Les mathématiques : utiles et vivantes

Daniel PERRIN

Forum des mathématiques, Aix-en-Provence, 3 février 2017

NOS SPONSORS

Sans eux, rien n'est possible

AIX EN PROVENCE LA VILLE

Aix*Marseille université

académie d'aix-marseille

irem

COUDOUX

maths pour tous

Rotary Pays d'Aix

ROTARY INTERNATIONAL

Allergan

BIBLIOTHÈQUE M MÉJANES

GALDERMA

Les 2G

GRAND HÔTEL ROI RENÉ

Éguilles

france bleu provence

ALPES PROVENCE

LCA

LES COMPÉT...

Réalisation Agence Kaiman - 04 42 600 120

Introduction

Les mathématiques sont utiles

- Dans les sciences et les techniques
- Dans la vie courante
- L'apprentissage du raisonnement

Les mathématiques qui ne servent pas aujourd'hui serviront peut-être demain

- Les coniques
- Les nombres premiers

Les mathématiques sont vivantes

- Problèmes ouverts
- Problèmes résolus

Introduction

- Les mathématiques ont mauvaise presse, ce n'est pas nouveau.

Introduction

- Les mathématiques ont mauvaise presse, ce n'est pas nouveau.
- Qui a écrit :
  J'étais alors en proie à la mathématique ...
  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 ?

Introduction

- Les mathématiques ont mauvaise presse, ce n'est pas nouveau.
- Qui a écrit :
  J'étais alors en proie à la mathématique ...
  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 ?
- Qui a dit :
  Et la racine de carrée de 25 ? Ça t'a déjà sorti d'une galère ce truc ? Tu es déjà sorti d'une soirée en te disant "heureusement qu'on la connaissait cette racine sinon on était dans la merde" ?

Quelques éminents détracteurs

- Certains mettent en doute leur utilité. En juillet 2012 Andrew Hacker* dans le New-York Times : *faut-il arrêter d'enseigner les mathématiques (et notamment l'algèbre) à l'école ?*

Quelques éminents détracteurs

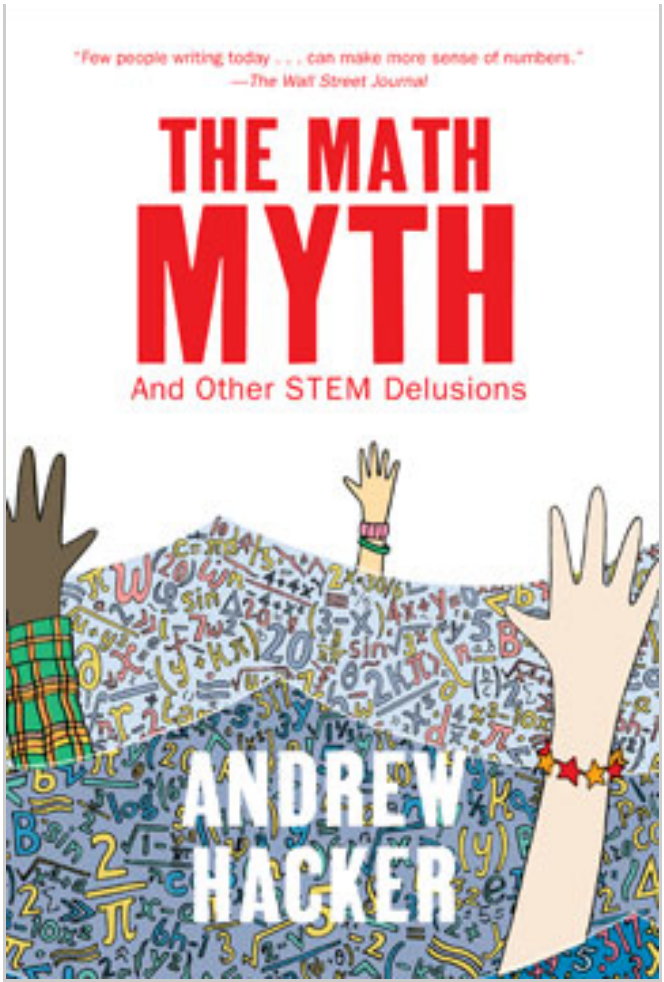
- Certains mettent en doute leur utilité. En juillet 2012 Andrew Hacker* dans le New-York Times : *faut-il arrêter d'enseigner les mathématiques (et notamment l'algèbre) à l'école ?*
- D'autres pensent qu'elles sont mortes (Claude Allègre : *L'ordinateur va nous conduire à reconsidérer les mathématiques comme un auxiliaire des sciences*).

Quelques éminents détracteurs

- Certains mettent en doute leur utilité. En juillet 2012 Andrew Hacker* dans le New-York Times : *faut-il arrêter d'enseigner les mathématiques (et notamment l'algèbre) à l'école ?*
- D'autres pensent qu'elles sont mortes (Claude Allègre : *L'ordinateur va nous conduire à reconsidérer les mathématiques comme un auxiliaire des sciences*).
- D'autres enfin dénoncent la dictature* qu'elles exercent dans l'enseignement.

Quelques éminents détracteurs

- Certains mettent en doute leur utilité. En juillet 2012 Andrew Hacker* dans le New-York Times : *faut-il arrêter d'enseigner les mathématiques (et notamment l'algèbre) à l'école ?*
- D'autres pensent qu'elles sont mortes (Claude Allègre : *L'ordinateur va nous conduire à reconsidérer les mathématiques comme un auxiliaire des sciences*).
- D'autres enfin dénoncent la dictature* qu'elles exercent dans l'enseignement.
- Nous allons tenter (modestement) de répondre à tout cela.


"Few people writing today . . . can make more sense of numbers."
—The Wall Street Journal
THE MATH
MYTH
And Other STEM Delusions
ANDREW
HACKER


Le Monde DE L'ÉDUCATION
cinéclasse
Non
à la dictature
des maths !
Quand les étudiants notent leurs profs
Le Sud à l'abandon
La fabrique Brighelli
Octobre 2006 N° 351

Les mathématiques sont utiles

Les mathématiques sont utiles dans les sciences et les techniques

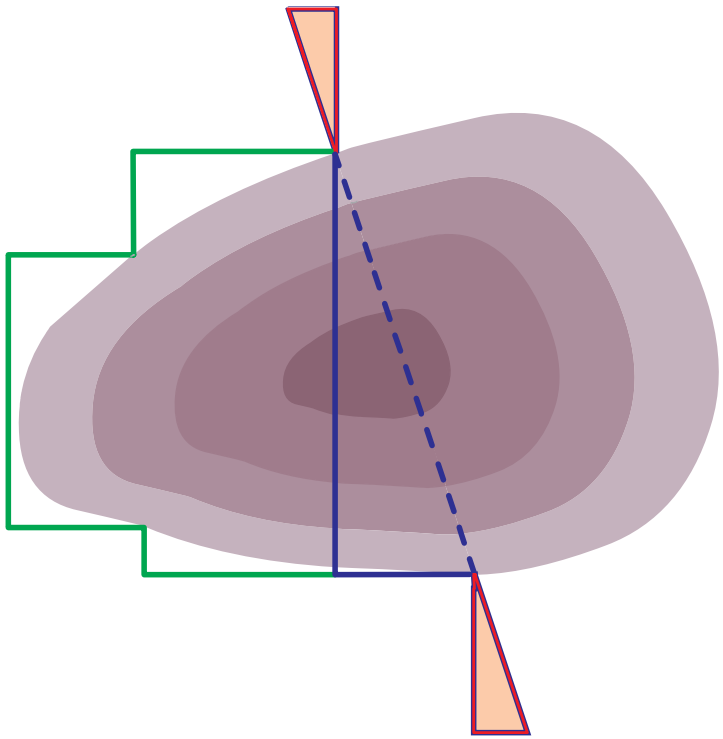
Il n'est pas facile de dire à quoi servent les mathématiques. Pourtant elles sont présentes partout, dans les sciences, les outils technologiques, mais aussi la médecine, l'économie, etc. Mais on est confronté à deux difficultés :

- elles ne sont pas apparentes,
- elles ne sont pas faciles.

Nous allons essayer de donner quelques exemples, en restant à un niveau relativement élémentaire.

À quoi sert la géométrie ?

Un exemple historique : la construction du tunnel de Samos selon Héron d'Alexandrie (voir Tom Apostol, *The tunnel of Samos* sur Internet)



À quoi servent les fonctions ?

Parmi les thèmes que l'on étudie au lycée le plus important est sans doute celui des fonctions. En effet, les notions de variable et de fonction, qui traduisent le fait qu'une quantité **dépend** d'un ou plusieurs paramètres, sont essentielles dans tous les domaines des sciences (expérimentales, humaines, économiques) et même dans la vie courante.

À quoi servent les fonctions : le calcul différentiel et intégral

Pour étudier les fonctions, les notions de dérivée et d'intégrale (inventées par Newton et Leibniz vers 1650) fournissent un outil fantastique, qui constitue un progrès essentiel de l'humanité, ramenant au niveau d'un lycéen des problèmes autrefois très difficiles. C'est le cas du calcul de l'aire du segment de parabole ou du volume de la sphère, réalisés par Archimède, des sommets des mathématiques de l'antiquité, qui deviennent des exercices pour un élève de terminale, voir sur ma page web la conférence de mars 2012 à l'IREM de Paris 7.

À quoi servent les fonctions, suite

Les fonctions apparaissent notamment au travers des équations différentielles qui relient une fonction et sa dérivée. Par exemple l'équation $y' = ay$ de la radioactivité (qui définit les fonctions exponentielles) est utilisée en archéologie (datation au Carbone 14), ou pour déterminer l'âge de la terre (datation au Rubidium-Strontium) ou encore pour détecter des faux en peinture, témoin la belle histoire de Van Meegeren. Voir la conférence aux journées APM 2016 sur ma page web pour des détails.

Vermeer et Van Meegeren

- Johannes Vermeer (dit Vermeer de Delft) (1632-1675). Deux exemples de tableaux : la jeune fille à la perle et la vue de Delft.

Vermeer et Van Meegeren

- Johannes Vermeer (dit Vermeer de Delft) (1632-1675). Deux exemples de tableaux : la jeune fille à la perle et la vue de Delft.
- Han Van Meegeren, né en 1889, est un peintre néerlandais de second ordre, marchand de tableaux à ses heures.

Vermeer et Van Meegeren

- Johannes Vermeer (dit Vermeer de Delft) (1632-1675). Deux exemples de tableaux : la jeune fille à la perle et la vue de Delft.
- Han Van Meegeren, né en 1889, est un peintre néerlandais de second ordre, marchand de tableaux à ses heures.
- En mai 1945, il est arrêté pour avoir vendu à Hermann Göring un tableau de Vermeer : *Jésus et la femme adultère*.

Vermeer et Van Meegeren

- Johannes Vermeer (dit Vermeer de Delft) (1632-1675). Deux exemples de tableaux : la jeune fille à la perle et la vue de Delft.
- Han Van Meegeren, né en 1889, est un peintre néerlandais de second ordre, marchand de tableaux à ses heures.
- En mai 1945, il est arrêté pour avoir vendu à Hermann Göring un tableau de Vermeer : *Jésus et la femme adultère*.
- Il risque la peine de mort pour haute trahison.

Vermeer et Van Meegeren

- Johannes Vermeer (dit Vermeer de Delft) (1632-1675). Deux exemples de tableaux : la jeune fille à la perle et la vue de Delft.
- Han Van Meegeren, né en 1889, est un peintre néerlandais de second ordre, marchand de tableaux à ses heures.
- En mai 1945, il est arrêté pour avoir vendu à Hermann Göring un tableau de Vermeer : *Jésus et la femme adultère*.
- Il risque la peine de mort pour haute trahison.
- Alors il révèle : *C'est un faux, c'est moi qui l'ai fait !* et ajoute qu'il a ainsi peint de nombreux autres faux Vermeer.

Vermeer et Van Meegeren (suite)

- Manque de chance, personne ne le croit. D'autant que parmi les faux qu'il revendique se trouvent *Les disciples d'Emmaüs*, vendus en 1938 au musée Boymans de Rotterdam pour une somme équivalente à 4 millions de dollars actuels et authentifiés par le plus grand expert de l'époque, Abraham Brédius.

Vermeer et Van Meegeren (suite)

- Manque de chance, personne ne le croit. D'autant que parmi les faux qu'il revendique se trouvent *Les disciples d'Emmaüs*, vendus en 1938 au musée Boymans de Rotterdam pour une somme équivalente à 4 millions de dollars actuels et authentifiés par le plus grand expert de l'époque, Abraham Brédius.
- Voilà ce que dit Bredius : *Grâce à Dieu, cette œuvre magnifique est sortie de l'ombre où elle se trouvait, immaculée, intacte comme si elle venait tout droit de l'atelier de l'artiste* et aussi *Nous avons ici un chef-d'œuvre, je dirais LE chef-d'oeuvre de Vermeer, un de ses tableaux les plus grands par ses dimensions, une œuvre totalement différente de toutes les autres, et dont pourtant chaque pouce ne peut être que de Vermeer.*

Vermeer et Van Meegeren (suite)

- Alors, pour convaincre les incrédules, dans sa cellule, entre juillet et septembre 1945, Van Meegeren peint un autre faux Vermeer *Jésus parmi les docteurs.*

Vermeer et Van Meegeren (suite)

- Alors, pour convaincre les incrédules, dans sa cellule, entre juillet et septembre 1945, Van Meegeren peint un autre faux Vermeer *Jésus parmi les docteurs.*
- Cela ébranle les magistrats. Une commission d'enquête est nommée, dirigée par Paul Coremans, qui reconnaît que les tableaux sont des faux. En octobre 1947 Van Meegeren est condamné à un an de prison ... pour faux.

Vermeer et Van Meegeren (suite)

- Alors, pour convaincre les incrédules, dans sa cellule, entre juillet et septembre 1945, Van Meegeren peint un autre faux Vermeer *Jésus parmi les docteurs.*
- Cela ébranle les magistrats. Une commission d'enquête est nommée, dirigée par Paul Coremans, qui reconnaît que les tableaux sont des faux. En octobre 1947 Van Meegeren est condamné à un an de prison ... pour faux.
- Malheureusement, il meurt d'une crise cardiaque en décembre 1947.

Vermeer et Van Meegeren (suite et fin)

- L'histoire ne s'arrête pas là car certains experts refusent d'admettre qu'ils se sont trompés.

Vermeer et Van Meegeren (suite et fin)

- L'histoire ne s'arrête pas là car certains experts refusent d'admettre qu'ils se sont trompés.
- Ce n'est qu'en 1967 que des chercheurs de l'université de Pittsburgh apportent une preuve définitive que les prétendus Vermeer ne pouvaient pas dater de cette époque, à l'aide d'une datation au plomb, donc de la radioactivité et de la fonction exponentielle.

Les recettes du dernier lapin (1)

Pour promouvoir les applications des mathématiques dans l'enseignement : étudier des situations pluridisciplinaires.

Dans la vie courante : la règle de trois

- Le problème de proportionnalité (ou de règle de trois) de ma voisine : la dotation des crèches.

Dans la vie courante : la règle de trois

- Le problème de proportionnalité (ou de règle de trois) de ma voisine : la dotation des crèches.
- Pour prendre conscience des difficultés rencontrées par certains avec les mathématiques, et notamment la règle de trois, voici des questions posées à deux (ex)-ministres :

Dans la vie courante : la règle de trois

- Le problème de proportionnalité (ou de règle de trois) de ma voisine : la dotation des crèches.
- Pour prendre conscience des difficultés rencontrées par certains avec les mathématiques, et notamment la règle de trois, voici des questions posées à deux (ex)-ministres :
- *Sachant que* 4 *stylos valent* $2,42$ *euros combien valent* 14 *stylos ?* (Pas de réponse)

Dans la vie courante : la règle de trois

- Le problème de proportionnalité (ou de règle de trois) de ma voisine : la dotation des crèches.
- Pour prendre conscience des difficultés rencontrées par certains avec les mathématiques, et notamment la règle de trois, voici des questions posées à deux (ex)-ministres :
- *Sachant que* 4 *stylos valent* $2,42$ *euros combien valent* 14 *stylos ?* (Pas de réponse)
- *Dix objets identiques coûtent 22 euros. Combien coûtent quinze de ces objets ?* (Réponse : 16,50 euros !)

Dans la vie courante : la règle de trois

- Le problème de proportionnalité (ou de règle de trois) de ma voisine : la dotation des crèches.
- Pour prendre conscience des difficultés rencontrées par certains avec les mathématiques, et notamment la règle de trois, voici des questions posées à deux (ex)-ministres :
- *Sachant que* 4 *stylos valent* $2,42$ *euros combien valent* 14 *stylos ?* (Pas de réponse)
- *Dix objets identiques coûtent 22 euros. Combien coûtent quinze de ces objets ?* (Réponse : 16,50 euros !)
- Ça se chante : *Mais comme dans la vie, je veux être ministre, moins je s'rai calé plus j'aurai d'valeur.*

Les limites de la règle de trois

- Un bassin de $10000\,l$ est pollué par $10\,kg$ d'un produit toxique. Le bassin est renouvelé en eau potable à raison de $1000\,l$ par heure. Le produit est dangereux pour la faune et la flore s'il reste plus de 6 heures à un taux de plus de $5\,kg$ pour $10000\,l$.

Les limites de la règle de trois

- Un bassin de $10000\,l$ est pollué par $10\,kg$ d'un produit toxique. Le bassin est renouvelé en eau potable à raison de $1000\,l$ par heure. Le produit est dangereux pour la faune et la flore s'il reste plus de 6 heures à un taux de plus de $5\,kg$ pour $10000\,l$.
- L'expert consulté (qui connaît la règle de trois, lui !) se veut rassurant :

  Il y a $10\,kg$ dans $10000\,l$. Chaque heure, dans les $1000\,l$ qui s'évacuent, il part $1/10$ du produit, donc $1\,kg$. Pas de problème, les $5\,kg$ seront largement évacués en $6\,h$.

Les limites de la règle de trois

- Un bassin de $10000\,l$ est pollué par $10\,kg$ d'un produit toxique. Le bassin est renouvelé en eau potable à raison de $1000\,l$ par heure. Le produit est dangereux pour la faune et la flore s'il reste plus de 6 heures à un taux de plus de $5\,kg$ pour $10000\,l$.
- L'expert consulté (qui connaît la règle de trois, lui !) se veut rassurant :

  Il y a $10\,kg$ *dans* $10000\,l$*. Chaque heure, dans les* $1000\,l$ *qui s'évacuent, il part* $1/10$ *du produit, donc* $1\,kg$*. Pas de problème, les* $5\,kg$ *seront largement évacués en* $6\,h$*.*
- Qu'en pensez-vous ?

Dans la vie courante : les pourcentages

- Le banquier à son client :

  Faites une affaire, le taux de notre livret d'épargne a augmenté de de 23 % !

  Bon d'accord, il avait baissé avant, mais attention, seulement de 20 %, donc vous y gagnez encore ...

Dans la vie courante : les pourcentages

- Le banquier à son client :

  Faites une affaire, le taux de notre livret d'épargne a augmenté de de 23 % !

  Bon d'accord, il avait baissé avant, mais attention, seulement de 20 %, donc vous y gagnez encore ...
- Qu'en pensez-vous ?

La ministre et les pourcentages

- Une (ex)-ministre a dit, à propos de ses adversaires politiques :

  Ils ont augmenté les impôts de 30% *dans le département, de* 58% *dans la région, soit en tout de* 88% *: c'est la double peine.*

La ministre et les pourcentages

- Une (ex)-ministre a dit, à propos de ses adversaires politiques :

  Ils ont augmenté les impôts de 30% *dans le département, de* 58% *dans la région, soit en tout de* 88% *: c'est la double peine.*
- Qu'en pensez-vous ?

Dans la vie courante : les impôts

- On entend souvent dire : *Oui, mais si je gagne plus, je vais franchir une tranche et au final, je vais y perdre.*
  Qu'en pensez-vous* ?

Dans la vie courante : les impôts

- On entend souvent dire : *Oui, mais si je gagne plus, je vais franchir une tranche et au final, je vais y perdre.*
  Qu'en pensez-vous* ?
- Une question plus délicate : quand a-t-on intérêt à demander le rattachement* d'un enfant majeur et non imposable au foyer fiscal de ses parents ?

Dans la vie courante : annuités d'un prêt

- Il n'est pas difficile (c'est un exercice classique de Terminale ES, mais cela impressionnera votre banquier) de calculer le montant des annuités a d'un prêt connaissant le capital prêté C, le taux annuel t et le nombre d'années N.

Dans la vie courante : annuités d'un prêt

- Il n'est pas difficile (c'est un exercice classique de Terminale ES, mais cela impressionnera votre banquier) de calculer le montant des annuités a d'un prêt connaissant le capital prêté C, le taux annuel t et le nombre d'années N.
- Voici le résultat :

$$a = \frac{Ct(1+t)^N}{(1+t)^N - 1}$$

Dans la vie courante : annuités d'un prêt

- Il n'est pas difficile (c'est un exercice classique de Terminale ES, mais cela impressionnera votre banquier) de calculer le montant des annuités a d'un prêt connaissant le capital prêté C, le taux annuel t et le nombre d'années N.
- Voici le résultat :

$$a = \frac{Ct(1+t)^N}{(1+t)^N - 1}$$

- Un exemple : on suppose que $C = 40000$ euros, $t = 5\%$ et $N = 15$ années. Quelle est l'annuité a ?

La nécessité de l'algèbre ?

- L'algèbre n'est pas toujours indispensable pour résoudre des problèmes. Par exemple : *Une basse-cour comporte des poules et des lapins, en tout il y a* 20 *animaux et ils ont* 56 *pattes. Combien y en a-t-il de chaque sorte ?*

La nécessité de l'algèbre ?

- L'algèbre n'est pas toujours indispensable pour résoudre des problèmes. Par exemple : *Une basse-cour comporte des poules et des lapins, en tout il y a* 20 *animaux et ils ont* 56 *pattes. Combien y en a-t-il de chaque sorte ?*
- En revanche, lorsque les choses sont plus complexes, comme dans l'exemple précédent, la formule

$$a = \frac{Ct(1+t)^N}{(1+t)^N - 1}$$

montre bien que l'utilisation des mathématiques nécessite une certaine maîtrise du calcul algébrique. C'est une des difficultés incontournables des mathématiques, n'en déplaise à Andrew Hacker.

Dans la vie courante : les statistiques et les sondages

- Lorsque les résultats d'un sondage sont donnés avec deux chiffres après la virgule (par exemple $51,17\%$) c'est – la plupart du temps – absurde, car l'incertitude, pour un sondage sur n personnes, est de l'ordre de $\sqrt{n}$. Sur 1000 personnes elle est donc de l'ordre de 30, c'est-à-dire de 3%.

Dans la vie courante : les statistiques et les sondages

- Lorsque les résultats d'un sondage sont donnés avec deux chiffres après la virgule (par exemple $51,17\%$) c'est – la plupart du temps – absurde, car l'incertitude, pour un sondage sur n personnes, est de l'ordre de $\sqrt{n}$. Sur 1000 personnes elle est donc de l'ordre de 30, c'est-à-dire de 3%.
- Moralité : ne nous Fillons pas trop aux sondages, sous peine de nous Trumper !

Dans la vie courante : les probabilités pour gagner aux jeux télévisés

- Il s'agit d'un jeu télévisé américain. Dans ce jeu le candidat a devant lui trois portes. Derrière l'une de ces portes il y a une voiture et derrière chacune des autres, une chèvre.

Dans la vie courante : les probabilités pour gagner aux jeux télévisés

- Il s'agit d'un jeu télévisé américain. Dans ce jeu le candidat a devant lui trois portes. Derrière l'une de ces portes il y a une voiture et derrière chacune des autres, une chèvre.
- Si le candidat désigne la porte derrière laquelle se trouve la voiture, il la gagne.

Dans la vie courante : les probabilités pour gagner aux jeux télévisés

- Il s'agit d'un jeu télévisé américain. Dans ce jeu le candidat a devant lui trois portes. Derrière l'une de ces portes il y a une voiture et derrière chacune des autres, une chèvre.
- Si le candidat désigne la porte derrière laquelle se trouve la voiture, il la gagne.
- Le jeu se passe ainsi. Le candidat désigne une porte. Le présentateur (qui sait où se trouve la voiture) n'ouvre pas cette porte, mais en ouvre une autre, derrière laquelle se trouve une chèvre.

Dans la vie courante : les probabilités pour gagner aux jeux télévisés

- Il s'agit d'un jeu télévisé américain. Dans ce jeu le candidat a devant lui trois portes. Derrière l'une de ces portes il y a une voiture et derrière chacune des autres, une chèvre.
- Si le candidat désigne la porte derrière laquelle se trouve la voiture, il la gagne.
- Le jeu se passe ainsi. Le candidat désigne une porte. Le présentateur (qui sait où se trouve la voiture) n'ouvre pas cette porte, mais en ouvre une autre, derrière laquelle se trouve une chèvre.
- Le candidat a droit à un autre essai dans lequel il peut maintenir son choix initial ou en changer. À votre avis, doit-il le maintenir, en changer, ou est-ce indifférent ?

Les recettes du dernier lapin (2)

Pour renforcer le lien entre l'enseignement des mathématiques et la vie courante : trouver le juste équilibre entre le sens et la technique.

Mathématiques et apprentissage du raisonnement

- L'exemple des chèvres montre une autre fonction des mathématiques, plus importante encore pour tous les citoyens, qui est de contribuer à l'apprentissage du raisonnement. Comme le dit Jean-Pierre Kahane :

Mathématiques et apprentissage du raisonnement

- L'exemple des chèvres montre une autre fonction des mathématiques, plus importante encore pour tous les citoyens, qui est de contribuer à l'apprentissage du raisonnement. Comme le dit Jean-Pierre Kahane :
- *Les mathématiques permettent de comprendre la différence entre condition nécessaire et condition suffisante, elles font le lien entre le général et le particulier, elles conduisent à organiser la pensée, à catégoriser les problèmes.*
  Elles forcent à expliciter les évidences, à décomposer les difficultés, à enchaîner les résultats, à dénombrer tous les cas possibles : elles sont la logique cartésienne en action.

Mathématiques et apprentissage du raisonnement

- L'exemple des chèvres montre une autre fonction des mathématiques, plus importante encore pour tous les citoyens, qui est de contribuer à l'apprentissage du raisonnement. Comme le dit Jean-Pierre Kahane :
- *Les mathématiques permettent de comprendre la différence entre condition nécessaire et condition suffisante, elles font le lien entre le général et le particulier, elles conduisent à organiser la pensée, à catégoriser les problèmes.*
  Elles forcent à expliciter les évidences, à décomposer les difficultés, à enchaîner les résultats, à dénombrer tous les cas possibles : elles sont la logique cartésienne en action.
- Un exemple personnel.

Les recettes du dernier lapin (3)

Pour améliorer la formation au raisonnement : utiliser des problèmes ouverts. Voir la conférence à l'IREM de Paris (2015) sur ma page web.

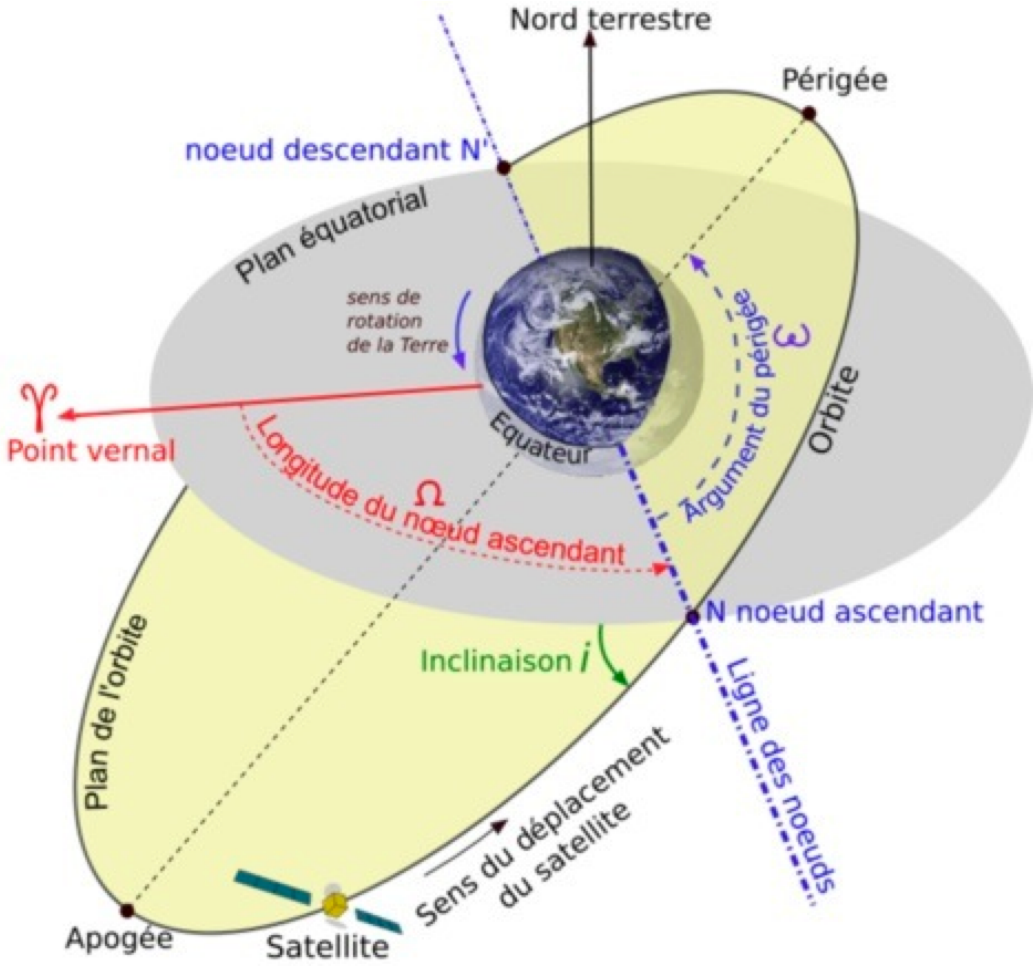
Les mathématiques qui ne servent pas aujourd'hui serviront peut-être demain

Les mathématiques qui ne servent pas aujourd'hui serviront peut-être demain. Exemple 1 : les coniques

- Lorsque les Grecs étudiaient les coniques* (ellipse, parabole, hyperbole), il s'agissait de mathématiques "pures ", c'est-à-dire qui n'avaient pas d'applications.

Les mathématiques qui ne servent pas aujourd'hui serviront peut-être demain. Exemple 1 : les coniques

- Lorsque les Grecs étudiaient les coniques* (ellipse, parabole, hyperbole), il s'agissait de mathématiques "pures ", c'est-à-dire qui n'avaient pas d'applications.
- Depuis, Kepler* ($\sim$ 1610) est arrivé ...


Nord terrestre
Périgée
noeud descendant N'
Plan équatorial
sens de rotation de la Terre
Point vernal
Longitude du nœud ascendant
Ω
Equateur
ω
Argument du périgée
Orbite
N noeud ascendant
Inclinaison i
Plan de l'orbite
Ligne des noeuds
Sens du déplacement du satellite
Apogée
Satellite

Exemple 2 : les nombres premiers

- Si en 1970 on avait demandé à un mathématicien : *à quoi servent les nombres premiers ?* Il aurait répondu : à rien, on les étudie *pour l'honneur de l'esprit humain* (comme disait Jacobi vers 1850)

Exemple 2 : les nombres premiers

- Si en 1970 on avait demandé à un mathématicien : *à quoi servent les nombres premiers ?* Il aurait répondu : à rien, on les étudie *pour l'honneur de l'esprit humain* (comme disait Jacobi vers 1850)
- et il aurait peut-être ajouté, comme mon collègue R. Godement (mort en juillet 2016) : *au moins, quand on fait de l'arithmétique, on ne travaille pas pour la bombe atomique !*

Exemple 2 : les nombres premiers

- Si en 1970 on avait demandé à un mathématicien : *à quoi servent les nombres premiers ?* Il aurait répondu : à rien, on les étudie *pour l'honneur de l'esprit humain* (comme disait Jacobi vers 1850)
- et il aurait peut-être ajouté, comme mon collègue R. Godement (mort en juillet 2016) : *au moins, quand on fait de l'arithmétique, on ne travaille pas pour la bombe atomique !*
- Grave erreur ...

Cryptographie et codes secrets, quelques exemples : Le code de Jules César

Il utilise les alphabets décalés

Le communiqué de César au soir de la bataille de Zela ?

TCLG TGBG TGAG

Codage par substitution

- **Un message :** A L' AIDE

Codage par substitution

- **Un message :** A L' AIDE
- **et sa transcription en chiffres :** 1 12 1 9 4 5

Codage par substitution

- **Un message :** A L' AIDE
- **et sa transcription en chiffres :** 1 12 1 9 4 5
- **Le codage** : 25 14 25 17 22 21

Codage par substitution

- **Un message :** A L' AIDE
- **et sa transcription en chiffres :** 1 12 1 9 4 5
- **Le codage** : 25 14 25 17 22 21
- **Transcription en lettres :** Y N Y Q V U

Codage par substitution

- **Un message :** A L' AIDE
- **et sa transcription en chiffres :** 1 12 1 9 4 5
- **Le codage** : 25 14 25 17 22 21
- **Transcription en lettres :** Y N Y Q V U
- La formule de codage ?

Le décodage par analyse de fréquence : Marie Stuart

- Marie Stuart, reine de France (1559-1560) puis d'Ecosse, fut capturée par la reine d'Angleterre Elisabeth 1ère en 1568.

Le décodage par analyse de fréquence : Marie Stuart

- Marie Stuart, reine de France (1559-1560) puis d'Ecosse, fut capturée par la reine d'Angleterre Elisabeth 1ère en 1568.
- En 1586 elle participe de sa prison à un complot contre Elisabeth et communique avec ses partisans au moyen de messages codés.

Le décodage par analyse de fréquence : Marie Stuart

- Marie Stuart, reine de France (1559-1560) puis d'Ecosse, fut capturée par la reine d'Angleterre Elisabeth 1ère en 1568.
- En 1586 elle participe de sa prison à un complot contre Elisabeth et communique avec ses partisans au moyen de messages codés.
- Mais son code est décrypté par Thomas Phelippes. Marie est accusée de complot, condamnée et décapitée en 1587.

Voir http ://codes.secrets.free.fr/stuart/stuart5.htm

Le décodage par analyse de fréquence : Edgar Poe

Le message du capitaine Kidd dans *Le scarabée d'or* :

53‡‡+305))6*;4826)4‡4‡);806*;48+8
960))85;1‡(;:+*8+83(88)5*+;46(;88*96
?;8)‡(;485);5*+2:*‡(;4956*2(5*-4)8
98*;4069285);)6+8)4‡‡;1(‡9;48081;8:8‡
1;48+85;4)485+528806*81(‡9;48;(88;4
(‡?34;48)4‡;161;:188;‡?;

Saurez vous décrypter ?

- SALCFCFVHLCNEANVHHPLGNZIPU
  UANAKNRNHHLBNCFVHNYOANEGL
  YHKNZKVSOANHUNARNGNHZLHH
  NVAHGNZFGNHHNZANOHUALYZLP
  HKNHNHMPFYHYFYOMKVHTVLSP
  NYHNONYPAUNKPZPOLOPFYH

Saurez vous décrypter ?

- SALCFCFVHLCNEANVHHPLGNZIPU
  UANAKNRNHHLBNCFVHNYOANEGL
  YHKNZKVSOANHUNARNGNHZLHH
  NVAHGNZFGNHHNZANOHUALYZLP
  HKNHNHMPFYHYFYOMKVHTVLSP
  NYHNONYPAUNKPZPOLOPFYH
- sachant que les lettres les plus fréquentes en français sont :
  E S A R I N T U O L (voire E A S I N T R L U O)

Attention aux fréquences ...

- Les élèves de la classe de sixième du collège Alain Fournier à Orsay m'ont proposé de décrypter un codage du message suivant :

Attention aux fréquences ...

- Les élèves de la classe de sixième du collège Alain Fournier à Orsay m'ont proposé de décrypter un codage du message suivant :
- Jadis vivait un garçon, dans un camping-car, dans un bois. Il n'avait pas un sou. Mais il avait un voisin. Franck avait un chaton blanc, qui adorait dormir. Pour nourrir son chaton, il ramassa un abricot. Alors Franck a vu son voisin sortir son chiot, jusqu'à un marchand d'animaux pour avoir un chat. Puis alla au parc où il trouva un ami fictif, Yoan. Yoan lui raconta alors sa fiction. Un jour Yoan, alors rugbyman cassa sa FIAT, alors qu'il finissait son rugby match. Il prit donc un taxi. Joris, un ami, qui finissait lui son triathlon, l'aida. Un soir, Romain, un larron, cambriola Yoan, donc il alla au QG du FBI dans un hall pour dormir. Il faisait doux.

Le code RSA (Rivest-Shamir-Adleman) et les nombres premiers

- L'histoire de la cryptographie est une longue bataille entre codeurs et déchiffreurs (exemples : le code de Vigenère, Turing et la machine Enigma).

Le code RSA (Rivest-Shamir-Adleman) et les nombres premiers

- L'histoire de la cryptographie est une longue bataille entre codeurs et déchiffreurs (exemples : le code de Vigenère, Turing et la machine Enigma).
- La difficulté, avec les codes usuels c'est que si l'on connaît la clé de codage, on connaît aussi celle de décodage.

Le code RSA (Rivest-Shamir-Adleman) et les nombres premiers

- L'histoire de la cryptographie est une longue bataille entre codeurs et déchiffreurs (exemples : le code de Vigenère, Turing et la machine Enigma).
- La difficulté, avec les codes usuels c'est que si l'on connaît la clé de codage, on connaît aussi celle de décodage.
- Ce n'est pas le cas du code RSA (1978), très simple (niveau terminale S) et très utilisé dans les transactions bancaires (et aussi ... par les militaires).

Le code RSA (Rivest-Shamir-Adleman) et les nombres premiers

- L'histoire de la cryptographie est une longue bataille entre codeurs et déchiffreurs (exemples : le code de Vigenère, Turing et la machine Enigma).
- La difficulté, avec les codes usuels c'est que si l'on connaît la clé de codage, on connaît aussi celle de décodage.
- Ce n'est pas le cas du code RSA (1978), très simple (niveau terminale S) et très utilisé dans les transactions bancaires (et aussi ... par les militaires).
- En effet, ce code est à sens unique : la clé de codage ne donne pas celle de décodage.

Le code RSA (suite)

Le principe du code RSA est le suivant :

- On sait fabriquer de très grands nombres premiers p et q, disons de 200 chiffres (voire beaucoup plus).

Le code RSA (suite)

Le principe du code RSA est le suivant :

- On sait fabriquer de très grands nombres premiers p et q, disons de 200 chiffres (voire beaucoup plus).
- Les multiplier est un jeu d'enfant pour une machine.

Le code RSA (suite)

Le principe du code RSA est le suivant :

- On sait fabriquer de très grands nombres premiers p et q, disons de 200 chiffres (voire beaucoup plus).
- Les multiplier est un jeu d'enfant pour une machine.
- Pour des nombres de cette taille (400 chiffres) **on ne sait pas** retrouver p et q à partir de leur produit pq.

Le code RSA (suite)

Le principe du code RSA est le suivant :

- On sait fabriquer de très grands nombres premiers p et q, disons de 200 chiffres (voire beaucoup plus).
- Les multiplier est un jeu d'enfant pour une machine.
- Pour des nombres de cette taille (400 chiffres) **on ne sait pas** retrouver p et q à partir de leur produit pq.
- Pour coder un message il suffit de connaître le produit pq (public), pour le décoder il faut connaître p **et** q (secrets).

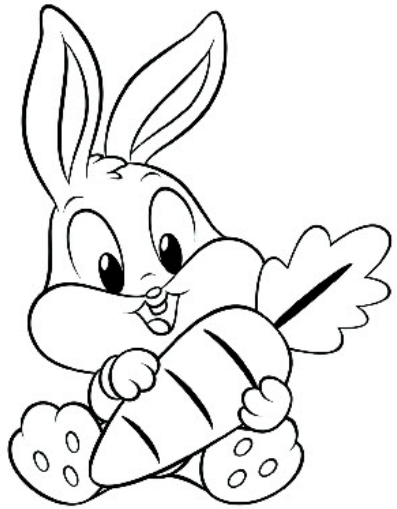
Le code RSA (suite)

Le principe du code RSA est le suivant :

- On sait fabriquer de très grands nombres premiers p et q, disons de 200 chiffres (voire beaucoup plus).
- Les multiplier est un jeu d'enfant pour une machine.
- Pour des nombres de cette taille (400 chiffres) **on ne sait pas** retrouver p et q à partir de leur produit pq.
- Pour coder un message il suffit de connaître le produit pq (public), pour le décoder il faut connaître p **et** q (secrets).
- Un exemple. Voir ma page web (rubrique Mathématiques et autres disciplines, Ch. 6) pour des détails.

Les recettes du dernier lapin (4)

Pour anticiper l'avenir : ne pas se focaliser sur l'utilité à court terme.



Les mathématiques sont vivantes

Les mathématiques sont vivantes : il reste beaucoup de problèmes à résoudre

Peut-être serez-vous étonnés de savoir qu'il y a beaucoup de questions sans réponses en mathématiques et que la recherche y est très active : on dit couramment qu'il s'est fait plus de mathématiques nouvelles depuis 1945 que de l'origine des temps à 1945.

Cependant, l'énoncé des problèmes actuels est en général incompréhensible (voir par exemple les problèmes du millenium), sauf en arithmétique et c'est donc là que nous allons choisir nos exemples.

Il reste beaucoup de problèmes à résoudre en mathématiques : quelques exemples autour des nombres

Nous venons de voir l'importance des nombres premiers pour la cryptographie. Il y a beaucoup de questions ouvertes sur ce thème. En voici une.

À partir de 10, les nombres premiers se terminent par $1, 3, 7, 9$. Voici une dizaine riche où les quatre possibles sont premiers : $11, 13, 17, 19$.

- Y a-t-il d'autres dizaines riches ?

Il reste beaucoup de problèmes à résoudre en mathématiques : quelques exemples autour des nombres

Nous venons de voir l'importance des nombres premiers pour la cryptographie. Il y a beaucoup de questions ouvertes sur ce thème. En voici une.

À partir de 10, les nombres premiers se terminent par $1, 3, 7, 9$. Voici une dizaine riche où les quatre possibles sont premiers : $11, 13, 17, 19$.

- Y a-t-il d'autres dizaines riches ?
- On sait depuis Euclide qu'il y a une infinité de nombres premiers, mais y a-t-il une infinité de dizaines riches ?

Et les dizaines pauvres ?

- Existe-t-il des dizaines pauvres (sans nombre premier) ?

Et les dizaines pauvres ?

- Existe-t-il des dizaines pauvres (sans nombre premier) ?
- Et des centaines pauvres ?

Et les dizaines pauvres ?

- Existe-t-il des dizaines pauvres (sans nombre premier) ?
- Et des centaines pauvres ?
- Peut-on trouver un million de nombres de suite sans aucun nombre premier ?

Pour se distraire : la suite de Collatz

- On part d'un entier n. S'il est pair on le divise par 2.

Pour se distraire : la suite de Collatz

- On part d'un entier n. S'il est pair on le divise par 2.
- S'il est impair on le multiplie par 3 et on ajoute 1, il devient pair et on recommence.

Pour se distraire : la suite de Collatz

- On part d'un entier n. S'il est pair on le divise par 2.
- S'il est impair on le multiplie par 3 et on ajoute 1, il devient pair et on recommence.
- **Exemples** $n = 7$, $n = 27$, etc.

Pour se distraire : la suite de Collatz

- On part d'un entier n. S'il est pair on le divise par 2.
- S'il est impair on le multiplie par 3 et on ajoute 1, il devient pair et on recommence.
- **Exemples** $n = 7$, $n = 27$, etc.
- **Conjecture :** La suite de Collatz finit toujours par revenir à 1.

Pour se distraire : la suite de Collatz

- On part d'un entier n. S'il est pair on le divise par 2.
- S'il est impair on le multiplie par 3 et on ajoute 1, il devient pair et on recommence.
- **Exemples** $n = 7$, $n = 27$, etc.
- **Conjecture :** La suite de Collatz finit toujours par revenir à 1.
- **Question subsidiaire :** À quoi ça sert ?

Un exemple de problème résolu : Dirichlet

- On a vu que les nombres premiers (sauf 2 et 5) se terminent par $1, 3, 7, 9$.

Un exemple de problème résolu : Dirichlet

- On a vu que les nombres premiers (sauf 2 et 5) se terminent par $1, 3, 7, 9$.
- Peter Lejeune-Dirichlet a montré en 1838 qu'il y a une infinité de nombres premiers qui se terminent par 1, par 3, par 7 et par 9.

Un exemple de problème résolu : Dirichlet

- On a vu que les nombres premiers (sauf 2 et 5) se terminent par $1, 3, 7, 9$.
- Peter Lejeune-Dirichlet a montré en 1838 qu'il y a une infinité de nombres premiers qui se terminent par 1, par 3, par 7 et par 9.
- Mieux, Sierpinski a montré en 1959 qu'il y a une infinité de nombres premiers commençant par une suite quelconque de chiffres $a_1 \cdots a_m$ et finissant par une suite $b_1 \cdots b_n$ quelconque aussi (avec $b_n = 1, 3, 7, 9$).

Un exemple de problème résolu : Dirichlet

- On a vu que les nombres premiers (sauf 2 et 5) se terminent par $1, 3, 7, 9$.
- Peter Lejeune-Dirichlet a montré en 1838 qu'il y a une infinité de nombres premiers qui se terminent par 1, par 3, par 7 et par 9.
- Mieux, Sierpinski a montré en 1959 qu'il y a une infinité de nombres premiers commençant par une suite quelconque de chiffres $a_1 \cdots a_m$ et finissant par une suite $b_1 \cdots b_n$ quelconque aussi (avec $b_n = 1, 3, 7, 9$).
- Par exemple, il y a une infinité de nombres premiers de la forme :

$$123456789 \cdots 987654321.$$

Les recettes du dernier lapin (5)

- Pour que le progrès des mathématiques continue : donner aux jeunes le goût de chercher en mathématiques. C'est facile car les mathématiques sont non seulement utiles, mais elles sont belles !

Les recettes du dernier lapin (5)

- Pour que le progrès des mathématiques continue : donner aux jeunes le goût de chercher en mathématiques. C'est facile car les mathématiques sont non seulement utiles, mais elles sont belles !

- Je vous remercie de votre attention.