

Éditorial

Dans cet ouvrage

Les algorithmes sont des « recettes » pour résoudre des problèmes. La recette consiste à ramener le problème à une suite finie d'opérations clairement identifiées, exécutables par un être humain ou éventuellement par une machine. Les algorithmes sont omniprésents en mathématiques et contribuent à leur incroyable efficacité. C'est pourquoi nous avons choisi le thème des algorithmes pour ce numéro. Dès le développement des premiers systèmes de numération, des algorithmes ont été mis au point pour effectuer les opérations de base, calculer des puissances ou extraire des racines. Les exemples présentés dans **Algorithmes au cours de l'histoire** illustrent le fait que ceux-ci peuvent dépendre du système de numération et des procédés techniques utilisés pour effectuer les calculs.

Mais il ne suffit pas d'avoir un algorithme. Encore faut-il pouvoir l'exécuter en un temps raisonnable. Les algorithmes de factorisation des grands nombres fascinent les mathématiciens : il est très facile de multiplier deux grands nombres premiers, mais beaucoup plus difficile de retrouver les facteurs. Ce thème est abordé dans deux articles.

Dans son article **L'héritage de Fermat pour la factorisation des grands nombres**, Jean-Marie De Koninck nous fait part de progrès dans cette direction, lesquels nécessitent le recours à l'essai-erreur.

L'article **Facile, difficile, ...** de Christiane Rousseau décrit comment la difficulté de factoriser de grands nombres a permis de construire un procédé de cryptographie, le code *RSA*, présentement inviolable sur nos ordinateurs, mais qui ne résistera pas à l'avènement de l'ordinateur quantique.

Le développement d'un algorithme est le fruit d'une réflexion théorique sur le type de problèmes ou d'opérations à effectuer. Dans **Émergence logarithmique : la « mirifique » invention de Napier**, Jérôme Camiré-Bernier et Bernard R. Hodgson décrivent la démarche qui a mené à l'invention des logarithmes par John Napier (1550-1617). Cette invention a permis le développement d'algorithmes très efficaces pour calculer un produit, une puissance ou la racine $n^{\text{ième}}$ de très grands nombres.

Il n'existe pas toujours de méthode exacte pour résoudre un problème d'optimisation en un temps raisonnable. Inspiré par la théorie de l'évolution de Charles Darwin (1809-1882), John Henry Holland (1929-2015) a développé une approche appliquant la notion de sélection naturelle à une population de solutions potentielles au problème posé. Dans **Algorithmes génétiques**, Charles Fleurent donne un aperçu de cette nouvelle famille d'algorithmes.

Dans un second paradoxe intitulé **L'information paradoxale**, Jean-Paul Delahaye nous présente un problème qui est soluble même si on peut à prime abord penser manquer d'information pour y parvenir.

Bonne lecture !
André Ross

Rédacteur en chef

André Ross

Professeur de mathématiques

Comité éditorial

Pietro-Luciano Buono

*Professeur de mathématiques
Université du Québec à Rimouski*

France Caron

*Professeure de didactique
des mathématiques
Université de Montréal*

Christian Genest

*Professeur de statistique
Université McGill*

Frédéric Gourdeau

*Professeur de mathématiques
Université Laval*

Bernard R. Hodgson

*Professeur de mathématiques
Université Laval*

Stéphane Laplante

*Enseignant de mathématiques
Collège de Montréal*

Christiane Rousseau

*Professeure de mathématiques
Université de Montréal*

Robert Wilson

*Professeur de mathématiques
Cégep de Lévis-Lauzon*

Production et Iconographie

Alexandra Haedrich

Institut des sciences mathématiques

Conception graphique

Pierre Lavallée

Néograf Design inc.

Illustrations de scientifiques et caricatures

Noémie Ross

Illustrations mathématiques

André Ross

Révision linguistique

Robert Wilson

*Professeur de mathématiques
Cégep de Lévis-Lauzon*

Accromoth

*Institut des sciences mathématiques
Université du Québec à Montréal
Case postale 8888, succ. Centre-ville
Montréal (Québec)
H3C 3P8 Canada*

redaction@accromath.ca
www.accromath.ca