# PEUT-ON DOUTER DES MATHÉMATIQUES ?

Causerie à l'ECP, le 14 mai 2012

Julianne UNTERBERGER

## I. QUELQUES CITATIONS de mathématiciens, philosophes et écrivains

- Le mathématicien est un oiselier capturant dans une volière des oiseaux aux brillantes couleurs. ***Platon*** (*427-347* av. J.-C.)
- Les Mathématiques sont considérées comme le langage avec lequel sont écrites les lois de la Nature. ***Galilée***
- Les schémas du mathématicien, comme ceux du peintre ou du poète, doivent être beaux ; les idées, comme les couleurs ou les mots, doivent s'assembler de façon harmonieuse. La beauté est le premier test : il n'y a pas de place durable dans le monde pour les mathématiques laides".

  *Godfrey Harold* ***Hardy*** (*1877-1947*)
- A quoi servent les mathématiques ? " C'est pour l'honneur de l'esprit humain ».

  *Carl Gustav Jakob* ***Jacobi*** *(1804-1851)*
- Un mathématicien n'est pas une machine à déduire, mais un être humain.

  *Paul* ***Halmos*** *(1916-2006)*
- Je veux connaître la vraie pensée de Dieu, le reste n'est que détail.

  *Albert* ***Einstein*** *(1879-1955)*
- Ma religion, c'est la certitude profondément ressentie qu'il existe une Raison Supérieure qui s'ouvre à nous dans le monde accessible à la connaissance. *Albert* ***Einstein*** *(1879-1955)*
- Les lois de la nature sont mathématiques. Dieu est géomètre. *Ian* ***Stewart*** *(1945- )*
- Il n'y a pas au monde d'étude qui mette toutes les facultés de l'esprit plus harmonieusement en action que les mathématiques… Le mathématicien vit longtemps et reste jeune; les ailes de son âme ne fléchissent pas de bonne heure et ses pores ne sont pas obstrués par la poussière qui s'élève des grandes routes poudreuses de la vie vulgaire.

  *James Joseph* ***Sylvester*** (*1814-1897*)
- Dieu a créé les nombres entiers ; le reste est l'œuvre de l'homme.

  *Leopold* ***Kronecker*** *(1823-1891)*
- La mathématique possède cette particularité de n'être pas comprise par les non-mathématiciens.

  *André* ***Weil*** *(1906–1998)*
- Les Mathématiques sont froides, sans plaisir, sans passion. *André* ***Weil*** *(1906–1998)*
- "Mathématiques : dessèchent le cœur."

  Dictionnaire de *Gustave* ***Flaubert*** *(1821 –1880*
- La Science est bien la fille des mathématiques. *Henri* ***Bergson*** *(1859 –1941)*
- La science ne pense pas. *Martin* ***Heidegger***

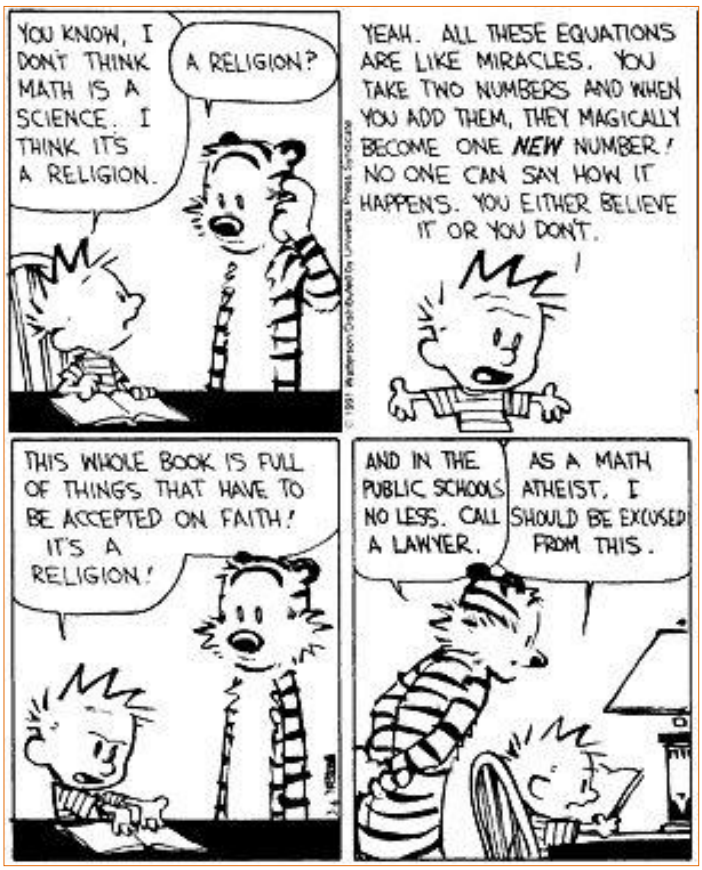
**Victor HUGO (1802 –1885) Quelques vers**

J'étais alors en proie à la mathématique.
Temps sombre ! Enfant ému du frisson poétique
On me livrait tout vif aux chiffres, noirs bourreaux
On me faisait de force ingurgiter l'algèbre
On me tordait depuis les ailes jusqu'au bec
Sur l'affreux chevalet des x et des y
Hélas, on me fourrait sous les os maxillaires
Le théorème orné de tous ses corollaires.

# MATHS À L'ECOLE

## Une BD

http://laffingboi.blogspot.com/2007/08/math-is-religion.html
Posted by Laughing Boy at 8/21/2007




**Traduction**

**-- Tu sais, je ne pense que les maths soient une science, je pense que c'est une religion.**

**-- Une religion ?**

**-- Ouais ! Toutes ces équations sont des miracles. Tu prends deux nombres et quand tu les additionnes, ils deviennent miraculeusement un nouveau nombre ! Personne ne peut dire comment cela arrive, ou tu le crois ou tu ne le crois pas !**
**Tout le livre est plein de choses qu'on doit *croire sans discuter*. C'est une religion !**

**En tant que *mathématicien athéiste*, je devrais être dispensé de ça.**

**-- Et en plus, cela se passe dans les écoles publiques ? Appelle un avocat.**

---.


---.

***EXEMPLE DE MAUVAISE UTILISATION DES MATHS AU LYCEE***

## BAC GENERAL 1998 - Épreuve de mathématiques

**EXERCICE 1**

A 16 ans, Julie pesait 50 kg. Depuis, son poids a augmenté de 2% chaque année par rapport à celui de l'année précédente.

1) Combien pesait-elle à 17 ans ? A 18 ans ?
2) Actuellement elle a 21 ans. Quel est son poids ?
3) Elle décide de faire un régime et de perdre désormais chaque année, pendant 5 ans, 2% du poids qu'elle avait l'année précédente. Quel sera, si elle tient son engagement, son poids à 26 ans ?

**EXERCICE 2**

1) Le 1/1/1998 Pierre a placé 20 000F au taux de 4% l'an, avec intérêts capitalisés chaque année. ... Calculer la somme dont Pierre disposera le 1/1/2005.
2) Même genre d'exercice avec Éric à la place de Pierre et des intérêts simples à la place des intérêts capitalisés

# II. INTRODUCTION

On ne peut définir les mathématiques que par des négations : les définitions *positives* que l'on peut donner sont toutes fausses parce qu'elles sont nécessairement réductives. Elles ne sont pas qu'une technique pour faire des calculs ou pour résoudre des problèmes, elles ne sont pas non plus, comme on l'entend dire souvent, qu'un "langage" et elles ne se réduisent pas non plus à la logique. Elles ne sont même pas une activité particulièrement rationnelle et consciente.
On peut comparer ce métier à celui de « musicien » : comme le mot *musicien* peut désigner un amateur de musique, un professeur de musique, un interprète, un compositeur,..., le mot mathématicien peut désigner un enseignant, un utilisateur des mathématiques, un chercheur,...
Dans ce texte, le mot mathématicien désigne un *chercheur* (créateur) en mathématiques (cela ne l'empêche pas d'enseigner, etc.).

## Des questions

- Qui peut douter des mathématiques?
- De quoi peut-on douter en mathématiques?
- Peut-on douter de l'utilité des mathématiques dans la vie courante?
- L'unique but des mathématiques est-il leurs applications aux autres sciences ?
- Les Mathématiques existent-elles en dehors de l'esprit des mathématiciens et donc indépendamment de nous?
- Le mathématicien est-il un virtuose des calculs et réciproquement ?
- Y a-t-il encore des résultats à trouver en mathématiques ou le mathématicien se borne-t-il à enseigner le legs des siècles passés ?
- Un mathématicien est-il un enseignant, un créateur ou un explorateur ?
- Peut-on douter des résultats mathématiques publiés?



## Des réponses

- Les mathématiciens ne doutent pas des mathématiques : les mathématiques sont ce que pratiquent les mathématiciens. Ils peuvent par contre douter de certaines démonstrations et aussi douter de certaines « énoncés » (mathématiques) non encore démontrés.
- Par contre, parmi les non-mathématiciens, on peut distinguer plusieurs attitudes :
  L'unique but des mathématiques est leurs applications aux autres sciences : ainsi pensaient Diderot, D'Alembert et Buffon, par exemple. Pour Diderot, les mathématiques avaient fait leur temps : elles n'ajoutaient rien à l'expérience et ne faisaient qu'interposer un voile entre la nature et le peuple au lieu de rendre la philosophie populaire.
- On ne peut douter de l'utilité des mathématiques dans la vie courante. Il suffit de consulter, par exemple, «la brochure « *L'explosion des mathématiques* » éditée en 2003 par les deux Sociétés mathématiques de Frances (disponible sur internet) pour s'en convaincre.
  Bernard Le Bouyer (ou Le Bovier) de **Fontenelle** écrivait en 1699 : «On appelle d'ordinaire inutiles les choses que l'on ne comprend pas. C'est une espèce de vengeance, et comme généralement les mathématiques et la physique ne sont pas comprises, elles sont déclarées inutiles.»

  Mais Depuis 2500 ans les mathématiques sont utilisées pour décrire certains phénomènes naturels le plus ancien et le plus génial étant Archimède. Depuis le dix-septième siècle, avec les travaux de Galilée, les mathématiques sont considérées comme le langage avec lequel sont écrites les lois de la Nature. Historiquement, l'un des premiers modèles fut celui des épicycles de Ptolémée qui décrivait le mouvement du soleil et les rétrogradations des planètes alors connues.
  Les mathématiques sont devenues, à côté du microscope et du télescope, un «instrument d'observation» révolutionnaire qui nous révèle chaque jour de nouvelles et mystérieuses facettes de notre Univers sans parler des résultats obtenus, en particulier dans le cadre de la Mécanique Quantique et de la Relativité générale.

Mais ces succès ne font que rendre plus mystérieuses la nature profonde des mathématiques et la cause de leur «redoutable efficacité». Que sont donc les (nos ?) mathématiques ? Soit elles ne sont «que» le fruit de notre esprit, soit elles existent indépendamment de nous. Formulé différemment : le mathématicien est-il un créateur (c'est-à-dire celui qui tire du néant) ou bien un explorateur (celui qui parcourt en observant) ?

Pour le mathématicien contemporain **Donal O'SHEA**, il est inconcevable qu'il n'y ait pas quelque part en dehors de notre petit monde d'autres intelligences, peut-être très différentes de la nôtre avec lesquelles on pourra un jour communiquer sur des objets ou théorèmes mathématiques. Un contact avec d'hypothétiques intelligences extra-terrestres (en supposant qu'un dialogue équitable est possible) lèverait certainement un petit coin du voile : dans *Contact*, roman de science-fiction publie en 1985, **Carl Sagan** faisait implicitement l'hypothèse platonicienne, en donnant, en particulier, la vedette aux nombres premiers et au nombre $\pi$....
Mais peut-être la réponse est-elle que le mathématicien est à la fois créateur et explorateur : certaines structures, probablement parmi les plus élémentaires, existeraient indépendamment de nous (les nombres entiers ordinaux et cardinaux, par exemple) alors que d'autres seraient notre œuvre (un peu comme il existe dans l'Univers un certain nombre de molécules naturelles et que nos chimistes en ont créé de nouvelles à partir des éléments de base que sont les atomes).
De plus, **chaque génération de mathématiciens** réinterprète et redéfinit le cadre des mathématiques des générations antérieures. **Apprendre les mathématiques, c'est les réinventer**.

Pour **Michel BROUÉ** (mathématicien contemporain), les mathématiques ont un aspect dual : d'une part un **langage**, extrêmement précis et codé, qui permet son application aux autres sciences ; d'autre part une **science** comme les autres, qui a néanmoins pour spécificité de questionner des objets un peu particuliers, puisqu'il s'agit **d'objets du monde des idées**. "Rien n'est plus fécond, tous les mathématiciens le savent, que ces obscures analogies, ces troubles reflets d'une théorie à l'autre, ces furtives caresses, ces brouilleries inexplicables ; rien aussi ne donne plus de plaisir au chercheur. Un jour vient où l'illusion se dissipe ; le pressentiment se change en certitude ; les théories jumelles révèlent leur source commune avant de disparaître ; comme l'enseigne la Gita, on atteint à la connaissance et à l'indifférence en même temps. La métaphysique est devenue mathématique, prête à former la matière d'un traité dont la beauté froide ne saurait plus nous émouvoir. "



ω @ ∞ ℵ ω @ ∞ ℵ ω @ ∞ ℵ ω @ ∞

Dans ce qui suit, nous donnons un bref aperçu des idées relatives à cinq thèmes mathématiques : la plupart des développements donnés ont été largement inspirés soit d'articles lus sur internet soit des livres cités dans la bibliographie):

☺ **LA GEOMETRIE** : les Éléments d'Euclide et les géométries non euclidiennes

☺ **LES INFINIS MATHEMATIQUES** : les travaux de Georg Cantor

☹ **LES NOMBRES PREMIERS** : l'hypothèse de Riemann et la cryptographie

⌘ **LE THÉORÈME DES QUATRE COULEURS :** colorier une carte **...**

** **LE THEOREME DE FERMAT-WILES**


**MODE D'EMPLOI : LES PARTIES PUREMENT MATHÉMATIQUES PEUVENT ÊTRE SAUTÉES !**

Ω @ ∞ ℵ ω @ ∞ ℵ ω @ ∞ ℵ ω @ ∞

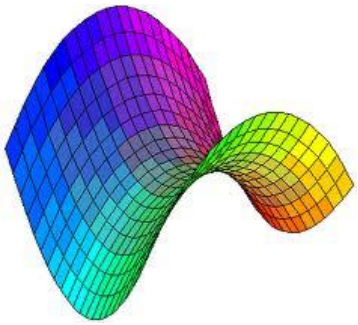
# LA GEOMETRIE

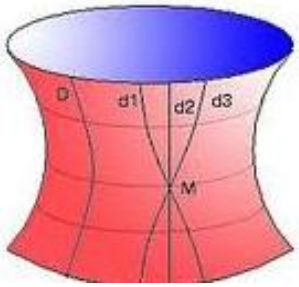
******.**********.**********.**********.**********.**********.******

## L'AXIOME D'EUCLIDE, OU CINQUIÈME POSTULAT D'EUCLIDE (réf. WIKIPEDIA)

L'axiome d'Euclide, ou cinquième postulat d'Euclide, est dû au savant grec Euclide (né vers -325, mort vers -265 à Alexandrie). C'est un axiome relatif à la géométrie du plan.
La nécessité de cet axiome a constitué la question la plus lancinante de toute l'histoire de la géométrie, et il a fallu plus de deux millénaires de débats ininterrompus pour que la communauté scientifique reconnaisse unanimement l'impossibilité de le réduire au statut de simple théorème.

L'énoncé original est exprimé dans le Livre I des Éléments d'Euclide sous la forme suivante:
«Si une droite tombant sur deux droites fait les 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 »
En langage moderne, cela pourrait donner:
«Si une droite coupe deux autres droites en déterminant deux angles internes dont la somme soit différente de deux angles droits, alors les deux droites se coupent dans le demi-plan pour lequel la somme est inférieure à deux angles droits»
ce qui est équivalent à l'énoncé bien connu, dit **POSTULAT DES PARALLÈLES :**
«Par un point donné, on peut mener une et une seule parallèle à une droite donnée».
Cette forme de l'axiome d'Euclide est due au mathématicien Antique Proclus. Elle est connue sous le nom de postulat des parallèles.






**Au XIXe siècle**, avec les recherches des grands mathématiciens Lobatchevski, Bolyai, Gauss, Riemann, Beltrami, Klein et Poincaré, on a pu trouver d'autres géométries possibles et non-contradictoires en conservant les axiomes de la géométrie Euclidienne sauf le postulat des parallèles; ces nouvelles géométries sont appelées non euclidiennes. L'histoire de cette découverte est un épisode fascinant de l'histoire de la géométrie.

On trouve deux manières différentes de pratiquer la géométrie sans l'axiome des parallèles.

1. Dans la première, la somme des angles d'un triangle est supérieure à 180°. On l'appelle (géométrie elliptique ou sphérique).
2. Dans l'autre, elle est inférieure à 180°. C'est la géométrie hyperbolique ou géométrie de Lobatchevski. Par exemple, en modifiant le cinquième axiome ainsi : «Par un point extérieur à une droite, on peut faire passer une infinité de droites parallèles à cette droite, et toutes différentes», on obtient la géométrie hyperbolique.

Dans les géométries non euclidiennes, le théorème de Pythagore n'est plus applicable. La proposition «Il existe des droites parallèles» vraie en géométrie euclidienne, est aussi vraie en géométrie hyperbolique mais fausse en géométrie sphérique.

Le commentaire qui suit est extrait du *Grigori Perelman face à la conjecture de Poincaré* de Donal O'SHEA. Pouvait-on déduire le postulat des parallèles des autres postulats de la géométrie euclidienne ou non ? Ou y avait-il, peut-être, quelque chose de plus évident à prendre comme axiome ? Des générations de mathématiciens furent obsédées par ces questions. De 1607 à 1880,

plus d'un millier de livres et de mémoires furent consacrés à ce 5ème postulat. Aucune proposition de démonstration ne résista à un examen soigné.
Il a fallu attendre l'après période de Lumières avec le vent qu'elles faisaient souffler, au début du XIXe siècle, pour résoudre ce problème : 3 mathématiciens y ont contribué en allant bien au-delà de ce cas particulier : ils devaient finalement clarifier le rôle du 5ème postulat et les richesses qu'il recelait.
Ce sont Johann Carl Friedrich GAUSS (1777-1855), le mathématicien le plus célèbre du début du XIXe et l'un des plus grands mathématiciens de tous les temps, Nikolaï Ivanovitch LOBATCHEVSKI (1792-1856) et János BOLYAI (1802-1860)
Au fil des ans, l'intérêt pour le 5ème postulat gagna la philosophie et la presse populaire. C'est pourquoi Gauss était méfiant et ne souhaitait pas publier ses résultats sur ce postulat dans le cas sphérique : ils auraient fait sensation et il ne voulait ni la publicité ni le tracas. Il nourrissait également de sains soupçons quant aux philosophes : « *quand un philosophe dit quelque chose de vrai, c'est une chose triviale. Quand un philosophe dit quelque chose de non trivial, c'est faux.* »
Bolyai y travailla en 1820 et ses carnets de note montrent qu'il avait commencé à développer ce que nous connaissons sous le nom de géométrie hyperbolique. En 1823, il écrivit à son père qu'il était en train de créer « un autre, un nouveau monde à partir de rien... ». Il semble avoir terminé en 1824. Mais il n'eut pas la reconnaissance souhaitée, Gauss s'y étant opposé. Il mourut en 1856 suite à une série d'attaques cérébrales.
Quant à Lobatchevski, il publia ses résultats sur les géométries non euclidiennes en 1829. Mais il rencontra des déboires car son article fut rejeté par le plus grand mathématicien russe de l'époque Mikhaïl Vasilevitch Ostrogradski, et ce qu'il publia par ailleurs passa complètement inaperçu. Ses dernières années furent gâchées par plusieurs soucis familiaux, sans compter son isolement dans la recherche qu'il poursuivait sans se faire reconnaître.

En conclusion, même en 1850, peu de monde reconnaissait qu'il pouvait exister des géométries dans lesquelles le 5ème postulat ne tenait pas. Si Gauss avait parlé, les choses auraient été différentes. Il a créé ou fait progresser plusieurs domaines des mathématiques et de l'astronomie jusqu'à sa mort à Göttingen en 1855, sans avoir publié quoi que ce soit sur le 5ème postulat.

Mais en temps et en heure, leurs résultats entreraient dans le courant principal des mathématiques.
Ces autres géométries n'étaient pas seulement des curiosités logiques, des anomalies nées de l'éventuelle incapacité des 4 premiers axiomes à capturer convenablement la réalité. Ces autres géométries étaient tout aussi réelles et tout aussi valables que la géométrie plane usuelle. Le changement radical de vision qui devait tout clarifier et initier notre compréhension moderne fut exposé en 1854 dans la soutenance d'habilitation d'un étudiant timide mais brillant de Gauss, Bernhard RIEMANN. Cette soutenance et une autre travail publié dans sa courte existence, furent l'un des plus grands moments dans l'histoire des sciences, et elle est essentielle pour notre compréhension du travail de Henri POINCARE et de toute la géométrie et la topologie modernes.
En conclusion : Les travaux de Poincaré, à leur tour, sont devenus le terreau fertile sur lequel ont fleuri la majeure partie des mathématiques du 20ème siècle. Quatre des problèmes du millénaire (prix CLAY) sont directement liés à des domaines dans lesquels il faut un pionnier. Ce n'est que récemment que nous avons commencé à pleinement saisir ce qu'il entr'aperçut au tournant du XXe.

## CONJECTURE d'Henri POINCARE (1904)

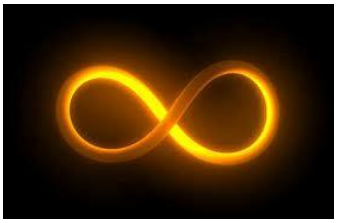
En voici l'énoncé, même s'il est incompréhensible pour les non-mathématiciens :

**Toute variété tridimensionnelle compacte sur laquelle tout chemin fermé peut être contracté en un point est homéomorphe à la sphère tridimensionnelle.**

Cette conjecture de Poincaré a été désignée comme l'un des 7 problèmes du millénaire en l'année 2000 par l'Institut CLAY qui a offert un prix de 1 million de dollars pour sa résolution. Elle a été démontrée par Grigori PERELMAN en 2003. Mais non seulement Perelman a diffusé sa première preuve sur internet en la mettant en ligne sur www.arXiv.org, le serveur internet de prépublication qui est devenu le lieu d'échange standard pour les nombreux domaines de la physique, des mathématiques et de l'informatique (elle n'a pas été soumise à un Journal mathématique comme le

voulait la tradition) mais encore il a refusé le prix CLAY et la médaille Fiels (2006) ainsi que toute interview avec des journalistes. C'est un génie solitaire qui vit avec son père à Saint-Pétersbourg.
Nous vivons dans l'ère la plus productive mathématiquement de l'histoire humaine. Les mathématiques sont **l'œuvre d'individus**. Mais **leurs concepts et leurs théorèmes n'appartiennent à aucune personne en particulier, à aucune ethnie, aucune religion, aucun groupe politique. Ils nous appartiennent à tous**. La connaissance mathématique se construit sur l'œuvre de ceux qui nous ont précédés. Les mathématiques nous rappellent à quel point nous dépendons des autres, à la fois de l'intuition, et de l'imagination de ceux qui nous ont précédés, et de ceux qui maintiennent les institutions sociales et culturelles, les écoles et les universités qui transmettent les idées de leur temps. En levant les yeux vers le ciel nocturne, vers les lointaines étoiles, les galaxies, il est inconcevable pour moi (Donal O'SHEA) qu'il n'y ait pas quelque part la dehors d'autres intelligences, peut-être très différentes de la nôtre avec lesquelles on pourra un jour communiquer sur des objets ou théorèmes mathématiques.

## LES INFINIS



La nature de l'infini a été un sujet de controverses depuis toujours :
♦Dans l'Antiquité : avec Zénon d'Élée et son paradoxe sur la notion d'infini (la tortue d'Achille précède Achille d'une distance de plus en plus petite ! Mais alors, il faut passer par une infinité de points en un temps fini.)
♦La mécanique de Newton résulte du calcul infinitésimal qu'il a inventé pour fonder la physique.
♦Au cours des XIXe et XXe siècles, sont apparus d'autres problèmes impliquant la notion d'infini au cours du développement de la théorie des ensembles (fondement de presque toutes les mathématiques contemporaines), et, en mathématiques, dans les apparitions de « singularités » et d' « horizons ».
♦En outre, l'infini a toujours eu des connotations théologiques qui ont joué un rôle dans le développement des concepts qu'on avait de l'infini (en mathématiques, en philosophie, en religion).



Tous ces courants de pensée ont convergé dans la vie et l'œuvre du mathématicien allemand **Georg CANTOR** (1845-1918). Il fut le fondateur de la théorie des ensembles, à partir de 1874. Avant lui, le concept d'ensemble était plutôt basique, et avait été utilisé implicitement depuis les débuts des mathématiques, depuis Aristote. Personne n'avait compris que cette théorie avait des éléments non implicites. Avant Cantor, il n'y avait en fait que les ensembles finis (qui sont aisés à comprendre) et les ensembles infinis (qui étaient plutôt sujets à discussion philosophique). En prouvant qu'il y a une infinité de tailles d'ensembles infinis, Cantor a établi que les bases de cette théorie étaient non-triviales. La théorie des ensembles joue ainsi le rôle d'une théorie fondatrice pour les mathématiques modernes, parce qu'elle interprète des propositions relatives à des objets mathématiques (par exemple, nombres et fonctions) provenant de toutes les disciplines des mathématiques (comme l'algèbre, l'analyse et la topologie) en une seule théorie, et fournit un ensemble standard d'axiomes pour les prouver ou les infirmer. Les concepts de base de celle-ci sont aujourd'hui utilisés dans toutes les disciplines des mathématiques. Mais il s'agit là vraiment d'un langage.

Certains, comme Galilée, avaient déjà remarqué qu'un ensemble infini, comme les carrés des nombres entiers, pouvait être mis en correspondance avec un ensemble infini le contenant strictement, en l'occurrence tous les entiers. Il y a d'une certaine façon « autant » de carrés de nombres entiers que de nombres entiers. Cantor est le premier à donner un sens précis à cette remarque, à l'aide de la notion de bijection qu'il introduit (sous un autre nom) à l'occasion, puis à la systématiser. Par exemple Cantor montre qu'il y a autant de nombres rationnels (ceux représentés

par des fractions) que de nombres entiers. Cantor va plus loin et découvre qu'il y a plusieurs infinis, au sens où ils ne peuvent être mis en correspondance entre eux par une bijection : il montre en 1874 que la droite réelle contient plus de nombres transcendants (« beaucoup plus ») que de nombres algébriques (solutions d'équations polynomiales à coefficients rationnels) ; il découvre aussi cette année-là, à sa grande surprise ("Je le vois, mais je ne le crois pas", écrit-il à Dedekind) que l'on peut mettre en bijection la droite et le plan (autrement dit, qu'il y a "autant" de points dans un petit segment que dans l'espace entier).

Entre 1879 et 1884, Cantor publia une série de six articles dans les Mathematische Annalen qui constituent une introduction à sa théorie des ensembles. En même temps grandissait une opposition croissante à ses idées, menée par Kronecker, qui n'admettait des concepts mathématiques que s'ils pouvaient être construits en un nombre fini d'étapes à partir des entiers, qu'il considérait comme seuls donnés intuitivement. Pour Kronecker, la hiérarchie des infinis de Cantor était inadmissible, et accepter le concept d'infini actuel ouvrirait la porte à des paradoxes qui mettraient en danger l'édifice mathématique tout entier.

**NOTATIONS et HYPOTHESE DU CONTINU**. En fin de sa vie, Cantor a adopté les notations suivantes : les **ω** pour les nombres ordinaux transfinis et la lettre **א** pour les nombres cardinaux transfinis. Tous les imprimeurs allemands possédaient les lettres hébraïques dans leurs polices de caractère !
Par exemple, le cardinal de l'ensemble des entiers est noté $\aleph_0$ alors que celui de l'ensemble des nombres réels est noté **א**. L'hypothèse du continu dit qu'il n'existe pas d'autre cardinal entre $\aleph_0$ et **א**. Mais, en 1963, le mathématicien Paul COHEN (université de Stanford) a utilisé les travaux du logicien Kurt Gödel pour démontrer que bien que l'hypothèse du continu soit compatible avec les axiomes d'une théorie standard des ensembles, elle en est également indépendante. On peut comparer avec le rôle similaire que joue le postulat d'Euclide en géométrie.



# LA SYMPHONIE DES NOMBRES PREMIERS

Référence : Article de Michel Alberganti paru dans l'édition du Monde du 14.10.2005
**« L'obsédante quête du Graal des mathématiques »**
Un thème qui "**brise l'image que la recherche en mathématiques serait achevée**".

Certains personnages se nomment Bernhard Riemann, Johann Peter Gustav Lejeune Dirichlet, Carl Friedrich Gauss, David Hilbert, André Weil, Andrew Wiles... . L'intrigue: une énigme sur laquelle planchent tous les mathématiciens de la planète depuis quelque 150 ans. Le décor : l'univers étrange des nombres premiers, dont l'unique originalité est de n'être divisibles que par eux-mêmes et par un. L'action: une succession d'espoirs, de fausses pistes, d'échecs, de défis et d'aventures. Le livre de Marcus du SAUTOY (500 pages), peut se dévorer ou se grignoter au hasard, tant il regorge de richesses scientifiques et humaines peu ou mal connues. "Je voulais écrire un roman", reconnaît l'auteur.

Une gageure. A priori, quoi de moins excitant qu'une suite de nombres ? Qui, hormis le club fermé des chercheurs en mathématiques, peut se passionner pour une série incohérente de chiffres ? Erreur. Les nombres premiers n'usurpent pas leur nom. Ils constituent "les pierres précieuses enchâssées dans l'immense étendue de l'univers infini des nombres", écrit Marcus du Sautoy. Les mathématiciens sont fascinés par ces "atomes de l'arithmétique", ce "don de la Nature". Leur découverte pourrait remonter à 6 500 ans avant J.-C., si l'on en croit les gravures de l'os d'Ishango, mis au jour en Afrique équatoriale en 1960. Pourtant, ils conservent, aujourd'hui encore, une bonne part de leur mystère.
La fascination qu'ils exercent depuis les découvertes réalisées par les Grecs s'explique simplement : "Tout nombre qui n'est pas premier peut être obtenu en multipliant les uns par les autres ces éléments fondamentaux. Pour le mathématicien, une liste de nombres premiers est comme le

tableau périodique des éléments chimiques, où les nombres 2, 3 et 5 correspondraient à l'hydrogène, à l'hélium et au lithium (...). La maîtrise de ces éléments lui permet d'espérer découvrir de nouvelles façons d'établir un cap pour parcourir la complexe grandeur du monde mathématique."

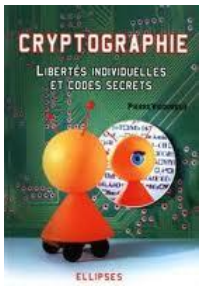
**LOI SECRÈTE et HYPOTHESE DE RIEMANN.** Euclide a démontré que les nombres premiers se poursuivent sans fin. Or la liste des nombres premiers contient une énigme majeure : existe-t-il une loi secrète régissant la façon dont ils s'égrènent sur la ligne infinie des nombres ? Au cours des siècles, les mathématiciens n'ont pas débusqué la règle qui, si elle existe, leur permettrait de calculer l'énième nombre premier ? L'un des héros de la quête de ce Graal des maths est sans conteste **Bernhard Riemann** (1826-1866). Riemann découvrit que si la suite des nombres premiers paraissait chaotique, les points sur sa « carte » (une autre interprétation du problème), eux, semblaient très ordonnés sur une même droite : mais était-ce vrai ou faux ? C'est ainsi que l'hypothèse de Riemann était née.
Enrico BOMBIERI en 1997 fit croire (ce n'était qu'un poisson d'avril !) que quelqu'un avait réussi à démontrer l'hypothèse de Riemann. La fausse nouvelle fit l'effet d'une bombe. Une telle démonstration aurait-elle des conséquences catastrophiques sur le monde fragile du commerce électronique ? Le cryptage des données sensibles utilise, en effet, les nombres premiers, et spécialement l'impossibilité de les calculer, pour protéger les transactions financières sur Internet. Découvrir l'ordre que Riemann laisse entrevoir remettrait-il en question les méthodes de chiffrement les plus utilisées, telles que le système RSA ?
Pour les initiés : Jacques Hadamard et Charles de la Vallée Poussin ont démontré le *théorème* dit *des nombres premiers* qui donne un ordre de grandeur du nombre de nombres premiers inférieurs à un très grand nombre.
Plus précisément, si N(q) désigne le nombre de nombres premiers inférieurs ou égaux à l'entier q, alors $N(q) \sim q / \log q$ : d'ailleurs, l'hypothèse de Riemann est équivalente à $N(q) = q/ \log q + O(q^{1/2} \log q)$.



**En fait, l'hypothèse de Riemann résiste encore aujourd'hui à la démonstration. Mais celui qui la démontrera gagnera le million de dollars offert par l'institut Clay de Cambridge.**

## LA CRYPTOGRAPHIE

### Exemple d'utilisation des nombres premiers et des courbes elliptiques



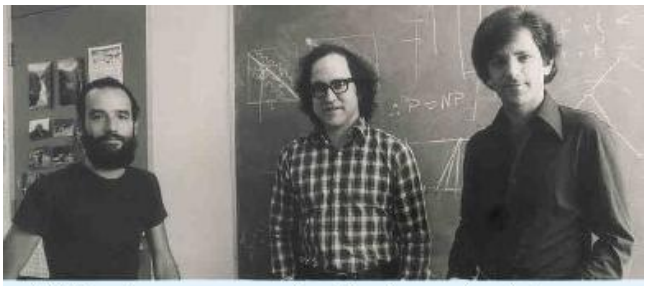

Le but de la cryptographie est de trouver de bonnes procédures de cryptage et de décryptage. Au cours du XXème siècle, ce domaine est passé de l'ère artisanale à l'ère scientifique. Dans le même temps, ses utilisateurs se sont multipliés : aux mondes militaire et diplomatique s'ajoutent désormais les mondes de la banque ou de la finance, celui du crime organisé, celui d'Internet et du commerce électronique, etc. Avec l'essor des télécommunications, la cryptographie est devenue un enjeu capital pour la société civile.

Pour communiquer à l'abri des indiscrets, il faut crypter les messages. Et pour inventer des méthodes de cryptage ou de décryptage, mieux vaut être mathématicien… Pour qu'un code soit difficile à déchiffrer, il devait être basé sur un problème mathématique dont la solution est difficile à calculer.

On distingue deux types de cryptages. Le premier, plus classique, est celui des méthodes à clef secrète.

L'autre type de cryptages est celui des codes à clef publique. Leur principe date de 1976. Dans ces méthodes, la connaissance de la clef servant au cryptage ne permet pas de déduire facilement la clef du décryptage. La clef de cryptage peut donc être publique, non secrète, tandis que la clef du décryptage n'est connue que du destinataire du message secret.

Le **RSA** (du nom des 3 mathématiciens qui l'ont trouvé : voir la photo) est encore le système cryptographique à clé publique le plus utilisé de nos jours. Son invention est due au hasard : au départ, Rivest, Shamir et Adleman voulaient prouver que tout système à clé publique possédait une faille. Cet algorithme servait encore en 2002 à protéger les codes nucléaires de l'armée américaine et russe.




Le principe de ce code est basé sur le **PETIT THÉORÈME DE FERMAT** qui dit que (pour les initiés) « si x est un nombre entier et si p est un nombre premier, alors $x^p - x$ est un multiple de p. »

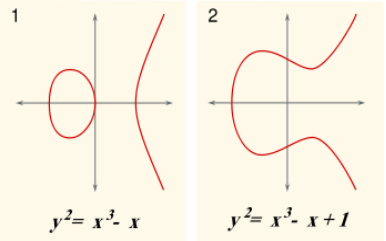
Rivest, informaticien au MIT depuis 1974, s'intéressait à l'interaction entre la théorie abstraite et les machines réelles. Il commença par puiser dans la masse de problèmes que les ordinateurs mettraient selon lui longtemps à résoudre (complexité calculatoire). Au MIT, se trouvaient près de lui deux mathématiciens, Leonard Adleman et Adi Shamir (israélien de passage) avec qui il discutait sans arrêt du problème. C'est ainsi qu'ils s'inspirèrent des idées de la théorie des nombres. « Un soir, alors que tous les trois avaient été invités chez un étudiant pour célébrer la première nuit de Pessah, l'illumination leur vint. Adleman ne boit pas, mais il se souvient que Rivest descendait un verre après l'autre du vin du seder. Il rentra chez lui vers minuit. Peu après, le téléphone sonna: c'était Rivest. « J'ai une autre idée... ». C'était la bonne, cette fois. » (cf *La symphonie des nombres premiers* de Marcus du Sautoy, p.349).

Mais au début des années 1980, ce genre de projet n'intéressait pas les entreprises commerciales. Les gens n'avaient pas encore d'ordinateur chez eux ! Donc pas de brevet commercial en vue! Seuls les services de renseignements s'inquiétèrent du développement de toute cette technologie et ont tout fait pour ralentir son développement. Placer la vie de leurs agents entre les mains des mathématiciens leur paraissait dangereux. Le projet fut mis au rancart. Pourtant dans les dix ans qui suivirent, le code RSA fit la preuve de sa valeur non seulement pour protéger la vie des espions, mais aussi dans le monde public du commerce.

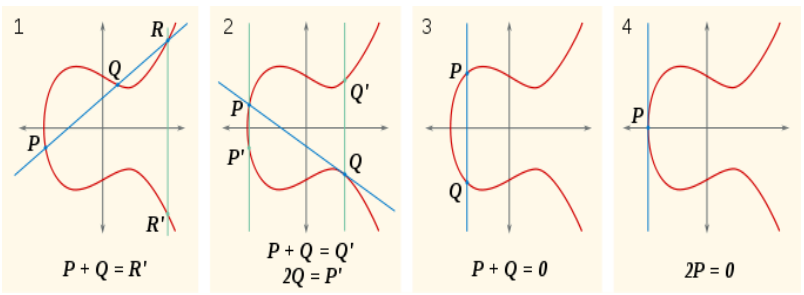


**POUR LES CURIEUX, CE COMPLÉMENT SUR L'UTILISATION DES COURBES ELLIPTIQUES EN CRYPTOGRAPHIE (par exemple pour l'envoi de SMS privés)**

De façon élémentaire, on peut définir les ***courbes elliptiques*** en tant que courbes algébriques du troisième degré (cubiques) dont l'équation peut se ramener à la forme : $\mathbf{y^2 = x^3 + ax + b}$
Selon le choix des coefficients a et b, les graphes correspondants ont essentiellement deux formes possibles. Voici par exemple les graphes réels associés à deux courbes elliptiques dans le plan affine.




En cryptographie, les courbes elliptiques, des objets mathématiques, peuvent être utilisées pour des opérations asymétriques comme des échanges de clés sur un canal non-sécurisé ou un chiffrement asymétrique, on parle alors de cryptographie sur les courbes elliptiques ou ECC (de l'acronyme anglais Elliptic curve cryptography). L'usage des courbes elliptiques en cryptographie a été suggéré, de manière indépendante, par Neal Koblitz et Victor Miller en 1985.




**ADDITION SUR LES COURBES ELLIPTIQUES :**

**illustrations des différents cas possibles**

Les clés employées pour un chiffrement par courbe elliptique sont plus courtes qu'avec un système fondé sur le problème de la factorisation comme RSA. De plus l'ECC procure un niveau de sécurité équivalent ou supérieur aux autres méthodes. Un autre attrait de l'ECC est qu'un opérateur bilinéaire peut être défini entre les groupes. Cet opérateur se base sur le couplage de Weil ou le couplage de Tate. Les opérateurs bilinéaires se sont récemment vus appliqués de nombreuses façons en cryptographie, par exemple pour le chiffrement basé sur l'identité. Un point négatif est que les opérations de chiffrement et de déchiffrement peuvent avoir une plus grande complexité que pour d'autres méthodes.

La résistance d'un système fondé sur les courbes elliptiques repose sur le problème du logarithme discret dans le groupe correspondant à la courbe elliptique. Les développements théoriques sur les courbes étant relativement récents, la cryptographie sur courbe elliptique n'est pas très connue et souffre d'un grand nombre de brevets qui empêchent son développement.

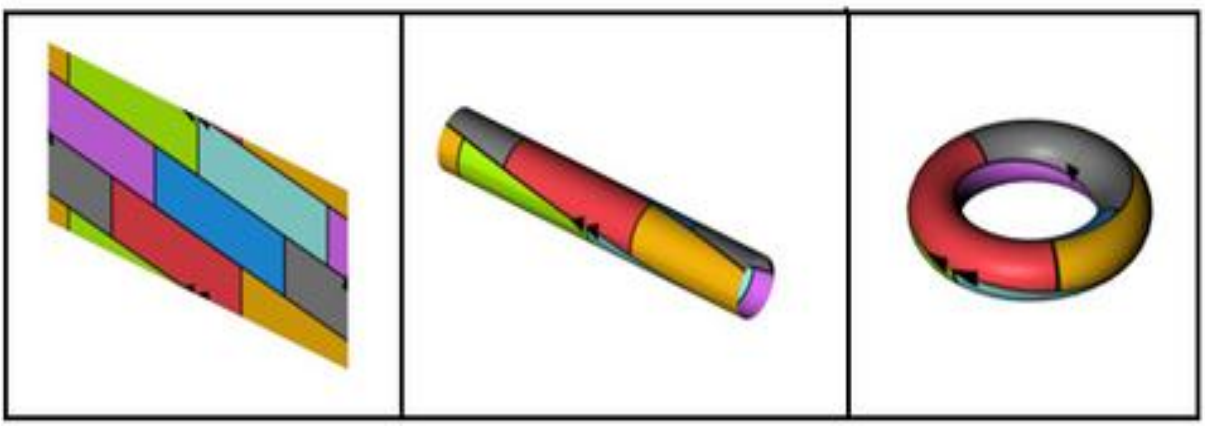
# LE THÉORÈME DES QUATRE COULEURS

Avec des extraits de WIKIPEDIA

**Le théorème des quatre couleurs** indique qu'il est possible, en n'utilisant que quatre couleurs différentes, de colorer1 n'importe quelle carte découpée en régions connexes, de sorte que deux régions adjacentes (ou limitrophes), c'est-à-dire ayant toute une frontière (et non simplement un point) en commun reçoivent toujours deux couleurs distinctes. L'énoncé peut varier et concerner, de manière tout à fait équivalente, la coloration des faces d'un polyèdre, ou des sommets d'un graphe planaire (par exemple, la résolution du **Sudoku** peut se ramener à un problème de coloration de graphe).

Dans le cas du coloriage d'une carte géographique, chacune des régions doit recevoir une couleur différente si les régions sont deux à deux adjacentes ; c'est le cas par exemple de la Belgique, du Luxembourg, de l'Allemagne et de la France dans une carte politique de l'Europe. D'où la nécessité des quatre couleurs dans le cas général. Par ailleurs, il ne peut exister cinq régions connexes deux à deux adjacentes (c'est la partie facile du théorème de Kuratowski).





## HISTOIRE

Le résultat fut conjecturé en 1852 par Francis Guthrie, intéressé par la coloration de la carte des régions d'Angleterre. La première mention publiée date toutefois de 18792. Deux premières démonstrations furent publiées, respectivement par Alfred Kempe en 1879 et Peter Guthrie Tait en 1880. Mais elles s'avérèrent erronées ; les erreurs ont été relevées seulement en 1890 par Percy Heawood et en 1891 par Julius Petersen.

Ironiquement, la fausse preuve de Kempe contient le schéma général de la vraie preuve.

La fausse preuve fournit en fait une démonstration du résultat analogue mais avec cinq couleurs au lieu de quatre, aujourd'hui connu sous le nom du théorème des cinq couleurs (dont l'unique intérêt

est d'admettre une courte preuve, donnée dans Gonthier 2000), comme l'a remarqué Percy Heawood en 1890.

Dans les années 1960 et 1970, Heinrich Heesch s'intéresse à la possibilité de prouver informatiquement le théorème des quatre couleurs. Finalement, en 1976, deux Américains, Kenneth Appel et Wolfgang Haken, affirment avoir démontré le théorème des quatre couleurs. Leur démonstration partage la communauté scientifique : pour la première fois, en effet, la démonstration exige l'usage de l'ordinateur pour étudier les 1478 cas critiques (plus de 1200 heures de temps machine de calcul).

Le problème de la démonstration du théorème se trouve alors déplacé vers d'autres problèmes:
-- d'une part de la validation de l'algorithme d'exploration,
-- d'autre part de la vérification de la justesse du programme,
-- et enfin de la vérification de la justesse de son exécution.
C'est un problème d'une grande **« complexité »,** sans demander apparemment de concepts intéressants, ce qui est exceptionnel en mathématiques.

Le mathématicien **Paul Erdös** pensait que le théorème des quatre couleurs était «un problème subtil et non pas un problème complexe». D'après lui, une démonstration simple, et même très simple, devait exister. Mais pour cela, il aurait fallu peut-être «compliquer le problème», en le formulant pour un ensemble de points plus vaste qu'un graphe planaire, et incluant celui-ci.

En tout cas, aucune preuve qui ne fasse pas appel à l'ordinateur n'a été découverte jusqu'ici ; cependant, de nombreux amateurs continuent à être convaincus d'y avoir réussi.

**LE « THÉORÈME DES QUATRE COULEURS » POUR DES SURFACES PLUS GÉNÉRALES QUE LE PLAN (par exemple sur la sphère, le tore, ...)**

Par exemple, un théorème (démontré) affirme que 7 couleurs suffisent pour colorer n'importe quelle carte sur le tore, et des exemples montrent que cela peut être nécessaire. Cette preuve n'utilise par d'ordinateur.



# LE THEOREME DE FERMAT-WILES

## LE DERNIER THÉORÈME DE FERMAT


Pierre de FERMAT, un mathématicien français du XVIIe siècle (1601-1665), s'était contenté de porter dans la marge de son cahier de travail : « $x^n + y^n = z^n$ impossible si n>2.
Il ajouta : « … J'ai trouvé une merveilleuse démonstration de cette proposition. Mais la marge est trop étroite pour la contenir. »

On ne retrouva jamais la "preuve" de Fermat (tout indique qu'il n'en avait d'ailleurs pas), et cette énigme, montrer que $x^n+y^n=z^n$ n'a pas de solutions entières pour n>2, fut la plus grande énigme qui agita le monde des mathématiciens pendant 4 siècles.

1. Le cas **n=4** fut rapidement résolu (par Fermat lui-même, en utilisant la méthode de la descente infinie).
2. Le premier progrès important fut ensuite réalisé par **Euler**, près d'un siècle plus tard, qui en utilisant les nombres complexes vint à bout du cas **n=3**.
3. Il fallut attendre encore 75 ans pour que les mathématiciens **Sophie Germain, Dirichlet et Legendre** prouvent le cas **n=5**.
4. Quatorze ans plus tard, le mathématicien **Lamé** enrichit encore la méthode pour traiter le cas **n=7**.

**CONJECTURÉ SANS DÉMONSTRATION PAR PIERRE DE FERMAT AU XVIIE SIÈCLE, CE RÉSULTAT A ÉTÉ DÉMONTRÉ PAR ANDREW WILES EN 1994.**

Après avoir été l'objet de fiévreuses recherches pendant près de 350 ans (depuis l'annonce de Fermat), n'aboutissant qu'à des résultats partiels mais enrichissant diverses questions (d'algèbre notamment), le théorème a finalement été démontré par le mathématicien Andrew Wiles. La démonstration, publiée en 1995, recourt à des mathématiques parmi les plus profondes et les plus difficiles.

**Andrew Wiles** a prouvé un cas particulier de la *conjecture de Shimura-Taniyama-Weil sur les courbes elliptiques*, dont on savait depuis quelque temps déjà, via les travaux d'Yves Hellegouarch, Gerhard Frey, Jean-Pierre Serre et Ken Ribet, qu'elle impliquait le théorème. La démonstration fait appel aux formes modulaires, aux représentations galoisiennes, à la cohomologie galoisienne, aux représentations automorphes, à une formule de traces…

La présentation de la démonstration par Andrew Wiles s'est faite en deux temps :

-- **en juin 1993**, en conclusion d'une conférence de trois jours, il annonce que le grand théorème de Fermat est un corollaire de ses principaux résultats exposés. Dans les mois qui suivent, le manuscrit de sa démonstration circule auprès d'un petit nombre de mathématiciens. Plusieurs critiques sont émises contre la démonstration que Wiles a présentée en 1993, presque toutes de l'ordre du détail et résolues rapidement, sauf une, qui met en évidence une lacune.

-- **en octobre 1994**, après plusieurs mois de nouvelles recherches et en collaboration avec Richard Taylor, Wiles réussit à contourner le problème soulevé. Le document final est publié en 1995.



## BIBLIOGRAPHIE

**DEHAENE Stanislas**, *La bosse des maths*,

**DIEUDONNÉ Jean**, *Pour l'honneur de l'esprit humain. Les mathématiques aujourd'hui*, Hachette Pluriel, 1987

**EINSTEIN Albert**, *Comment je vois le monde*, Champs Flammarion, 1979

**KOYRÉ Alexandre**, *Du monde clos à l'univers infini*, Gallimard, 2003

**KOYRÉ Alexandre**, *Éléments d'histoire de la pensée scientifique*, Gallimard ; 3e éd. 1990

**O'SHEA Donal**, *Grigori Perelman face à la conjecture de Poincaré*, Dunod, 2007

**SAUTOY (du) Marcus**, *La symphonie des nombres premiers*, Points Sciences, 2005

**SINGH Simon**, *Le dernier théorème de Fermat*, Hachette Pluriel, 1998

**STEWART Ian**, *Dieu joue-t-il aux dés ? Les mathématiques du chaos*, Champs Flammarion, 1998

**THUILLIER Pierre**, *D'Archimède à Einstein, Les faces cachées de l'invention scientifique*, Fayard (poche), 1988.

----------.----------