Mathématiques

Cours d'algèbre. Primalité. Divisibilité. Codes.

Michel Demazure. Éditions Cassini.

Depuis le XVIIIe siècle, la mécanique, l'électromagnétisme, la thermodynamique, et les théories de la relativité et de la mécanique quantique ont inspiré les travaux des plus grands mathématiciens. Depuis quelque temps, des questions mathématiques bénéficient, de même, d'un nouvel éclairage et de nouveaux moyens d'investigation apportés par l'informatique. Cette dernière est même la source de nouveaux problèmes. Le mathématicien contemporain ne peut plus ignorer que l'arithmétique, longtemps considérée comme la reine des mathématiques pures, est devenue, avec l'apparition de l'informatique, un domaine de mathématiques appliquées.

Le cours d'algèbre de Michel Demazure, paru aux éditions Cassini, est une démonstration de cette transformation.

La première partie, intitulée «Primalité», nous entraîne dans le sillage tracé par Euclide il y a plus de 2 000 ans, lorsqu'il établit l'existence d'une infinité de nombres premiers et qu'il identifia l'algorithme qui porte aujourd'hui son nom, pour le calcul du «plus grand commun diviseur». Les théorèmes de Fermat et d'Euler nous amènent au test de primalité de Miller-Rabin. L'étude des résidus quadratiques (un résidu quadratique modulo un nombre *n* est un nombre qui est un carré modulo *n*) se conclut par un autre test de primalité : celui de Solovay. Grâce à la notion de racine primitive, le critère de primalité de Lucas-Lehmer nous permet de découvrir de très grands nombres premiers (le plus grand, découvert il y a un an, comprend près de un million de chiffres décimaux !). Tout cela n'est envisageable qu'à l'aide de la transformation de Fourier rapide, qui fait l'objet d'un chapitre.

La deuxième partie traite de la divisibilité dans les anneaux commutatifs (un anneau est un ensemble dont les éléments peuvent être additionnés ou multipliés ; l'anneau est commutatif si la multiplication est commutative, c'est-à-dire si le produit de deux éléments *a* et *b* est égal au produit de *b* et *a*). Les notions classiques d'idéaux, d'anneaux quotients, le théorème des restes chinois, les anneaux factoriels et euclidiens y sont abordés (un anneau est factoriel s'il existe une notion de décomposition en facteurs premiers analogue à celle qui existe pour l'ensemble des entiers).

La dernière partie propose, après avoir traité des corps finis, de leur construction et du problème de la décomposition des polynômes dans ces corps, une présentation des codes correcteurs d'erreurs sans lesquels nous ne pourrions recevoir des images venues du fin fond de l'espace, écouter nos disques laser ou «surfer» sur *Internet*.

L'originalité de ce cours tient dans sa démarche délibérément algorithmique. Certes, peu d'ouvrage traitant de la notion de PGCD de deux éléments d'un anneau euclidien omettent de mentionner l'algorithme d'Euclide, mais, inversement, peu s'intéressent à la réalisation effective des calculs amenés par cet algorithme. Non seulement de nombreux algorithmes ponctuent ce cours (certains sont même implantés en CAML-Light, langage utilisé dans certaines classes de préparation aux grandes écoles, ou en langage C), mais eux-mêmes, ou les calculs qui sont induits, font l'objet d'études particulières. Car à quoi bon posséder un algorithme s'il n'est pas utilisable en pratique?

C'est ainsi que sont présentés le calcul rapide de la multiplication des grands entiers, celui des puissances, nécessaires au système de cryptographie RSA. L'ignorance actuelle d'algorithmes efficaces pour tester la primalité des entiers ou pour déterminer leur factorisation amène l'auteur à traiter des algorithmes probabilistes qui font appel au hasard pour mener leurs calculs et supplantent tous les algorithmes déterministes connus. Arrivés là, nous ne sommes plus très loin de l'un des plus célèbres problèmes de l'informatique théorique, à savoir la coïncidence entre la classe des problèmes que l'on peut résoudre en temps polynomial et celle des problèmes dont on peut vérifier une solution en temps polynomial.

Il ne faudrait cependant pas croire que ce cours d'algèbre n'est destiné qu'aux ingénieurs (il est enseigné à l'École polytechnique). Il s'agit bien d'un cours de mathématiques qui ne cède en rien aux canons de la rigueur et qui traite de sujets mathématiques.

À l'heure où l'on parle d'une prochaine réforme de l'enseignement des mathématiques dans l'enseignement secondaire, visant entre autres à introduire des questions liées à l'informatique, comment ne pas conseiller la lecture de cet ouvrage à tous les candidats au CAPES ou à l'agrégation, ainsi qu'à toute personne désireuse de rafraîchir ou de compléter ses connaissances en arithmétique et en algèbre, ou encore de les redécouvrir sous un nouveau jour?

Éric WEGRZYNOWSKI

Histoire

La Grande Guerre chimique, 1914-1918

Olivier Lepick. Presses universitaires de France.

Les apprentis sorciers : Fritz Haber, Werner von Braun, Edward Teller

Michel Rival. Éditions du Seuil.

Le 26 avril 1915, à 17 heures, l'armée allemande déverse 150 tonnes de chlore, enfermé dans 5 830 cylindres, sur un front de six kilomètres de large, près du village de Langermarck, dans le saillant d'Ypres, au Sud de la Belgique. Un nuage verdâtre, poussé par le vent, se dirige, à la vitesse de deux à trois mètres par seconde, vers les lignes françaises ; dans la panique indescriptible qui s'ensuit, le front français est rompu sur près de deux kilomètres.

C'est ainsi que naquit la «guerre chimique» – l'expression «guerre des gaz» est moins appropriée, car de nombreuses armes chimiques ne sont pas des gaz – qui marqua la mémoire collective européenne. Spécialiste d'histoire militaire, Olivier Lepick donne un ouvrage fondamental sur ce sujet. Le sérieux de son étude n'étonne pas, puisqu'elle fut réalisée dans le cadre d'un doctorat d'histoire ; ce qui surprend très agréablement, c'est la lisibilité parfaite de l'ouvrage et le talent avec lequel l'auteur fait partager ses découvertes.

L'emploi de l'arme chimique durant la «Grande Guerre» fut la réaction à une situation stratégique que les états-majors français et allemands n'avaient pas prévue : on avait misé sur une guerre rapide, avec beaucoup de pertes, car la puissance de feu des belligérants semblait empêcher une guerre longue. Erreur : si les premiers mois ont bien été très meurtriers, ils ont fait sombrer la guerre dans une gigantesque guerre de siège, la «guerre des taupes», où une ligne continue de tranchées séparait les adversaires, de la mer du Nord à la Suisse. L'auteur montre comment, dans l'impasse, les états-majors ont recherché l'arme qui ferait revenir à une guerre de mouvement.

Malgré les conventions internationales qui proscrivaient l'utilisation de «gaz asphyxiants ou délétères», tous les belligérants avaient employé, dans les premiers mois, des munitions chimiques