exemple) sont exclus par les organisateurs. Je trouve cette option discutable, car un test probabiliste fait de telle façon qu'il ne reste qu'une probabilité d'erreur inférieure à 10^{-1000} serait aussi sûr qu'un test fait (même plusieurs fois) sur des machines qui ont chacune une probabilité de mauvais fonctionnement supérieure à 10^{-100}. Cette clause n'est toutefois pas pénalisante, car les tests probabilistes ne savent pas traiter efficacement des nombres de plusieurs millions de chiffres.

Il n'est pas impossible et pas interdit par les règles du concours EFF que quelqu'un réclame le prix en proposant non pas un long calcul, mais une formule facilement exploitable *f(n) (voir l'article de janvier 1999 de cette rubrique sur les formules pour les nombres premiers)* avec la démonstration mathématique que, pour toute valeur du paramètre n, la formule $f(n)$ produit un nombre premier.

Si, par exemple, la formule de Marcel Pagnol $4n^2 + 4n - 1$ avait été correcte, comme c'est une formule simple à mettre en œuvre pour obtenir des nombres de un million, dix millions, cent millions, et même un milliard de chiffres, le grand écrivain aurait pu (aidé d'un informaticien pour expliciter les développements décimaux de ses propositions) réclamer d'un coup tous les prix offerts par l'EFF. Si vous détenez une telle formule, vous êtes riche.

Pour qu'un prétendant gagne un prix, l'annonce de son résultat, avec un minimum de précisions sur la méthode permettant de prouver la primalité, doit être publiée dans une revue académique. De telles revues procèdent à l'expertise préalable des articles publiés en les soumettant à des spécialistes reconnus. Même si l'article rendant compte du record ne comporte qu'une seule page, il assure que le prix est attribué en accord avec les expertises scientifiques.

Si vous proposez une formule nouvelle, l'article devra comporter la preuve qu'elle donne des nombres premiers et des indications sur son exploitation concrète pour engendrer des nombres premiers de un million de chiffres ou plus. Si quelqu'un proposait une formule simple dont la démonstration qu'elle ne donne que des nombres premiers est complexe (il est fréquent en arithmétique que les démonstrations occupent des dizaines de pages), la vérification pourrait prendre plusieurs mois.

Les organisateurs se réservent la possibilité de demander le développement décimal complet des nombres proposés. Expliciter ce développement décimal pour une formule du genre $3^{1000000} + 17$ n'est pas très facile, mais les spécialistes y arrivent pour des nombres de quelques millions de chiffres, voire quelques milliards de chiffres. Si votre proposition est simple, on ne vous demandera pas d'en expliciter le développement décimal ; si elle est inhabituelle, alors il faudra que vous prouviez que vous êtes capable de l'exploiter. Si vous avez trouvé une méthode, vous réussirez sans peine à convaincre un spécialiste de vous aider… contre une partie de la récompense.

7. LES DIVISEURS PREMIERS DE M_p

Il est plus facile de démontrer que les nombres de Mersenne sont premiers que d'autres nombres, car un diviseur premier de $2^p - 1 = M_p$ (p premier supérieur à 2) est toujours de la forme $2mp + 1$.

En effet, soit q un diviseur premier de $2^p - 1 = M_p$ (p premier et > 2).

On a : $2^p - 1 = 0 \pmod q$, donc $2^p = 1 \pmod q$.

Les solutions positives de l'équation $2^x = 1 \pmod q$ sont les multiples d'un nombre positif, k, plus petite solution positive de l'équation $2^x = 1 \pmod q$ (cela résulte du fait évident que, si x et x' sont deux solutions positives de cette équation, leur différence aussi).

Le plus petit k tel que $2^k = 1 \pmod q$ est donc un diviseur de p, c'est-à-dire 1 ou p. Ce ne peut pas être 1, car $2^1 \neq 1 \pmod q$, c'est donc p.

En utilisant le petit théorème de Fermat (qui dit que, si q est premier, alors pour tout nombre a qui n'est pas multiple de q, il existe un q positif tel que $a^k = 1 \pmod q$) et que le plus petit k positif vérifiant cette équation divise $q - 1$), on en déduit que p divise $q - 1$, autrement dit $q = hp + 1$ pour un certain h. Ce nombre h est pair, car sinon hp serait impair et donc q serait pair, ce qui ne se peut pas puisque q est un diviseur premier d'un nombre impair. Donc $h = 2m$, et donc $q = 2mp + 1$.

Ce théorème permet de déterminer rapidement les M_p qui sont premiers. Ainsi, pour étudier la primalité de $M_{13} = 2^{13} - 1 = 8\,091$, il suffit de tester si ce nombre est divisible par un nombre premier de la forme $26k + 1$ inférieur à $\sqrt{8091} = 90{,}504$. Les nombres de la forme $26k + 1$ inférieurs à 91 sont 27, 53 et 79. Seuls 53 et 79 sont premiers. Deux divisions suffisent pour prouver que M_{13} est premier.

UN MARCHÉ DU CALCUL?

Les promoteurs pourraient développer ainsi un marché du temps de calcul. D'une part, chaque propriétaire d'une machine (même de puissance moyenne) n'utilise que très peu la puissance de sa machine et, si on lui proposait quelques francs par jour pour que sa machine travaille quand il ne s'en sert pas, il serait heureux et gagnant (en quelques mois, il récupérerait le prix d'achat de sa machine). D'autre part, de nombreux projets scientifiques pourraient bénéficier de l'existence de ce marché qui éviterait le gâchis formidable de 99 pour cent de la capacité de calcul dont dispose l'humanité.

Des projets fonctionnant aujourd'hui sur le principe du bénévolat ont déjà été mis en place (le projet GIMPS dont nous avons parlé ci-dessus en est un exemple). Ces calculs géants en réseaux auxquels chacun peut associer sa machine portent sur la factorisation de grands entiers, sur la recherche des chiffres binaires de π, sur l'étude détaillée de signaux radio provenant du ciel pour y découvrir d'éventuels signes d'intelligence extraterrestre (projet SETI), sur le craquage de codes cryptographiques créés par défi ou par des firmes qui veulent montrer qu'elles vendent des méthodes résistant aux attaques les plus sérieuses.

Le réseau Internet pourrait changer l'univers de l'information, mais aussi l'univers du commerce. Avec les projets de calculs distribués, il pourrait aussi bouleverser l'univers du calcul pour atteindre des puissances de calcul aujourd'hui réservées aux riches institutions. Il se pourrait aussi que la loi de Moore (doublement de la puissance de calcul tous les 18 mois) puisse par ces moyens être dépassée (doublement tous les 12 mois, voire tous les 6 mois).

Jean-Paul DELAHAYE est professeur d'informatique à l'Université de Lille.

http://www.mersenne.org/prime.html : The Great Internet Mersenne Prime Search. Pour participer à la recherche de nouveaux nombres premiers records.

http://entropia.com : organisation dédiée à des projets de calculs distribués.

http://eff.org et http://eff.org/coop-awards/ : à propos des prix proposés par l'Electronic Frontier Foundation.

http://www.scruznet.com/~luke/mersenne.htm : à propos de Marin Mersenne.

http://www.utm.edu/research/primes/ Le meilleur site internet sur les nombres premiers (C. Caldwell).

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