

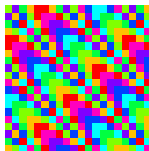
CES MATHÉMATIQUES QUE L'ON DIT PURES, ET LEURS  
APPLICATIONS : DES OBJETS MATHÉMATIQUES AUX OBJETS  
INDUSTRIELS, TECHNOLOGIQUES, INFORMATIQUES

Michel Rigo

<http://www.discmath.ulg.ac.be/>  
[M.Rigo@ulg.ac.be](mailto:M.Rigo@ulg.ac.be)

Palais des congrès de Liège, 14 novembre 2013

Université  
de Liège



# LES MATHÉMATIQUES DOIVENT-ELLES ÊTRE “UTILES” ?

J'avais raison de ne pas me soucier des applications [de mon théorème] : elles vinrent plus tard.

Jacques Hadamard (1865–1963),  
cité par Didier Nordon, Des cailloux dans les choses sûres

Mathematics arose from the awakening of the human soul.  
The mathematician does not look for truth with a practical purpose.  
To cultivate mathematics only for its practical purpose is to despoil the soul of mathematics. The theory that we study today, and that appears to us impractical, might have implications in the future that are unimaginable to us. Who can imagine the repercussions of an enigma through the centuries?

Malba Tahan, Júlio César de Mello e Souza  
*The Man Who Counted*

Abstractness, sometimes hurled as a reproach at mathematics, is its chief glory and its surest title to practical usefulness. It is also the source of such beauty as may spring from mathematics.

Eric Temple Bell (1883–1960)

To isolate mathematics from the practical demands of the sciences is to invite the sterility of a cow shut away from the bulls.

Pafnuty Chebyshev (1821–1894),  
dans G. Simmons, *Calculus Gems*, McGraw Hill (1992).

There is no trivial mathematics, there are only trivial mathematicians!  
A mathematician is trivial if he or she believes that there exists trivial mathematics.

Mathematicians who believe that Applied Math. is Bad Math. are not mathematicians at all. A true mathematician has respect for all parts of mathematics, and does not believe in arbitrary divisions into *Pure*, *Applied*, *Theoretical*, *Practical*, *Conceptual*, *Computational*. Mathematics is a Web, an infinite dimensional tapestry with everything intertwined.

Un des grands problèmes... est la gestion des grands programmes informatiques qui font de plus en plus souvent plus d'une centaine de million de lignes de code.... les entreprises qui sont de plus en plus nombreuses à le rencontrer développent des méthodes assez artisanales et ad hoc pour en venir tant bien que mal à bout.

Il y a un monde immense de problèmes issus de l'informatique qui attendent celui, celle ou ceux qui les comprendront et parviendront à les mettre en forme mathématique...

... l'attente de l'industrie prête à accueillir (voire couvrir d'or) ceux qui voudront bien l'aider à apporter ou améliorer des solutions et je voudrais surtout que l'on fasse dans l'enseignement prendre conscience à nos élèves de cette formidable opportunité qui s'ouvre à eux.

Maurice Nivat,  
Gazette des Mathématiciens, Octobre 2013

# REAL WORLD PROBLEM

- ▶ Un problème réel n'est pas fourni avec la méthode de résolution à appliquer.
- ▶ Un problème réel nécessite de combiner des méthodes diverses provenant de plusieurs contextes.
- ▶ Un problème réel peut nécessiter l'apprentissage de nouvelles méthodes.
- ▶ Dans le monde réel, on ne dispose pas de “solutionnaire” et pourtant le problème doit être résolu.

Ainsi, l'obtention d'une solution nécessite

- ▶ un important bagage théorique (compris en profondeur), se construire une boîte à outils dans laquelle puiser,
- ▶ une (longue) habitude à l'abstraction: on ne peut la contourner,
- ▶ une bonne dose de persévérance.

## 4 exemples

- ▶ Les grands réseaux complexes
- ▶ Les codes correcteurs
- ▶ La théorie de la complexité en informatique théorique
- ▶ La compression d'images et le format JPEG

# QUELQUES EXEMPLES (1/4)

Google : comment classer des milliards de pages web ?  
<http://www.discmath.ulg.ac.be/mam/pratique.html>

$$M = \begin{pmatrix} 1 & 3 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 3 \\ 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 2 \\ 4 & 0 & 0 & 0 & 0 \end{pmatrix}$$

$$M^6 = \begin{pmatrix} 1537 & 471 & 219 & 222 & 669 \\ 892 & 1380 & 84 & 72 & 396 \\ 592 & 48 & 48 & 96 & 144 \\ 584 & 888 & 24 & 48 & 168 \\ 628 & 876 & 444 & 24 & 1380 \end{pmatrix}$$

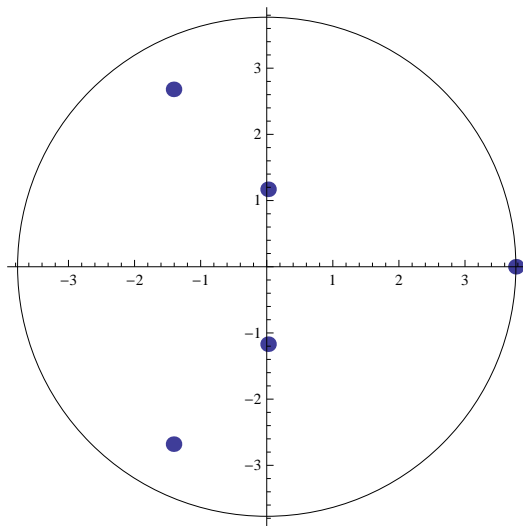
# QUELQUES EXEMPLES (1/4)

Google : comment classer des milliards de pages web ?  
<http://www.discmath.ulg.ac.be/mam/pratique.html>

$$M = \begin{pmatrix} 1 & 3 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 3 \\ 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 2 \\ 4 & 0 & 0 & 0 & 0 \end{pmatrix}$$

$$M^6 = \begin{pmatrix} 1537 & 471 & 219 & 222 & 669 \\ 892 & 1380 & 84 & 72 & 396 \\ 592 & 48 & 48 & 96 & 144 \\ 584 & 888 & 24 & 48 & 168 \\ 628 & 876 & 444 & 24 & 1380 \end{pmatrix}$$

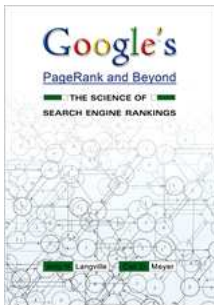




$$\begin{pmatrix} 0.9426 \\ 0.8703 \\ 0.2814 \\ 0.5304 \\ 1 \end{pmatrix}$$

## THÉORÈME DE PERRON (1907)

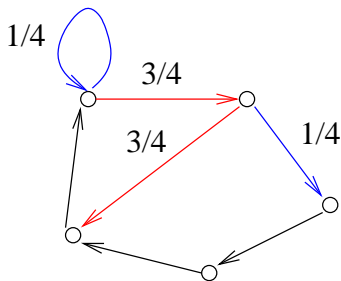
Soit  $A$  une matrice primitive. La matrice  $A$  possède une valeur propre  $\lambda$  réelle, dominante et simple. Il existe un vecteur propre (à gauche, resp. à droite) associé à  $\lambda$  dont toutes les composantes sont  $> 0$ .



Google's PageRank and Beyond: The Science of Search Engine Rankings, A. Langville, C. Meyer

Applications : théorie des probabilités, chaînes de Markov;  
PageRank, économie, analyse input-output  $(I - S)x = d, \dots$

$$S = \begin{pmatrix} 1/4 & 3/4 & 0 & 0 & 0 \\ 0 & 0 & 1/4 & 0 & 3/4 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix}$$

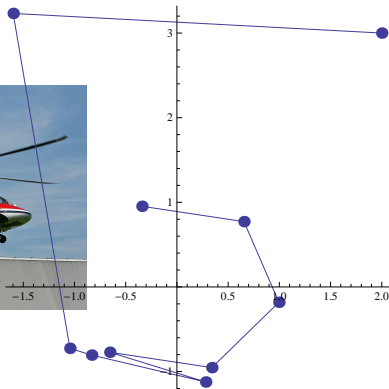


vecteur propre à gauche :  $(0.5217, 0.08696, 0.02174, 0.02174, 0.3478)$ .

Théorie du contrôle – système dynamique où la trajectoire est mise à jour par un contrôleur (feedback)

$$A = \frac{1}{2} \begin{pmatrix} 1 & -\sqrt{3} \\ \sqrt{3} & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 1/3 & 2/3 \\ 1/4 & 3/4 \end{pmatrix}$$

$$\dots A.A.A.A.B.A.B.B.A.A. \begin{pmatrix} 2 \\ 3 \end{pmatrix}$$



## PROBLÈME DE LA “MORTALITÉ DE MATRICES”

Données :  $k$  matrices  $M_1, \dots, M_k \in \mathbb{Z}^{n \times n}$ .

Existe-t-il un produit de ces matrices tel que  $M_{i_1} \cdots M_{i_\ell} = 0$  ?

## THÉORÈMES

Pour  $n \geq 3$ , le problème est **indécidable** (Patterson 1970)

Pour  $n \geq 45$  et  $k = 2$ , le problème est indécidable  
(Cassaigne, Karhumäki)

Pour  $n \leq 33$  et  $k = 2$ , le problème est décidable  
(Blondel, Tsitsiklis 1996)

Pour  $n = 2$  et  $\det(M_1), \dots, \det(M_k) \in \{-1, 0, 1\}$ ,  
le problème est décidable (Nuccio, Rodaro 2008)

## PROBLÈME DE SKOLEM–PISOT

Soit  $M$  une matrice de  $\mathbb{Z}^{n \times n}$ .

Existe-t-il une puissance de  $M$  dont le coin supérieur droit est nul ?

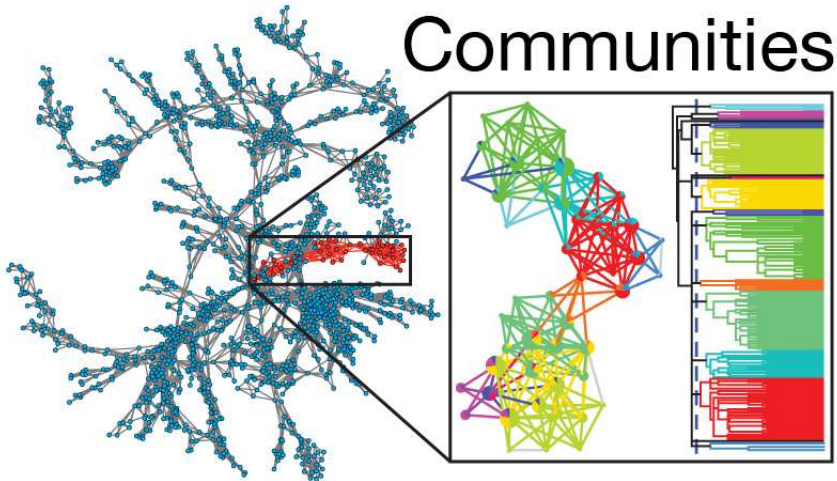
## THÉORÈMES

Pour  $n = 3$ , problème décidable (Vereshchagin, 1985)

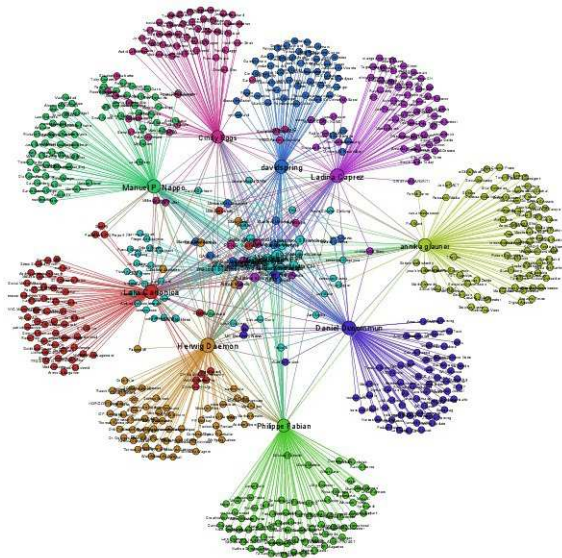
Pour  $n = 4$ , problème décidable

(V. Halava, T. Harju, M. Hirvensalo, J. Karhumäki, 2005)

# Communities



Détection de communautés dans de grands graphes

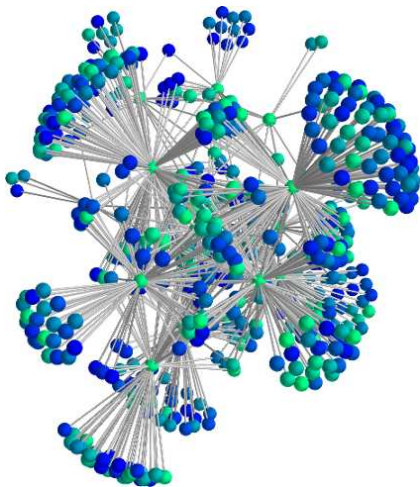


Twitter follower-graph

<http://www.fernfachhochschule.ch/ffhs/afe/lws/forschung/research>







## Movie recommender system

<http://www.fernfachhochschule.ch/ffhs/afe/lws/forschung/research>

# CONCLUSION DE L'EXEMPLE 1

Les outils utilisés :

- ▶ Calcul matriciel / Systèmes d'équations linéaires
- ▶ Algèbre linéaire
- ▶ Théorie des graphes (Terminale ES en France)
- ▶ Interprétation probabiliste
- ▶ Intuition géométrique
- ▶ Notions de convergence, de distance,...

Le langage de l'algèbre linéaire est omniprésent dans toutes les branches des mathématiques.

## QUELQUES EXEMPLES (2/4)

Codes correcteurs : *des vecteurs dans mon iPod !*  
<http://www.discmath.ulg.ac.be/mam/pratique.html>



Théorie de l'information / Compression / Codes correcteurs

(sans parler des aspects de sécurité, chiffrement de données)

## FAIT

Pour détecter/corriger des erreurs, on introduit de la redondance.

But : Répéter un minimum et corriger un maximum.

Nous vivons dans un monde “digital” construit sur des **structures mathématiques élaborées**, exemple...

# Metacyclic Error-Correcting Codes

Roberta Evans Sabin<sup>1</sup>, Samuel J. Lomonaco<sup>2</sup>

<sup>1</sup> Computer Science Department, 4501, N. Charles St. Loyola College, Baltimore, Maryland 21210-2699, USA, E-Mail: RES@Loyola.edu  
<sup>2</sup> Computer Science Department, University of Maryland, Baltimore County, Catonsville, Maryland 21228, USA, E-Mail: Lomonaco@cs.umbc.edu

Received March 17, 1993; revised version July 30, 1993

**Abstract.** Error-correcting codes which are ideals in group rings where the underlying group is metacyclic and non-abelian are examined. Such a group  $G(M, N, R)$  is an extension of a finite cyclic group  $\mathbb{Z}_M$  by a finite cyclic group  $\mathbb{Z}_N$  and has a presentation of the form

$$(\mathcal{S}, T: \mathcal{S}^M = 1, T^N = 1, T \cdot \mathcal{S} = \mathcal{S}^R \cdot T)$$

where  $M, R = 1 \pmod N$ ,  $R \neq 1$ . Group rings that are semi-simple, i.e., whose characteristic of the field does not divide the order of the group, are considered. In all cases, the field of the group ring is of characteristic 2, and has a unique direct sum decomposition into minimal two-sided ideals (central codes). In every case, a technique to vary the decomposition is described. This technique is described in detail.

The analysis of the structure of the group ring yields a unique direct sum decomposition of  $FG(M, N, R)$  to minimal two-sided ideals (central codes). In every case, a technique to vary the decomposition is described. This technique is described in detail.

# QUELQUES CHIFFRES

**94B** *Theory of error-correcting codes and error-detecting codes*

11 440 résultats sur MathSciNet

**94** *Information and communication, circuits*

78 378 résultats sur MathSciNet

	2010	2011	2012	2013
94B	536	559	561	296
94	3688	4484	5529	3022
92	4333	4458	4299	2368

**92** *Biology and other natural sciences* 70 672 résultats sur MathSciNet

**93** *Systems theory; control* 113 220 résultats sur MathSciNet

# CONCLUSION DE L'EXEMPLE 2

Les outils utilisés :

- ▶ Arithmétique
- ▶ Abstraction, Structures algébriques  
(théorie des groupes, corps, espaces vectoriels, polynômes, ...)
- ▶ **Dénombrement / Combinatoire**
- ▶ **Statistique et probabilité**

Il faut une habitude à l'abstraction.

Pour la cryptographie, en outre :

- ▶ Théorie des nombres
- ▶ Géométrie algébrique (courbes elliptiques...)



# QUELQUES EXEMPLES (3/4)

P versus NP ? (Stephen Cook and Leonid Levin, 1971)



Il s'agit de l'un des sept problèmes du Millénaire  
(Clay Mathematics Institute)

L'ordinateur ne peut tout résoudre

- ▶ Il existe des problèmes indécidables
- ▶ Si un problème est décidable, il est peut-être très difficile !

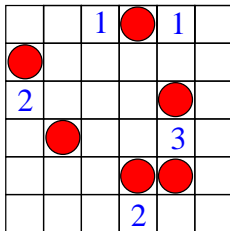
## BUT

- ▶ Comment formaliser ces concepts ?
- ▶ Comment dire que deux problèmes ont la même “complexité” ?
- ▶ Si je ne trouve pas de solution “simple” à un problème, est-ce pour autant “qu’il n’y en a pas” ?

Comment gagner 1 million de dollars en jouant au démineur ?

		1		1	
2					
				3	
			2		

Comment gagner 1 million de dollars en jouant au démineur ?



Des problèmes *très difficiles* et pourtant bien “réels”  
l'arithmétique de Presburger (1929)

$\forall, \wedge, +, =, \rightarrow, \leftrightarrow, \neg, \forall, \exists$

$$\varphi = (\exists x)(\forall y)(x + y = y)$$

$$\psi = (\forall x)(\exists y)(x = y + y)$$

Applications : optimisation sous contraintes linéaires, géométrie convexe, images 3D, preuves automatiques / vérification de programmes ...



Paris : Ligne 14, Saint-Lazare — Olympiades

## THÉORÈME (FISHER–RABIN 1974)

There exists a constant  $c > 0$  such that for every decision procedure (algorithm)  $AL$  for Presburger arithmetic  $PA$ , there exists an integer  $n_0$  so that for every  $n > n_0$  there exists a sentence  $F$  of length  $n$  for which  $AL$  requires more than  $2^{2^{cn}}$  computational steps to decide whether  $F \in PA$ .

The previous theorem applies also in the case of non-deterministic algorithms. This implies that not only algorithms require a super-exponential number of computational steps, but also proofs of true statements concerning addition of natural numbers are super-exponentially long.

<http://publications.csail.mit.edu/lcs/pubs/ps/MIT-LCS-TM-043.ps>

# CONCLUSION DE L'EXEMPLE 3

Les outils utilisés :

- ▶ **Equations / Inéquations**
- ▶ Résolution de systèmes
- ▶ Géométrie convexe
- ▶ **Logique** formelle (implication, négation, quantificateurs, ...)

Pour l'analyse d'algorithmes :

- ▶ Comportements asymptotiques, **analyse** mathématique, calculs de limites
- ▶ Analyse "en moyenne" : **probabilités**, **combinatoire**, analyse complexe, ...

# QUELQUES EXEMPLES (4/4)

## Photographie et la compression JPEG (1992)

Joint Photographic Experts Group

80% des images sur le web... MP3, MPEG, miniDV

100% fidelity

Image is 725kB



90%

250kB



10%

37kB



1%

20kB



**JPG IS ONLY FC** **JPG IS ONLY FC** **JPG IS ONLY FC** **JPG IS ONLY FC**

The problem with The problem with The problem with The problem with

JPEG algorithm n JPEG algorithm n JPEG algorithm n JPEG algorithm n



## Transformée discrète en cosinus (DCT-3)

G. Strang, The DCT, SIAM Review 1999

$$\forall j, k \in \{0, \dots, 7\}, \quad U_{j,k} = \begin{cases} \sqrt{2}/4 & \text{si } j = 0 \\ \frac{1}{2} \cos\left(j\left(k + \frac{1}{2}\right)\frac{\pi}{8}\right) & \text{sinon} \end{cases}$$

$U \in \mathbb{R}^{8 \times 8}$  est une matrice orthogonale :  $U \tilde{U} = I$

Les **lignes** de  $U$  (sauf la première) satisfont :

$$\sum_{k=0}^7 U_{j,k} = 0, \quad \forall j \in \{1, \dots, 7\}$$

Donc, si  $\mathbf{x} \in \mathbb{R}^8$  est un vecteur **constant**, alors  $\forall j \in \{1, \dots, 7\}$

$$\langle \mathbf{x}, (U_{j,k})_{0 \leq k \leq 7} \rangle = 0$$

si  $\mathbf{x} \in \mathbb{R}^8$  est “*presque constant*”, alors  $\langle \mathbf{x}, (U_{j,k})_{0 \leq k \leq 7} \rangle \simeq 0$

La matrice  $U$ :

$$U = \frac{1}{2} \begin{pmatrix} \frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2} \\ \cos \frac{\pi}{16} & \cos \frac{3\pi}{16} & \cos \frac{5\pi}{16} & \cos \frac{7\pi}{16} & \cos \frac{9\pi}{16} & \cos \frac{11\pi}{16} & \cos \frac{13\pi}{16} & \cos \frac{15\pi}{16} \\ \cos \frac{2\pi}{16} & \cos \frac{6\pi}{16} & \cos \frac{10\pi}{16} & \cos \frac{14\pi}{16} & \cos \frac{18\pi}{16} & \cos \frac{22\pi}{16} & \cos \frac{26\pi}{16} & \cos \frac{30\pi}{16} \\ \cos \frac{3\pi}{16} & \cos \frac{9\pi}{16} & \cos \frac{15\pi}{16} & \cos \frac{21\pi}{16} & \cos \frac{27\pi}{16} & \cos \frac{33\pi}{16} & \cos \frac{39\pi}{16} & \cos \frac{45\pi}{16} \\ \cos \frac{4\pi}{16} & \cos \frac{12\pi}{16} & \cos \frac{20\pi}{16} & \cos \frac{28\pi}{16} & \cos \frac{36\pi}{16} & \cos \frac{44\pi}{16} & \cos \frac{52\pi}{16} & \cos \frac{60\pi}{16} \\ \cos \frac{5\pi}{16} & \cos \frac{15\pi}{16} & \cos \frac{25\pi}{16} & \cos \frac{35\pi}{16} & \cos \frac{45\pi}{16} & \cos \frac{55\pi}{16} & \cos \frac{65\pi}{16} & \cos \frac{75\pi}{16} \\ \cos \frac{6\pi}{16} & \cos \frac{18\pi}{16} & \cos \frac{30\pi}{16} & \cos \frac{42\pi}{16} & \cos \frac{54\pi}{16} & \cos \frac{66\pi}{16} & \cos \frac{78\pi}{16} & \cos \frac{90\pi}{16} \\ \cos \frac{7\pi}{16} & \cos \frac{21\pi}{16} & \cos \frac{35\pi}{16} & \cos \frac{49\pi}{16} & \cos \frac{63\pi}{16} & \cos \frac{77\pi}{16} & \cos \frac{91\pi}{16} & \cos \frac{105\pi}{16} \end{pmatrix}$$

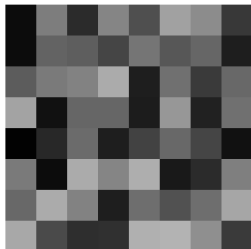
$$M \mapsto UM\tilde{U}$$

- 1) on calcule  $UM$  (vu les propriétés des lignes de  $U$ )
- 2) on calcule  $(UM)\tilde{U}$  (les colonnes de  $\tilde{U}$  sont les lignes de  $U$ )

*“les valeurs significatives ont tendance à être  
poussées vers le coin supérieur gauche”...*

$$U \begin{pmatrix} 100 & 100 & 100 & 100 & 100 & 100 & 100 & 100 \\ 100 & 100 & 100 & 100 & 100 & 100 & 100 & 100 \\ 100 & 100 & 100 & 100 & 100 & 100 & 100 & 100 \\ 100 & 100 & 100 & 100 & 100 & 100 & 100 & 100 \\ 100 & 100 & 100 & 100 & 100 & 100 & 100 & 100 \\ 100 & 100 & 100 & 100 & 100 & 100 & 100 & 100 \\ 100 & 100 & 100 & 100 & 100 & 100 & 100 & 100 \\ 100 & 100 & 100 & 100 & 100 & 100 & 100 & 100 \end{pmatrix} \tilde{U}$$

$$= \begin{pmatrix} 800 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$



$$A = \begin{pmatrix} 5 & 49 & 17 & 52 & 31 & 63 & 55 & 22 \\ 5 & 39 & 37 & 27 & 46 & 34 & 40 & 12 \\ 36 & 48 & 51 & 67 & 12 & 44 & 23 & 41 \\ 64 & 7 & 40 & 40 & 11 & 59 & 13 & 44 \\ 1 & 16 & 42 & 12 & 26 & 41 & 27 & 7 \\ 48 & 5 & 67 & 52 & 68 & 10 & 17 & 50 \\ 41 & 67 & 51 & 12 & 43 & 32 & 43 & 65 \\ 66 & 29 & 18 & 19 & 69 & 70 & 56 & 23 \end{pmatrix}$$

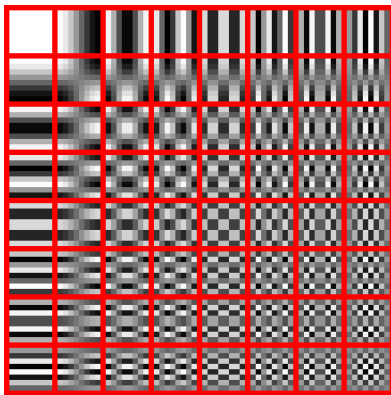
En pratique, les éléments de  $A$  appartiennent à  $[-128, 127]$

$$B = UA\tilde{U} = \begin{pmatrix} 291. & -5.52 & -18.9 & 8.43 & -11.6 & -2.09 & 19.3 & 1.37 \\ -22.3 & -4.91 & -25.0 & -17.7 & -26.2 & 13.6 & -15.9 & -44.4 \\ 28.6 & -18.0 & 0.730 & 33.4 & -18.5 & -17.0 & -46.5 & 1.23 \\ -15.6 & -11.7 & -20.2 & -24.3 & 0.0815 & -9.21 & -13.1 & 22.4 \\ -17.4 & -19.1 & -3.49 & 49.7 & -15.9 & 15.2 & 8.89 & -18.0 \\ 30.0 & 5.53 & 35.2 & -17.3 & 10.4 & 0.0188 & 12.6 & -28.5 \\ 20.5 & 7.70 & -16.3 & -4.78 & 30.8 & 21.5 & 7.27 & -10.9 \\ -8.38 & -3.42 & 2.93 & -12.8 & -39.7 & -13.2 & -20.4 & -16.9 \end{pmatrix}$$

Puisque  $B = U\tilde{A}\tilde{U}$ , on a aussi  $A = \tilde{U}B\tilde{U}$  donc,

$$A_{j,k} = \sum_{m=0}^7 \sum_{n=0}^7 U_{m,j} B_{m,n} U_{n,k} = \frac{1}{4} \sum_{m=1}^7 \sum_{n=1}^7 B_{m,n} \cos\left(m(j + \frac{1}{2})\frac{\pi}{8}\right) \cos\left(n(k + \frac{1}{2})\frac{\pi}{8}\right) \\ + \frac{1}{8} \sum_{n=1}^7 \sqrt{2} B_{0,n} \cos\left(n(k + \frac{1}{2})\frac{\pi}{8}\right) + \frac{1}{8} \sum_{m=1}^7 \sqrt{2} B_{m,0} \cos\left(m(j + \frac{1}{2})\frac{\pi}{8}\right) + \frac{1}{8} B_{0,0}$$

La matrice  $A$  est décomposée en une somme de 64 matrices,



Etape 2 : pour une matrice  $Q$  donnée, on définit *in fine*  $C$

$$C_{j,k} = \lfloor B_{j,k} / Q_{j,k} \rfloor$$

Seul l'arrondi n'est pas **inversible** (pertes inévitables).

La matrice Q contrôle le taux de compression,

$$Q = \begin{pmatrix} 16 & 12 & 14 & 14 & 18 & 24 & 49 & 72 \\ 11 & 12 & 13 & 17 & 22 & 35 & 64 & 92 \\ 10 & 14 & 16 & 22 & 37 & 55 & 78 & 95 \\ 16 & 19 & 24 & 29 & 56 & 64 & 87 & 98 \\ 24 & 26 & 40 & 51 & 68 & 81 & 103 & 112 \\ 40 & 58 & 57 & 87 & 109 & 104 & 121 & 100 \\ 51 & 60 & 69 & 80 & 103 & 113 & 120 & 103 \\ 61 & 55 & 56 & 62 & 77 & 92 & 101 & 99 \end{pmatrix}$$

Le résultat final

$$C = \begin{pmatrix} 18 & 0 & -1 & 1 & -1 & 0 & 0 & 0 \\ -2 & 0 & -2 & -1 & -1 & 0 & 0 & 0 \\ 3 & -1 & 0 & 2 & 0 & 0 & -1 & 0 \\ -1 & -1 & -1 & -1 & 0 & 0 & 0 & 0 \\ -1 & -1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \end{pmatrix}$$

# CONCLUSION DE L'EXEMPLE 4

Les outils utilisés :

- ▶ **Matrices** orthogonales, inversibles
- ▶ **Trigonométrie**
- ▶ Décomposition dans une **base**, changement de bases, endomorphismes
- ▶ idée de la transformée de Fourier

Pour aller plus loin :

- ▶ FFT, pour accélérer les calculs de produits
- ▶ JPEG 2000, transformée en ondelettes
- ▶ Compression "fractal", IFS, théorèmes de point fixe, ...



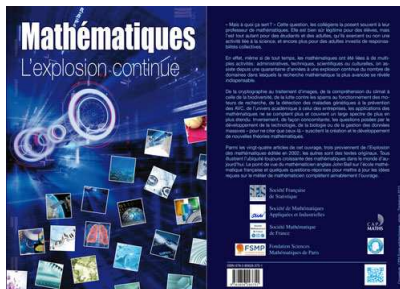
# DOES ONE HAVE TO BE A GENIUS TO DO MATHEMATICS?

The answer is an emphatic NO. In order to make good and useful contributions to mathematics, one does need to work hard, learn one's field well, learn other fields and tools, ask questions, talk to other mathematicians, and think about the “big picture”. And yes, a reasonable amount of intelligence, patience, and maturity is also required. But one does not need some sort of magic “genius gene” that spontaneously generates ex nihilo deep insights, unexpected solutions to problems, or other supernatural abilities.

Terrence Tao,

<http://terrytao.wordpress.com/career-advice/does-one-have-to-be-a-genius-to-do-maths/>

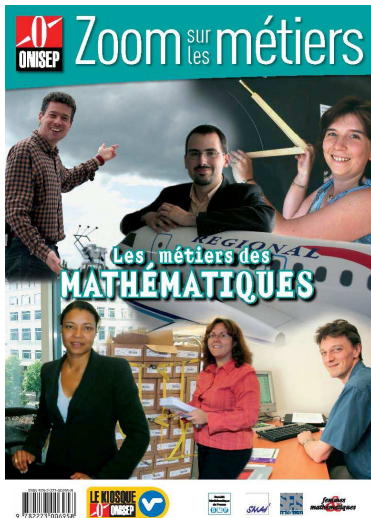
<http://smf.emath.fr/MathematiquesExplosionContinue>



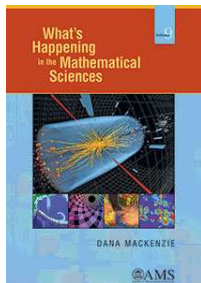
“De la cryptographie au traitement d’images, de la compréhension du climat à celle de la biodiversité, de la lutte contre les spams au fonctionnement des moteurs de recherche, de la détection des maladies génétiques à la prévention des AVC, de l’univers académique à celui des entreprises, les applications des mathématiques ne se comptent plus et couvrent un large spectre de plus en plus étendu. Inversement, de façon concomitante, les questions posées par le développement de la technologie, de la biologie ou de la gestion des données massives – pour ne citer que ceux-là – suscitent la création et le développement de nouvelles théories mathématiques.”

# QUELQUES DOCUMENTS

[http://smf.emath.fr/Publications/  
ZoomMetiersDesMaths/Presentation/](http://smf.emath.fr/Publications/ZoomMetiersDesMaths/Presentation/)



## What's Happening in the Mathematical Sciences, volumes 1–9



<http://www.whymath.org/>

Fin

# QUELQUES EXEMPLES (5)

## Images de synthèse et jeux vidéos

- ▶ Splines
- ▶ Courbes/surfaces de bézier
- ▶ Géométrie fractale
- ▶ Quaternions et rotations