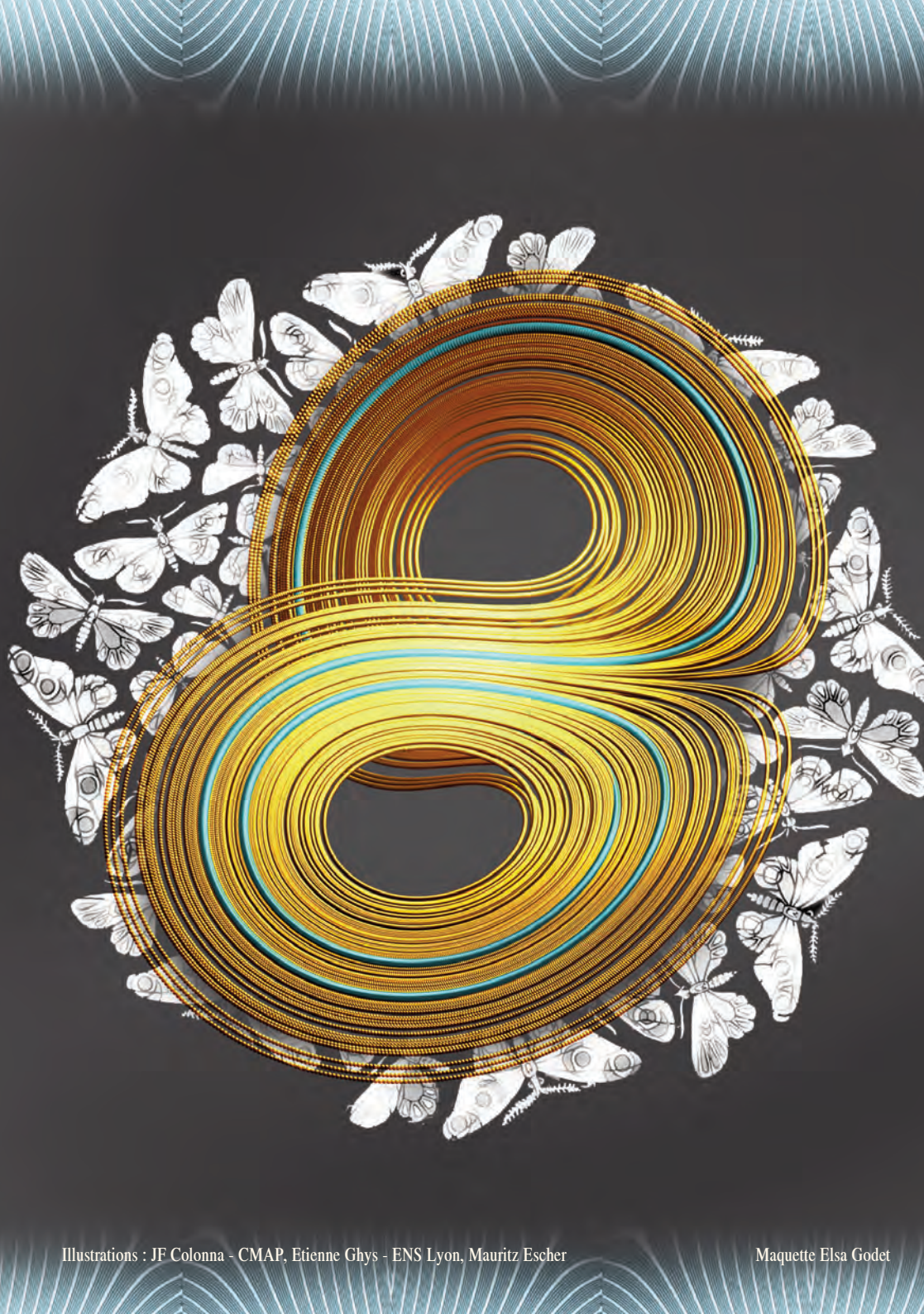
Le Comité international
des jeux mathématiques présente :

Maths Enigmes Express

www.cijm.org



Illustrations : JF Colonna - CMAP, Etienne Ghys - ENS Lyon, Mauritz Escher

Maquette Elsa Godet

Enigmes Mathématiques

d'hier et d'aujourd'hui

2006
Une nouvelle médaille Fields Française
2007
Il y a 300 ans naissait Léonard EULER

Deux belles occasions pour le Comité International des Jeux Mathématiques de se lancer dans l'aventure qui consiste en quelques pages à évoquer les *Enigmes Mathématiques d'Hier et d' Aujourd'hui* .

Notre volonté d'ancrer les mathématiques dans leur histoire, de prouver qu'elles sont riches, belles et, ô combien vivantes, trouvait sous ce thème un magnifique champ d'exploration.
Pour vous parler de cet incroyable foisonnement d'idées nous avons divisé cet ouvrage en trois parties.

La première partie retrace le développement à travers les âges, de trois thèmes fondateurs des mathématiques : le calcul et les équations, les géométries et la logique. Trois thèmes qui furent riches en rebondissements et qui ont généré de nombreuses questions.

La deuxième partie traite des énigmes de notre temps et des défis pour le futur. Toute cette science mathématique, faite par des femmes et des hommes, perpétue une longue tradition d'échanges, de voyages et de rencontres. Parfois en pensée libre, parfois en pensée *commandée* par notre quotidien, la médecine, l'industrie ou la conquête de l'espace, de l'infiniment grand à l'infiniment petit, ils mêlent les idées pour en trouver de nouvelles et ainsi mieux appréhender notre monde. Ils font surgir des liens inattendus entre des domaines à priori bien distincts !

Enfin la dernière partie vous emmène à la rencontre de ces mathématiciens qui à travers les époques ont su tirer profit de certains aspects ludiques des mathématiques. On mesure mieux, avec le recul, l'influence que cette approche a eu sur l'élaboration de théories très complexes.
Enigmes, poèmes, jeux, défis se sont répondu à travers les âges pour le plus grand plaisir de chacun, abordant ainsi par un biais plus *plaisant et délectable** des problèmes d'une grande complexité.

Pour conclure, je voudrais remercier toutes celles et tous ceux qui nous ont aidés pour la rédaction de ces pages ainsi que les organismes qui nous apportent leur soutien et nous permettent d'éditer cette brochure. J'espère enfin que vous, lecteur, aurez quelque satisfaction à parcourir ces lignes sachant qu'en mathématiques, le chemin qui mène à la résolution d'une énigme est souvent difficile.

Bonne lecture

Marie José Pestel

*Extrait du titre du premier recueil de jeux mathématiques.

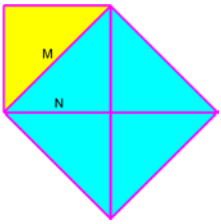
L'infini, entre logique et paradoxes

Hervé LEHNING

Notre monde, comment est -il ?
Discret ou continu ?
Logique ou indécidable ?
Mesurable ou incommensurable ?

Dans le monde imaginé par Pythagore au VI^e siècle avant Jésus-Christ, *tout est nombre*, c'est-à-dire nombre entier ou rapport de nombres entiers, ce que nous nommons *nombre rationnel*. Pythagore pense à un monde composé de particules insécables, toutes identiques. Les droites y sont constituées de points contigus, de même épaisseur. Dans ce modèle, si deux segments contiennent N et M points, le rapport de leurs longueurs est égal à N / M. Plus généralement, deux grandeurs de même nature : surfaces, volumes, temps, etc. sont toujours commensurables.

Pourtant l'école pythagoricienne a détruit ce mythe. Pour preuve la version simplifiée du théorème :



En construisant le carré bleu sur la diagonale du carré jaune on montre l'existence de deux entiers N et M tels que : $M^2 = 2\,N^2$. En factorisant M et N, on obtient un nombre pair de facteurs 2 dans M^2 et un nombre impair dans $2\,N^2$, ce qui interdit l'égalité de ces deux nombres.

Le modèle discret

Le rêve de Pythagore s'écroule, et avec lui l'idée d'un monde discret, c'est-à-dire formé de particules identiques insécables. Zénon (V^e siècle avant Jésus-Christ) a réfuté ce modèle d'une manière plus radicale. Supposons, après lui, le temps discret, il est ainsi composé d'instants insécables. Nous pouvons les dénombrer : instant 1, instant 2, instant 3, etc. Imaginons alors deux trains de trois wagons roulant en sens opposés, à la vitesse d'un wagon par instant. Si les deux premiers wagons se croisent à l'instant 1, les deux trains sont côte à côte à l'instant 2.

À quel instant le wagon de tête du premier train croise-t-il le deuxième du second ? Jamais ?

Le modèle continu

Le monde n'étant pas discret, il est logique de le supposer continu : toute quantité est divisible à l'infini. Pourtant, après avoir récusé le premier modèle, Zénon récuse également celui-ci. Supposons l'espace continu. Alors pour franchir une distance de 1 024 mètres, par exemple, nous devons d'abord franchir les 512 premiers mètres ce qui nous amène à un instant 1. Nous franchissons alors les 256 mètres suivants d'où un instant 2. Les 128 mètres suivants donnent un instant 3 et ainsi de

suite en divisant chaque fois l'espace restant par deux. Comme l'espace est divisible à l'infini, nous sommes amenés à vivre une infinité d'instants, ce qui est impossible. Selon Zénon, le modèle continu interdit le mouvement. De nos jours, ce paradoxe est vu comme une erreur de calcul car une somme d'un nombre infini de termes peut être finie. Plus précisément aujourd'hui on montre que :

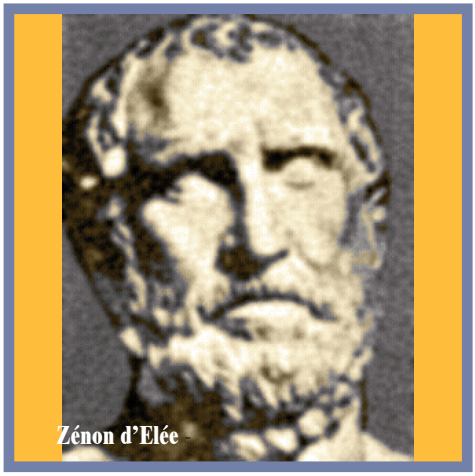
$$\frac{1}{2}+\frac{1}{4}+\frac{1}{8}+\frac{1}{16}+etc,=1$$

En fait, l'idée de Zénon est ailleurs. Il récuse seulement la divisibilité du temps à l'infini. L'instant n'existe pas, il n'existe que des intervalles de temps, éventuellement très courts.

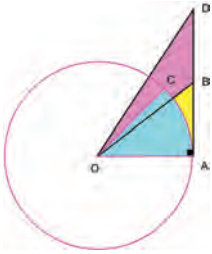
L'interdiction de l'infini

À la suite de ces paradoxes, les anciens Grecs s'interdisent le recours à l'infini. Plus précisément, celui-ci n'est plus conçu que comme potentiel : tout nombre peut être dépassé. Ainsi, Euclide (III^{e} siècle avant Jésus-Christ) évite de parler d'une infinité de nombres premiers. Il préfère énoncer :

" *l'ensemble des nombres premiers est plus grand que tout sous-ensemble de nombres premiers donné* " ce qui revient à dire : donnez-moi un nombre premier, j'en trouverai un plus grand. Ce refus de l'infini se situe essentiellement au niveau de la preuve. Le recours à l'infini actuel dans la recherche préliminaire reste clair. Par exemple, pour lier l'aire d'un cercle à sa circonférence, Archimède (III^{e} siècle avant Jésus-Christ) découpe le cercle en


Zénon d'Elée

petits triangles curvilignes égaux. Au triangle curviligne OAC, il fait correspondre le triangle rectangle OAB tel que la longueur du côté AB soit égale



à celle de l'arc AC. En construisant D tel que BD = AB, on obtient un triangle OBD de même aire que OAB car bases et hauteurs sont égales. Puis il assemble des triangles de même aire que OAB pour former un triangle rectangle (T) dont les côtés ont pour longueur respectivement le rayon et la circonférence du cercle.

Alors que l'idée sous-jacente est un découpage infini du cercle, Archimède ne prouve pas son théorème ainsi. Il considère l'aire S du cercle et celle S' = 1/2 x P x R du triangle (T) (où P est le périmètre et R le rayon du cercle) et montre en utilisant un découpage fini que les deux hypothèses S > S' et S < S' sont absurdes. Il exclut ainsi soigneusement l'infini de sa démonstration, même si le résultat ne peut être conçu sans y avoir recours.

Retour de l'infini, puis de la rigueur

Le recours explicite à l'infini revient en grâce bien plus tard. Aux XVII^{e} et XVIII^{e} siècles, le pragmatisme supplante la ri-gueur logique pour le contrôle des résultats. Un analyste du XVIII^{e} siècle n'hésite pas à considérer un découpage du cercle en parties infiniment petites. Il trace le même dessin que précédement, où chaque arc et chaque triangle sont considérés comme infiniment petit. Il calcule l'aire du secteur circulaire en fonction de la longueur t de l'arc AB et connaît donc l'aire du triangle OAB. Il ajoute le nombre de triangles du découpage et il trouve l'aire du cercle S comme somme d'aires de parties infiniment petites. Cependant pour achever le raisonnement, il faut remarquer que la différence entre l' aire du triangle AOC et celle du triangle OAB est un infiniment petit de l'ordre de t^2. Leur somme reste donc infiniment petite. Sans préciser ce dernier point, il est facile d'aboutir à des résultats fantaisistes.

La figure suivante propose ainsi une *preuve* de l'égalité $\pi = 2$.

La longueur du demi-cercle bleu ainsi que celle des courbes rouges, jaunes, etc est égale à πR. Ces courbes tendent vers le diamètre du cercle donc : $\pi R = 2R$

réel numéro 1 : 0,A_____
réel numéro 2 : 0,_B_____
réel numéro 3 : 0,__C_____
réel numéro 4 : 0,___D_____
réel numéro 5 : 0,____E_____
etc.
diagonale : 0,ABCDE_____
réel construit : 0,A'B'C'D'E'_____

Pour éviter ce type de paradoxes les mathématiciens du XIX^{e} siècle reviendront à l'exigence de rigueur des anciens Grecs. Ils précisent dans quels cas on peut donner un sens à la somme d'un nombre infini de termes. Pour revenir à l'exemple associé à Zénon, il s'agit d'étudier les sommes finies :

$$1/2 + 1/4 + 1/8 + 1/16 + ... + 1/2^n$$

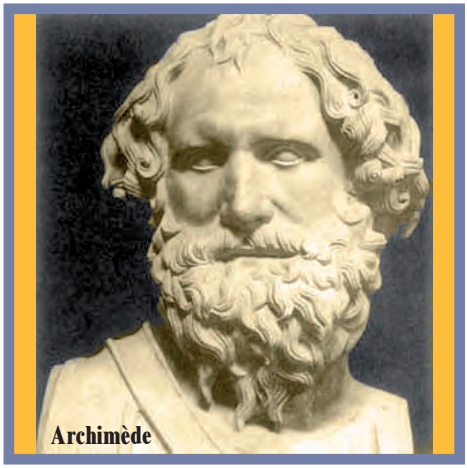
et montrer qu'elles s'approchent aussi près de 1 que l'on veut . En effet :

$$1/2+1/4+1/8+1/16+...+1/2^n = 1-1/2^n$$

et $1/2^n$ peut être rendu aussi petit qu'on le désire.

Par exemple, cette quantité est inférieure à 0,001 si $n > 10$ et à 0,000 001 si $n > 20$, etc.

Les infiniment petits ont ainsi été exclus des raisonnements pour être cantonnés au domaine de l'intuition jusqu'à la seconde moitié du XX^{e} siècle, quand Abraham Robinson a créé l'Analyse non standard qui permet de leur donner un nouveau droit de cité. De façon assez naturelle, ce retour inattendu est dû à des progrès en logique qui permettent d'affirmer l'existence d'un corps comprenant les nombres réels usuels ainsi que des infiniment petits.


Archimède

Preuve par l'infini

Avant ce retour en grâce, la notion d'infini est utilisée par les mathé-

maticiens du début du XX^{e} siècle pour aboutir à des démonstrations étranges et à de nouveaux paradoxes.

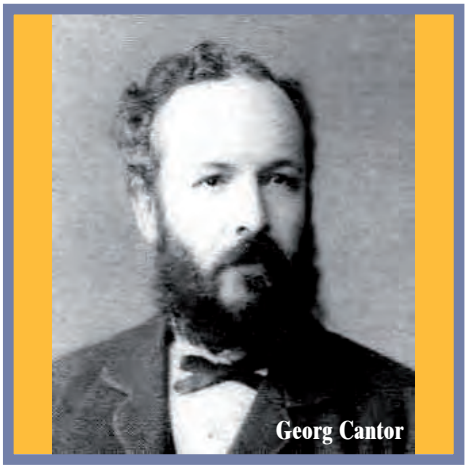
Cantor distingue plusieurs infinis. Il nomme *dénombrables* les ensembles dont on peut numéroter les éléments comme ceux des entiers ou des rationnels. Il en existe de plus compliqués, comme celui des nombres algébriques, les racines d'équations polynômiales à coefficients entiers telles par exemple que :

$$x^2 - 2 = 0 \text{ ou } x^5 - 5x^2 + 3 = 0.$$

Par la méthode de construction connue sous le nom de diagonale de Cantor, on montre qu'il n'est pas possible de construire une numérotation de tous les nombres entre 0 et 1.

Supposons que, à tout nombre réel entre 0 et 1, on puisse faire correspondre un entier naturel. Par exemple :
à l'entier 1 correspond 0,2359...
à l'entier 2 correspond 0,3598...
à l'entier 3 correspond 0,8248...
...
à l'entier n_k correspond $0,c_{k1}c_{k2}...c_{kk}c_{kk+1}...$
...
alors le réél $r = 0,e_{11}e_{22}e_{33}...e_{ii}...$
avec $e_{11} \neq c_{11}$, ... $e_{ii} \neq c_{ii}$..., ainsi construit, est différent de tous les réels répertoriés et donc ne peut être numéroté.

L'ensemble des nombres réels n'étant pas dénombrable, Cantor en déduit l'existence de nombres transcendants, c'est-à-dire non algébriques. Cette preuve par différence de nature des infinis est déroutante car elle ne permet pas de nommer un seul nombre transcendant. Pour certains, cette utilisation de l'infini est même choquante car elle s'accompagne de nombreux paradoxes, souvent


Georg Cantor

associés à l'auto-référence. Ils sont tous de même nature que le paradoxe du barbier de Russel : *Dans un village, un barbier déclare raser tous les hommes ne se rasant pas eux-mêmes. Qui rase le barbier ?* Ce type de paradoxes montre que l'on ne peut pas nommer n'importe quoi *ensemble* sinon, nous pouvons considérer deux sortes d'ensemble : ceux qui appartiennent à eux-mêmes et les autres.

Que dire alors de l'ensemble des ensembles n'appartenant pas à eux-mêmes ?

Le rêve de Hilbert

Avec la théorie des ensembles, Cantor a créé un outil puissant. Il a aussi montré la fragilité des fondements des mathématiques. Au début du XX^{e} siècle, David Hilbert pense assurer leur solidité en systématisant la méthode axiomatique des anciens Grecs. Dans son rêve, toutes les vérités mathématiques découlent d'axiomes et de règles de déduction logique. Par exemple, toutes les vérités arithmétiques doivent se déduire des axiomes que Peano, un contemporain de Hilbert, a énoncés. Malheureusement, Gödel prouve trente ans plus tard que

l'arithmétique de Peano contient des assertions vraies et improuvables. Pour démontrer ce résultat, on pourrait dénombrer les assertions prouvables et les autres. Plus précisément, on peut imaginer de numéroter les assertions prouvables en tenant compte de leurs longueurs par exemple. Ainsi, on obtient une assertion numéro 1, une assertion numéro 2, etc. Autrement dit, l'ensemble des assertions prouvables est infini mais dénombrable. En revanche, il est facile d'imaginer que l'ensemble des assertions vraies n'est pas dénombrable. Ainsi, il ne peut se réduire à l'ensemble des assertions prouvables. Gödel ne procède pas ainsi. Il est plus explicite : il exhibe des assertions vraies improuvables !

Les mathématiques ne sont pas mécanisables

Dans le projet de Hilbert, il reste l'espoir qu'une machine puisse démontrer toutes les assertions prouvables d'une théorie. Imaginons donc un logiciel qui, à partir d'un système d'axiomes et de règles de déduction, produise les assertions prouvables les unes après les autres. Donnons nous une assertion particulière, soit A, dont on veut savoir si elle est prouvable ou non. Nous pouvons modifier notre logiciel de sorte qu'il s'arrête si A est prouvable et boucle indéfiniment sinon. Nous sommes ainsi amenés à nous poser le problème de l'arrêt des logiciels informatiques. Qu'est-ce qu'un logiciel ? Il s'agit d'un texte écrit dans un certain langage de programmation. Dans le jargon de l'informatique, on parle de son *code*. La nature de celui-ci et le langage dans

lequel il est écrit importent peu pour l'argument qui suit. Dans ce même jargon, le texte entré au clavier est appelé l'*argument du logiciel*. Ceci précisé, nous pouvons nous poser la question suivante :

Existe-t-il un logiciel L qui, prenant en entrée un logiciel X, c'est-à-dire son " code " puis un argument x, sait dire si X s'arrête ou non pour l'entrée de l'argument x ?

Supposons L écrit et notons L (X, x) le résultat de son exécution pour les données X et x. Nous pouvons alors construire un logiciel P s'arrêtant si : L (X, x) = "non" et bouclant indéfiniment si L (X, x) = "oui".

Que se passe-t-il si on applique P à lui-même ? S'il s'arrête, il boucle et s'il boucle, il s'arrête !

Un tel logiciel ne peut exister ce qui ruine définitivement le projet d'Hilbert de mécanisation de la preuve.

Tant mieux, sinon quel serait l'intérêt des mathématiques ?

Equations et racines, une traque universelle

Elisabeth BUSSER

Qu'elles soient agricoles (découpage de terrains), patrimoniales (partage d'héritages) ou consumeristes (achat et vente), les mathématiques s'invitent dans la vie quotidienne dès l'Antiquité. Leurs premières traces sont faites de calculs qui, sans le dire, ne sont autres que des équations. Les méthodes de résolution n'ont cessé, à travers le monde entier, de se codifier et de s'affiner jusqu'à aujourd'hui.

Une algèbre en devenir

Les Babyloniens de la première dynastie, vers 1700 avant J-C. étaient déjà allés assez loin dans les méthodes de résolution d'équations, y compris celles du second ou du troisième degré.

Connus pour être de grands constructeurs de tables, ils les utilisèrent pour résoudre des équations. La table des inverses leur permit par exemple de résoudre des équations du type ax = b. Il leur suffisait de trouver 1/a dans la table et de le multiplier par b pour obtenir la solution. Evidemment, les calculs en base soixante (système hexadécimal) étaient un peu lourds, et ne se faisaient bien souvent que par approximation, certains nombres comme 13 ne possédant pas d'inverse exact. Pour les équations du second degré, les Babyloniens connaissaient pratiquement déjà l'algorithme de calcul actuel.

Tablette babylonienne

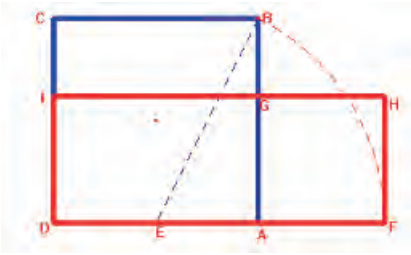
C'est une autre table, celle des valeurs de $n^2 + n^3$, qui leur permit de résoudre une équation plus compliquée, du type $ax^3 + bx^2 = c$. Nous dirions aujourd'hui que le changement de variable $x = by/a$ transforme cette équation en $y^3+y^2=ca^2/b^3$. La table donnait une valeur de y et, pour trouver x, on recalculait, à l'envers, by/a. Il suffisait d'y penser ! Ici, pas question de notation algébrique, mais quelle intelligence dans la technique de résolution !

Dans l'ancienne Egypte, quelques siècles plus tard, toujours pas de symbolique algébrique, mais des calculs d'inverses allégés par l'utilisation de fractions de numérateur égal à 1.

Les Grecs, eux, ont fait de la géométrie leur dogme et transforment les problèmes algébriques en constructions géométriques à la règle et au compas. Dans les treize livres des Eléments d'Euclide (environ 300 avant J-C.), pas de résolution explicite d'équation mais des constructions géométriques fournissant les solutions.

Equations et racines, une traque universelle

Dans le livre I, Proposition 44, pour résoudre l'équation ax = b, Euclide propose de représenter a et x comme des mesures de longueur et b comme l'aire d'un rectangle. La proposition 30 du Livre VI contient en proposant le *partage en moyenne et extrême raison* tout ce qu'il faut pour résoudre une équation de degré 2 du type $x^2 + ax = a^2$.



Il construit le carré ABCD de côté [AB] et le rectangle DFHI de même aire et tel que AFHG soit aussi un carré. Il a pris soin d'exposer auparavant cette construction (par exemple en utilisant l'arc BF de centre E, milieu de [AB]). Les deux carrés de la figure étant semblables, GB/GA = GH/GI, donc GB/GA = GA/AB.

Le point G est celui qui partage le segment [AB] en moyenne et extrême raison.

Euclide ne le dit pas explicitement, mais la résolution graphique de l'équation $x^2 + ax = a^2$ est immédiate. Le côté du carré ABCD représente a et la construction précédente fournit aussitôt le côté du carré AFHG c'est à dire x.

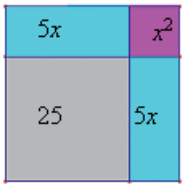
C'est plus tard, vers 250 après J-C., qu'on voit apparaître, chez Diophante, un début d'écriture algébrique où l'inconnue s'appelle *le nombre* et se nomme par une lettre de l'alphabet.


carré et rectangle sont de même aire

Les " pros " de l'algèbre

La voie est ouverte pour créer l'algèbre et son cortège de notations, ce que vont faire les mathématiciens arabes du Moyen-Age, héritiers directs de la culture mathématique grecque, qu'ils ont beaucoup étudiée. Ils vont l'enrichir de leurs propres techniques algorithmiques. Al-Khwarizmi (780-850), premier savant de l'école de Bagdad, celui-là même dont le nom a donné le mot "algorithme", pratique par exemple couramment la résolution des équations du second degré. Il commence par donner les racines avec des radicaux, puis confirme ses résultats par une démonstration géométrique et donne enfin une application numérique. Ses calculs se fondent sur deux opérations fondamentales : *al-jabr* (d'où le mot "algèbre"), transposition des termes, et *al-muqabala*, réduction des termes semblables. Sa géométrie est celle d'Euclide et utilise abondamment la "complétion du carré".

A propos d'un problème d'argent : *" Un carré et dix racines sont égaux à 39 dirhams ",*
il doit donc résoudre $x^2 + 10x = 39$.



Le premier carré construit a pour côté l'inconnue, les deux rectangles représentent les dix racines, le tout ayant une aire de 39. On complète la figure pour en faire un carré. Il a pour côté 8 puisque 39 + 25 = 64 = 8^2. Il ne reste plus qu'à faire la différence 8 - 5 pour obtenir x = 3.

Si Al Khwarizmi n'a pas dépassé le degré 2, un autre mathématicien arabe célèbre, Omar Al-Kayyam traita, lui, vers 1074, des équations de degré 3, reprenant le problème d'Archimède : *découper une sphère par un plan de manière que les volumes des deux calottes soient dans un rapport donné.* Al-Kayyam reconnaît que la solution tient dans l'intersection d'une parabole et d'une hyperbole, mais ne va pas jusqu'au bout de sa résolution.

Il faudra attendre la Renaissance et la grande époque des mathématiciens italiens Del Ferro (vers 1515), Cardan et Tartaglia (vers 1545) pour arriver à une étude complète de la résolution algébrique des équations de degré 3. Les formules de Cardan qui permettent de trouver à ces équations une solution réelle, ont fait faire à la génération suivante de mathématiciens, comme Bombelli (vers 1572) un pas vers la création des nombres complexes. En effet, que répondre à la question :

Que se passe-t-il quand cette formule ne s'applique plus et où pourtant l'équation a une solution réelle ?

Page du plus vieux livre d'algèbre du monde, le *Kitab al-Jabr wal-Muqabala* du mathématicien Al Khwarizmi

La révolution cartésienne

Les mathématiciens français vont prendre le relais des Italiens. Viète, vers 1593, simplifie les notations algébriques et donne une méthode de résolution des équations de degré 3 et plus. On raconte même que, pour relever le défi lancé par Adrien Romain, il trouva les 23 racines positives d'une équation de degré 45 !

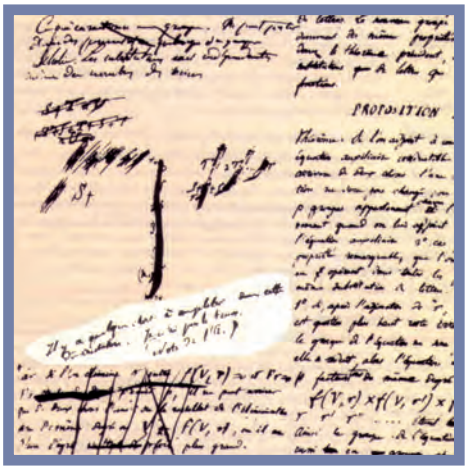
On doit à Descartes (1596-1650) l'utilisation systématique des lettres en mathématiques : celles du début de l'alphabet pour les quantités déterminées, celles de la fin pour les indéterminées. Il propose également une résolution générale des équations au moins jusqu'au degré 6 grâce à la géométrie analytique. Parallèlement, Newton (1671) et Raphson (1690), préfigurant les travaux d'aujourd'hui, imaginent des méthodes de résolution par approximations. Lorsqu'il s'agit par exemple de *réduire en suite infinie* l'équation $y^3 - 2y = 5$. On part de 2 comme première approximation de la solution. En remplaçant y par 2+*p*, et en éliminant certains termes *à cause de leur petitesse*, on arrive à affiner : $p = 0{,}1$.

Et on recommence à poser $p = 0{,}1 + q$, à éliminer les termes non significatifs pour obtenir $q = -0{,}0054$, etc…

Quelle belle anticipation sur les algorithmes informatiques actuels !

L'effet Galois

Avec Lagrange puis avec Abel, on passe à la vitesse supérieure. Lagrange lie, en 1770, la résolubilité par radicaux des équations de degré trois et certaines propriétés d'invariance par permutations des racines. Il étudie donc les propriétés de ces ensembles de permutations qui prendront avec Galois le nom de *groupes*. Utilisant les résultats de Lagrange, Abel travaille sur les équations de degré 5, prouvant qu'elles ne sont pas résolubles par radicaux. Il généralise en 1829 aux classes d'équations ainsi résolubles. Reprenant leurs idées, Galois (1811-1832) définit le concept de groupe : il englobe dans cette notion les permutations des racines d'une équation telles qu'une relation algébrique satisfaite par ces racines le reste après permutation des dites racines. Le *groupe de Galois* d'une équation polynômiale est né ! Le génie de Galois ne s'arrête pas là : il va lier les propriétés de ce groupe au fait que l'équation associée soit ou non résoluble par radicaux. Il introduira pour les besoins de son étude des notions qui constitueront la théorie des groupes, pilier de l'algèbre moderne. On est passé du *terrain*, celui de la résolution d'équations algébriques à la théorie, celle qui fonde les mathématiques d'aujourd'hui.



Extrait du mémoire d'Evariste Galois.
La veille du duel qui lui coûta la vie à 21 ans, Galois écrit en marge de ses notes :

Il y a quelque chose à compléter dans cette démonstration. Je n'ai pas le temps.

Géométrie, une longue histoire

Elisabeth BUSSER

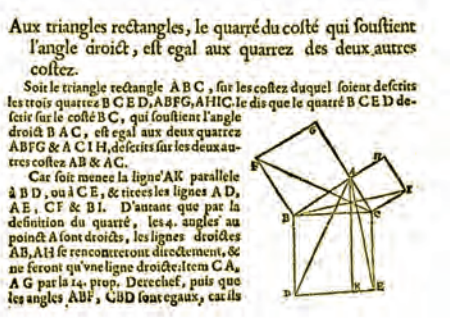
Dés l'époque secondaire, les mollusques construisaient leur coquille en suivant les leçons de géométrie transcendante disait Gaston Bachelard. C'est dire l'emprise de la géométrie sur nos vies et cela pourrait expliquer pourquoi l'approche du monde des premiers mathématiciens a été géométrique. La géométrie, science des figures au départ, a permis le développement de la pensée mathématique pendant deux millénaires. Ce sont des problèmes connexes à la géométrie qui ont permis parallèlement le développement d'autres branches des mathématiques. La géométrie a beaucoup évolué au cours des siècles et aujourd'hui ses *images* permettent de comprendre les concepts mathématiques qu'elle a fait émerger et qui ont maintenant un développement autonome.

L'héritage grec

Au départ, la géométrie est la science des figures. Ainsi, en Egypte ancienne, où la géométrie d'arpentage est de mise, naît, à côté de la pratique, un début de science géométrique, mettant en particulier en évidence certaines propriétés du triangle et du cercle.

En Grèce, il reste du VI[e] siècle avant J-C. un grand nombre de résultats géométriques et les noms de grands géomètres : Thalès, le premier savant philosophe, le premier à faire de l'angle une grandeur fondamentale, comme la longueur, l'aire ou le volume, puis Pythagore, Hippocrate de Chios, Eudoxe de Cnide, … Avec eux, on traite de l' inscription d'une sphère dans un cône, la similitude des triangles, les propriétés du cercle, des polygones et des polyèdres, des coniques. Les Eléments d'Euclide (-330, -270) constituent la première synthèse, avec le souci de *fonder* la géométrie et d'en faire une science démonstrative au sens d'Aristote. *Ce que nous appelons savoir c'est connaître par la démonstration* disait ce dernier.

Le théorème de Pythagore vu par Euclide



Aux triangles rectangles, le quarré du costé qui soustient l'angle droict, est egal aux quarrez des deux autres costez.

Soit le triangle rectangle ABC, sur les costez duquel soient descrits les trois quarrez BCED, ABFG, AHIC. Ie dis que le quarré BCED descrit sur le costé BC, qui soustient l'angle droict BAC, est egal aux deux quarrez ABFG & ACIH, descrits sur les deux autres costez AB & AC.

Car soit menee la ligne AK parallele à BD, ou à CE, & tirees les lignes AD, AE, CF & BI. D'autant que par la definition du quarré, les 4. angles au poinct A sont droicts, les lignes droictes AB, AH se rencontreront directement, & ne feront qu'vne ligne droicte: Item CA, AG par la 14. prop. Derechef, puis que les angles ABF, CBD sont egaux, car ils

On retient surtout d'Euclide la rigueur de la méthode et la tentative de classification des résultats. On doit à Archimède (-287, -212), plus physicien que mathématicien, la première valeur précise du nombre π, entre 3 + 10/71 et 3 + 10/70. L'un des ouvrages les plus complets de la mathématique grecque est les *Coniques d'Apollonius de Perge* (fin du III[e] siècles avant J-C.). Il y rassemble des résultats déjà connus auxquels il mêle les siens propres, traitant toutes les sections coniques à partir du même cône. Après Apollonius, les mathématiciens comme

Hipparque de Metaponte (environ vers 150 avant J-C.) établissent des tables donnant les mesures des cordes d'un cercle équivalentes à nos tables de sinus, dont la précision va augmenter avec les travaux de Ptolémée (IIe siècle après J-C.) Après Ptolémée va s'instaurer une tradition d'étude des connaissances mathématiques des siècles antérieurs, dont les développements vont apparaître dans le monde arabo-islamique.

Si les mathématiciens arabes sont allés bien au-delà des Grecs dans le domaine algébrique et numérique, on trouve peu de géométrie si ce n'est celle des Grecs dans les ouvrages de mathématiques arabes du Moyen-Age, qui la présentent plutôt sous un jour calculatoire (aires, longueurs…). Dans les ouvrages d'Al-Khwarizmi et d'Abul-Wafa les formules sont nombreuses. Par exemple Le *Livre nécessaire aux scribes* est en fait un mémoire de calcul : calcul de l'aire d'un triangle semblable à celle de Héron, calcul de l'aire d'une sphère en fonction de celle d'un de ses grands cercles, calcul du volume en fonction de la surface.

De l'algèbre dans la géométrie

Allant au-delà de la géométrie de figures, les Grecs ont préparé le terrain à l'étude la géométrie analytique. Ils ont eu l'idée de lier géométrie et relation entre certaines quantités variables en faisant intervenir deux paramètres préfigurant nos actuelles coordonnées. Apollonius les utilise par exemple pour écrire des *équations* des coniques.

Nicolas Oresme, lui, va au XIVe siècle imaginer une représentation graphique

Portulan extrait de l'atlas dressé en 1467 par le navigateur Grazioso Benincasa. Ce sont les cartes marines les plus précises et renseignées de l'époque.

utilisant une *latitudo* et une *longitudo*, comme abscisse et ordonnée. Descartes reprendra dans sa *Géométrie* les calculs d'Apollonius et les généralisera au lieu de les limiter à une figure donnée. Ses notations symboliques, où constantes et variables sont représentées par des lettres, vont considérablement alléger ses calculs, contrairement à Fermat qui, pour arriver aux mêmes résultats, continue d'utiliser l'algèbre géométrique des Grecs. Sa technique permet à Descartes d'aborder des problèmes de lieux géométriques restés jusqu'alors sans solution évidente. La géométrie analytique s'étend à l'espace avec Clairaut vers 1731 et Euler, qui donne en 1748 une formule claire de changement d'axes.

Lagrange (vers 1770) va rompre avec ce mélange de considérations géométriques et analytiques en faisant de la géométrie sans figure, par une approche purement analytique. Monge (1746-1818), dont l'œuvre géométrique est immense, utilise à fond la géométrie analytique : il étudie par exemple les surfaces uniquement à l'aide d'équations aux dérivées partielles. Il imagine aussi

des représentations de solides de l'espace en les projetant sur deux plans : c'est le début de la géométrie dite *descriptive*.

Géométrie projective : une autre approche

La géométrie projective est née de l'étude de la représentation en perspective. Ce qui était difficile pour les Anciens, même s'ils percevaient déjà la notion de *point de fuite*, est devenu naturel pour les peintres italiens du Quattrocento, sous l'impulsion d'architectes comme Brunellesci et Alberti vers 1435. Piero Della Francesca (1416-1492) est le premier théoricien de la perspective et Léonard de Vinci, à la fin du XV^{e} siècle donne des règles du dessin perspectif, suivi par Dürer qui les établit rigoureusement dans son traité *Unterweysung der Messung* (entre 1525 et 1538). La perspective de ces peintres est la projection centrale, associant à tout point de l'objet à représenter sa projection sur le plan du tableau, c'est-à-dire l'intersection entre le plan du tableau et la droite joignant l'œil de l'observateur au point à représenter. Dans ce mode de représentation, les parallèles non parallèles au plan du dessin sont représentées comme sécantes au point de fuite. Les parallélogrammes ne sont donc pas représentés par des parallélogrammes, les cercles pas par des cercles, les milieux ne sont pas conservés, mais les alignements subsistent. Quelles sont alors les propriétés qui restent vraies ? L'alignement, certes, mais aussi le birapport de quatre points alignés A, B, C, D, défini en son temps par Apollonius et Pappus (II^{e} siècle après J-C.).

La géométrie de Dürer

C'est la conservation du birapport qui va fonder la géométrie projective, l'étude des propriétés des figures qui se conservent par une succession de perspectives centrales, des transformations projectives. Le point de fuite sera le point à l'infini de toutes droites d'une même direction perpendiculaire au plan du tableau. L'architecte-ingénieur Desargues (1593-1662) va tenter de simplifier cette nouvelle théorie, suivi par Pascal qui, vers 1658, théorise ses idées.

Un peu tombée dans l'oubli, la géométrie projective renaît à la fin du XVIII^{e} siècle avec Monge (1795), Poncelet (1822), Chasles (1837). A la fin du XIX^{e} siècle, Hilbert, Klein et Darboux vont en formuler rigoureusement les axiomes. Cette approche de la géométrie, non par les propriétés des seules figures mais par leurs transformations, ainsi que l'étude des invariants de ces transformations, va donner une autre tournure à cette branche des mathématiques, qu'on utilise abondamment aujourd'hui dans les systèmes de rendu graphique sur ordinateur.

Les nouvelles géométries

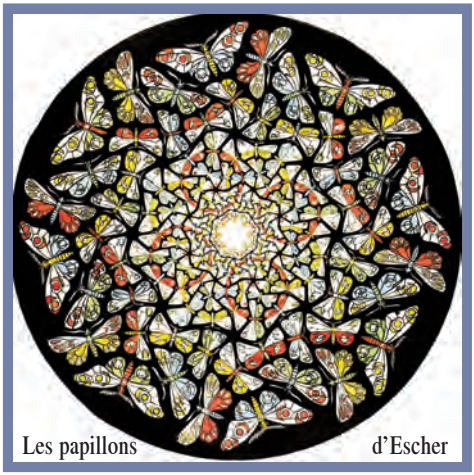
Si la géométrie projective a revisité les vues d'Apollonius sur les coniques, il est une des *demandes* d'Euclide qui agita fort les géomètres, c'est le fameux *cinquième postulat* . D'après l'énoncé d'Euclide, *Si une droite, tombant sur deux droites, fait des angles intérieurs du même côté plus petits que deux droits, ces droites prolongées à l'infini se rencontreront du côté où les angles sont plus petits que deux droits*. La géométrie euclidienne estime qu'il n'a pas besoin d'être démontré, d'autres, comme Saccheri en 1733, pensent pouvoir précisément en faire la preuve mais en vain. A la fin du XIX^{e} siècle, avec Hilbert, puis au XX^{e}, avec Choquet la géométrie euclidienne se modernise avec des axiomes indépendants et non contradictoires.

On peut donc désormais construire des géométries en abandonnant le postulat des parallèles : les géométries non euclidiennes sont nées.

Soit les angles intérieurs du cinquième postulat sont aigus, et c'est la *géométrie de Lobatchevski* (entre 1826 et 1856).

Soit ces angles sont obtus, et c'est la *géométrie de Riemann* (1854).

A la fin du XIX^{e} siècle, Klein donna la preuve que ces deux géométries sont chacune non contradictoires et Poincaré définit un modèle pour la géométrie de Lobatchevski : le demi-plan (dit *de Poincaré*), où les droites sont les demi-cercles centrés sur le bord. Dans cette géométrie, on peut mener d'un point une infinité de parallèles à une droite et alors



Les papillons d'Escher

la somme des angles d'un triangle est inférieure à deux droits. Pour la géométrie de Riemann, le modèle sera celui de la sphère, dont les droites sont les grands cercles. On ne peut alors, par un point hors d'une droite, mener aucune parallèle à cette droite et la somme des angles d'un triangle est supérieure à un angle plat. Les mathématiciens, en reconnaissant aux géométries non euclidiennes un droit de cité ont renoncé à considérer la géométrie comme une simple description du monde physique. C'est l'ouverture proposée par Klein, dans le programme d'Erlangen (1872), qui conduit à concevoir une géométrie comme l'action d'un groupe G de transformations sur un ensemble. L'étude des objets géométriques devient donc celle des invariants par l'action de certains sous-groupes de G.

On est alors en mesure d'utiliser cette géométrie ainsi axiomatisée pour décrire en retour le monde physique, comme par exemple en théorie de la relativité.

La conjecture de Riemann

Un problème pour un millénaire

Benoît RITTAUD

Quels seront les problèmes qui occuperont le plus les mathématiciens des mille prochaines années ? Difficile de prétendre répondre à cette question si l'on pense aux incroyables bouleversements qui ont accompagné les mathématiques depuis l'an mil.

Des mathématiciens ont pourtant relevé le défi.

Offerte par l'Institut Clay de Mathématiques, fondé par Landon Clay et sa femme à la fin des années 1990, la somme est à la hauteur de l'importance des questions posées par ces problèmes.

CLAY MATHEMATICS INSTITUTE

Sept problèmes, un million de dollars pour chacun d'eux.

P vs NP
Conjecture de Hodge
Conjecture de Poincaré
L'hypothèse de Riemann
Yang-Mills et hiérarchie de masse
Navier-Stokes et comportement continu
Conjecture de Birsch et Swinnerton-Dyer

Difficile de résumer en quelques mots la teneur des questions mises à prix par l' Institut Clay : certaines d'entre elles sont extrêmement difficiles, comme la *conjecture de Hodge*, pour laquelle les mathématiciens même spécialistes doivent consacrer plusieurs heures rien que pour en comprendre l'énoncé !

Parmi les sept problèmes, la conjecture de Riemann, communément appelée hypothèse de Riemann, occupe une place à part. Cette conjecture postule que, en-dehors de cas triviaux sans grand intérêt, les solutions s de l'équation :

$$1+1/1^8+1/2^8+1/3^8+1/4^8+1/5^8+\cdots=0$$

sont toutes des nombres complexes de partie réelle égale à 1/2 .

Il existe différents énoncés équivalents de la conjecture posée au XIX^e siècle par Georg Riemann, celui que nous donnons fait appel, outre à la notion de *série* (l'idée selon laquelle on peut ajouter des nombres les uns aux autres de façon répétée et infinie), à celle de *nombre complexe*.

Un nombre complexe est un nombre, que l'on peut toujours écrire sous la forme a+b*i*, et dans lequel a et b sont deux nombres *réel*s ordinaires et où *i* est une abstraction mathématique définie pour l'occasion et qui vérifie que $i^2 = -1$ (alors que, comme chacun sait, il n'existe aucun nombre réel qui, multiplié par lui-même, donne une valeur négative). Les opérations sur les nombres complexes généralisent de façon assez naturelle celles sur les nombres réels auxquels nous sommes plus habitués, même s'ils recèlent aussi des pièges parfois inattendus.

La conjecture de Riemann

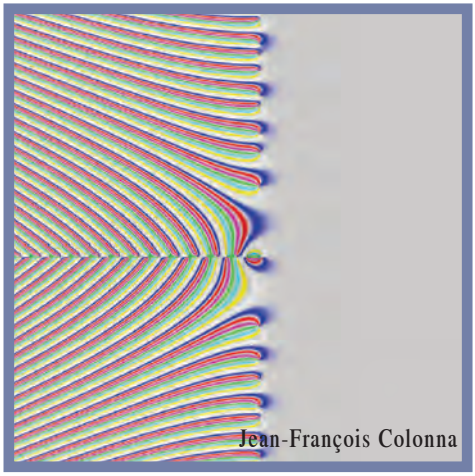
La somme z(s), définie par
$1+1/1^8+1/2^8+1/3^8+1/4^8+1/5^8+\cdots$
avec le nombre complexe s = a+bi, ne tend vers un nombre fini que pour a >1. Mais on arrive à donner un sens à cette somme par une technique devinée par Euler et expliquée complétement par Riemann.

Ce qu'affirme la conjecture de Riemann, c'est que, sauf dans des cas particuliers simples à traiter, la somme z(s) ne vaut 0 que lorsque le nombre complexe s = a+bi vérifie a = 1/2 (il s'agit d'une condition nécessaire mais non suffisante, c'est-à-dire qu'il faut que a = 1/2 pour espérer que z(s) soit nul, mais que le fait que a = 1/2 ne le garantit pas à lui tout seul - loin de là).

Cette conjecture peut paraître bien éloignée de ce que pourraient être des préoccupations légitimes d'ingénieurs, d'informaticiens et plus généralement d'utilisateurs de mathématiques, tournées vers la fabrication d'ailes d'avion toujours mieux profilées, d'algorithmes toujours plus rapides ou encore de ponts toujours plus grands et solides.

On sait pourtant aujourd'hui que la conjecture de Riemann est probablement le *Graal des mathématiques*, c'est-à-dire que sa démonstration changerait à jamais la face de la discipline.

L'impact des démonstrations de la conjecture de Riemann (ou sa réfutation) sur notre vie de tous les jours, serait réel et concernerait notamment certains protocoles sécurisés sur internet qu'il conviendrait de modifier pour éviter que les immenses connaissances sur les nombres que donnerait



Visualisation tri-dimensionnelle de la fonction Zeta, les zéros sont alignés sur la droite critique à l'extrémité des zones bleues.

cette conjecture ne facilite par trop le travail des pirateurs de tout poil.

Mais l'essentiel serait bien ailleurs. L'essentiel est qu'une nouvelle page de la science mathématique serait tournée et que le mathématicien, ou probablement l'équipe de mathématiciens, qui tranchera définitivement la question posée par Riemann permettra aux mathématiques de son siècle (qui n'a aucune raison d'être le nôtre, tant la question paraît difficile) d'être définitivement transfigurées.

Une ambition bien plus vaste que de celle de gagner quelques sous sur internet.

Pour en savoir (un peu) plus

Keith DEVLIN aux éditions Le Pommier, en 2005
Les énigmes mathématiques du 3ème millénaire, .

http://www.math.univ-paris13.fr/~rittaud

La percolation à la température critique

Wendelin WERNER

Nous allons décrire un modèle de configurations aléatoires obtenues en coloriant au hasard les couleurs de chaque site dans un réseau plan, pour lequel de nouveaux résultats ont été démontrés récemment. Nous présenterons quelques idées et outils utilisés pour les démontrer et nous les placerons dans un contexte un peu plus général. Cet article étant de nature introductive, il décrit surtout des idées générales, dues à des physiciens et des mathématiciens. La dernière partie abordera des aspects plus récents.

Aléa microscopique et déterminisme macroscopique.

De nombreux événements se prêtent à une interprétation probabiliste. Avant qu'ils ne se produisent, leur issue est incertaine, mais on peut tout de même la décrire à travers sa loi. Si l'on tire à *pile* ou *face*, on aura une chance sur deux d'observer *pile*. Les phénomènes aléatoires peuvent ensuite se combiner pour former de nouveaux événements, aléatoires eux aussi. Par exemple, on peut tirer 10 000 fois à *pile* ou *face* et regarder le nombre total de résultats *pile*.

L'un des buts de la théorie des probabilités est de décrire mathématiquement le comportement de très grands systèmes dans lesquels se combinent un très grand nombre de phénomènes aléatoires. Traditionnellement, le premier résultat probabiliste enseigné aux étudiants de niveau licence est la loi des grands nombres, que l'on peut décrire à l'aide du modèle de pile ou face précédent. Cette loi affirme que l'incertitude du résultat devient de plus en plus petite lorsque la taille du système augmente. A la limite quand celui-ci devient infini, le résultat de l'expérience a perdu son caractère aléatoire et devient déterministe (on a alors 50% de *pile*). Parmi les systèmes bien modélisés de manière probabiliste, on peut mentionner les systèmes de particules physiques. Au niveau microscopique, le comportement désordonné des particules peut être supposé aléatoire. Comme on s'intéresse au comportement d'un système qui comporte un très très grand nombre de composantes microscopiques, le problème est de même nature : on observe le résultat au niveau macroscopique d'une *expérience* aléatoire au niveau microscopique. C'est le principe de la Physique Statistique. Là encore, les principaux résultats montrent un comportement macroscopique déterministe malgré l'aléa microscopique.

Aléa microscopique, aléa macroscopique : la percolation critique.

Le second résultat probabiliste enseigné en Licence est le théorème de la limite centrale qui décrit (dans le cas d'un grand nombre de tirages à *pile* ou *face* décrit précédemment) la loi de la (très petite) déviation entre le résultat effectif et le résultat déterministe prévu. Si l'on chausse des lunettes très sensibles, on voit malgré tout que le

résultat est aléatoire, et on peut décrire sa loi. Ce résultat est à la base de nombreuses applications en statistiques (par exemple les sondages d'opinion).

Nous allons considérer un autre modèle pour lequel on obtient des résultats aléatoires au niveau macroscopique. Nous allons encore effectuer un très grand nombre de tirages à *pile* ou *face*, et nous intéresser à d'autres phénomènes observables que la proportion de tirages *pile*. Découpons un grand losange sur un réseau en forme de nid d'abeille. Pour chaque cellule microscopique en forme d'hexagone, on tire à *pile* ou *face* sa couleur (qui est noire si on tire *pile*, ce qui se produit donc avec une chance sur deux, et blanche si on tire *face*). Ainsi, on obtient un coloriage aléatoire du losange. On recherche alors un chemin blanc (ou un chemin noir) sans coupure qui va d'un bord au bord opposé du losange.

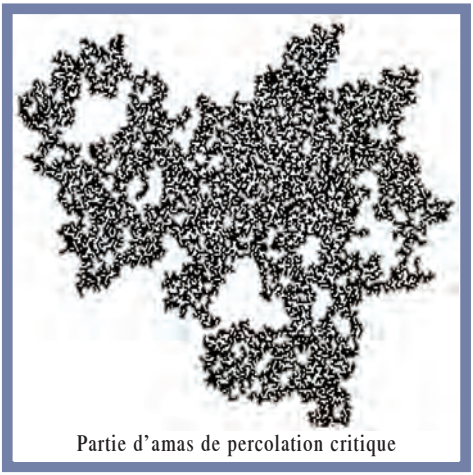
Il existe un jeu sur plateau appelé *Hex* où deux joueurs déposent tour à tour un pion de leur couleur sur un tel losange de taille 10x10. Le gagnant est celui qui arrive à placer un chemin joignant les côtés opposés du losange avant que son adversaire ait réussi à le bloquer en plaçant un chemin joignant les deux autres côtés opposés. On peut montrer qu'il n'existe pas de partie nulle à ce jeu : lorsque le losange est entièrement rempli, l'un, et uniquement l'un des deux types de chemin, est présent.

Dans le cas où le coloriage est aléatoire, il est clair, par symétrie, que les deux événements : *il existe un chemin blanc de bas en haut* et *il existe un chemin noir de gauche à droite* ont

Jeu de Hex ayant appartenu à Claude Berge, le grand théoricien des graphes.

autant de chances l'un que l'autre d'être réalisés. Ceci est vrai indépendamment de la taille du losange. Ainsi, pour ce modèle, certains évènements restent aléatoires au niveau macroscopique. La manière dont les aléas microscopiques se combinent pour décider s'*il existe un croisement blanc de gauche à droite* est de nature différente de l'exemple précédent. On peut penser que le fait d'avoir tiré plus de *piles* que de *faces* aide à construire un croisement. C'est bien le cas, mais dans la limite où la maille du réseau est très petite, les deux événements *il existe un croisement noir de gauche à droite* et *on a tiré plus d'hexagones noirs que d'hexagones blancs* deviennent asymptotiquement indépendants (ce résultat dû à Benjamini, Kalai et Schramm n'est pas du tout simple). On peut aussi montrer - c'est un résultat des mathématiciens Russo, Seymour et Welsh vers la fin des années 1970 - que si l'on remplace les losanges par d'autres formes, les probabilités de croisement ne tendent ni vers un ni vers zéro lorsque la maille du réseau considéré devient infiniment

petite ; l'évènement reste aléatoire. Une autre approche consiste à étudier la forme des îles noires (on dit mathématiquement des «composantes connexes» noires).
Voici ci-contre, une partie d'une (grande) île. Le précédent résultat suggère l'existence d'une loi limite pour la forme de ces grandes îles. Elles ont un bord extérieur, que l'on peut diviser en deux parties : la plage extérieure (tournée vers l'océan) et les fjords (desquels on ne peut s'échapper directement sans repasser près de la plage extérieure).


Partie d'amas de percolation critique

Présentons quelques résultats prédits par les physiciens théoriciens, et prouvés récemment par les mathématiciens :
- La probabilité pour qu'il existe un croisement de gauche à droite d'un rectangle donné tend vers une limite lorsque le réseau devient très petit.
- On peut donner un sens rigoureux au fait que les grandes composantes connexes ont une forme aléatoire limite.
- Une grande composante connexe de diamètre N contiendra (en moyenne) environ $N^{91/48}$ points. Son bord extérieur contiendra (en moyenne) environ $N^{7/4}$ points, et la plage extérieure contiendra (en moyenne) environ $N^{4/3}$ points.
- Il peut y avoir en même temps de l'ordre de $N^{3/4}$ points blancs tels que si un seul d'entre eux changeait de couleur, il n'y aurait plus de croisement d'un losange donné de taille N alors qu'il y en avait un avant. Ces résultats sont en fait liés à la notion de dimension fractale. Ils ne sont pas démontrés par une méthode énumérative consistant à donner des formules exactes pour les modèles sur réseau. Il faut utiliser plusieurs idées et concepts mathématiques sophistiqués, et c'est ce qui fait leur intérêt mathématique.

Quelques outils utilisés.

Ce modèle de percolation est l'archétype du modèle *critique* en physique. On peut le généraliser en décidant de tirer à pile ou face avec une pièce biaisée qui a une probabilité p de tomber sur *pile* et 1- p de tomber sur *face*. Si p>50%, les probabilités de croisement tendent vers un (à grande échelle, on a un seul grand continent), et si p<50%, elles tendent vers 0 (on a alors à grande échelle un seul grand océan et de petites îles). Ainsi, lorsque l'on fait varier le paramètre p, on a un changement qualitatif abrupt, une *transition de phase* lorsque p passe par 50%. Comprendre un modèle *critique* permet aussi de comprendre son comportement lorsque le paramètre est proche du point critique. Par exemple, en utilisant les résultats obtenus pour la percolation critique, on peut montrer que, lorsque p est supérieur (mais très

proche) de 50%, alors la densité du continent infini (c'est-à-dire la proportion de sites qui sont dans le continent infini) est de l'ordre de $(p-0,5)^{5/36}$.

Une clé pour comprendre la percolation critique consiste à montrer que **ce modèle est asymptotiquement invariant conforme**. Ceci peut être formulé de la manière suivante. Considérons la percolation critique dans un carré (pour un réseau hexagonal de maille très fine). On observe alors des composantes connexes blanches et noires. Puis, regardons l'image obtenue en envoyant le carré dans le disque par une application conforme, c'est à dire une déformation qui conserve les angles droits. On observe alors une image de composantes connexes distordues. L'invariance conforme dit que cette image a cependant la même loi que celle que l'on aurait obtenue en considérant directement une percolation (de maille très très fine) dans le disque. Cette propriété, conjecturée par les physiciens théoriciens, a été démontrée en 2001 par le mathématicien russe Stanislav Smirnov.

Une seconde clé consiste à comprendre comment exploiter cette propriété. Vers 1999, le mathématicien israélien Oded Schramm à décrit le comportement (lorsque la maille du réseau est très très fine) des frontières extérieures de percolation par l'intermédiaire d'**itérations d'applications conformes aléatoires**. Ceci permet d'identifier les seules limites

Trajectoire d'un lacet brownien

invariantes conformes possibles pour les formes des amas de percolation critique. Il faut alors comprendre les propriétés des itérations d'applications conformes, et les relier au modèle de percolation discrète, ce que nous avons fait en collaboration avec Greg Lawler et Oded Schramm, et avec Stanislas Smirnov.

Une troisième idée, développée avec Greg Lawler et Oded Schramm, consiste à montrer que **les formes aléatoires ainsi définies ne sont pas propres au modèle de percolation critique.** Par exemple, le dessin ci-dessus représente l'ensemble des points visités par une marche aléatoire dans le plan. Plus précisément, on imagine qu'un promeneur choisisse au hasard parmi toutes les balades possibles qu'il peut faire (en un très long temps donné) en partant et en retournant à sa maison.

Ainsi, il fera beaucoup de va-et-vient et passera de nombreuses fois par certains points (et n'ira pas très loin). Mathématiquement, on dit que cette trajectoire est un lacet brownien.

La percolation à la température critique

Un résultat récent de 2005 montre que la forme aléatoire de la *plage* ainsi définie a exactement la même loi que celle définie par les très grands amas de percolation critique. Ceci est à rapprocher de la conjecture de Benoît Mandelbrot (démontrée avec Lawler et Schramm en 2001) qui dit que la dimension fractale de cette plage est 4/3 (ce qui correspond au nombre $N^{4/3}$ de points sur la plage des amas de percolation).

En conclusion

La percolation que nous venons de décrire n'est qu'un modèle parmi d'autres pour lequel les idées mathématiques tournant autour de l'invariance conforme et de l'itération d'applications conformes aléatoires s'appliquent.

Cependant, il reste de nombreuses questions fondamentales ouvertes pour des modèles naturels. Par exemple, on ne sait pas montrer l'invariance conforme de la percolation critique sur d'autres réseaux plans.

Mentionnons l'importance des contributions des physiciens théoriciens (par exemple via le développement de la théorie conforme des champs dans les années 1980) comme Cardy, Nienhuis, Duplantier ou Saleur (ces deux derniers sont au Commissariat à l'Energie Atomique sur le plateau de Saclay).

J'ai effectué mes études secondaires et supérieures en France. A l'issue de ma scolarité à l'Ecole Normale Supérieure en 1991, j'ai été chargé de recherches au CNRS, et, depuis 1997, je suis professeur à l'université Paris-Sud (Orsay). Pour mes travaux sur les phénomènes aléatoires plans, dont beaucoup ont été effectués en collaboration avec Greg Lawler et Oded Schramm, j'ai obtenu la médaille Fields en été 2006.

Wendelin Werner

Pour en savoir (un peu) plus :

WendelinWerner : liens vers des articles et interviews à partir de la page web http://www.math.u-psud.fr/~werner/vulga.html

WendelinWerner : La Recherche Mai 2007 : Les frontières aléatoires entre physique et mathématiques

Des lunettes pour un télescope spatial

sans aller dans l'espace ?

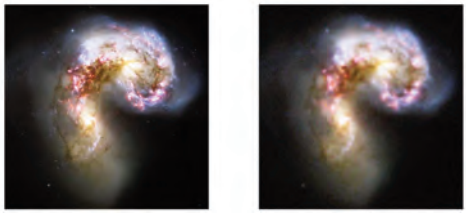
Erwann Le PENNEC et Dominique PICARD

Le télescope spatial Hubble a été lancé en avril 1990, il devait fournir des images d'une qualité inaccessible pour des télescopes terrestres. Les premières images reçues par les astronomes s'avérèrent extrêmement floues du fait d'un défaut physique sur le miroir principal du télescope. Pour corriger ce problème, il suffit d'ajouter quelques optiques supplémentaires, de véritables lunettes... Mais le satellite est en orbite et une telle opération de maintenance est très complexe. Elle ne put être effectuée qu'en décembre 1993, car il fallait trouver une solution à ce problème sans aller dans l'espace.

Les mathématiciens interviennent...

Ce sont les mathématiciens qui ont fourni des outils permettant de créer des lunettes virtuelles corrigeant en grande partie les défauts de l'optique de Hubble. Ils y reconnaissent un exemple d'une classe de problèmes classiques en mathématiques, la classe des problèmes inverses. Il s'agit de retrouver une image de l'espace qui a été dégradée par un opérateur (l'optique du télescope est défectueuse) et l'addition d'une perturbation, (on parle de *bruit* : les capteurs ne sont pas parfaits), à partir de l'observation dégradée et bruitée. En statistique, on dit qu'on cherche à *estimer* l'image initiale. Il n'existe bien sûr pas de méthode universelle pour résoudre ces problèmes. Un principe simple, héritier de la pensée d'Occam, un moine franciscain du XIV^{e} siècle, résume cependant le principe de la plupart des méthodes modernes. Le principe du rasoir d'Occam stipule que *parmi toutes les explications plausibles, il faut choisir la plus simple*. Que signifie ce principe général ici ?

Une *explication* est une image que l'on suppose être l'image initiale. Cette explication est *plausible* si, quand on lui fait subir la dégradation due à l'optique dégradée du télescope et l'addition d'un bruit, elle *ressemble* à l'image observée. La simplicité de l'explication correspond alors à la simplicité de l'image...

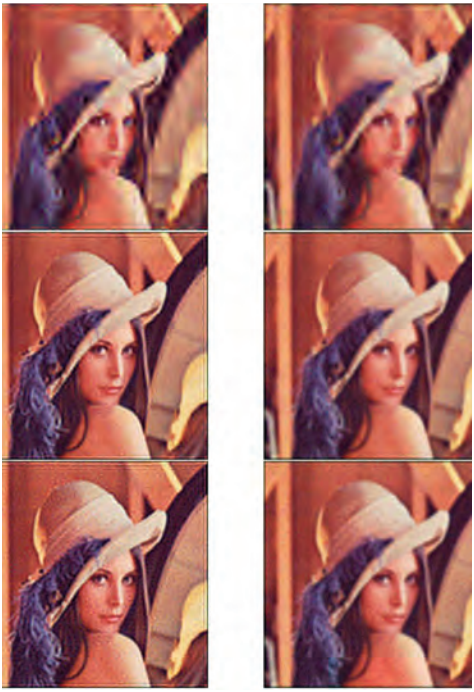


Une image idéale à gauche et l'image floue et bruitée observée par Hubble, à droite

Mais qu'est-ce qu'une image simple ?

Il n'y a malheureusement pas de définition universelle de la simplicité d'une image et encore moins de définition universelle mathématique. Les mathématiciens s'accordent cependant sur la notion de concision : une image simple est une image qui se décrit avec peu de paramètres. Encore faut-il savoir décrire mathématiquement une image... La décomposition dans une base orthonormée fournit souvent un outil efficace pour cela. Comme une position sur le globe terrestre est donnée par sa latitude et sa longitude, une image peut être spécifiée par ses coordonnées

dans une base. La simplicité d'une image se traduit alors par la simplicité de ses coordonnées, par exemple le fait que beaucoup d'entre elles soient nulles. Cette simplicité dépend alors de la base utilisée et le choix d'une base adaptée aux images est donc crucial. Une image numérique est une mosaïque (une matrice) de pixels. La couleur de chacun de ces pixels est spécifiée par une valeur de rouge, une valeur de vert et une valeur de bleu. Si toutes les coordonnées sont nulles le pixel est noir. Une image peut ainsi être décrite par la liste de ces valeurs et cela correspond à la décomposition dans une base dite canonique. Malheureusement, les images simples dans cette base ne correspondent pas aux images naturelles simples. Il existe cependant des bases dans lesquelles les images simples correspondent bien aux images naturelles simples : les bases multi-échelles d'ondelettes qui décrivent les images comme des superpositions d'imagettes élémentaires simples et identiques mais dont on fait varier les tailles et les positions.

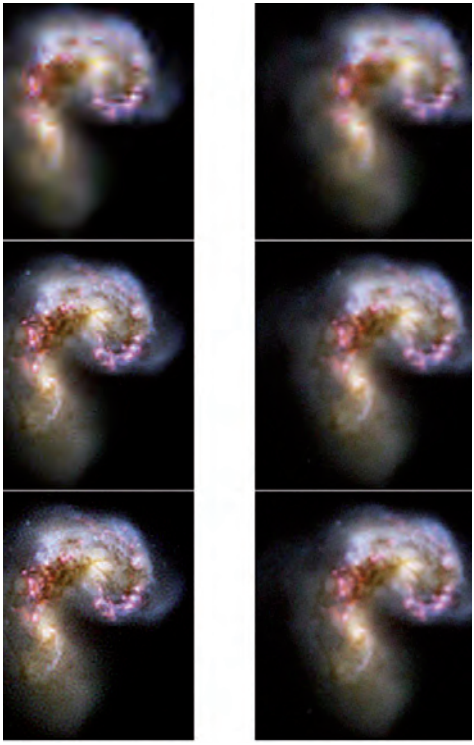


Des explications de plus en plus complexes de haut en bas et à droite leurs versions floutées et bruitées. L'image du milieu est le meilleur compromis entre simplicité (l'image de gauche n'est pas trop complexe) et une bonne explication (l'image de droite ressemble à l'image perçue)

Vers un bon compromis ...

Pour estimer une image à partir de son observation dégradée et bruitée, il faut donc faire un compromis entre la simplicité de l'image et l'adéquation entre cette image et l'observation. Il existe de nombreuses manières de définir mathématiquement ce compromis et de rechercher une image réalisant le meilleur compromis. Les statisticiens parlent de méthode de seuillage, de sélection de modèles, de modélisation bayésienne et de bien d'autres choses... Pour comparer ces estimateurs, on peut

regarder leurs performances sur des données réelles (traitement du signal) ou leurs propriétés mathématiques (statistique). Ce problème est en fait délicat et les deux types de comparaison sont nécessaires. En effet, il est indispensable qu'une méthode soit satisfaisante en pratique, néanmoins il n'est pas possible de la tester sur 'toutes' les images et le fait qu'elle donne de bons résultats sur quelques cas ne préjuge pas de sa qualité sur les autres. Une étude mathématique est donc nécessaire.



Des explications de plus en plus complexes de haut en bas et à droite leurs versions floutées et bruitées. L'image du milieu est le meilleur compromis entre simplicité (l'image de gauche n'est pas trop complexe) et une bonne explication (l'image de droite ressemble à l'image perçue par Hubble)

Le télescope spatial Hubble - crédit NASA

Cependant on retrouve là le problème de la description mathématique d'une image qui n'est pas définitivement résolue. Les modèles que nous possédons actuellement sont encore partiels. Heureusement, la plupart du temps ce sont les mêmes estimateurs qui sont les meilleurs selon les deux critères.

La théorie et la pratique se rejoignent..

Les mathématiques ont constitué pour moi une aventure rencontrée par hasard (au lycée) et qui a pris petit à petit une grande place dans ma vie. L'étude mathématique des phénomènes probabilistes m'a montré, que si on ne maîtrisait pas le hasard, on pouvait toutefois apprendre à le comprendre et parfois à le déjouer.

Dominique Picard

Pour en savoir (un peu) plus :

Le rasoir d'Occam :
http://en.wikipedia.org/wiki/Occam

E. Le Pennec La compression d'images dans "Images des mathématiques,
http://www.math.cnrs.fr/imagesdesmaths/

Nos pages web qui contiennent des références plus spécialisées :
www.math.jussieu.fr/~lepennec
www.proba.jussieu.fr/pageperso/picard/picard.html

Itération de polynômes

dans le plan complexe

Jean-Christophe YOCCOZ

Les nombres complexes ont été initialement découverts comme racines manquantes d'équations polynomiales : c'est ainsi que le nombre *imaginaire* i est la racine carrée du nombre - 1. Au XIX^{e} siècle, Cauchy, Riemann et Weierstrass développent le calcul différentiel de Leibnitz et Newton dans le champ complexe et en exposent la richesse très spécifique. Au début du XX^{e} siècle, Pierre Fatou et Gaston Julia étudient l'itération de polynômes et fractions rationnelles dans le plan complexe, s'appuyant sur les idées développées quelques années plus tôt par Henri Poincaré. Après quelques décennies de stagnation relative, leur théorie prend un essor nouveau au début des années 1980, en raison notamment des possibilités de simulation numérique et production d'images offertes par les ordinateurs.

Les nombres complexes s'identifient aux points du plan, appelé dans ce cas plan complexe. Chaque nombre complexe a un module, sa distance à l'origine, et un argument, l'angle que forme le rayon qui le relie à l'origine avec le rayon horizontal positif. L'addition des nombres complexes est celle des vecteurs. Pour multiplier deux nombres complexes, on multiplie leurs modules et on ajoute leurs arguments.

Etant donné un polynôme P à coefficients complexes, on définit une suite à partir de sa valeur initiale z_0 par la relation de récurrence $z_{n+1} = P(z_n)$. On veut comprendre le comportement de cette suite pour tous les choix possibles de z_0. Le cas le plus simple est celui d'un point fixe vérifiant $z_0 = P(z_0) = z_1$ ou plus généralement d'un point périodique vérifiant $z_0 = z_N$ pour un entier $N \geq 1$

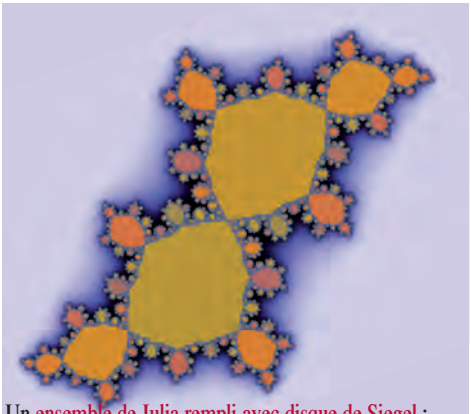
Le cas où P est de degré 1 étant élémentaire, on supposera que le degré de P est au moins égal à 2. On appelle alors ensemble de Julia rempli l'ensemble K des valeurs initiales z_0 pour lesquelles la suite z_n ne s'échappe pas à l'infini. Lorsque la valeur initiale se trouve à l'intérieur de K, le comportement de la suite z_n est simple : soit elle converge vers une orbite périodique, soit elle tourne autour d'une orbite périodique suivant un mouvement de rotation (déformée) d'angle incommensurable avec 2π. Lorsque la valeur initiale z_0 se trouve au contraire sur le bord de K (ce bord constitue l' ensemble de Julia proprement dit), le comportement de la suite z_n est typiquement chaotique, s'apparentant à une suite de tirages au sort d'un dé ou d'une pièce de monnaie.

L'existence de domaines où la dynamique s'apparente à une rotation (de tels domaines sont appelés disques de Siegel) n'était pas connue de Fatou et Julia. Elle dépend de problèmes dits de petits dénominateurs, bien connus des astronomes depuis le XVIII^{e} siècle, mais seulement résolus à partir de 1942 par C.L. Siegel puis un peu plus tard par A. Kolmogorov, V. Arnold et J. Moser (la "théorie KAM"). A la suite des travaux de A. Brjuno et moi-même,

on connaît exactement quels angles donnent lieu à des disques de Siegel pour les polynômes quadratiques.

L'ensemble de Julia est en général un objet fractal : par exemple, pour le polynôme $P(z) = z^2 + c$ avec c petit mais non nul, l'ensemble de Julia est une courbe entourant l'origine dont la dimension fractale est strictement comprise entre 1 et 2.

L'ensemble de Julia n'a pas d'intérieur ; a-t-il pour autant une aire nulle ? La question, évoquée par Julia, a pris de l'importance avec les travaux de D. Sullivan dans les années 1980. Poursuivant une stratégie proposée par A. Douady au début des années 1990, X. Buff et A. Chéritat viennent de montrer que la réponse est négative, en construisant des polynômes quadratiques pour lesquels l'aire de l'ensemble de Julia est strictement positive. Par une suite de perturbations très soigneusement contrôlées, ils font disparaître l'intérieur d'un disque de Siegel sans affecter sensiblement son aire.



Un ensemble de Julia rempli avec disque de Siegel ; l'angle de rotation est égale au nombre d'or.

Crédit photo : Arnaud Chéritat

Après la première étape de la construction de Duff et Chéritat : l'ensemble de Julia rempli, proche du précédent, a un intérieur beaucoup plus mince.

Crédit photo : Arnaud Chéritat

C'est Michel Herman qui m'a initié à la recherche à partir de 1977 alors que j'étais élève à l'Ecole Normale Supérieure. Un long séjour à l'IMPA de Rio de Janeiro a été le prélude à des relations privilégiées avec le Brésil depuis plus de 25 ans. Après avoir été chargé de recherches au CNRS au Centre de Mathématiques de l'Ecole Polytechnique, j'ai été professeur à l'Université Paris-Sud (Orsay) avant d'occuper au Collège de France depuis 1996 la chaire d'Equations Différentielles et Systèmes Dynamiques. Je suis membre des Académies des Sciences française et brésilienne, ainsi que de la TWAS (académie des sciences des pays en développement). J'ai reçu la Médaille Fields en 1994 pour mes travaux sur la théorie des Systèmes Dynamiques.

Jean-Christophe YOCCOZ

Pour en savoir (un peu) plus :

A.F. BEARDON, Iteration of Rational Functions, Springer (1991).

L. CARLESON, T.W. GAMELIN, Complex Dynamics, Springer (1993).

J. MILNOR, Dynamics in one complex variable : introductory lectures, Arxiv preprint math.DS/9201272 (1990).

J-C. YOCCOZ, Ensembles de Julia de mesure positive et disques de Siegel des polynômes quadratiques [d'après X. Buff et A. Chéritat], Séminaire Bourbaki n° 966, 2005-2006, p. 385-401.

La dynamique qualitative

Étienne GHYS

Depuis Newton, on sait que les forces modifient le mouvement. Si la terre était seule dans l'espace, elle se déplacerait à vitesse constante le long d'une trajectoire rectiligne. Mais la force de gravitation exercée par le Soleil modifie cette trajectoire et la Terre tourne autour du Soleil. Il est souvent facile de comprendre les forces qui agissent, mais il est par contre beaucoup plus difficile d'en déduire les trajectoires du mouvement qui en résulte. C'est le but de la *théorie des équations différentielles*.

Pendant deux siècles, il s'agissait de résoudre les équations différentielles, c'est-à-dire de trouver une formule décrivant la trajectoire cherchée. Vers la fin du dix-neuvième siècle, Henri Poincaré prit conscience du fait qu'il est bien souvent impossible de trouver une telle formule. Il décida alors de créer une théorie qualitative, à la fois plus modeste et plus ambitieuse. Lorsqu'un élève essaye de tracer le graphe d'une fonction (sans utiliser sa calculette !), il commence par déterminer ses points remarquables, ses maxima, ses points d'inflexion, ses asymptotes, et ensuite, à main levée, il en déduit l'allure générale de la courbe, ce qui est une information très riche, souvent suffisante pour les applications. Dans la théorie qualitative des systèmes dynamiques, on détermine de même quelques trajectoires remarquables, les positions d'équilibre, les asymptotes, et on essaye ensuite d'en déduire l'allure générale des trajectoires. Pour développer sa théorie, Poincaré a besoin de construire de toutes pièces une autre théorie, préliminaire à toute description qualitative des formes en mathématiques : la topologie.

Un exemple important vient de la mécanique céleste. Si trois masses dans l'espace s'attirent selon les lois de Newton, quelles sont les trajectoires ? Existe-t-il des configurations pour lesquelles le mouvement est périodique ? C'est sur cet exemple que Poincaré met en évidence *le concept de mouvement chaotique*. Depuis un siècle, les théories des systèmes dynamiques et de la topologie se sont largement développées et un tissu serré de liens a été établi avec toutes les autres parties des mathématiques. Par exemple, en 1964, le météorologiste E. Lorenz étudiait le problème extrêmement complexe de la convection dans l'atmosphère. Il n'hésita pas à simplifier l'équation de manière presque caricaturale, passant d'une équation différentielle en dimension infinie à une équation en dimension 3. Lorsqu'il traça les trajectoires de son système avec un ordinateur, il observa un objet remarquable, qu'on appelle aujourd'hui l'attracteur de Lorenz. Appliquée à la météorologie, l'idée de trajectoire chaotique devient le fameux effet papillon : un battement des ailes d'un papillon au Brésil pourrait provoquer un ouragan au Texas ! Les conséquences scientifiques et philosophiques de ce genre d'idées sont importantes, pas seulement en mathé-

matiques. L'attracteur de Lorenz est devenu un objet emblématique de la théorie, d'abord parce qu'il est joli, mais aussi parce qu'il résiste aux perturbations. Dans les années 1980, Birman et Williams ont analysé la nature topologique des trajectoires périodiques : ce sont des courbes fermées dans l'espace qui peuvent donc être nouées. Quels sont les nœuds que l'on rencontre dans l'attracteur ? Il s'agit en quelque sorte de mesurer la complexité topologique de l'objet. Des liens inattendus entre les systèmes dynamiques et la théorie des nombres se sont avérés extrêmement féconds.

Un nombre irrationnel comme π par exemple a un développement décimal infini 3,141592653589... On cherche à l'approcher par des fractions comme 22/7 ou 355/113. On peut toujours le faire, avec n'importe quelle précision, mais le mathématicien aimerait estimer la taille des numérateurs et des dénominateurs en fonction de la précision. C'est le problème de *l'approximation diophantienne* qui peut se traduire dans la dynamique de ce qu'on appelle les *géodésiques sur la surface modulaire*. C'est aussi un système dynamique dans l'espace, dont les trajectoires périodiques ont été étudiées depuis longtemps : elles correspondent aux *entiers quadratiques* comme le nombre d'or !

L'étude topologique de ces entiers quadratiques et des nœuds qu'ils définissent dans l'espace vient d'être réalisée. La surprise est que les nœuds modulaires ainsi obtenus sont *les mêmes* que les trajectoires périodiques

Attracteur de Lorenz - *EG*

dans l'attracteur de Lorenz. Un lien est donc établi entre deux objets d'origines bien différentes :

un plaisir pour le mathématicien !

Après une thèse à Lille en 1979, j'ai eu la chance de faire deux stages post-doctoraux passionnants à l'IMPA de Rio de Janeiro et à l'université de New York. Je travaille sur les systèmes dynamiques et la géométrie, en essayant de mettre l'accent aussi souvent que possible sur les interactions entre les diverses parties des mathématiques. « Provincial convaincu », j'ai participé depuis 1988 à la création et au développement du laboratoire de mathématiques de l'ENS de Lyon. J'ai l'honneur de travailler au CNRS et d'être membre de l'Académie des Sciences.

Étienne GHYS

Pour en savoir (un peu) plus :

A. Chenciner, article dans l'Encyclopédie Universalis. Systèmes dynamiques différentiables,

E. Ghys et J. Leys, Lorenz and modular flow, a visual introduction, http://www.ams.org/featurecolumn/archive/lorenz.html

J. Gleick, chez Flammarion
La théorie du chaos : vers une nouvelle science,

I. Stewart, chez Flammarion
Dieu joue-t-il aux dés ? Les mathématiques du chaos,

Théorie du chaos :
http://fr.wikipedia.org/wiki/Theorie_du_chaos

Transport Optimal

Cédric VILLANI

Vous tenez le standard d'une entreprise de taxis et ce matin vous devez donner des instructions à dix voitures, éparpillées dans Paris, pour récupérer dix clients dans dix endroits différents. *Comment allez-vous apparier voitures et clients de manière à minimiser le temps d'attente total ?*

Comment transporter à moindre frais ?

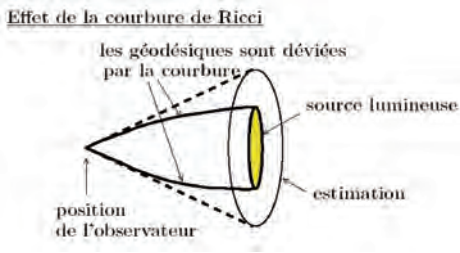
Le problème posé ci-dessus est un cas particulier du problème de **transport optimal**, défini pour la première fois vers 1780 par Gaspard Monge. Ingénieur et mathématicien, père de la géométrie descriptive, ardent révolutionnaire, fondateur de l'École Polytechnique et proche de Napoléon, Monge était l'un des savants français les plus influents de son époque. Son *problème des déblais et des remblais* est du même type que le problème des taxis : *comment transporter des matériaux de construction afin de minimiser le coût de transport total ?*

En 1942, le grand mathématicien russe Leonid Kantorovich (Prix Nobel d'économie) définissait une classe plus générale de problèmes d'optimisation et introduisait de puissants outils pour leur étude théorique et numérique. La *théorie du transport optimal* était née.

Du transport des déblais à la notion de courbure.

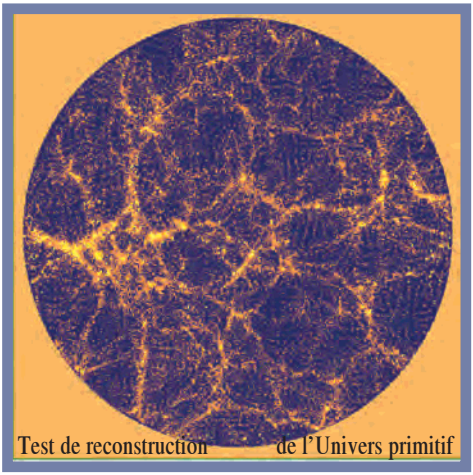
À partir de la fin des années 1980, des chercheurs d'horizons très divers constataient avec surprise que la théorie du transport optimal permettait d'établir des liens entre leurs domaines respectifs : équations des fluides incompressibles, systèmes dynamiques, météorologie, cosmologie, etc. C'est ainsi que vers 2000, une équipe mixte composée de physiciens et mathématiciens publiait une méthode de reconstitution des fluctuations de l'Univers primitif basée sur le transport optimal. Une direction de recherche, très active en ce moment, concerne les applications du transport optimal à la géométrie, et plus particulièrement à l'étude de la **courbure**, qui mesure quantitativement la vitesse de séparation des géodésiques, ou trajectoires des rayons lumineux.

Les géomètres utilisent différentes notions de courbure ; celle qui est le plus directement liée au transport optimal est la courbure dite de Ricci, bien connue pour son rôle majeur dans la théorie de la relativité générale d' Einstein. Dans cette théorie, les corps célestes déforment l'Univers en lui imposant une courbure non



nulle, ce qui dévie les rayons lumineux et modifie les observations : par exemple, si la courbure est positive, on a tendance à surestimer la surface de l'objet observé. Voici maintenant un autre effet de la courbure, que l'on peut exprimer en termes de mécanique des fluides plutôt que de rayons lumineux. Je l'appelle *l'expérience du gaz paresseux,* c'est une expérience de pensée, représentation informelle d'un énoncé mathématique précis (que je ne chercherai pas à infliger à des non-spécialistes !) basé sur le transport optimal.

L'expérience consiste à se donner une répartition de gaz dans l'espace, avec des fluctuations de densité d'une région à l'autre. On impose au gaz une nouvelle configuration, à atteindre en un temps limité, disons une minute. Le gaz obtempère, mais comme il est paresseux, il le fait en évoluant de manière à minimiser l'effort total (mesuré à chaque instant par l'énergie cinétique). Entre le temps initial et le temps final, on étudie les valeurs de l'**entropie**, qui mesure en un certain sens bien précis l' étalement du gaz (l'entropie est d'autant plus grande que la densité est faible). Si l'on vit dans un espace à courbure positive, alors la courbe d'entropie est **concave** ; en particulier elle est située au-dessus de la droite joignant les valeurs initiale et finale. La propriété de concavité est en fait caractéristique des espaces à courbure positive ; ce qui ouvre de nouveaux horizons pour étudier (voire pour redéfinir) les espaces à courbure positive.



Test de reconstruction de l'Univers primitif

En mélangeant des notions d'ingénierie, de mécanique des fluides et de physique statistique, on a ainsi obtenu de nouveaux outils géométriques !

Après ma sortie des classes préparatoires, j'ai fait toute ma carrière dans le merveilleux système des Écoles Normales Supérieures; d'abord à Paris en tant qu'élève et agrégé-préparateur; puis à l'ENS de Lyon en tant que professeur. J'ai découvert le transport optimal grâce aux travaux du Japonais Hiroshi Tanaka qui eut l'idée de l'appliquer à l'étude de l'équation de Boltzmann ---le sujet de ma thèse. Des contacts avec les meilleurs spécialistes européens du sujet m'ont permis d'approfondir le sujet. Deux séjours de longue durée aux États-Unis ont joué un rôle crucial dans mes recherches ultérieures : le premier à Atlanta en 1999 où j'ai été invité à dispenser un cours avancé ; le second à Berkeley en 2004 où j'ai rencontré un proche collaborateur. Ce parcours illustre des phénomènes généraux : les voyages à l'étranger, la préparation de cours spécialisés et les collaborations sont des moteurs efficaces (et attrayants) de la recherche mathématique.

Cédric VILLANI

Pour en savoir (un peu) plus :

C. Villani, Transport optimal : coup de neuf pour un très vieux problème; Images des Mathématiques 2004, publication du CNRS :
www.spm.cnrs-dir.fr/actions/publications/idm04.htm

Ma page Web contient des références plus spécialisées :
www.umpa.ens-lyon.fr/~cvillani

Les grandes matrices aléatoires

Alice GUIONNET

Même si le concept d'aléa est palpable dans la vie de tous les jours et sert de base à des activités lucratives depuis fort longtemps, la théorie des probabilités ne s'est réellement développée qu'au cours du vingtième siècle.

Dans les années vingt, Kolmogorov mit au centre de cette théorie la notion de variable aléatoire. Une variable aléatoire est une fonction qui prend ses valeurs avec une probabilité donnée.

Par exemple, dans un jeu de pile ou face où une pièce est lancée, nous pouvons considérer une fonction qui représente l'événement *la pièce tombe côté pile*. La variable aléatoire vaut un dans ce cas et zéro sinon. Cette fonction prend donc les valeurs zéro et un, chacune avec probabilité un demi... si la pièce n'est pas truquée ! Une autre variable pourrait compter le nombre de fois où pile est apparu pendant n tirages, indépendants les uns des autres (l'indépendance ici signifie que le résultat d'un tirage n'influence pas les autres). On voit ici que les probabilités peuvent être reliées à des problèmes combinatoires. Mais elles sont loin de se restreindre à ce cadre et elles apparaissent aujourd'hui dans de nombreux domaines des mathématiques.

Je m'intéresse au cas où les variables aléatoires prennent des valeurs dans les matrices et non comme plus haut dans un espace à deux états zéro et un.

Une matrice aléatoire est donc un tableau avec M colonnes de longueur N dont les éléments sont des variables aléatoires.

J'étudie particulièrement le cas où M et N sont grands. Ces objets mathématiques apparaissent, comme nous allons le voir, dans des domaines très différents, ouvrant la porte à des connections à explorer.

Les matrices aléatoires sont apparues pour la première fois à la fin des années vingt en statistique dans les travaux de Wishart. La matrice représente alors un tableau de données à analyser. Pour comprendre si ce tableau révèle une corrélation importante des données, Wishart propose de le comparer à ce qui serait observé si les éléments de la matrice étaient choisis de façon aléatoire et indépendante. Les matrices de Wishart servent aujourd'hui à calculer la capacité de réseaux de téléphones portables ! Dans les années cinquante, Wigner proposa d'utiliser les matrices aléatoires en mécanique quantique afin d'interpréter les observations de la dynamique de noyaux soumis à une forte excitation (par exemple le noyau d'hydrogène). La dynamique d'un système quantique est décrite par un opérateur, le Hamiltonien. Wigner modélise ce Hamiltonien par une matrice, choisie la plus aléatoirement possible dans la limite des contraintes connues du modèle. L'expérience confirme ce modèle.

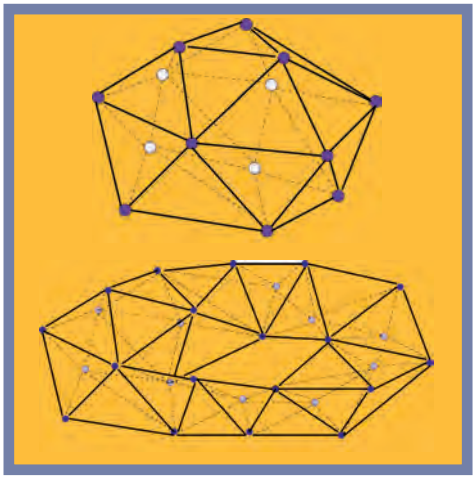
Les grandes matrices aléatoires

Les matrices aléatoires ont également été liées numériquement, sans explication théorique, aux dynamiques chaotiques et à la fonction Zeta de Riemann.

Dans un tout autre contexte, Tutte étudia dans les années soixante la question combinatoire suivante : *de combien de façons peut-on paver un ballon avec 100 triangles ? Que se passe-t-il si on veut paver une bouée ?*

En 1978, Brézin, Itzykson, Parisi et Zuber montrèrent, en spécialisant une idée de Gérard 't Hooft, que cette question était reliée à des matrices aléatoires. Les matrices aléatoires permettent de résoudre des problèmes d'énumération de pavages ou de graphes qui n'ont pas encore trouvé de solution combinatoire.

Dans les années quatre-vingts, Voiculescu introduisit les probabilités libres ; c'est une théorie de probabilité pour des variables aléatoires prenant leurs valeurs dans un espace encore plus général que celui des matrices. Les matrices aléatoires, dans la limite où leur taille tend vers l'infini, se placent naturellement dans ce cadre. Voiculescu montra que des matrices aléatoires indépendantes, quand leur taille tend vers l'infini, convergent vers des variables dites libres. Le concept de liberté est fondamental en théories des groupes et d'algèbres d'opérateurs. Dès lors, les matrices aléatoires devinrent une source d'exemples et d'inspiration dans la théorie des algèbres d'opérateurs.



Un domaine merveilleux où se côtoient et se nourissent physique, algèbres d'opérateurs, combinatoire et probabilités !

Issue des classes préparatoires, je suis rentrée à l'Ecole Normale Supérieure où je me suis prise au jeu de la recherche. Je travaille au CNRS depuis ma sortie de l'Ecole, d'abord chargée de recherche (à l'université d'Orsay, à l'Ecole Normale supérieure de Paris puis de Lyon) et, depuis 2005, directrice de recherche.
Les probabilités se sont imposées à moi comme une des branches des mathématiques la plus proche des applications, aussi bien en physique, statistique ou finance.
Mais l'aventure de la recherche est bien de nous mener où elle veut, d'idées en questions, et aujourd'hui mes intérêts sont bien loin de mes premières préoccupations.

Alice GUIONNET

Pour en savoir (un peu) plus :

M.L. Mehta, Random Matrices (Elseiver)

P. Di Francesco, P. Ginsparg, J. Zinn Justin, Article de revue 2D gravity and random matrices, Phys. Rev. 254 (1995)

Site personnel http://www.umpa.ens-lyon.fr/aguionne/(deux articles de revue)

La cryptologie moderne et Jacques Stern

Médaille d'or du CNRS

Laurent DEMONET

Jacques Stern a reçu en 2006 la Médaille d'or du CNRS pour ses travaux fondateurs en cryptologie moderne. Cette distinction, la plus haute pour des travaux de recherche en France, est décernée chaque année depuis 1954 à un chercheur ayant contribué au rayonnement de la recherche française dans le monde. A 57 ans, Jacques Stern est directeur du Département d'informatique de l'ENS, chercheur d'exception aux nombreux disciples dans l'école française de cryptologie.

La cryptologie, science de paradoxes

L'art de crypter des messages est pratiquement aussi ancien que l'art militaire. Malgré cela, ce n'est que très récemment que la cryptologie est née en tant que discipline scientifique à part entière, rigoureuse, par opposition à la cryptographie empirique traditionnelle. La cryptologie rassemble essentiellement deux branches :

- la cryptographie qui consiste à inventer de nouvelles méthodes de cryptage, souvent appelées protocoles cryptographiques ;
- la cryptanalyse qui consiste à casser des protocoles cryptographiques, c'est-à-dire à trouver le moyen de décrypter des données sans posséder le code qui a permis de les crypter.

Ces deux branches sont intimement liées dans la cryptologie moderne, puisque trouver un protocole cryptographique efficace revient à diminuer au maximum la possibilité pour un adversaire de le casser. Au-delà de cette observation, il est extrêmement difficile de formaliser scientifiquement cette notion : comment garantir qu'un protocole résistera aux attaques des cryptanalystes sans connaître a priori les méthodes qu'ils utiliseront ? On sait aujourd'hui que cette question n'a pas de réponse absolue.

La question de la sécurité des protocoles cryptographiques est plus que jamais fondamentale, pour deux raisons : leur usage s'est banalisé, passant d'un usage militaire à un usage civil intensif (en particulier dans le cadre des transactions financières) d'une part, et les moyens potentiels de cryptanalyse ont explosé (naissance puis progrès de l'informatique). Par conséquent, la nécessité de prouver la sécurité de protocoles cryptographiques est devenue vitale, et c'est dans ce cadre qu'interviennent les mathématiques les plus poussées et, en un sens, les plus abstraites, utilisées dans les applications les plus concrètes. C'est dans ce domaine que Stern a obtenu de remarquables avancées.

Comment prouver un protocole cryptographique ?

Tout d'abord, il n'est pas possible d'inventer une méthode cryptographique absolument sûre, dans la mesure où il restera toujours une probabilité, éventuellement extrêmement faible, de réussir à décrypter un message quel que

soit le protocole utilisé. Le but est donc de limiter le plus possible cette probabilité relativement aux autres contraintes (en particulier aux contraintes de puissance : il faut par exemple que le cryptage du numéro d'une carte bancaire lors d'un achat sur Internet puisse être effectué par un ordinateur personnel en un temps extrêmement court, alors que l'on peut imaginer s'autoriser plus de temps et plus de puissance pour des applications militaires). Par ailleurs, il faut considérer qu'aucun des canaux de transmission n'est sûr (si c'était le cas, on n'aurait pas besoin de crypter) ; l'hypothèse que l'on fait donc habituellement en cryptologie est que le secret du cryptage est une donnée relativement petite, appelée clé. Dans le cadre de la preuve d'un protocole, on considère toujours le pire, c'est-à-dire le cas où le cryptanalyste possède toute l'information possible sur le protocole, sauf la clé. Le reste de la démarche consiste à démontrer que casser le protocole cryptographique revient à résoudre un problème qui est très difficile.

Cryptographie asymétrique : un progrès fondamental

La cryptographie habituelle est dite symétrique. C'est-à-dire que les deux personnes qui veulent communiquer partagent un secret (la clé) qui permet à la fois de crypter et de décrypter les messages. Par exemple, la méthode qui consiste à permuter les lettres de l'alphabet est un protocole symétrique : l'envoyeur et le destinataire du message


Jacques Stern

doivent tous deux savoir la manière dont sont permutées les lettres, manière qui constitue la clé.

La cryptographie asymétrique, parfois appelée aussi cryptographie à clé publique fait intervenir deux clés, une clé privée et une clé publique, qui sont liées ; la sécurité du protocole sera alors d'autant plus grande que la difficulté de déterminer la clé privée à partir de la clé publique est grande. La clé publique est alors publiée, et n'importe qui peut envoyer des messages cryptés au seul individu qui connaît la clé privée (puisqu'il ne l'a donnée à personne). On peut même utiliser ce principe pour crypter et signer des messages en même temps (signer un message consiste à prouver l'identité de l'envoyeur). Ainsi supposons qu'Alice veuille envoyer un message à Bob. Elle commence par crypter ce message avec la clé publique de Bob, puis elle crypte le message crypté avec sa clé privée. Ensuite, Bob commence par décrypter le message avec la clé publique d'Alice puis avec sa propre clé privée. Comme il faut la clé privée de Bob pour décrypter le

message, Alice est sûre que seul Bob pourra le lire. Par ailleurs, quand Bob aura décrypté le message et découvert quelque chose d'intelligible, il saura que c'est bien Alice qui l'a écrit puisque personne d'autre ne connaît la clé privée d'Alice.

Les avantages de la cryptographie asymétrique sont multiples : en particulier, elle permet de ne jamais avoir à transmettre la clé secrète, ce qui lui évite d'être interceptée par un individu malveillant ; par ailleurs, cela permet à chaque individu (ou à l'ordinateur de chaque individu) de n'avoir à retenir qu'une seule clé (sa clé privée), les clés publiques étant disponibles dans une sorte d'annuaire. Le défaut est alors qu'il faut qu'il existe un organisme jouant le rôle de cet annuaire ayant la confiance de tous (puisqu'il serait facile à cet organisme de remplacer par la sienne la clé publique de Bob). Ces organismes sont ceux qui produisent les certificats que les navigateurs Internet demandent d'accepter, en particulier lors de transactions.

Un exemple de protocole asymétrique est le protocole RSA (utilisé par exemple lors d'achats par cartes bancaires). La clé privée est un couple de deux grands nombres premiers et la clé publique est le produit de ces deux nombres. On considère actuellement que le fait de retrouver les deux facteurs du produit est un problème extrêmement difficile (on ne sait actuellement pas factoriser les entiers de plus de quelques centaines de chiffres).

Depuis toujours, Jacques Stern, pro-

fondément marqué par les travaux de Gödel et Turing, est attiré *par les sciences au tempo rapide, où les recherches trouvent rapidement des prolongements concrets*. L'entrée de la cryptologie dans le domaine académique, l'invention du concept à clé publique allaient ouvrir à ses recherches la voie d'une reconversion logique et en or !

Il lui fallut alors apprendre à programmer, travailler en théorie des nombres, transiter par la complexité algorithmique et potasser l'histoire de cette nouvelle science. Ses efforts paient ! A 37 ans, ses travaux en lien avec la cryptologie lui valent sa première invitation à un colloque international. Dix ans plus tard, il est à la tête du Laboratoire d'informatique, commun ENS-CNRS tout en ne négligeant pas l'enseignement car pour lui il s'agit *d'une activité où l'on voit les générations se former, et qui force un chercheur à clarifier ses idées*.

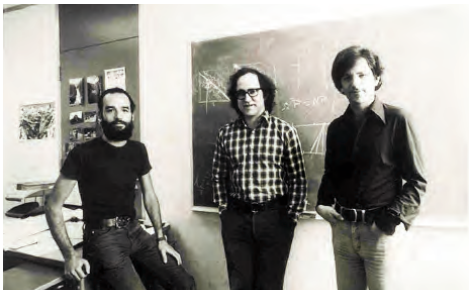
Le remarquable ouvrage qu'il publia en 1998 chez Odile Jacob *La science du secret* est à la fois le prolongement de cet enseignement, la nécessité d'ancrer ses

travaux dans une dynamique historique et la volonté de nouer des relations entre sciences et société.

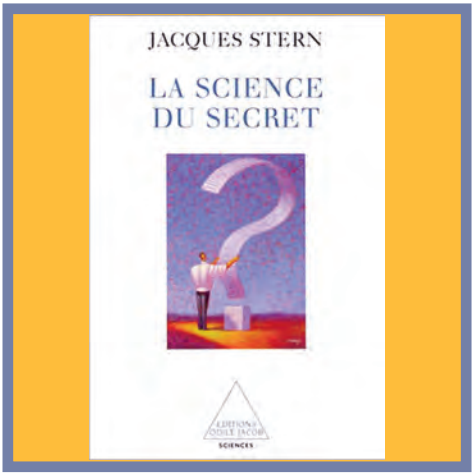
Il est membre du Conseil Scientifique de la Défense, du Conseil Stratégique de l'Information et il travaille à l'Observatoire de la Sécurité des Cartes de Paiement.

Jacques Stern est bien placé pour savoir que *Internet reste la zone de tous les dangers* mais il reste persuadé que la *cryptologie va sûrement évoluer vers de nouveaux concepts qui prendront en compte les mauvaises habitudes de l'utilisateur naïf qui, par exemple, ne met pas à jour régulièrement son système d'exploitation.*

Alors ce n'est plus un secret pour personne, Jacques Stern, premier informaticien au palmarès de la Médaille d'or du CNRS, avec ses nombreux étudiants, reste un expert des plus redoutés des inventeurs de code !



L'algorithme asymétrique de cryptographie à clé publique, **RSA**, très utilisé dans le commerce électronique et en particulier pour la circulation des données sur Internet, a été décrit en 1977 par trois jeunes américains Ron **R**ivest, Adi **S**hamir et Len **A**dleman.



Biographie de Jacques Stern

1949 : naissance de Jacques Stern
1968 : entrée à l'École Normale Supérieure
1971 : 1er à l'agrégation de mathématiques
1975 : doctorat de mathématiques
1979 : obtention du grade de professeur d'université (Caen)
1993 : professeur à l'ÉNS
1996 : directeur du laboratoire d'informatique de l'ÉNS
1998 : rapport sur la cryptologie remis au gouvernement qui aboutira l'année suivante à la nouvelle réglementation sur la cryptographie
1999 : devient directeur du département d'informatique de l'ÉNS
chevalier de la Légion d'honneur
2003 : prix Lazare Carnot de l'Académie des sciences
2005 : Médaille d'argent du CNRS
2006 : Médaille d'or du CNRS

Pour en savoir (un peu) plus :

Les livres suivants sont accessibles au grand public :

- *Jacques Stern*, La science du secret, Editions Odile Jacob, 1998

- *Jacques Stern,* Chapitre 6 de Paradigmes et enjeux de l'informatique (avec P. Nguyen), Editions Lavoisier, 2005 (ouvrage sous la direction de N. Bidoit, L. Fariñas del Cerro, S. Fdida, B. Vallée)

Statistique des écarts

de la vie quotidienne à la conjecture de Riemann

Michel BAUER et Philippe Di FRANCESCO, CEA

De nombreux phénomènes font intervenir des séries de nombres rangés par ordre croissant et dont la répartition des écarts est souvent révélatrice.

Nous allons en donner quelques exemples.

Les horaires d'autobus

Même si les horaires de l'autobus qui s'arrête près de chez nous sont programmés au long d'une journée à intervalles réguliers, par exemple toutes les 15 minutes, les heures de passage réelles peuvent être différentes. Nous avons tous un jour attendu bien plus d'une demi-heure. Il arrive aussi que deux autobus se suivent à moins d'une minute. Il est possible de quantifier ces fluctuations en faisant un histogramme qui compte combien de fois l'écart entre deux bus successifs a été, par exemple, de moins de 5 minutes, de 5 à 10 minutes, de 10 à 15 minutes, etc. Si T_i est l'heure de passage du $i+1^{ème}$ (à T_0 passe le premier bus, le suivant à T_1, etc), on compte pour combien de valeurs de i, T_{i+1}-T_i est plus petit que 5 minutes, compris entre 5 et 10 minutes, 10 et 15 minutes, etc.

En l'absence de tout aléa sur le parcours, on s'attend à ce que presque tous les écarts soient proches de 15 minutes, donc que seules les tranches entre 10 et 20 minutes soient représentées. En revanche, si de nombreux petits incidents viennent perturber chaque trajet mais qu'ils sont assez brefs pour n'avoir une influence notable que sur un des bus, le résultat peut ressembler à celui décrit dans la figure 1, dont l'interprétation, surprenante au premier abord, est que de nombreux bus se suivent de près, mais que ceci est compensé par de rares écarts très importants ; phénomène effectivement observé dans de grandes villes.

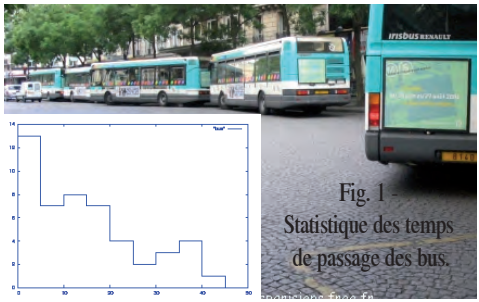


Fig. 1
Statistique des temps de passage des bus.

Les cageots de fruits

De nos jours, les fruits de l'étal du marchand sont calibrés, mais malgré cela, deux pommes du même cageot n'ont pas exactement le même poids. Muni d'une balance de précision, on peut trier les pommes du cageot par poids croissant, P_0 est le poids de la plus légère, P_1 le poids suivant, etc, jusqu'au poids de la pomme la plus lourde, P_n si le cageot contient n + 1 pommes. Pour un cageot réel, n serait typiquement de l'ordre de la cinquantaine. L'écart de poids moyen Δ est simplement la différence entre le poids de la plus légère et de la plus lourde (P_n-P_0) divisé par n. On peut faire le même type d'histogramme que pour les temps d'attente entre deux bus : pour combien de valeurs de i la différence P_{i+1} - P_i est-elle de moins d'1/5 de l'écart moyen Δ, ou comprise

entre 1/5 et 2/5 de Δ , etc ? Et on observe un résultat analogue : à nouveau, de nombreuses pommes ont des poids qui ne diffèrent que d'une faible fraction de l'écart moyen, et ceci est compensé par quelques écarts bien plus grands que la moyenne. Dans le cas présent, on dispose d'un modèle probabiliste très simple pour expliquer le résultat. Ce modèle prédit que si le nombre de pommes est très grand, dans une échelle appropriée, l'histogramme s'approche d'une exponentielle, comme sur la figure 2. La statistique des écarts des bus ne suit que qualitativement cette loi limite car le nombre d'échantillons est faible.

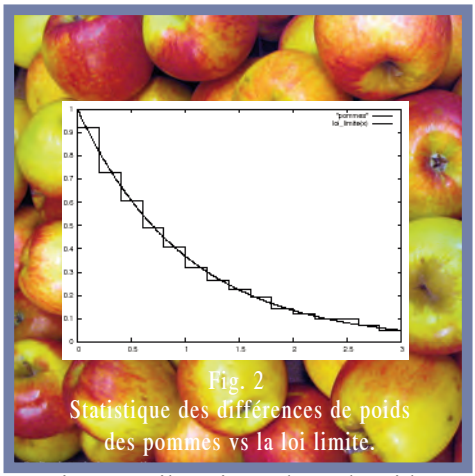


Fig. 2
Statistique des différences de poids des pommes vs la loi limite.

Les vibrations en construction automobile

L'exemple suivant est inspiré de l'automobile. Il n'y a pas si longtemps, il n'était pas rare que, pour certains régimes moteur, la carrosserie d'un véhicule vibre tout à fait perceptiblement. Le phénomène est analogue à celui d'une personne qui pousse un enfant sur une balançoire. Si elle choisit la bonne fréquence, il suffit de donner des pichenettes pour que l'amplitude augmente fortement. Les vibrations d'un véhicule sont une nuisance et l'utilisation d'ordinateurs pour la conception a permis de supprimer quasiment le phénomène. On peut voir la carrosserie comme un ensemble de pièces p_0 , ... , p_n liées plus ou moins fortement les unes aux autres et on peut quantifier ceci dans une tableau de nombres m_{ij}, $0 < i, j < n$ d'autant plus grands que la liaison entre les pièces numérotées i et j est forte. Un tel tableau de nombres s'appelle une matrice, et il existe des algorithmes mathématiques pour déduire de ce tableau de nombres les fréquences d'excitation qui feront vibrer fortement la carrosserie, il y en a en général n+1, que l'on peut ordonner de f_0 (la plus petite) à f_n, la plus grande. On peut alors s'intéresser à la statistique des écarts, comme pour les pommes et les bus. Nous ne connaissons pas l'allure de l' histogramme des écarts de fréquence pour la carrosserie d'une voiture, mais les mêmes objets mathématiques décrivent des systèmes physiques plus "fondamentaux", avec des résultats remarquables.

Généralisons à tout système physique

Si l'on ne craint pas d'être caricatural, on peut dire que le principe fondamental de la mécanique quantique est que tout système physique est décrit par un tableau de nombres (une matrice appelée *hamiltonien*), même si l'interprétation des nombres m_{ij} dans ce cas est délicate, et assez différente de celle de l'exemple d'une carrosserie. Il reste néanmoins vrai que la première chose à comprendre est l'ensemble des fréquences de vibrations correspondantes, que l'on

appelle dans ce cas les niveaux d'énergie, et qui forment le spectre du système considéré. Les raies d'émission (ou raies spectrales) des atomes sont par exemple liées à des écarts entre niveaux d'énergie. Dans certains systèmes, mais rares, on peut calculer exactement les niveaux d'énergie. L'atome d'hydrogène est un exemple très important. Mais le spectre des noyaux même les plus simples, échappe à une approche analytique. En fait le *hamiltonien* des noyaux lui même est encore très mal compris aujourd'hui sur le plan fondamental. Les mesures expérimentales du spectre donnent des résultats qui semblent chaotiques. C'est ce qui a amené au début des années 1950 le physicien Eugène Wigner à poser la question suivante : peut-on comprendre certains aspects du spectre en remplaçant les coefficients m_{ij} mal connus par des nombres aléatoires ? Il n'y a pas d'espoir que les niveaux d'énergie individuels soient reproduits par un système aléatoire, mais la statistique des écarts de niveaux par exemple est un meilleur candidat car c'est une quantité moyenne sur le spectre. De plus, expérimentalement, les écarts entre les niveaux d'énergie ont une statistique simple et grosso modo indépendante du noyau considéré. Cette statistique est bien différente de celles des écarts entre les temps de passage des autobus ou entre les poids des pommes comme le montre la figure 3.

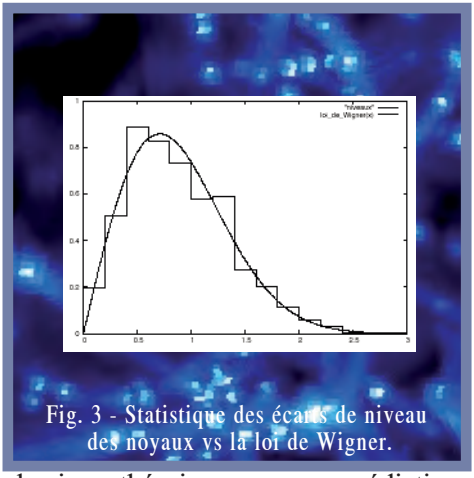


Fig. 3 - Statistique des écarts de niveau des noyaux vs la loi de Wigner.

Wigner et les matrices aléatoires

En particulier, les petits écarts sont peu nombreux : on dit que les niveaux d'énergie se repoussent. Le calcul de Wigner est un des grands succès de la physique théorique, car ses prédictions sont très proches des résultats expérimentaux. Son approche originale, qui a donné naissance à la vaste théorie des matrices aléatoires, ne cesse de trouver des applications dans tous les domaines de la science ou presque. (voir l'article d'Alice Guionnet sur les Grandes Matrices Aléatoires qui évoque le vaste champ d'application des permutations aléatoires).

Riemann et nombres premiers

Un exemple plus surprenant encore est donné par la théorie des nombres. Nous avons appris au collège que tout nombre entier s'écrit sans ambiguité comme un produit de nombres premiers (premier car divisible que par 1 et lui même). La suite des nombres premiers (qui est infinie, on le sait depuis Euclide) commence ainsi : 2, 3, 5, 7, 11, 13, ... Leur répartition reste aujourd'hui encore mystérieuse. Il est possible de coder tous les nombres premiers implicitement dans une fonction appelée fonction Zeta. Cette fonction qui lie une somme portant sur tous les entiers et un produit où interviennent les nombres premiers permet de définir une droite spéciale D, dite droite critique, sur laquelle s'alignent tous les zéros de la fonction. C'est sur cette fonction que

Riemann formula une fameuse conjecture abstraite (voir article de Benoît Rittaud).

Le théorème dit *des nombres premiers*, un résultat difficile, peut se formuler intuitivement comme suit : si n est un entier très grand, les nombres premiers proches de n représentent une fraction $1/\ln n$ de la totalité des entiers proches de n. Par exemple, la densité de nombres premiers autour de 10^{10} est en gros double de la densité des nombres premiers autour de 10^{20}. Le théorème des nombres premiers est un résultat asymptotique : plus n est grand et plus la densité des nombres premiers proches de n tend vers $1/\ln n$. On aimerait connaître l'erreur typique, et la conjecture de Riemann est équivalente au fait que cette erreur est d'ordre de l'inverse de racine carrée de n. On pourrait penser que cette formulation concrète se prête mieux à démonstration que la conjecture sur la fonction Zeta, mais pour l'heure c'est l'approche abstraite qui est jugée comme la plus prometteuse.

Et les statistiques d'écarts ?

On pourrait essayer d'appliquer les idées précédentes sur la statistique des écarts aux nombres premiers, mais le fait qu'il soient justement entiers est un obstacle. En revanche, la famille des zéros critiques situés sur le droite critique D, forme un ensemble de points isolés et ordonnés. A l'aide d'ordinateurs on peut en calculer numériquement des millions et le résultat est que la statistique des écarts semble être exactement celle des écarts d'énergie des noyaux ou des matrices aléatoires correspondantes !

Au prix de nombreuses simplifications que les experts pourront juger outrancières, nous avons illustré deux statistiques d'écarts dans les lignes précédentes. La théorie des matrices aléatoires a permis d'en mettre en évidence un petit nombre d'autres qui semblent universelles. Comprendre leur ubiquité, et plus ambitieusement encore démontrer qu'en un sens elles sont les seules statistiques d'écarts possibles est un défi scientifique d'actualité. Ces questions sont vraiment à la frontière de la physique, des mathématiques voir de la biologie.

visualisation artistique
de la fonction Zeta de Riemann
Jean François Colonna

Une anecdote pour conclure.

En certains endroits d'Amérique latine, la statistique des écarts entre passages ressemble plus au cas des niveaux d'énergie des noyaux qu'à celui des poids des pommes d'un cageot, en particulier les bus ne se suivent jamais de près ; une explication est que dans ces endroits les bus sont la propriété des chauffeurs, qui sont donc rémunérés en proportion directe du nombre de passagers qu'ils transportent et n'ont aucun intérêt à passer juste après leur prédécesseur, induisant ainsi un phénomène de répulsion tout comme pour les niveaux d'énergie des noyaux.

Le théorème des quatre couleurs

Benjamin WERNER - INRIA

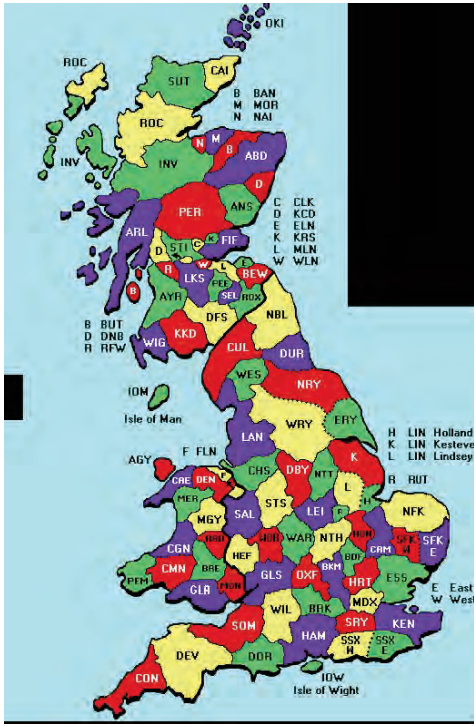
Le théorème des quatre couleurs doit sans doute sa renommée à la simplicité et au caractère concret de son énoncé : il peut être expliqué facilement à un non-mathématicien.

Etant donnée une carte, il est toujours possible de la colorier en assignant une couleur à chaque pays, sans que deux pays ayant une frontière commune n'aient la même couleur et ce avec quatre couleurs seulement !

Remarquons que "frontière commune" ne veut pas juste dire "se toucher en un point". Si ce n'était pas le cas, toute tarte coupée en plus de quatre parts constituerait un contre-exemple au théorème des quatre couleurs.

C'est un 1852 que remonte la première observation du phénomène. Francis Guthrie, cartographe britannique se rend compte qu'il arrive à colorier toutes les cartes qui lui sont présentées en quatre couleurs ; par exemple la carte des comtés britanniques. Ce qu'il n'arrive pas à déterminer, c'est si cette propriété est vraie pour toutes les cartes possibles et imaginables, ou si, au contraire, on sera capable de construire un jour une carte suffisamment compliquée pour que quatre couleurs ne suffisent pas.

S'assurer d'une propriété pour une famille *infinie* d'objets, comme la famille de toutes les cartes, est une question pour les mathématiciens. Par chance, Guthrie étudie alors les mathématiques et suit le cours du grand



logicien Augustus de Morgan. Il pose alors la question : *quatre couleurs suffisent - elles ?*

De Morgan ne trouve pas la réponse, mais prend rapidement conscience de l'intérêt de la question et la transmet à d'autres éminents mathématiciens. La renommée du problème va alors grandissante. La simplicité du problème contraste avec la difficulté pour y répondre. Cela a suffi, et suffit encore, à attiser la curiosité d'innombrables amateurs, qui ont tenté, et tentent encore, de proposer des *preuves* élémentaires.

Le théorème des quatre couleurs

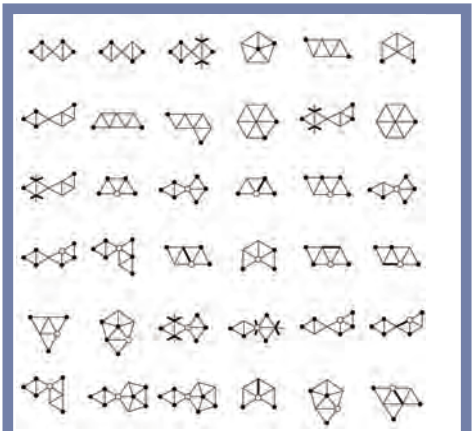
En 1879, Alfred Kempe propose une preuve qui convainc tout le monde, ou plutôt qui convainc tout le monde pendant un certain temps car, en 1890, Percy Heawood découvre une erreur dans l'argument de Kempke : ce dernier n'a en fait démontré que le théorème des cinq couleurs!

Pendant près d'un siècle, rares sont alors les mathématiciens qui n'ont pas passé au moins un peu de temps à essayer de résoudre ce mythique casse-tête. De fait la première preuve correcte est présentée en 1976. Mais paradoxalement, elle ne fait que renforcer le halo de mystère qui entoure le théorème des quatre couleurs. En effet, elle fait appel à des calculs si compliqués que ceux-ci ne peuvent être faits qu'à l'aide d'ordinateurs.

Il faut se rendre compte qu'en 1976 les ordinateurs sont encore incomparablement moins répandus qu'aujourd'hui. Ils coûtent également très chers ; la preuve construite par Kenneth Appel et Wolfgang Haken nécessite 1 200 heures de calculs des ordinateurs les plus puissants de l'époque. C'était un investissement important de la part de leur université.

Pourquoi le calcul ?

Pourquoi de si importants calculs ? En fait, la preuve reprend les idées développées par Kempe en 1879, mais à une plus grande échelle. D'abord, il faut considérer plus de cas : Appel et Haken identifient 1 476 petites cartes particulières appelées *configurations*. Ils vérifient que pour toute carte qui nécessiterait potentiellement plus de quatre couleurs, apparaît une de ces petites cartes. Il est bien sûr difficile de vérifier cela à la main, mais reste encore possible si suffisamment de personnes s'y mettent. C'est ensuite que les choses se corsent vraiment ; pour chacune de ces 1476 configurations, il faut vérifier qu'il est possible d'étendre un coloriage du reste de la carte à un coloriage de la configuration. Or cela est en général seulement possible après un certain nombre de *réarrangements* du coloriage du reste de la carte. C'est alors qu'il faut considérer les manières dont peuvent s'agencer les coloriages possibles sur la frontière de la configuration, c'est-à-dire pour une seule configuration jusqu'à 50 millions de cas !


Extrait des 633 configurations

En 1995, on a proposé une variante de la preuve de Appel et Haken où l'on ne distingue *que* 633 configurations. Les calculs restent, bien sûr, hors de portée si l'on ne dispose pas d'ordinateurs. Il faut d'ailleurs remarquer que c'est parce que les mathématiciens de 1995 disposaient de machines plus performantes qu'en 1976 qu'ils ont pu trouver une preuve (un peu) simplifiée : on ne prête qu'aux riches !

Un cas particulier ?

Aujourd'hui, les calculs nécessaires pour établir le théorème des quatre couleurs peuvent être achevés en une dizaine de minutes par un ordinateur personnel moderne. Il n'empêche que le théorème des quatre couleurs reste fascinant. D'une certaine façon, c'est le premier exemple d'une vérité mathématique qui ne nous est accessible qu'à travers l'utilisation d'une machine : l'ordinateur devient alors *l'instrument du mathématicien.*

Cette situation est-elle appelée à se reproduire ? On connaît maintenant d'autres théorèmes dont la preuve fait appel au calcul informatique. L'un des plus important est appelé la conjecture de Kepler. Là encore, l'énoncé est simple et explicable sans utiliser le jargon mathématique :

Lorsque je veux ranger des boules de même taille (par exemple des oranges ou des boules de pétanque), y a-t-il une meilleure manière de faire que celle que l'on voit sur les étals des marchés?

Même si l'on était, en général, convaincu qu'il n'y avait pas de meilleure manière d'agencer les boules, on n'arrivait pas à *démontrer* le résultat. Or si l'énoncé avait été *conjecturé* dès 1612 par Johannes Kepler, il a fallu attendre 1998 pour que Thomas Hales, de l'université de Pittsburgh présente une *preuve*. Or cette preuve, fait appel à la fois à des concepts mathématiques plus évolués que ceux sous-jacents à la preuve du théorème des quatre couleurs, mais aussi à des calculs informatiques encore plus complexes.

Dans tous ces nouveaux résultats, le

rapport à la vérité mathématique a fondamentalement changé. En effet, le mathématicien ne peut plus *comprendre pourquoi* un résultat comme le théorème des quatre couleurs est vrai. Il ne peut qu'utiliser un maximum de rigueur lors de l'écriture du programme et éventuellement reproduire l'expérience en faisant tourner des variantes du programme sur d'autres ordinateurs.

De fait, Hales a eu un certain mal pour convaincre la communauté mathématique de la correction de sa preuve. En particulier, il est difficile de s'assurer qu'un programme complexe est entièrement libre de *bug* ; le mieux étant finalement de laisser ce travail à l'ordinateur et à un autre programme !

Pour en savoir (un peu) plus :

http://www.inria.fr/actualites/2005/theoreme4couleurs.fr.html

http://www.lix.polytechnique.fr/Labo/Benjamin.Werner/publications.html

Les énigmes d'Archimède

Michel CRITON

Archimède (- 287 ; - 212) est un des plus grands savants de l'Antiquité. Mathématicien et physicien, il a laissé une oeuvre importante qui ne nous est que partiellement connue. A cette époque lointaine, on ne distinguait pas les mathématiques proprement dites des jeux mathématiques : les mathématiques étaient un jeu intellectuel et les jeux mathématiques un prétexte pour faire avancer la connaissance.

Ainsi, Archimède a proposé un problème antique, celui *des bœufs de Thrynacie* ou *boeufs du Soleil* à Eratosthène de Cyène, chef de file de l'Ecole d'Alexandrie. Les mathématiciens d'Alexandrie ne parvinrent pas à résoudre ce problème difficile dont la résolution conduit à un système de sept équations à huit inconnues et dont les plus petites solutions sont de l'ordre du million.

Archimède s'est aussi intéressé à un puzzle : le stomachion, au point de lui consacrer un de ses ouvrages dont voici la fabuleuse et rocambolesque aventure.

Le Stomachion est donc le livre qu'Archimède a consacré à l'étude de ce puzzle. On n'en connaissait que des fragments ; il fut longtemps considéré comme une oeuvre mineure, jusqu'à la découverte du palimpseste d'Archimède et à son déchiffrage qui en permet aujourd'hui une meilleure connaissance.

Pendant des siècles, on n'a connu du Stomachion que les citations qu'en font les auteurs romains Marius Victorinus, Atilius Fortunatianus et Ausonius (IV^{e} siècle de notre ère).

Ce n'est qu'à la fin du XIX^{e} siècle qu'on trouva des fragments du texte d'Archimède. Le premier fragment fut découvert dans un texte arabe par l'orientaliste H. Suter, qui en publia une traduction allemande en 1899.
Et commence alors l' aventure...

Le paléographe Papadopoulos Kerameus découvre, dans le monastère du Saint-Sépulcre de Jérusalem, un parchemin qui a été effacé pour être réutilisé comme livre de prières par des moines autour du XIII^{e} siècle. Sur ce document, appelé palimpseste, les textes et les figures mathématiques, mal effacés, transparaissent cependant sous les textes des prières et sont partiellement identifiables. Le parchemin contient trois livres d'Archimède : *Des corps flottants*, déjà connu, *Stomachion* et *De la méthode*, dont les textes n'étaient pas connus. Heiberg publiera une édition de ces fragments en 1913. Entre temps, le palimpseste avait disparu, acheté par des collectionneurs. Il ne réapparaîtra qu'en 1998 lors d'une vente chez Christie's où un acheteur américain anonyme l'acquerra pour 2 millions de dollars avant de le remettre à des experts scientifiques pour l'étudier et compléter

son déchiffrage qui est encore en cours, compliqué en raison de l'ajout de fausses images religieuses par des faussaires qui pensaient augmenter ainsi la valeur du manuscrit. Les pages du manuscrit original ont été pliées par le milieu et cousues pour obtenir un livre de format moitié du format original, ce qui explique que les textes réécrits par-dessus les textes originaux soient perpendiculaires à ces derniers.

Sur la photo, on distingue les deux textes

et des figures géométriques. Le palimpseste, qui a été confié au Walters Art Museum, est toujours à l'étude et son déchiffrage devrait durer jusqu'en 2008. L' université de Stanford a prêté son synchrotron, un accélérateur de particules qui permet de faire ressortir les textes effacés en faisant briller le fer contenu dans les résidus d'encre.

Les pièces du loculus d'Archimède

Le stomachion, appelé aussi Loculus (petite boîte) d'Archimède est un puzzle constitué d'un carré découpé en quatorze pièces. Il semble que le jeu ait existé avant Archimède, mais que celui-ci l'ait modifié afin que toutes les aires des morceaux soient entre elles dans un rapport commensurable (autrement dit rationnel).

Certains historiens considèrent même aujourd'hui qu'il ne s'agit pas d'une oeuvre mineure du mathématicien mais d'un premier traité de combinatoire, le puzzle n'étant qu'un prétexte à dénombrements.

Ce n'est qu'en 2003 qu'un spécialiste américain des puzzles, Bill Cutler, trouva toutes les solutions de l 'assemblage des pièces du puzzle d'Archimède en carré, à l'aide d'un programme informatique. Les solutions sont au nombre de 536, sans compter les rotations et les symétries.

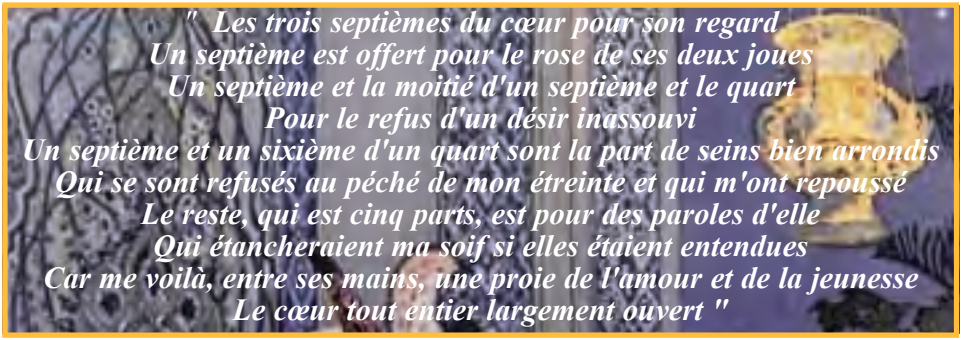
Pour en savoir (un peu) plus :

http://www.maa.org/editorial/mathgames/mathgames_11_17_03.html

Enigmes et jeux dans le monde arabe

du IX^e au XVI^e siècle

Marie José PESTEL



Ainsi les mathématiciens arabes, poètes à leur heure, versifiaient pour proposer des énigmes mathématiques.

Dans ce monde de lettrés et de riches princes, chacun avait à cœur de participer au débat scientifique et appréciait de se lancer des défis et énigmes sous forme ludique et même poétique.
Pour piquer la curiosité de ses lecteurs, Ibn al-Bannâ, mathématicien de Marrakech du XIV^e siècle titrait son ouvrage sur le calcul : *Le soulèvement du voile sur les formes des opérations du calcul* et presque 100 ans plus tard Qunfudh, son collègue de Constantine lui répondait en publiant un ouvrage intitulé *L'abaissement de la voilette sur les formes des opérations du calcul*.
Cependant aussi jolis soient-ils on ne saurait réduire les mathématiques arabes du IX^e au XVI^e siècle à quelques titres accrocheurs.
Utilisant avec éclat l'héritage géométrique grec et les apports des mathématiques indiennes, les mathématiciens arabes furent particulièrement novateurs en algèbre et en trigonométrie avec le développement de l'astronomie. Leur contribution dans le renouveau des mathématiques en Europe est ainsi capitale.

Bagdad (capitale de l'actuel Irak) sera le fief de la connaissance dès le règne du calife Al Mansour (seconde moitié du VII^e siècle). Il y fut créé de nombreuses écoles et bibliothèques. En 832, le calife Al Mamoun y fonde la maison de la Sagesse (Baït al Hikma).
Les plus grands mathématiciens arabes ont participé à cette diffusion ludique de la culture. Citons : Al Khwarizmi, Thabit Ben Q'ra, Abu Kamil, Al Battani, Abu Al Wafa, Al Kashi, Ibn Al Haytham (Al Hazen) et sans oublier le grand philosophe Ibn Abdallah ibn Sina, dit Avicenne.
Parfois ces mathématiciens ont repris des textes anciens venus de Chine ou d'Inde en les actualisant. Par exemple, ce problème de volatiles : *Un homme va au marché avec 25 dirhams en*

poche et il achète 25 volatiles : des oies à 5 dirhams l'unité, des poulets à 4 dirhams l'unité et des étourneaux à 1 dirham la dizaine. Combien a-t-il acheté de volatiles de chaque espèce ?

Dans de nombreux cas, ces problèmes étaient des occasions de construire et résoudre des systèmes d'équations dont le nombre des solutions pouvait varier de la dizaine au millier.

On voit aussi apparaître des problèmes liés à la vie quotidienne comme le transport ou le négoce, d'autres textes semblent avoir été produits dans le cadre des activités multiformes de la cité islamique. On peut citer certains problèmes combinatoires comme celui qui consiste à déterminer le nombre maximal de prières que le musulman doit faire … sans en oublier

Les problèmes qui illustrent certaines méthodes de raisonnement sont aussi fort intéressants. Quand un peu de magie se mêle aux mathématiques l'attrait est encore plus grand. Tel est le cas des *nombres pensés* mais aussi de ce délicieux texte pour retrouver le doigt qui porte le bague …

Glisse cette bague sur l'un de tes doigts sans que je le voie. Regarde ta main et compte trois pour chaque doigt avant la bague , deux pour chaque doigt après la bague et quatre pour le doigt de la bague. Si tu me dis ce que tu trouves en ajoutant ces nombres, je te dirai sur quel doigt tu as glissé la bague ….

Abou I-Wafa', grand scientifique du X^{e} siècle, dans son ouvrage intitulé *Livre sur ce qui est nécessaire à l'artisan en*

constructions géométriques nous suggère non seulement de nous interroger sur les méthodes mais d'entrer dans le débat mathématiques pures ou mathématiques appliquées. Son magnifique découpage de trois carrés identiques pour refaire un seul carré privilégie les méthodes basées sur les propriétés géométriques de base, comme la symétrie, aux méthodes basées sur des calculs.

Les mathématiciens arabes auront donc joué un rôle essentiel dans la transmission de la science indienne, chinoise et grecque. Cette transmission va se faire parfois sans grande modification mais souvent avec des apports fondamentaux tant sur la forme , en tenant compte du contexte culturel, que sur les contenus et les méthodes.

Leurs influences dans les grands centres scientifiques de l'Europe médiévale est considérable.

Pour en savoir (un peu) plus :

Ahmed Djebbar - La Recherche mai juin 2000 -
Les récréations dans les mathématiques du monde musulman

Leonardo Pisano Fibonacci

Abdelkader NECER

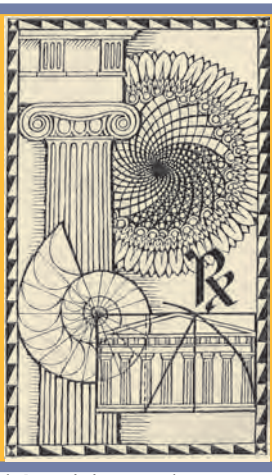
Léonard de Pise est *le plus grand mathématicien de son temps et du Moyen-Age* (E. Kantorowicz, 1988). Son œuvre *est de celles qui honorent l'humanité et appartiennent au patrimoine scientifique de celle-ci* (Paul Ver Eecke, 1952). Au regard de son génie et de sa production en mathématiques, nous connaissons très peu de choses sur la vie de Léonard de Pise dit Fibonacci (qui serait la contraction de Filiorm Bonacci *de la famille de Bonacci* ou bien de Filius Bonacci *Fils de Bonacci*). Nous savons qu'il est né à Pise vers 1170 (probablement entre 1170 et 1180). Son père, qui exerce la fonction de *scribe officiel à la douane de Béjaïa en Algérie, en mission pour les commerçants de Pise, le fit venir auprès de lui alors qu'il était enfant*.

Etant donné les fonctions de son père, nous pouvons supposer, sans risque d'erreur, que le jeune Léonard a appris à lire, écrire (en latin) et évidemment à compter. C'est dans la ville de Béjaïa -une ville portuaire, à l'est d'Alger, très prospère alors- que Léonard de Pise, s'initie à l'utilisation de l'abaque. Il découvre les chiffres indo-arabes et leur utilisation quotidienne dans les calculs des marchands pour les besoins du commerce et du négoce. Comme il le dit lui-même dans l'introduction à son livre *Liber Abaci* (le livre de l'abaque ou du calcul), son initiation au calcul, fut un enseignement admirable (*mirabili magisterio*). Dans cette même introduction, nous apprenons qu'il perfectionne sa formation grâce à ses voyages en Syrie, Egypte, Grèce, Sicile et en Provence. Le *Liber Abaci* fût publié en 1202 et réédité en 1228. Dans la première partie de ce livre, Fibonacci introduit les chiffres indo-arabes (0, 1, 2, 3, 4, 5, 6, 7, 8, 9), montre comment tout nombre peut être construit à partir de ces chiffres (et décrit ainsi le système de numération de position) et, avec un très grand souci pédagogique, donne des exemples pour décrire les opérations élémentaires sur ces nombres, y compris les fractions. Les exemples donnés dans ce livre, sont souvent puisés dans la vie de tous les jours des marchands : *De l'achat et de la vente de choses vénales et de questions semblables* (chapitre 8) ou encore *Du recours aux monnaies, des règles qui les concernent, de leur usage* (Chapitre 11). Rappelons que c'est dans ce même livre que figure l'un des problèmes les plus connus de Fibonacci : *Quelqu'un plaça un couple de lapins dans un lieu clos de murs de tous côtés pour savoir combien de bêtes seraient engendrées par ce couple en une seule année. La nature de ces animaux veut qu'un couple engendre un autre couple chaque mois. Les petits sont, à leur tour, capables de se reproduire le second mois qui suit leur naissance*. La résolution de ce problème célèbre fait intervenir la suite de nombres, 1, 2, 3, 5, 8, 13, ... , suite que E. Lucas (1842-1891) propose d'appeler *série de Fibonacci* et dont les rapports de deux termes consécutifs approchent le non moins célèbre *Nombre d'Or*.

Leonardo Pisano Fibonacci

La rencontre de Fibonacci avec des savants de la cour de l'empereur Frédéric II vers 1225, lui permit de montrer ses talents de mathématicien, notamment en résolvant des problèmes difficiles. Certains lui ont été proposés par Jean de Palerme, philosophe à la cour, lors d'un tournoi organisé par l'empereur. Deux de ces problèmes figurent dans le livre Flos (Fleur de solutions de certaines questions relatives au nombre et à la géométrie) publié par Fibonacci lui même. A cette époque, Fibonacci est au sommet de ses capacités comme le montre la publication de l'une de ses productions majeures en arithmétique et théorie des nombres, à savoir le livre intitulé *Liber quadratum* ou livre des nombres carrés. Dans cet excellent ouvrage dédié à Frédéric II, Fibonacci résout des équations, dites diophantiennes (les solutions sont des entiers ou des fractions) du premier, second ou troisième degré. On constate que Fibonacci sait, par exemple, que la somme des premiers nombres entiers impairs est un carré ou encore que le produit de deux sommes de deux carrés est une somme de deux carrés. Le dernier livre rédigé par Léonard de Pise, concerne la géométrie. Il s'intitule *Practica Geomtriae* et constitue une réelle avancée par rapport aux travaux des géomètres latins qui l'ont précédé.

Signalons également que Fibonacci est considéré, par plusieurs historiens contemporains des sciences, comme un continuateur des mathématiques dites arabes. Il s'est en effet beaucoup inspiré en les reprenant (en partie) des travaux des



mathématiciens tels que El-Khawarizmi (780-850) ou Abou Kamil (vers 850-930) en les prolongeant et les approfondissant de manière très originale. Décédé à Pise vers 1250, nous savons, d'après un document qui date de 1240, que Léonard de Pise bénéficiait avant sa mort d'une pension pour services rendus à la communauté. La première pension d'état pour faire de la recherche !

Pour en savoir (un peu) plus

[1] *D. Aissani et D. Valerian,* Mathématiques, commerce et société à Béjaïa (Bugia) au moment du séjour de Léonard Fibonacci (XIIe-XIIIe siècles), Bolletino di Storia delle Scienze Matematiche- Vol. XXIII, fasc. 2, 2003

[2] *J. Gies et F. Gies,* Leonardo of Pisa and the new mathematics of the middle ages, Thomas Y. Crowell Company, New York, 1969

[3] *J.P.-Levet,* Léonard de Pise. Des chiffres Hindous aux Racines Cubiques, Cahiers d'Histoire des Mathématiques et d'Epistémologie, IREM de Poitiers, juin 1997

[4] *J.P.-Levet,* Léonard de Pise. Divisions et proportions, Perles et Animaux, Cahiers d'Histoire des Mathématiques et d'Epistémologie, IREM de Poitiers, décembre 1997

[5] *E. Lucas* Recherches sur plusieurs ouvrages de Léonard de Pise et sur diverses questions d'arithmétique supérieure, extrait du Bullettino di bibliografia di storia delle scienze matematiche e fisiche, Tomo X. Rome, Marzo, Aprile et Maggio1877

[6] *R. Rashed,* Fibonacci e la matematica araba, Estratto dal volume frederico II e le scienze, Sellrio editore Palermo

[7] *R. Rashed,* Fibonacci et le prolongement latin des mathématiques arabes, Bolletino di Storia delle Scienze Matematiche- Vol. XXIII, fasc. 2 (2003)

Bachet de Méziriac

Michel CRITON

Claude Gaspar Bachet, sieur de Méziriac, a été le premier à publier en français un livre exclusivement consacré aux récréations mathématiques. Il s'agit des *Problèmes plaisants et délectables qui se font par les nombres.* La première édition de ce livre remonte à 1612 et de très nombreuses éditions ont suivi jusqu'à nos jours. Bachet n'est pas seulement un mathématicien. Il est d'abord un grammairien, spécialiste des langues anciennes : latin, hébreu, grec. Il a aussi écrit des poésies et des chansons.


DIOPHANTI
ALEXANDRINI
ARITHMETICORVM
LIBRI SEX.
LVTETIAE, PARISIORVM,
M. DC. XXI

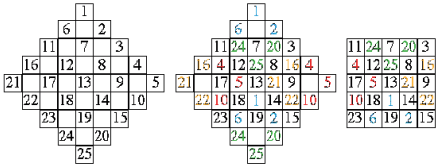
Sa qualité d'expert en langues anciennes l'amena à traduire du grec au latin les *Arithmétiques* de Diophante. Il ne se contentera d'ailleurs pas de les traduire, mais il y ajoutera de nombreux commentaires. C'est dans la marge d'un exemplaire de cette traduction que Fermat notera l'énoncé de son fameux grand théorème.

Le livre de Bachet contient une cinquantaine de problèmes qui sont tous de grands classiques des récréations mathématiques. Plusieurs de ces problèmes consistent à deviner un ou plusieurs nombres pensés en demandant au joueur d'effectuer certaines opérations et en lui posant une ou des questions. Des variantes de ce type de problème sont exposées à partir des cartes d'un jeu de cartes qu'un joueur doit choisir mentalement. Bachet consacre plusieurs de ses récréations aux carrés magiques. On trouve également des problèmes de transvasement, de traversées, de poids et de monnaie. Tous ces problèmes n'étaient pas originaux lorsque Bachet les a publiés. Beaucoup d'entre eux trouvent leur origine chez les mathématiciens arabes et certains, comme les carrés magiques, sont encore plus anciens. La nouveauté des *Problèmes plaisants et délectables qui se font par les nombres* est que les récréations mathématiques y constituent le coeur de l'ouvrage, alors qu' habituellement elles étaient reléguées en annexe de matières réputées plus sérieuses. L'autre intérêt est que Bachet explique de façon détaillée ses propres méthodes de résolution qui sont souvent originales, contrairement aux énoncés des problèmes eux-mêmes.

Habituellement, des problèmes amusants viennent illustrer de sérieux théorèmes. Chez Bachet, on part de problèmes récréatifs et on va chercher des mathématiques utiles pour les résoudre.

L'exemple des carrés magiques

Une règle de construction des carrés magiques d'ordre impair porte le nom de *méthode de Bachet*, celui-ci étant le premier à l'avoir exposée. Cette méthode, applicable à tous les carrés d'ordre impair, est illustrée par la figure ci-après.



Le théorème de Bachet-Bezout

Le théorème suivant : *Deux entiers relatifs a et b sont premiers entre eux si et seulement si il existe deux entiers u et v tels que au + bv = 1*, est connu sous le nom de théorème de Bezout.

Dans une note des *Problèmes plaisants et délectables qui se font par les nombres,* Bachet expose une méthode de résolution de l'équation indéterminée du premier degré à deux inconnues. Cet exposé laisse apparaître que Bachet connaissait le théorème appelé plus tard théorème de Bezout.

Voici la méthode de Bachet appliquée sur un exemple. *Trouver le premier multiple de 211 qui surpasse de 10 un multiple de 1007.*
En fait, il s'agit de trouver la plus petite solution de l'équation 211x = 1007y + 10.

Bachet procède de la façon suivante.

Il divise 1007 par 211.

	4	1	3	2
1007	211	163	48	19
163	48	19	10	

Le quotient est 4 et le reste 163.
Il divise 211 par 163.
Le quotient est 1 et le reste 48.
Il divise 163 par 48.
Le quotient est 3 et le reste 19.
Il divise 48 par 19.
Le quotient est 2 et le reste 10.
On a alors l'égalité 1 x 48 = 2 x 19 + 10.


Claude Gaspar Bachet de Méziriac

Bachet recopie ensuite les quotients dans l'ordre sur une ligne (en rouge).

4	1	3	2		
43	9	7	2	1	0

Sur une deuxième ligne, à droite du dernier quotient, on écrit le nombre 1.
Puis on calcule :
1 x 2 + 0 = 2.
On écrit 2 à gauche du 1.
2 x 3 + 1 = 7.
On écrit 7 à gauche du 2.
7 x1 + 2 = 9.
On écrit 9 à gauche du 7.
9 x 4 + 7 = 43.
On écrit 43 à gauche du 9.

La solution du problème est
43 x *211* = *9* x *1007* + *10.*

Claude-Gaspar Bachet de Méziriac peut être considéré comme le type même de l'honnête homme et de l'humaniste du XVIIe siècle. Il pratiquait aussi bien la poésie que les langues anciennes ou les mathématiques, mais c'est essentiellement par ses Problèmes Plaisants et Délectables et les méthodes de résolution qu'il y propose que nous le connaissons aujourd'hui.

Leonhard Euler

Marie José PESTEL

Leonhard Euler naissait, il y a trois cents ans, à Bâle en Suisse. Il allait devenir un des plus grands mathématiciens de tous les temps.
Il faut dire que de nombreuses fées mathématiques s'étaient penchées sur son berceau. Leonhard est le fils aîné d'un pasteur Paul Euler, lui même élève et ami des Bernoulli, grande famille de physiciens et de mathématiciens. C'est donc son père qui l'initia aux mathématiques avant de l'envoyer à la faculté de Bâle où il fit de brillantes études. Son chemin croisa encore la famille Bernoulli puisqu'il reçut des cours particuliers de Jean Bernoulli avant de rejoindre à Saint Pétersbourg, dans la nouvelle Académie des Sciences fondée par la Grande Catherine, Daniel et Nicolas Bernoulli…

Euler fut probablement le premier mathématicien européen. Il a traversé le siècle des lumières, rencontrant les plus grands , Voltaire entre autres, à la cour de Frédéric II de Prusse puis auprès de Catherine de Russie. Il travailla non seulement en mathématiques mais aussi en physique, en astronomie, …
Son œuvre en mathématique est immense et on ne compte plus les formules, constantes, théorèmes, résultats auxquels on a donné son nom. En mathématiques il s'est passionné pour les domaines les plus variés sans jamais négliger la composante ludique.

Evoquons tout d'abord, le problème des *ponts de Koenigsberg* et écoutons Euler nous le proposer :

A Koenigsberg, en Poméranie, il y une île appelée Kneiphof ; le fleuve qui l'entoure se divise en deux bras sur lesquels sont jetés les sept ponts a, b, c, d, e, f, g. Cela étant posé, peut-on arranger son parcours de telle sorte que l'on passe sur chaque pont, et que l'on ne puisse y passer qu'un seule fois ?
Dans la suite du mémoire, où Euler présente et généralise le problème, il expose des méthodes pour chercher la solution. Le monde mathématique s'accorde à voir dans ce mémoire tous les ingrédients de la future théorie des graphes. En fait ce mémoire ne traite que de l'impossibilité de trouver le fameux chemin et c'est dans une note, annexe de ce mémoire, que l'on trouve la théorie de la possibilité.

Avec des méthodes de raisonnement aussi puissantes, il n'est pas étonnant de voir Euler se passionner pour le jeu d'Echec et des problèmes posés bien avant lui (on en trouve trace dans un manuscrit de 1512 de R.Guarini di Forti) : *Est-il possible de parcourir avec un cavalier toutes les cases d'un échiquier, sans parvenir jamais deux fois à la même, et en commençant par une case donnée ?*
Euler devait déjà avoir une solide réputation de théoricien du jeu d'échec puisqu'il semble qu'un champion international d'échec d'alors, François André Philidor, présent à la cour de Frédérique II de Prusse, ait tenté vainement de le rencontrer.

Leonhard Euler

Du parcours du cavalier sur l'échiquier aux carrés magiques, les méthodes mathématiques mises au point par Leonhard tracent des chemins et donnent des méthodes de raisonnement fort intéressantes .

Les problèmes posés par les carrés magiques remontent à la nuit des temps mais ils ont toujours fasciné et il n'est guère étonnant de constater que Léonhard Euler va explorer les pistes de recherche qu'ils offrent.

En 1782 Leonhard Euler imagine le problème mathématique suivant :
On considère six régiments différents, chaque régiment possède six officiers de grades distincts. On se demande maintenant comment placer les 36 officiers dans une grille de 6 x 6, à raison d'un officier par case, de telle manière que sur chaque ligne et chaque colonne contiennent tous les grades et tous les régiments.

Il s'agit d'un carré gréco-latin d'ordre 6 (un carré latin pour les régiments, un carré latin pour les grades). Euler avait pressenti à l'époque, que ce problème était impossible : *Or, après toutes les peines qu'on s'est données pour résoudre ce problème, on a été obligé de reconnaître qu'un tel arrangement est absolument impossible, quoiqu'on ne puisse en donner de démonstration rigoureuse*, écrit-il. Il avait même conjecturé que ce problème des carrés gréco latins serait impossible pour tous les ordres *impairement pairs*, c'est à dire du type 4n+2. Or Euler se trompait !!! La non-existence de carrés gréco-latins d'**ordre six** a été définitivement confir-

mée en 1901 par le mathématicien français Gaston Tarry qui fit l'énumération exhaustive de tous les arrangements possibles de symboles. Cinquante-huit ans plus tard, en 1959, avec l'aide d'ordinateurs, deux mathématiciens américains, Bose et Shrikhande trouvèrent des contre-exemples à la conjecture d'Euler. La même année, Parker trouva un contre-exemple d'**ordre dix**. En 1960, Parker, Bose et Shrikhande démontrèrent que la conjecture d'Euler était fausse pour tous les entiers supérieurs ou égale à dix. Donc en fait le seul carré gréco latin qui n 'existe pas, si on met à part celui d'ordre deux, évidemment impossible, est celui d'ordre six, celui des officiers !

Pour célébrer le tricentenaire de la naissance d'Euler, le CIJM propose, aux visiteurs du salon de la culture et des jeux mathématiques, mieux qu' un carré gréco latin d'ordre 9, un double sudoku sur neuf chiffres 1, 2, ….9 et neuf fonds de calligraphie différents dessinés par le calligraphe Laurent Pflughaupt et ses élèves.

De quoi fêter dignement Leonhard Euler !

Sam Loyd et Henry Ernest Dudeney

Michel CRITON

L'un est américain et l'autre anglais. Le premier était l'aîné du second d'une quinzaine d'années. Tous deux ont abandonné leurs études assez vite, mais ont continué à étudier les mathématiques en autodidactes et tous deux ont pratiqué avec passion le jeu d'échecs. C'est pourquoi on rapproche souvent ces deux grands créateurs d'énigmes que furent Loyd et Dudeney. Une certaine rivalité a existé entre eux, mais on sait aussi qu'ils s'appréciaient mutuellement.

Sam Loyd (1841-1911)

Samuel Loyd est né à Philadelphie en 1841. Joueur d'échecs depuis son plus jeune âge, il publie son premier problème d'échecs à l'âge de 14 ans. Le jeu d'échecs et la composition de problèmes l'occupent à tel point qu'il finit par quitter les bancs de l'école à l'âge de dix-sept ans. Contraint de gagner sa vie, il se lance dans le journalisme en proposant à divers journaux des rubliques et des problèmes d'échecs.

Bien qu'étant un joueur d'échecs moyen, Sam Loyd a composé des centaines de problèmes d'échecs, certains avec une bonne dose d'humour et de fantaisie.

Un exemple en est ce problème où il demande de trouver une méthode permettant de mettre mat un roi isolé au milieu d'un échiquer à l'aide de deux tours et d'un cavalier, ... sans préciser les dimensions de l'échiquier qui comportait seulement trois rangées de quatre cases !

A partir de 1870, Sam Loyd se désintéresse des échecs et se lance dans l'invention de casse-tête mathématiques ; il les diffuse dans les journaux et magazines ainsi que par la publicité. Sam Loyd a fait breveter plusieurs de ses trouvailles comme par exemple le jeu *Teddy et les lions* où, selon la position du disque central, on peut voir sept chasseurs et sept lions ou bien six chasseurs et huit lions.

Mais le jeu le plus célèbre popularisé par Loyd est sans conteste le taquin commercialisé en 1873.

Ce casse-tête est constitué de quinze petits carrés pouvant coulisser dans un cadre de 4 cases sur 4, la case vide permettant les mouvements.

Les carrés étaient disposés dans l'ordre naturel, à l'exception du 14 et du 15 qui étaient intervertis. Sam Loyd offrait 1000 dollars à qui trouverait une suite de mouvements permettant de remettre le 14 et le 15 à leur place. Sam Loyd savait que le problème était impossible pour une raison de parité, l'ensemble de toutes les configurations possibles étant partagé en configurations *paires* et en configurations *impaires*, le passage d'un type à l'autre étant impossible sans démonter le jeu.

Sam Loyd et Henry Ernest Dudeney

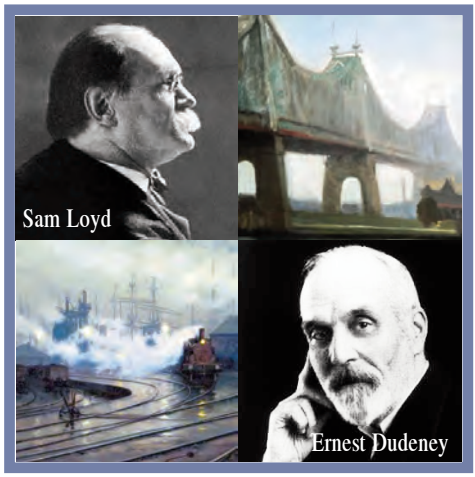
Après la mort de son père, Samuel Loyd Junior publiera *Cyclopedia of puzzles*, recueil de plus de 5000 casse-tête créés par son père.

Henry Ernest Dudeney (1857-1930)

Plus jeune que Loyd de seize ans, Henri Ernest Dudeney nourrissait la même passion que son aîné pour le jeu d'échecs et pour les énigmes à ressort mathématique. Il commença très tôt à proposer ses créations à plusieurs magazines anglais. A partir de 1890, Dudeney collabora avec Sam Loyd pour le magazine anglais Tit-Bits. Par la suite, Dudeney et Sam Loyd décidèrent d'échanger leurs énigmes qu'ils proposaient à des journaux différents, ce qui explique que l'on retrouve parfois des énigmes identiques chez les deux auteurs sans savoir qui en est le véritable créateur. Mais Dudeney finit par s'offusquer du fait que Sam Loyd ne le citait pas toujours comme étant l'inventeur de certains jeux dans les livres qu'il publait.

Si Sam Loyd possédait d'incontestables dons de mise en scène des énigmes qu'il créait, Dudeney était davantage mathématicien.

Une invention de Dudeney est un puzzle où un triangle équilatéral formé de quatre morceaux articulés entre eux peut se réarranger en un carré.



Dudeney présenta ce découpage de son invention à la Royal Society de Londres en 1905.

Parmi les énigmes créées par Dudeney, on peut citer le premier cryptarithme : S E N D + M O R E = M O N E Y, message adressé à son éditeur et opération codée où chaque lettre remplace un chiffre (deux lettres différentes remplaçant toujours deux chiffres différents et deux chiffres différents étant toujours remplacés par deux lettres différentes.

Sam Loyd et Henry Ernest Dudeney, chacun à sa manière, préfigurent les grands vulgarisateurs modernes.

Pour en savoir (un peu) plus :

Les recueils de problèmes publiés par Dudeney sont :
The canterbury Puzzles (1907),
Amusements in Mathematics (1917),
Modern Puzzles (1926)
et Puzzles and Curious Problems (1931), publié après sa mort.

Le texte intégral de Cyclopedia of puzzles peut être téléchargé au format pdf sur :
http://www.mathpuzzle.com/downloads/

Solution du cryptarithme : 9 567 + 1 085 = 10 652

Edouard Lucas

Michel CRITON

Edouard Lucas (1842 - 1891) est un grand mathématicien français de la fin du 19e siècle. Son apport aux mathématiques se situe principalement en théorie des nombres, notamment dans l'étude des nombres premiers. Un test de primalité porte le nom de *test de Lucas-Lehmer*.

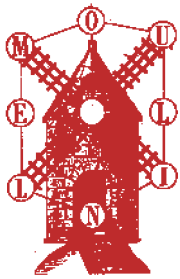
Mais Lucas est aussi un pionnier de la popularisation des mathématiques par le jeu, avec les quatre tomes de ses *Récréations Mathématiques* et son *Arithmétique Amusante*, qui constituent une véritable encyclopédie des récréations mathématiques.

Edouard Lucas pensait que chaque notion mathématique pouvait être présentée aux jeunes et au grand public sous la forme d'un jeu ou d'une énigme : *si ces pages inspirent à quelques jeunes intelligences le goût du raisonnement et le désir des jouissances abstraites, alors je serai satisfait*.

Seuls les deux premiers tomes des Récréations de Lucas ont paru de son vivant. Décédé prématurément en 1891 à la suite d'une infection, Edouard Lucas ne verra pas la publication des deux derniers tomes, réalisée par ses amis à partir des notes qu'il a laissées. Il en est de même pour L'Arithmétique Amusante, éditée à partir d'un projet de livre retrouvé chez Lucas.

Les jeux étudiés par Lucas sont pour la plupart des jeux connus, pour lesquels il existe des raisonnements susceptibles de conduire à une résolution complète du jeu. On peut citer les labyrinthes, les taquins, le jeu de caméléon, le baguenaudier.

Le baguenaudier est un jeu constitué d'anneaux enfilés sur une navette, ces anneaux étant enchevêtrés à l'aide de fils de fer, et qu'il s'agit de désenchevêtrer. Le jeu a probablement été inventé en Chine, et il est cité par Jérôme Cardan en 1550.



Le Moulin Rouge est un jeu commercialisé à l'époque de Lucas. On place dix jetons portant les dix lettres L E M O U L I N au hasard, puis on doit les remettre dans l'ordre en déplaçant les pions. La case centrale communique avec les cases extérieures par les ailes du moulin.

Edouard Lucas

Mais le plus célèbre des jeux popularisés par Edouard Lucas reste la tour de Hanoï dont il est par ailleurs l'inventeur. Ce jeu était conçu pour expliquer la numération binaire. Voici la présentation qu'en fait Lucas :

" *Un de nos amis, le professeur N. Claus (de Siam) mandarin du collège de Li-Sou-Stian, a publié, à la fin de l'année dernière, un jeu inédit qu'il a appelé la Tour d'Hanoï, véritable casse-tête annamite qu'il n'a pas rapporté du Tonkin, quoi qu'en dise le prospectus. Cette tour se compose d'étages superposés et décroissants, en nombre variable, représentés par huit pions en bois percés à leur centre, enfilés dans l'un des trois clous fixés sur une tablette. Le jeu consiste à déplacer la tour en enfilant les pions sur un des deux autres clous et en ne déplaçant qu'un seul étage à la fois, mais avec défense expresse de poser un étage sur un étage plus petit. Le jeu est toujours possible et demande deux fois plus de temps chaque fois que l'on ajoute un étage à la tour ... .*

Le nom prétendu de l'inventeur du jeu, N. Claus de Siam, mandarin de Li-Sou-Stian est tout simplement l'anagramme de "Lucas d'Amiens, professeur au lycée Saint Louis". Lucas aimait agrémenter ses récréations de pointes d'humour. Selon Lucas, N. Claus de Siam préparait la publication des écrits du mandarin Fer-Fer Tam-Tam (Lucas avait fondé le projet de publier les oeuvres de Fermat). Il rapporte également la légende d'une tour de Hanoï situé à Bénarès et comportant 64 disques.

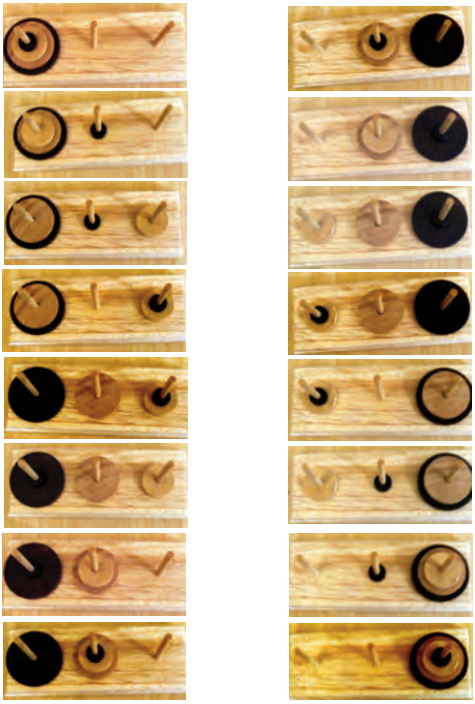
illustration de la tour de Hanoï dans les Récréations Mathématiques.

Lorsque les 2^{64}-1 c'est à dire :

18 446 744 073 709 551 615

mouvements nécessaires au transport des 64 disques auront été effectués, *les brahmes tomberont et ce sera la fin du monde !*

Résolution d'une tour de Hanoï de 4 disques.
Cette résolution nécessite 2^4 - 1 soit 15 mouvements.



Martin Gardner

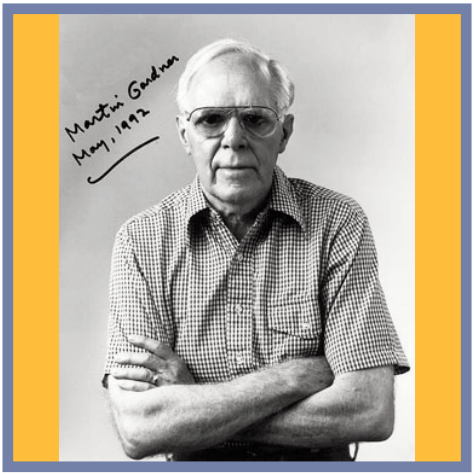
Jean-Jacques DUPAS

- Elève Gardner, qu'est-ce que je vois là ? Un morpion ! Je rêve ! J'aimerais qu'à l'avenir vous ne fassiez plus que des mathématiques pendant les cours de mathématiques ! Le jeune Martin Gardner essayait de trouver une stratégie gagnante. Ce qui veut dire qu'il faisait des mathématiques. Ce sujet aurait sans doute passionné tous ses camarades et l'enseignant avait là une belle occasion de parler de combinatoire, de probabilité, de symétrie… Les jeux peuvent être une formidable introduction aux mathématiques.

Martin Gardner est né le 21 octobre 1914 à Tulsa, Oklahoma. Il suivit les cours de l'université de Chicago où il obtint une licence de philosophie, mais pas sa maîtrise. Sa prodigieuse culture générale est le résultat de ses innombrables lectures et de ses infatigables recherches en bibliothèques. Martin Gardner adulte sera le champion des jeux mathématiques et des mathématiques amusantes. Il a su populariser ce genre et lui donner ses lettres de noblesse. Il faut dire qu'à l'époque de sa jeunesse les livres sur le sujet étaient rares, il y avait bien quelques années auparavant des précurseurs comme le génial Lucas, Loyd, Dudeney.... Mais en 1956, pour se procurer le classique *Essais et Récréations Mathématiques*, de W.W.Rouse Ball, il fallait écrire à H.S.M Coxeter. La popularité de Martin Gardner est essentiellement due, au départ, à sa rubrique *Mathematical Games* du *Scientific American* qui commença en 1956 et s'arrêta en 1982 mais qui fut publiée par *Pour la Science*, à partir de 1977 dans son édition française . En 1983, Gardner fut désigné écrivain scientifique de l'année en 1983 par l' Institut Américain de Physique. Dès le début, sa rubrique fut un immense succès. La première présentait les flexagones, bande de papier repliée dont les faces apparaissent suivant des cycles. En observant ces bandelettes de papier obtenues par découpage, Feynman, montra que les mathématiques qui se cachent derrière elles, sont très profondes. Ce premier article eut tellement de succès qu'il n'était pas rare de croiser, à cette époque, aux Etats-Unis, un passant manipulant un flexagone.

Dans le courrier reçu du monde entier, Martin Gardner trouvait la substance de ses articles. Il popularisera de nombreux sujets. On ne peut que faire un choix difficile pour en citer quelques uns. Les Polyominos sont des figures obtenues en collant des carrés par leurs côtés. Les cubes de Soma lui avaient été confiés par le danois Piet Hein, inventeur aussi du jeu de Hex, jeu que Wendelin Werner évoque pour illustrer ses recherches. Le célèbre Jeu de la vie de John Conway est un jeu de simulation qui devint si populaire qu'à l'époque de sa publication, les rares ordinateurs furent paralysés pendant des semaines, occupés par ce jeu. Les pavages de Roger Penrose, pavage du plan apériodique à partir de deux pièces de base ont trouvé des applications inattendues en cristallographie. N'oublions pas

que c'est aussi dans le monde de l'art, que Martin Gardner a fait connaître au grand public l'œuvre de Maurits Escher. Dans un domaine plus austère, il fut autorisé, par les auteurs eux même, à dévoiler le système de codage révolutionnaire, RSA, à clef publique. Ses rubriques lui permettront également d'introduire des personnages imaginaires pittoresques comme le Docteur Irving Joshua Matrix, numérologiste. Les rencontres avec le docteur Matrix et sa jolie fille Yva Toshiyori seront l'occasion pour Martin Gardner de dénoncer, avec beaucoup d'humour, la numérologie et ses mé-thodes. Une grande partie de la vie de Martin Gardner sera consacrée à la lutte contre les pseudo sciences et le paranormal. Pourtant depuis son plus jeune âge, Martin était passionné de magie ce qui n'a rien d'étonnant car n'avez-vous pas remarqué que les gens dont l'illusion est la profession sont extrêmement rationalistes et sont souvent les mieux placés pour dénoncer les charlatans de tous poils ? C'est en employant les méthodes et ressorts psychologiques des illusionnistes que Martin Gardner a donné à ses textes ce charme si particulier. Les textes de Martin Gardner ne se résument pas à sa rubrique, même si celle-ci l'a rendu célèbre. Il a également publié, plus de 70 ouvrages sur les mathématiques, la philosophie, la littérature, la lutte contre le paranormal. Nous avons donc affaire à un auteur à la fois prolixe et éclectique. Toute sa vie durant, il a posé un nombre incroyable d'énigmes et a eu à cœur de nous faire partager leurs solutions. Il a



essayé de faire entrer les mathématiques récréatives dans l'enseignement et il a bien mérité ainsi d'être honoré sur le Salon de la culture et des jeux mathématiques.

Pour en savoir (un peu) plus :

Martin Gardner, Les Jeux mathématiques, Pour la science, Octobre 1998.
Martin Gardner, Jeux Mathématiques du Scientific American, adapté par mon ami Yves Roussel, ADCS, Amiens, 1996

Un premier avril mémorable

Dans sa rubrique d'avril 1975, Martin Gardner relatait, non sans malice, 6 découvertes sensationnelles qui avaient échappées aux média. Cela allait de l'invention par Léonard de Vinci de la chasse d'eau à un résultat extraordinaire de la théorie des nombres en passant par une carte compliquée où il était nécessaire d' utiliser 5 couleurs pour en effectuer le coloriage, confirmant ainsi la soi-disante intuition de H.S.M Coxeter alors que dans le même temps le théorème des 4 couleurs venait d'être démontré ! Martin Gardner savait que son dessin était fallacieux. Cet article de légende lui valut un torrent de courrier. Beaucoup de lecteurs prirent les articles au premier degré, trompé par les références prestigieuses et le style de Martin Gardner! Comme quoi, le premier avril il faut se méfier même des journaux scientifiques et garder son esprit critique, mais n'est-ce pas là l'essence même de la science!

Ose la recherche avec le CNRS

Tu veux en savoir plus sur un sujet que tu as étudié ?
Au CNRS, cela peut se faire de mille façons : en invitant un chercheur à parler pendant un de tes cours, en assistant à une expérience scientifique… et que dirais-tu de visiter un labo ? C'est possible !

Le CNRS te permettra de parler avec ceux "qui font la science" et de leur poser toutes tes questions. Ta curiosité bouillonne ? Une rencontre avec un chercheur n'est pas suffisante ? Le CNRS coordonne des clubs dans toute la France. Il y en a forcément un près de chez toi !

Tu peux aussi rencontrer les chercheurs lors de manifestations scientifiques et mettre un zeste de CNRS dans tes projets. Parles-en à ton prof, et réfléchissons ensemble aux moyens de rencontrer les acteurs de la science. Il n'y a que l'embarras du choix, nous avons un mot à dire sur… presque tout !

Dans les **"Clubs CNRS Jeunes"** tu rencontreras les scientifiques de ta région, tu découvriras leurs recherches, et pourquoi pas celles du monde entier ? Faire partie d'un club, c'est retrouver des amis curieux pour **vivre les instants privilégiés de l'aventure scientifique.**

www2.cnrs.fr/jeunes

CNRS
CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE

www.cnrs.fr *www2.cnrs.fr/jeunes*

Fondée en 1872,
la Société Mathématique de France
est riche de ses deux mille adhérents et adhérentes.

Reconnue d'utilité publique,
la SMF a pour seul objectif le développement des mathématiques en France. Elle veille à maintenir l'excellence et le dynamisme des mathématiques françaises, à améliorer leur ouverture et à leur diversité. Elle s'attache à créer des liens avec les industries et les services, à développer le dialogue avec les autres sciences et à encourager la diffusion des oeuvres culturelles de qualité concernant les mathématiques. Elle développe les échanges culturels et scientifiques internationaux, défend la diversité linguistique, travaille à mettre en place l'espace scientifique européen et promeut la solidarité avec les pays du sud.

La SMF travaille à encourager un enseignement de qualité à tous les niveaux. Participer à la formation des nouvelles générations, partager avec elles notre amour des mathématiques, c'est préparer l'avenir de notre communauté scientifique.

La SMF publie des mathématiques depuis sa création. Ses publications sont ouvertes à la communauté mathématique internationale. La qualité des textes choisis est garante de leur pérennité et les revues et ouvrages de la SMF constituent des références mondialement connues encore citées des dizaines d'années après leur parution.

La SMF diffuse des informations utiles pour l'insertion des jeunes mathématiciens et mathématiciennes à la vie professionnelle.Elle attache beaucoup d'importance à leur participation à ses activités. http://smf.emath.fr

Le CIJM association créée en 1993 par des professeurs de mathématiques désireux de proposer une autre réflexion sur leur discipline fédère trente deux compétitions intéressant ainsi plusieurs millions de personnes tant en France qu' à l'étranger.

Le CIJM édite *Panoramath*, annales corrigées de ses compétitions et crée des jeux élaborés à partir de ces textes pour permettre à tous de connaître la joie de la recherche mathématique ! Il propose des expositions avec animations pour mettre la culture mathématique à la portée du plus grand nombre.

Le CIJM dynamise son site internet, pour développer à travers le monde des liens forts entre ses associations membres, ses nombreux partenaires et son public.

Le CIJM organise une grande fête des mathématiques,
le salon de la culture et des jeux mathématiques,
début juin à Paris, lieu de rencontre de nombreux pays et espace privilégié de vulgarisation et de promotion de la culture mathématique.

www.cijm.org

Grâce au soutien
du CNRS, du CEA, de l'INRIA et de la SMF

Sous la direction de
Marie José Pestel
Comité International des Jeux Mathématiques

avec l'aide de
Stéphane Jaffard
Professeur Université Paris 12

Cette brochure a réuni les signatures de

Hervé Lehning
Elisabeth Busser
Benoît Rittaud
Wendelin Werner
Erwann le Pennec et Dominique Picard
Jean-Christophe Yoccoz
Etienne Ghys
Cédric Villani
Alice Guionnet
Laurent Demonet
Michel Bauer et Philippe Di Francesco
Benjamin Werner
Michel Criton
Marie José Pestel
Abdelkader Necer
Jean-Jacques Dupas

Qu'ils soient ici tous remerciés pour avoir eu, au milieu de leur emploi du temps surchargé, la patience et la gentillesse de s'être livrés au jeu de l'écriture.

Illustrations de couverture
Elsa Godet - www.sciencegraphique.com

Réalisation
Patrick Arrivetz
CIJM
8 rue Bouilloux-Lafont 75015 Paris
tél :01 40 37 08 95 ***www.cijm.org***

Impression FP Impression 01 39 72 21 72

Les énigmes d'hier à aujourd'hui

Découvertes mathématiques d'aujourd'hui

2000 ans d'énigmes mathématiques


culture et jeux
mathématiques
C
I
J
M


ministère
éducation
nationale
enseignement
supérieur
recherche
ministère délégué
à l'enseignement supérieur
et à la recherche


CNRS
CENTRE NATIONAL
DE LA RECHERCHE
SCIENTIFIQUE


cea


INRIA


îledeFrance


Société
Mathématique
de France
SMF