Mathématiques

Quelques mathématiciens

- Archimède
- Pythagore

Des impressions

- Cauchemar
- Forêt obscure
- Pureté

Des « descriptions »

- Raisonnement
- Calcul
- Compter

On ne dit jamais que c'est utile

- Archimède
- Pythagore
- Cauchemar
- Forêt obscure
- Pureté
- Raisonnement
- Calcul
- Compter

Mathématiques

A quoi ça sert ????

LES MATHS ÇA SERT À RIEN

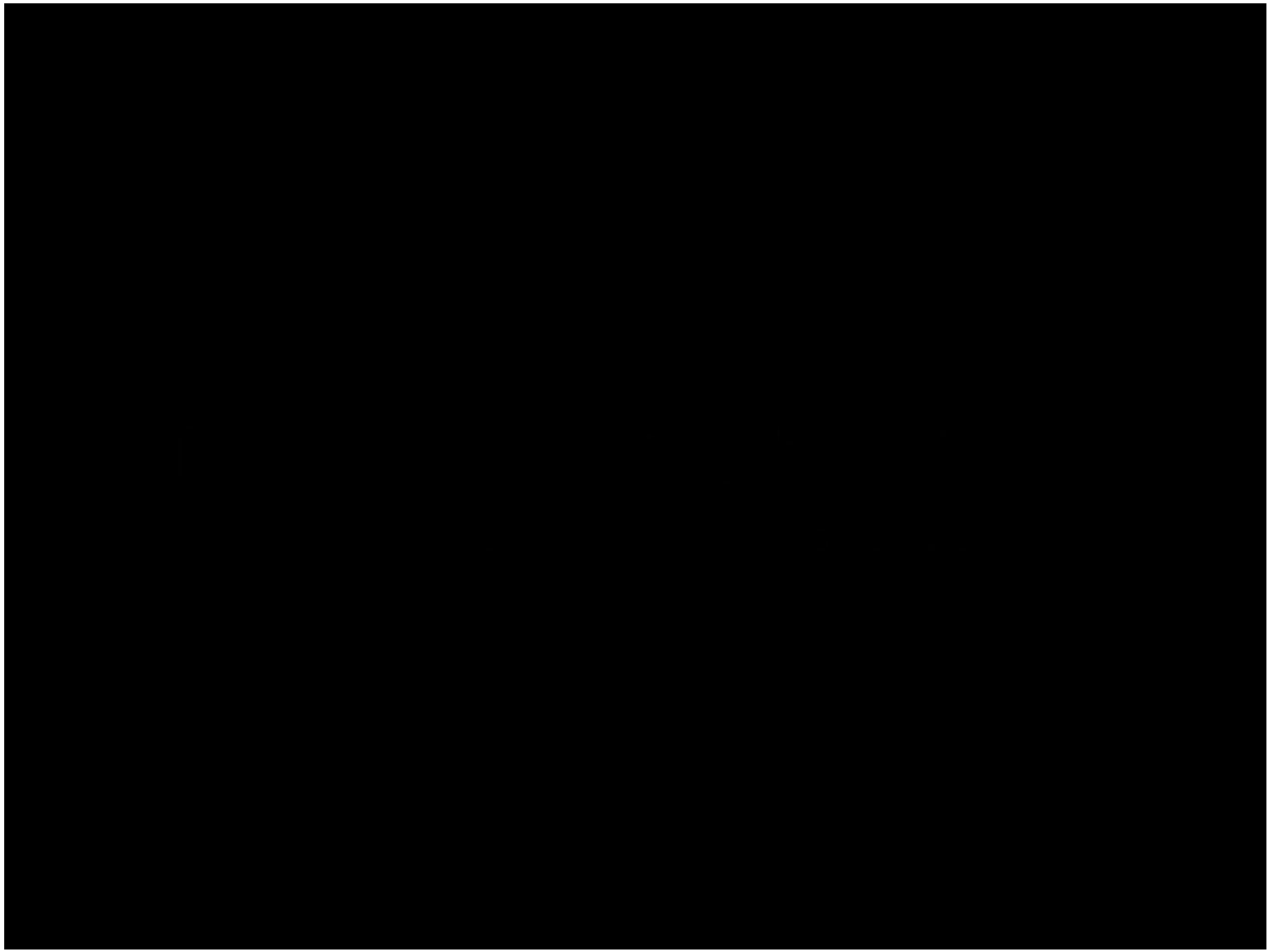
LMRS

UNIVERSITÉ DE ROUEN NORMANDIE

cnrs

contact : sorciersdesalem@univ-rouen.fr
sorciersdesalem.math.cnrs.fr

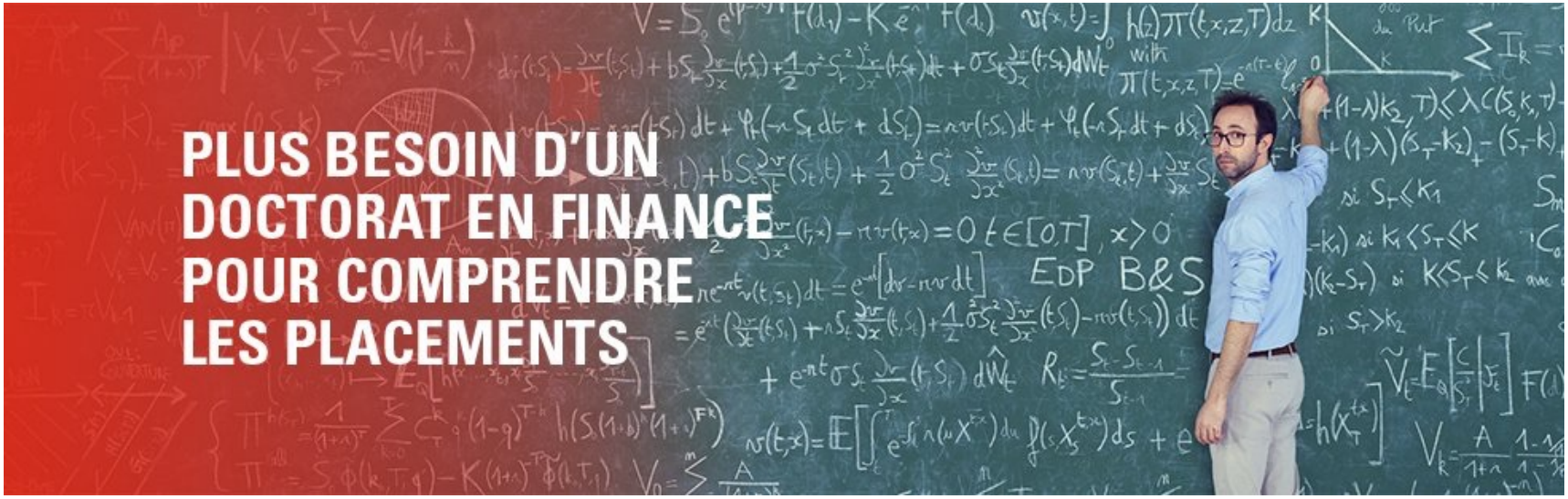
COMPTER



Les mathématiques,
ça n'est pas seulement
compter.

Finances

Au Royaume-Uni, les maths représentent16 % du PIB (10 % des emplois), essentiellement par la finance.


PLUS BESOIN D'UN
DOCTORAT EN FINANCE
POUR COMPRENDRE
LES PLACEMENTS

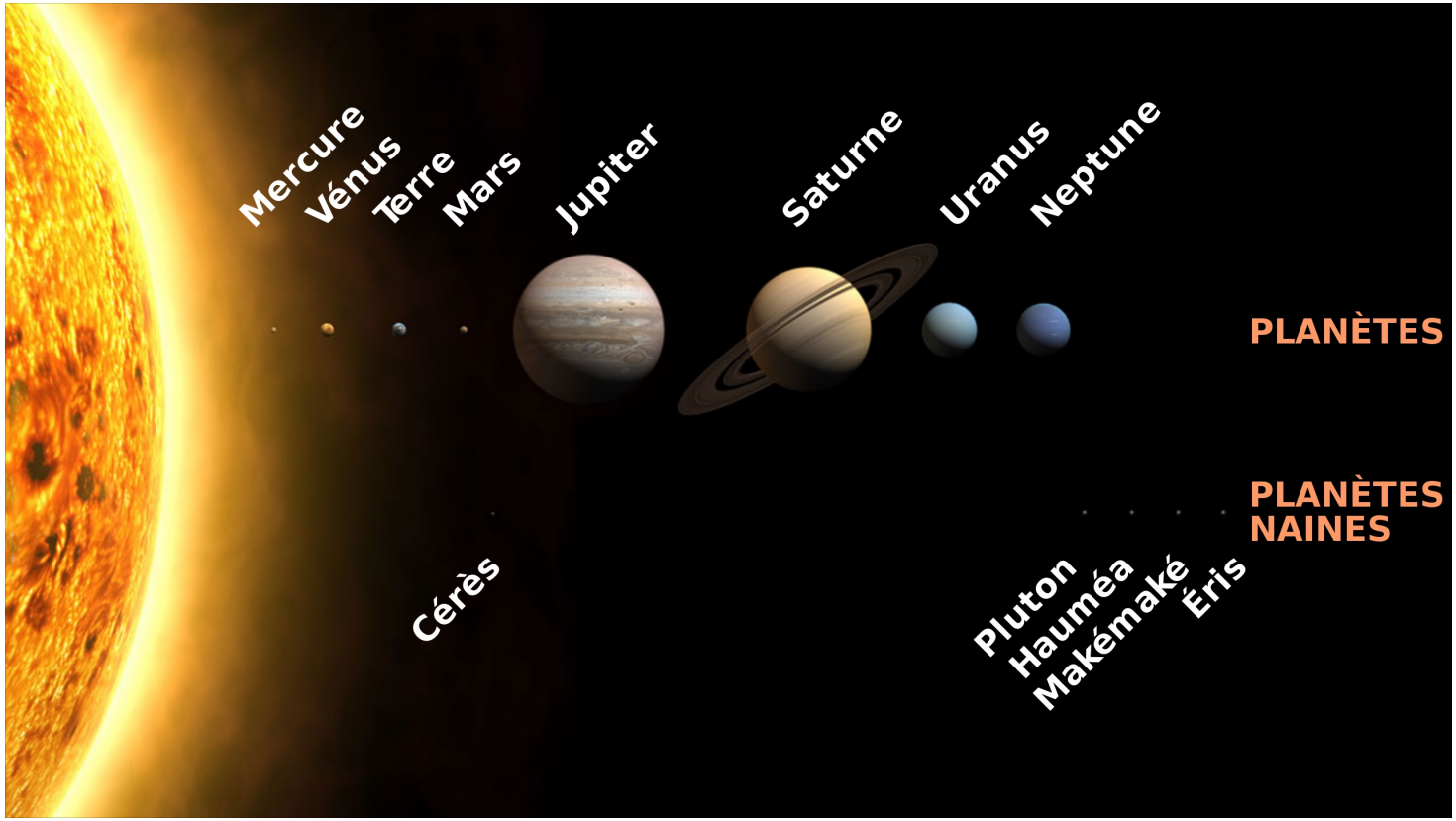
Équation de Black-Scholes-Merton

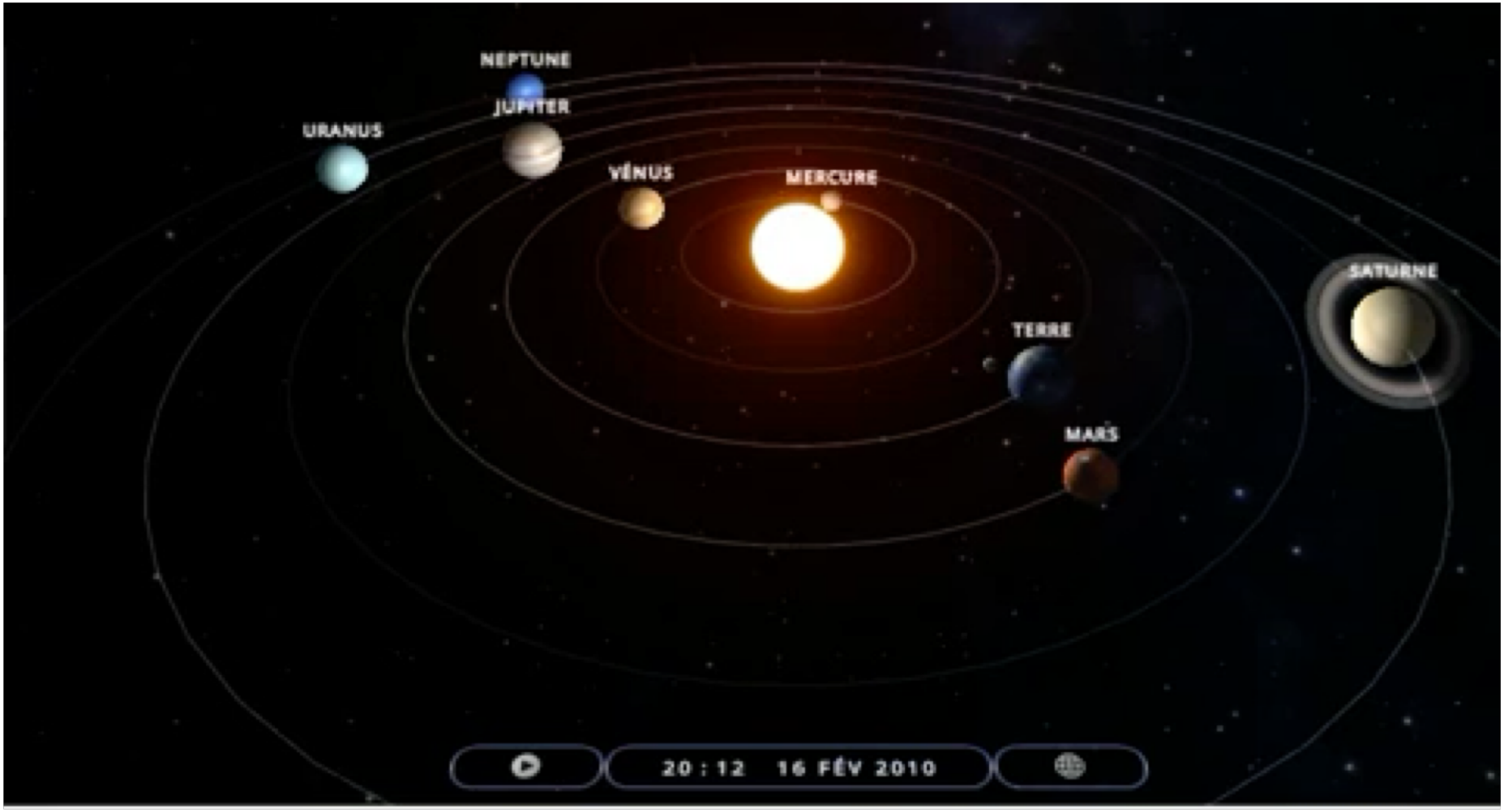
$$C(S_0,K,r,t,\sigma) = S_0\mathcal{N}(d_1) - K\,\mathrm{e}^{-rT}\mathcal{N}(d_2)$$

- C est l'espérance sous probabilité risque neutre du *payoff* terminal actualisé
- S_0 = valeur actuelle de l'action sous-jacente
- T = temps qu'il reste à l'action avant son échéance (en années)
- K = prix d'exercice fixé par l'option
- r = taux d'intérêt sans risque
- σ = volatilité de l'action

Mécanique céleste

Système solaire



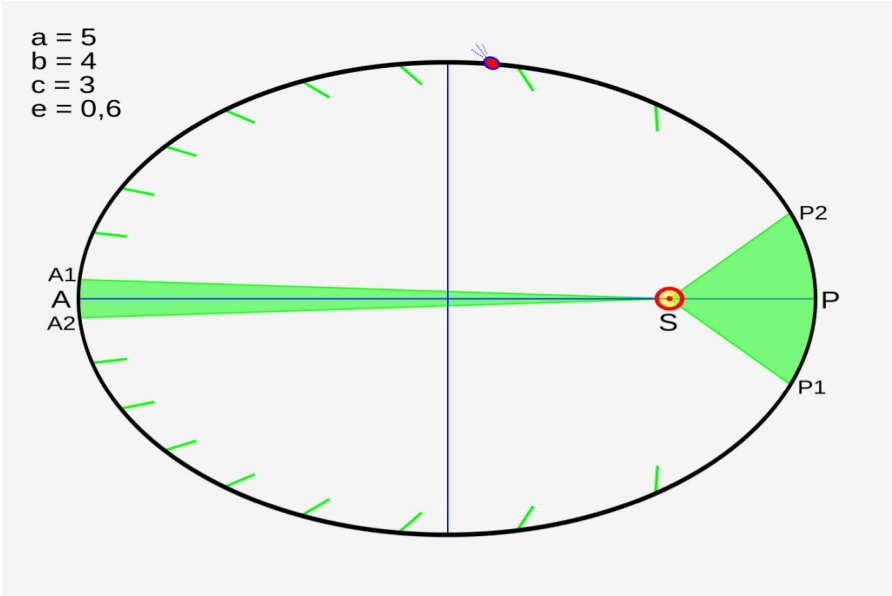

NEPTUNE
JUPITER
URANUS
VÉNUS
MERCURE
SATURNE
TERRE
MARS
20 : 12 16 FÉV 2010

- Première loi de Kepler (1609)

Les trajectoires sont des ellipses

- Deuxième loi de Kepler (1609)

Loi des aires



- Troisième loi de Kepler (1618)

$$T = k\, R\sqrt{R}$$

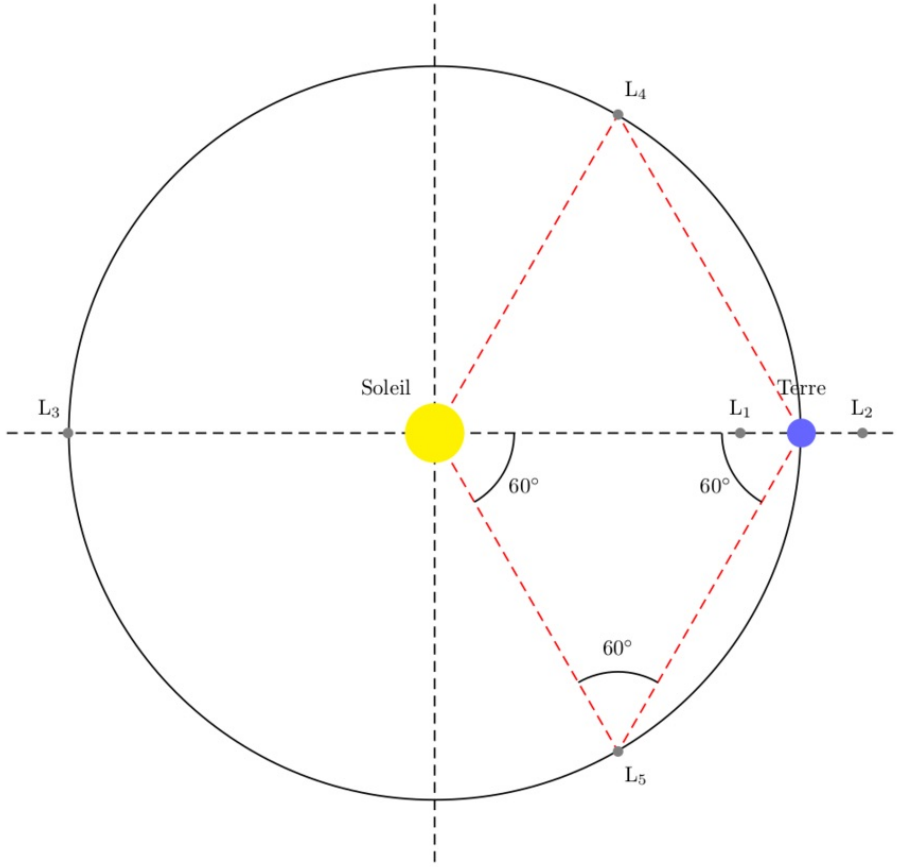
Neptune

Découvert à l'observatoire de Berlin en 1846 à la suite de calculs d'Urbain Le Verrier en 1839 (étude de la trajectoire d'Uranus)

Problème des trois corps


Animation de synthèse 3D Simone Gerlier
Musique Dexter Britain - The Time To Run Finale

Points de Lagrange

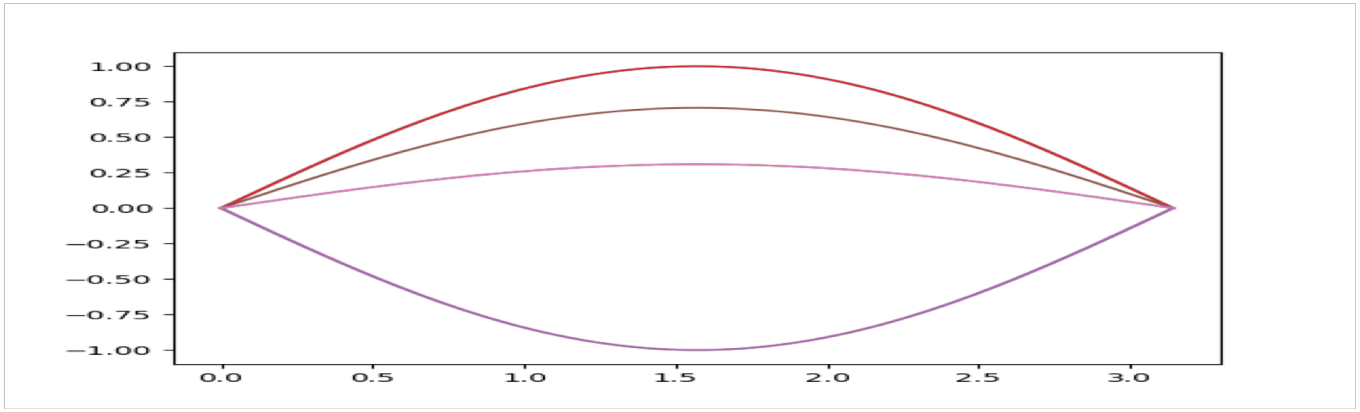


Positions des 5 points de Lagrange

Musique

Cordes vibrantes

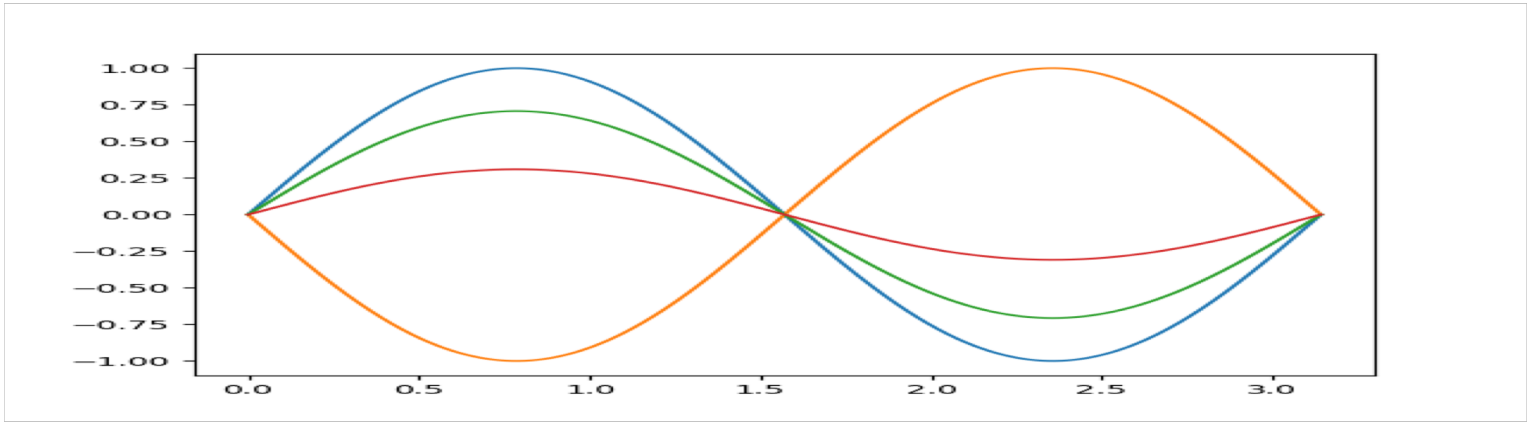
corde à vide



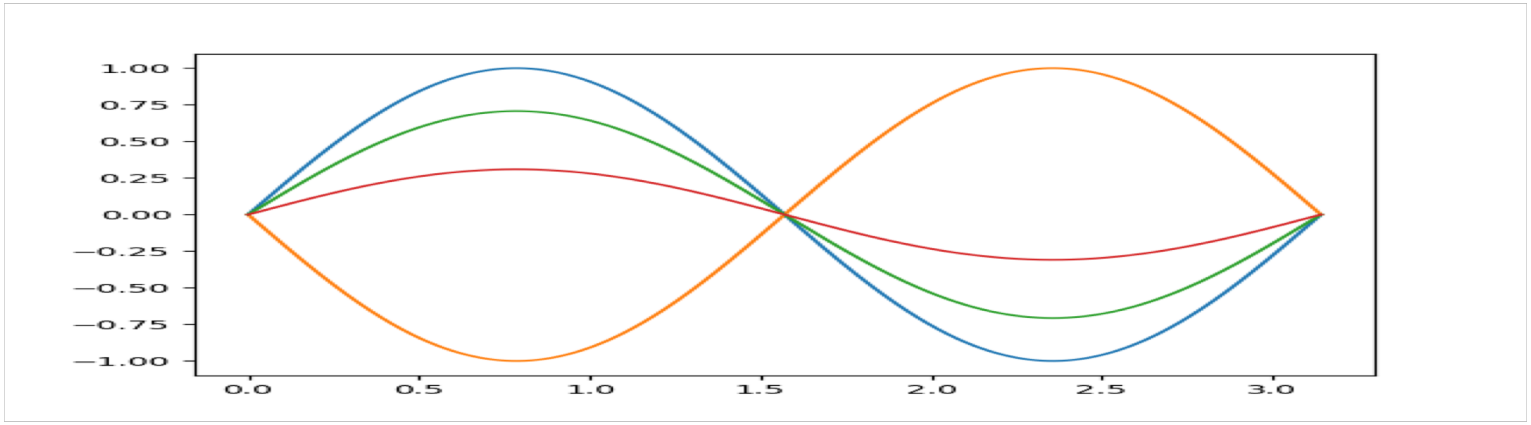
La 3 = 440 Hz

Sol 2 ≈ 196 Hz

Un nœud

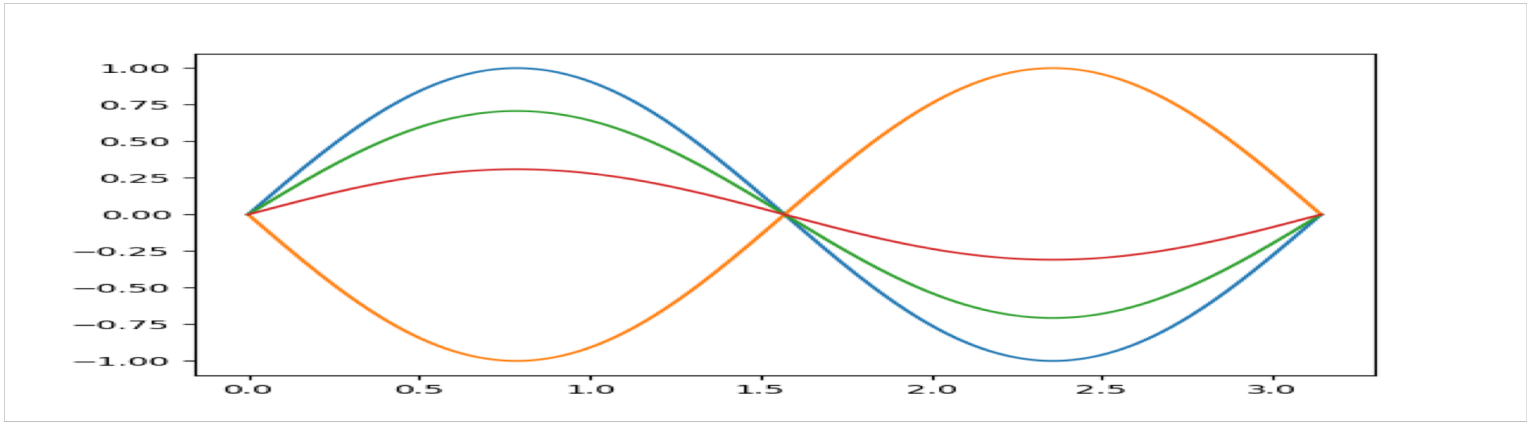


Un nœud



Sol 3 ≈ 392 Hz

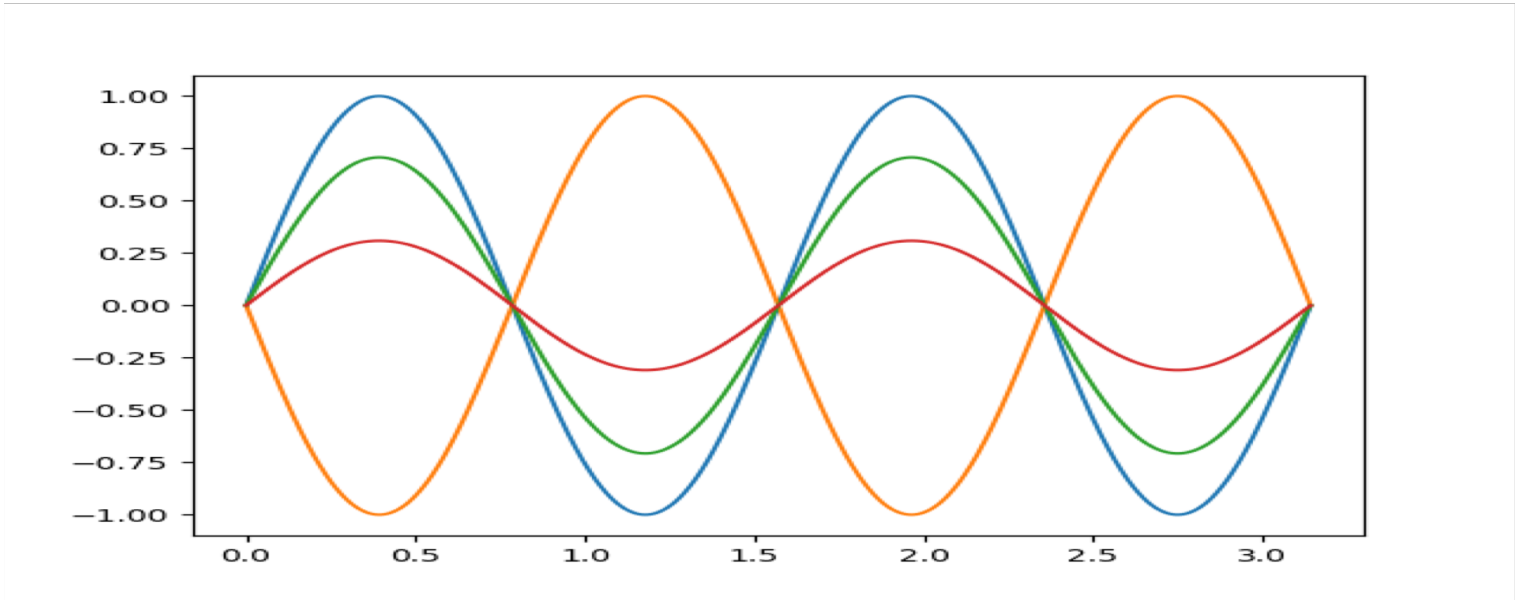
Un nœud



Sol 2 ≈ 196 Hz

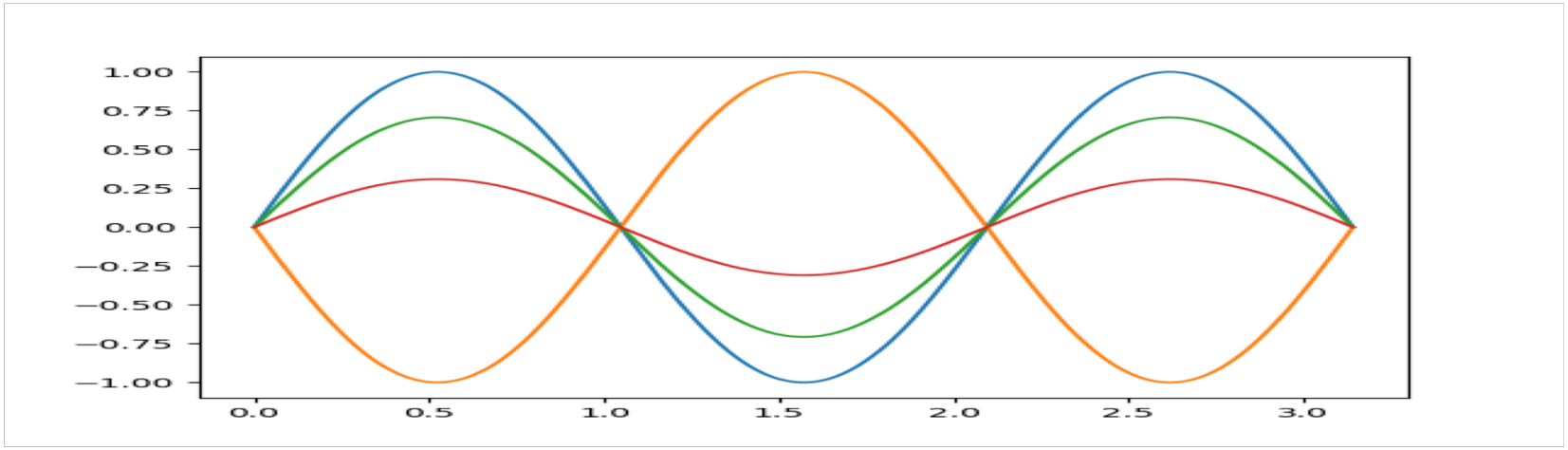
Sol 3 ≈ 392 Hz

Trois nœuds



$$\text{Sol}\,2 \approx 196\ \text{Hz}$$
$$\text{Sol}\,3 \approx 382\ \text{Hz}$$
$$\text{Sol}\,4 \approx 764\ \text{Hz}$$

Deux nœuds



Deux nœuds

Ré 3 ≈ 294 Hz

Sol 2 ≈ 196 Hz

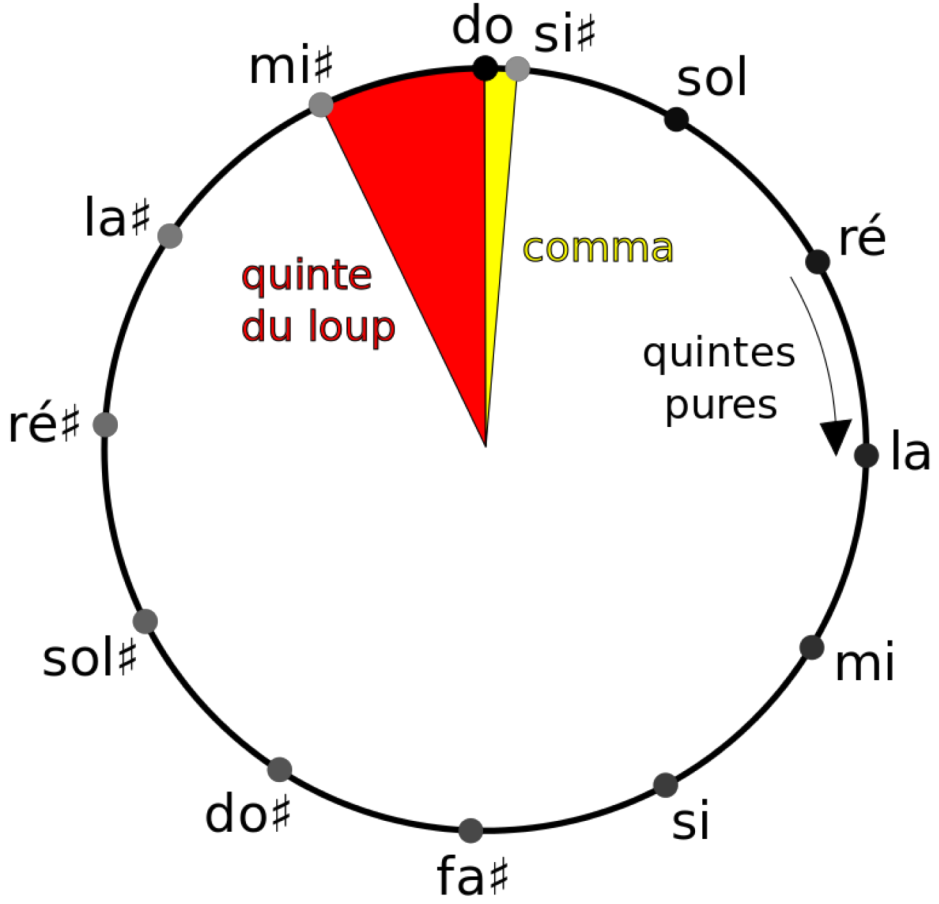
Ré 4≈ 588 Hz

Ré 3 ≈ 294 Hz

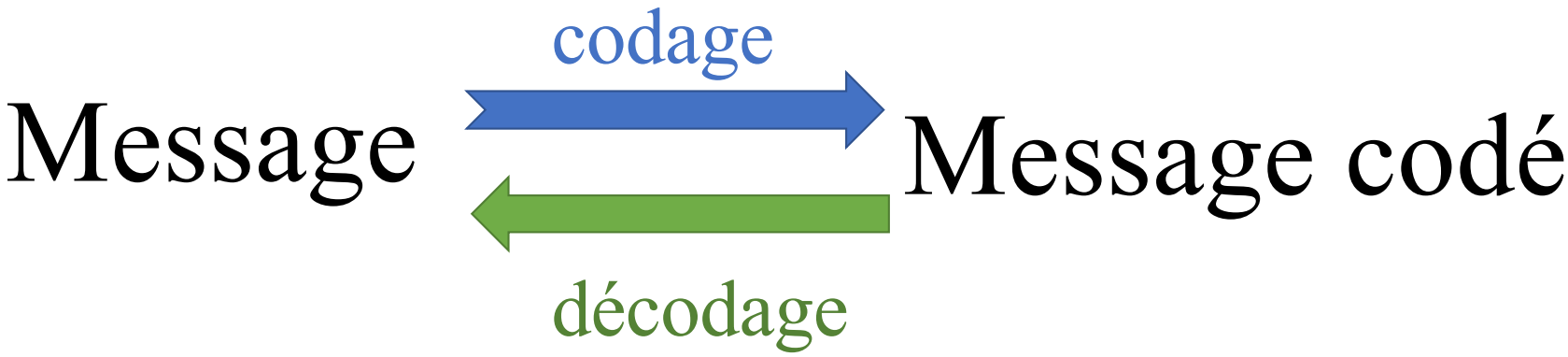
Quinte juste

rapport de fréquences = 3/2

Quinte du loup



Cryptographie


codage
Message
Message codé
décodage

Codage de César

décalage d'une lettre

- a → b
- b → c

…

- x → y
- y → z
- z → a

yves devient : zwft

Codage de César

décalage de 3 lettres

- a → d
- b → e

…

- w → z
- x → a
- y → b
- z → c

yves devient : byhv

décalage de 3 lettres

- Si le message codé est :

qlfroh

décalage de 3 lettres

- Si le message codé est :

qlfroh

- On peut décoder :

nicole

décalage de 3 lettres

- Si le message codé est :

qlfroh

- On peut décoder :

nicole

- Si on connaît le nombre de lettres à décaler, le décodage est facile

Et si on ne sait pas de combien de lettres on doit décaler ?
Réponse codée de Daniel :

yt ct bt egdcdcrt eph

Les réponses possibles :

1 : xs bs as dfcbcbqs dog
2 : wr ar zr cebabapr cnf
3 : vq zq yq bdazazoq bme
4 : up yp xp aczyzynp ald
5 : to xo wo zbyxyxmo zkc
6 : sn wn vn yaxwxwln yjb
7 : rm vm um xzwvwvkm xia
8 : ql ul tl wyvuvujl whz
9 : pk tk sk vxututik vgy
10 : oj sj rj uwtstshj ufx
11 : ni ri qi tvsrsrgi tew
12 : mh qh ph surqrqfh sdv
13 : lg pg og rtqpqpeg rcu
14 : kf of nf qspopodf qbt
15 : je ne me prononce pas
16 : id md ld oqnmnmbd ozr
17 : hc lc kc npmlmlac nyq
18 : gb kb jb molklkzb mxp
19 : fa ja ia lnkjkjya lwo
20 : ez iz hz kmjijixz kvn
21 : dy hy gy jlihihwy jum
22 : cx gx fx ikhghgvx itl
23 : bw fw ew hjgfgfuw hsk
24 : av ev dv gifefetv grj
25 : zu du cu fhededsu fqi

Les réponses possibles :

1 : xs bs as dfcbcbqs dog
2 : wr ar zr cebabapr cnf
3 : vq zq yq bdazazoq bme
4 : up yp xp aczyzynp ald
5 : to xo wo zbyxyxmo zkc
6 : sn wn vn yaxwxwln yjb
7 : rm vm um xzwvwvkm xia
8 : ql ul tl wyvuvujl whz
9 : pk tk sk vxututik vgy
10 : oj sj rj uwtstshj ufx
11 : ni ri qi tvsrsrgi tew
12 : mh qh ph surqrqfh sdv
13 : lg pg og rtqpqpeg rcu
14 : kf of nf qspopodf qbt
15 : je ne me prononce pas
16 : id md ld oqnmnmbd ozr
17 : hc lc kc npmlmlac nyq
18 : gb kb jb molklkzb mxp
19 : fa ja ia lnkjkjya lwo
20 : ez iz hz kmjijixz kvn
21 : dy hy gy jlihihwy jum
22 : cx gx fx ikhghgvx itl
23 : bw fw ew hjgfgfuw hsk
24 : av ev dv gifefetv grj
25 : zu du cu fhededsu fqi

Codage de Vigenère (XVI^{e} siècle)

On dispose d'une clé de codage qui permet de préciser de combien de lettres on doit décaler, position par position.

Clé : amopa,

texte à coder : c i n q m a r s

clé de codage : a m o p a a m o p

1 13 15 16 1 1 13 15 16

texte codé : d v c g n n h i

- a = 1ère lettre de l'alphabet, la première lettre du texte à coder est décalée d'une unité, c devient d
- m = 13ème lettre de l'alphabet, la 2ème lettre du texte à coder est décalée de 13 unités, i devient v
- o = 15ème lettre de l'alphabet… n devient c

…

- Facile à décoder si on connaît la clé
- Difficile dans le cas contraire

Codages à sens unique

- Tout le monde dispose de la méthode pour coder
- Pour décoder, il faut disposer d'une clé de décodage

Système RSA (brevet MIT, 1977)

- Ronald Rivest
- Adi Shamir
- Leonard Adleman

- La clé publique est fournie par deux nombres : n, produit de deux nombres premiers très grands p et q ($n = pq$) et un autre entier d

  mais p et q restent secrets

- Pour décoder, on a besoin d'un troisième entier e qui permet de décoder

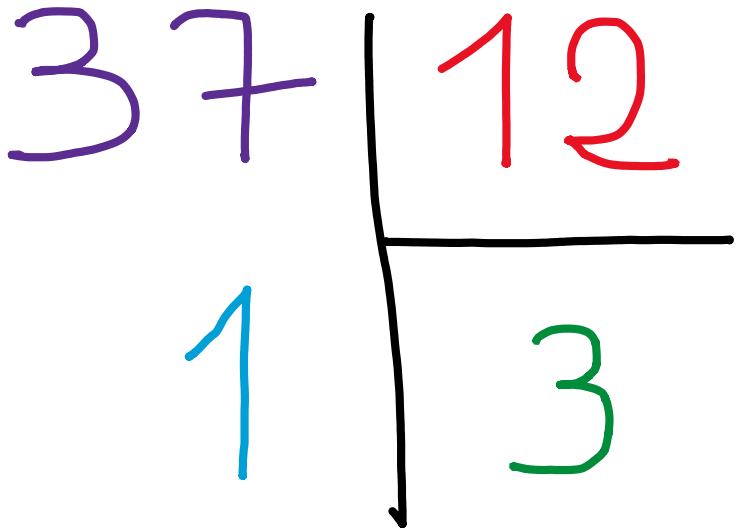
  et presque impossible à trouver si on ne connaît pas p et q

- On commence par transformer le message à coder en un grand nombre, en associant à chaque lettre un numéro :
  a → 01
  b → 02

  …
  z → 26
- A l'espace et aux signes de ponctuation on associe 00

cinq mars devient ainsi : 03 09 14 17 00 13 01 18 19
A = 030 914 170 013 011 819

Division euclidienne



37 = dividende

12 = diviseur

3 = quotient

1 = reste

Codage, décodage

- $A = 030\,914\,170\,013\,011\,819.$
- On calcule A^d (c'est-à-dire $A * A * A * \cdots * A$) et on divise le résultat obtenu par n

- On récupère le reste r de cette division, r sera le message codé

- Pour décoder, on calcule r^e, on divise par n, et on récupère le reste de cette division, c'est A.

Avantages du système

- On travaille sur le message en entier, et non lettre par lettre.
- Pour décoder, il suffit de connaître e (celui qui convient), mais si on ne connaît que n et d, c'est très difficile (à moins de connaître p et q)

Dans la pratique, p et q sont des nombres qui s'écrivent avec 300 chiffres, et donc n s'écrit avec 600 chiffres.

Un exemple

- Daniel a fini par accepter de répondre à Nicole. Il lui a envoyé le message codé suivant :

  03 459 886 326 948 034 145 627 850

La réponse de Daniel était

…….

Ca m’étonnerait

Mes données

- p=529 178 053 429 087
- q=621 397 455 395 323
- n=328 829 895 851 884 940 389 331 960 101
- d = 301 001 300 052 015 141 405 180 109
- e = 65 606 253 785 340 541 849 360 978 899

Mes données

- p=529 178 053 429 087
- q=621 397 455 395 323
- n=328 829 895 851 884 940 389 331 960 101
- d = 301 001 300 052 015 141 405 180 109
- e = 65 606 253 785 340 541 849 360 978 899

- Temps pour trouver e estimé à 3 ans.

Littérature

Maths vues par des non mathématiciens

Lautréamont (1846 – 1870)

Ô mathématiques sévères, je ne vous ai pas oubliées depuis que vos savantes leçons, plus douces que le miel, filtrèrent dans mon cœur, comme une onde rafraîchissante. J'aspirais instinctivement, dès le berceau, à boire à votre source, plus ancienne que le soleil, et je continue encore de fouler le parvis sacré de votre temple solennel, moi, le plus fidèle de vos initiés.

...

(8 pages)

....

Ô mathématiques saintes, puissiez-vous, par votre commerce perpétuel, consoler le reste de mes jours de la méchanceté de l'homme et de l'injustice du Grand-Tout !"

Jules Supervielle (1884 – 1960)

Mathématiques

Quarante enfants dans une salle,
Un tableau noir et son triangle.
Un grand cercle hésitant et sourd
Son centre bat comme un tambour.

Des lettres sans mots ni patrie
Dans une attente endolorie.

Le parapet dur d'un trapèze,
Une voix qui s'élève et s'apaise
Et le problème furieux
Se tortille et se mord la queue.

La mâchoire d'un angle s'ouvre.
Est-ce une chienne ?

Est-ce une louve ?
Et tous les chiffres de la terre,
Tous ces insectes qui défont
Et qui refont leur fourmilière
Sous les yeux fixes des garçons.

Gustave Flaubert (1821 – 1880)

Dictionnaire des idées reçues

- **Mathématiques** Dessèchent le cœur

Maths vues par des mathématiciens

Jacques Pelletier du Mans (1517 – 1582)

A ceux qui blâment les mathématiques

Tant plus je vois que vous blâmez
Sa noble discipline,
Plus à l'aimer vous enflammez
Ma volonté encline.

Car ce qui a moins de suivants,
D'autant plus il est rare,
Et est la chose entre vivants
Dont on est plus avare.

Il n'est pas en votre puissance
Qu'y soyez adonnés ;
Car le ciel dès votre naissance
Vous en a détournés ;

Ou ayant persuasion
Que tant la peine en coûte,
Est la meilleure occasion
Qui tant vous en dégoûte.

Le ciel orné de tels flambeaux
N'est-il point admirable ?
La notice de corps si beaux
N'est-elle désirable ?

Du céleste ouvrage l'objet,
Si vrai et régulier,
N'est-il sur tout autre sujet
Beau, noble et singulier ?

Robert Musil (1880 – 1942)

Les Désarrois de l'élève Törless

Pendant la leçon de mathématiques, une idée était venue à Törless.

Depuis quelques jours déjà, il suivait toutes les leçons avec un intérêt particulier, en disant : « Si tout cela doit vraiment nous préparer à la vie, comme ils disent, il doit bien s'y trouver aussi quelque reflet de ce que je poursuis. »

Quand il s'était dit cela, il pensait précisément aux mathématiques, à cause des réflexions qu'il avait faites sur l'infini.

Et tout à coup, en pleine leçon, ç'avait été comme un éclair brûlant dans sa tête. L'heure avait à peine sonné qu'il était allé s'asseoir à côté de Beineberg, le seul avec qui il pût parler ainsi.

- Dis-moi, tu as tout compris dans cette histoire ?

- Quelle histoire ?

- Celle des nombres imaginaires.

- Oui. Ce n'est pas si compliqué que ça. Il suffit de se rappeler que l'unité de calcul, c'est la racine carrée de moins un.

- Justement, cette racine n'existe pas ! Tout nombre, qu'il soit positif ou négatif, donne, élevé au carré, un…

Robert Musil

L'homme sans qualités

D'Ulrich, en revanche, on pouvait dire au moins ceci en toute certitude, qu'il aimait les mathématiques à cause de ceux qui ne pouvaient les souffrir. Il était moins scientifiquement qu'humainement amoureux de la science.

Boris Vian (1920 – 1959)

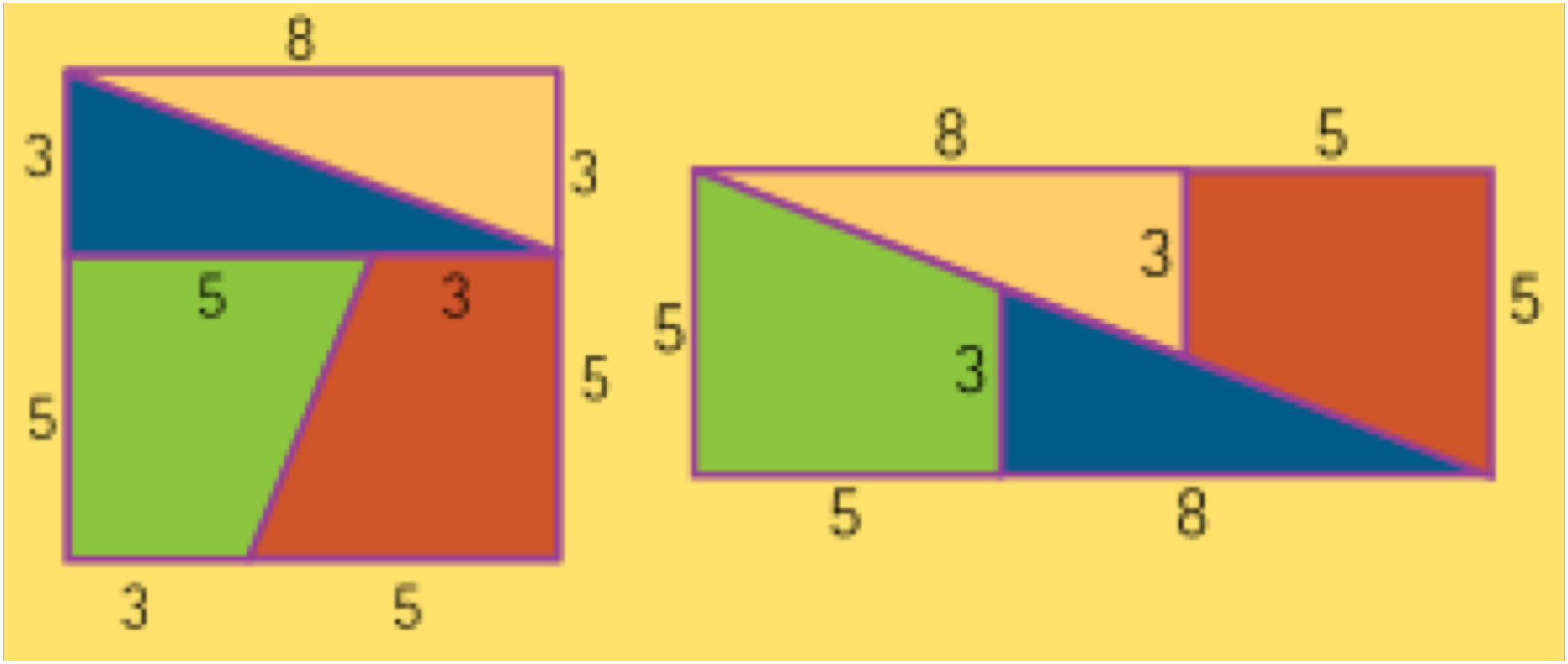
C'est très joli, c'est extrêmement connu et extrêmement courant de dire en français, de dire avec orgueil : « Moi, je ne comprends rien aux maths. » Personnellement, je fais la réflexion suivante : « Si je ne comprends rien aux maths, j'aurais plutôt honte de le dire. « Se présenter de but en blanc comme un imbécile n'est pas le meilleur moyen de se présenter. Un type-qui-ne-comprend-rien-aux-maths est un imbécile fieffé, un point c'est tout.

Lewis Carroll Charles Lutwidge Dodson (1832 – 1898)

Enigme de dessert

Carroll la présentait comme ceci : « Prenez deux gobelets, l'un qui contient 50 cuillérées de cognac, l'autre 50 cuillérées d'eau pure. Prélevez dans le premier une cuillérée de cognac ; transférez-la, sans la renverser, dans le second gobelet et remuez. Puis, prenez une cuillérée du mélange et reportez-le, sans le renverser, dans le premier gobelet. Ma question est : si vous considérez l'ensemble de l'opération, a-t-il été transféré plus de cognac du premier gobelet au second, ou plus d'eau du second au premier? »

Aire du carré : 64
Aire du rectangle : 65

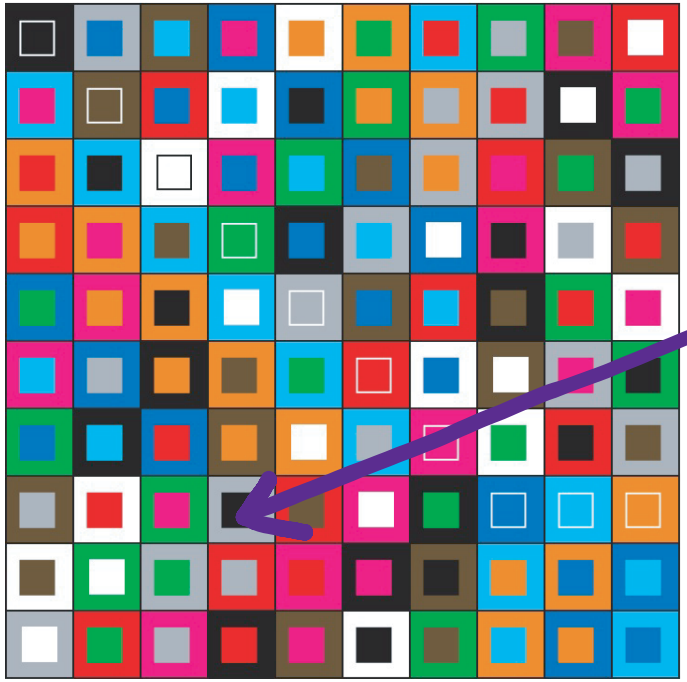


Oulipo

Ouvroir de littérature potentielle

- François Le Lionnais
- Raymond Queneau
- Italo Calvino
- Georges Perec

La Vie mode d'emploi



Carré bilatin d'ordre 10

Chapitre 23 : une citation de Verne, une de Vallès

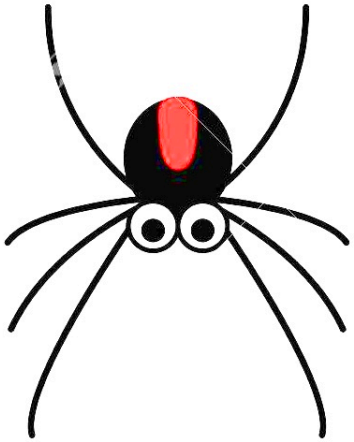
Le personnage principal est une formule

La Formule de Stokes, roman
Michèle Audin

- 1er janvier 1862
- 5 janvier 1857
- 9 janvier 1895
- 13 janvier 2012
- 16 janvier 1898
- ...

Cédric Villani

Théorème vivant



Date: Mon, 19 Jan 2009 13:42:27 +0100
From: Clement Mouhot <clement.mouhot@ceremade.dauphine.fr>
To: Cedric Villani <Cedric.VILLANI@umpa.ens-lyon.fr>
Subject: Re: transfert

Salut Cedric,

ca devient de plus en plus monstrueux;) !!

*

Extraits du fichier global-3 (18 janvier 2009)

4.7 Bihybrid norms

We shall be led to use the following more complicated norms :

Définition 4.15. We define the space $\mathcal{Z}^{(\lambda,\lambda'),\mu;p}_{(\tau,\tau')}$ by

$$\|f\|_{\mathcal{Z}^{(\lambda,\lambda'),\mu;p}_{(\tau,\tau')}} = \sum_n \sum_m \frac{1}{n!(n-m)!}$$

$$\times \left\| \left(\lambda(\nabla_v + 2i\pi\tau k)\right)^m \left(\lambda'(\nabla_v + 2i\pi\tau' k)\right)^{n-m} \widehat{g}(k,v) \right\|_{L^p(dv)}.$$

(...)

After trial and error, the best we could do was to recover this decay in the "bi-hybrid" norms described in Subsection 4.7 :

Proposition 5.6 (regularity-to-decay estimate in hybrid spaces). *Let $f = f_t(x,v)$, $g = g_t(x,v)$, and*

$$\sigma(t,x) = \int_0^t \int f_\tau(x - v(t-\tau), v)\, g_\tau(x - v(t-\tau), v)\, dv\, d\tau.$$

Then

$$\|\sigma(t)\|_{\mathcal{F}^{\lambda+\mu}} \leq \left(\frac{C}{\lambda - \lambda}\right) \sup_{0<\tau<t} \|f_\tau\|_{\mathcal{Z}^{\lambda,\mu;1}_\tau} \sup_{0<\tau<t} \|g_\tau\|_{\mathcal{Z}^{(\lambda,\lambda'),\mu;\cdot}_{(\tau,0)}}$$

CHAPITRE 13

Princeton, le 21 janvier 2009

Grâce à l'astuce trouvée le soir de la visite au Muséum, j'ai pu repartir. Et aujourd'hui, je suis plein d'espoir et d'effroi mêlés. Face à une difficulté majeure, j'ai fait quelques calculs explicites et j'ai fini par comprendre comment gérer un terme trop gros. En même temps, je suis saisi de vertige devant la complexité de ce qui s'ouvre à moi.

La brave équation de Vlasov, que je croyais commencer à connaître, fonctionnerait donc par à-coups ? Le calcul montre, sur le papier, qu'il y a des temps particuliers où elle réagit trop vite par rapport aux stimuli. Je n'ai jamais entendu parler de quelque chose de tel, ce n'est pas dans les articles et les livres que j'ai lus. Mais en tout cas on avance.

*

Date: Wed, 21 Jan 2009 23:44:49 -0500
From: Cedric VILLANI <Cedric.VILLANI@umpa.ens-lyon.fr>
To: Clement Mouhot <clement.mouhot@ceremade.dauphine.fr>
Subject: !!

Ca y est, apres des heures a patauger lamentablement je suis persuade d'avoir identifie la raison qui cancelle le O(t) dont je me plaignais au telephone aujourd'hui.
C'est MONSTRUEUX !

Quelques romans

- Antoine Billot : *La conjecture de Syracuse*
- Denis Guedj : *Le théorème du perroquet*
  La Méridienne
- Guillermo Martinez : *Mathématique du crime*
- Umberto Eco : *Le nom de la rose*
- Edgar Poe : *Double assassinat dans la rue Morgue*
- Paolo Giordano : *La solitude des nombres premiers*

Une biographie

François-Henri Désérable :
Évariste