. Cette situation a conduit de nombreux mathématiciens à croire que les recherches sur l'hypothèse de Riemann étaient utiles, même dans une optique d'applications pratiques.

Est-il vraiment utile de démontrer Riemann?

La situation créée par l'algorithme de Miller est qu'on dispose sans doute d'un algorithme efficace de test de primalité dont le bon fonctionnement dépend de la vérité de l'hypothèse de Riemann généralisée. Ce qu'énonce le résultat de Vladik Kreinovich et Luc Longpré est : si vraiment l'hypothèse de Riemann généralisée ne possède pas de preuve simple, alors l'algorithme de Miller pour des entiers de tailles raisonnables fonctionne correctement pour la quasi-totalité des cas qu'on peut lui soumettre. On n'a donc pas besoin en pratique de la démonstration de l'hypothèse de Riemann généralisée si l'on désire utiliser cet algorithme.

Cette inutilité pratique de l'hypothèse de Riemann dans le cas des tests de primalité est d'ailleurs corroborée par l'usage informatique réel : dans les applications cryptographiques où l'utilisation des nombres premiers est intensive, on se sert le plus souvent des méthodes probabilistes de test de primalité, c'est-à-dire de méthodes dont le bon fonctionnement est justifié par un raisonnement relativement simple, mais qui ne donnent un résultat que d'une manière probabiliste, autrement dit avec un risque, jugé négligeable, d'erreur.

Tout n'est pas terminé

Notons, pour l'amusement, que le résultat de Vladik Kreinovich et Luc Longpré possède une démonstration assez courte (environ une page) : il n'est donc pas impossible, d'après ce qu'il nous apprend, qu'il soit un résultat concrètement utile !

Notons aussi qu'en toute rigueur, malgré les longues recherches faites à son sujet, il n'est pas logiquement exclu que la conjecture de Riemann possède une démonstration simple. Si c'est le cas, l'hypothèse de Riemann pourrait être pratiquement utile. Nous devons continuer à en rechercher la preuve, même si l'intérêt mathématique pur ne nous semble pas une raison suffisante de nous y intéresser.

Précisons que, même si, après une traduction mathématique sous une certaine forme particulière, on a réussi à établir que le difficile est inutile, il ne faut pas donner une importance excessive au résultat de Vladik Kreinovich et Luc Longpré qui fixent, dans leurs définitions, le sens des mots peut-être un peu rapidement.

Dans le cœur de tous les mathématiciens est inscrite la conviction que plus c'est difficile, plus c'est beau et important, et donc utile au moins par l'approfondissement et une meilleure vision que cela procure à notre perception du monde des entités abstraites. «Le but unique de la science, c'est l'honneur de l'esprit humain», écrivait le mathématicien Jacobi dans une lettre adressée à son collègue Legendre en 1830. Il est peu vraisemblable que le formalisme mathématique s'empare un jour de cette vérité philosophique-là !

G. Bachelard, *La philosophie du non*, Presses Universitaires de France, Paris, 1940.

W. H. Zurek, *Algorithmic Randomness and Physical Entropy*, in *Physical Review A*, n° 8, vol. 40, pp. 4731-4751, 1989.

***The Philosophy of Mathematics*, sous la direction de W. H. Hart, Oxford University Press, 1996.**

Ming Li et Paul Vitanyi, *An Introduction to Kolmogorov Complexity and Its Applications*, Springer-Verlag, New York, 1997.

J.-P. Delahaye, *Information, complexité et hasard*, Hermès, Paris, 1999.

V. Kreinovich et L. Longpré, *How Important Is Theory for Practical Problems?*, in *Bulletin of the European Association for Theoretical Computer Science* (EATCS), n° 71, pp. 160-164, 2000.