En mathématiques

que cherche-t-on ?

comment cherche-t-on ?

Daniel PERRIN

Plan

1. Les mathématiques c'est utile

2. Un exemple : nombres premiers et codes secrets

3. En mathématiques, il y a beaucoup de problèmes qu'on ne sait pas résoudre

4. Comment travaille un chercheur

Pourquoi faut-il faire des mathématiques ?

Les mathématiciens professionnels ont leurs propres réponses : parce que c'est beau, parce que cela fait partie de l'héritage culturel de l'humanité, parce que c'est ce que j'aime faire, mais ces réponses ne vous satisferont sans doute pas. Une première raison, qui vaut pour beaucoup de gens (ingénieurs, statisticiens, physiciens, informaticiens, financiers, mais aussi au-delà pour tous les citoyens) est :

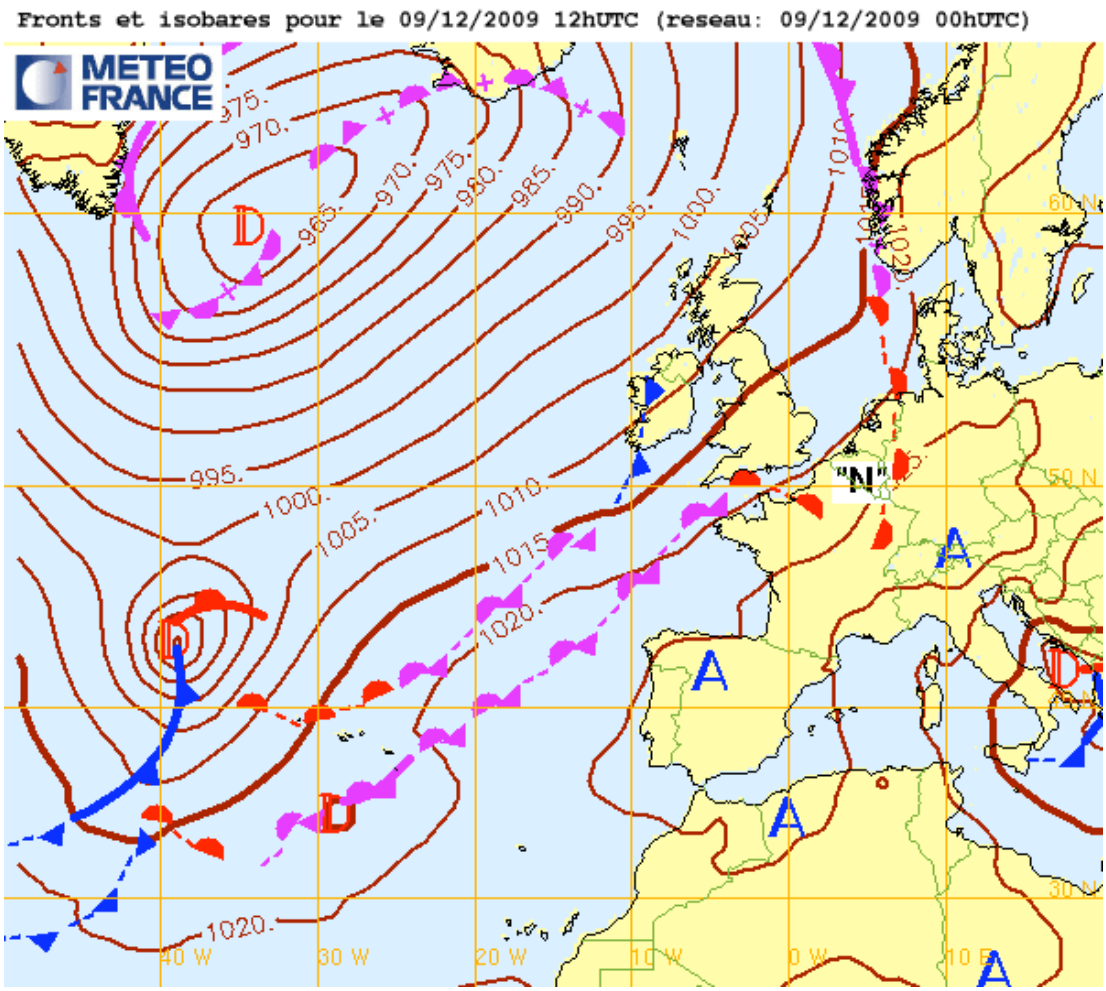
parce qu'elles sont utiles

À quoi sert l'arithmétique ?

Les codes barres, comme les numéros de sécurité sociale, comportent une clé de vérification qui se calcule par division.

À quoi sert l'analyse ?

Les fronts et isobares



Les cartes météorologiques sont établies avec trois ingrédients : les équations de la mécanique des fluides, des modèles d'analyse mathématique (dérivées, etc.), des logiciels de calcul.

À quoi servent les statistiques ?

Par exemple à séquencer le génome (ADN) de la bactérie Escherichia coli :

aaacaaaccgaaagcaacgaaaaagtgggtcgttagctcag
ggtagagcagttgacttttaatcaattggtcgcaggttcgaat
cacgacccaccaatcgctaaggtggaagcggtagtaaaac
ggataacgttgcatgagcaacggcccgaagggcgagacg
agtcatcctgcacgacccaccactaacatagttagttgtagtat
gcgtagtatcgggtgattagctcagctgggagagcacctccctt
aggaggggtcggcggttcgatcccgtcatcacccaccaccg
ttagctcagttggtagagcagttgacttttaatcaattggtcgca
gaatcctgcacgacccaccagttttaacatcgaagacagatgtta
gtgtaggataacgttgcgtcagcaacggcccgtagggcgagcg
cgagtcatcctggacccaccactaatgacggtgggttcggtg
gtttgtagtatccagcgcaggggtgattagctcagctggg
...

a= adénine, g=guanine, t=thymine, c=cytosine

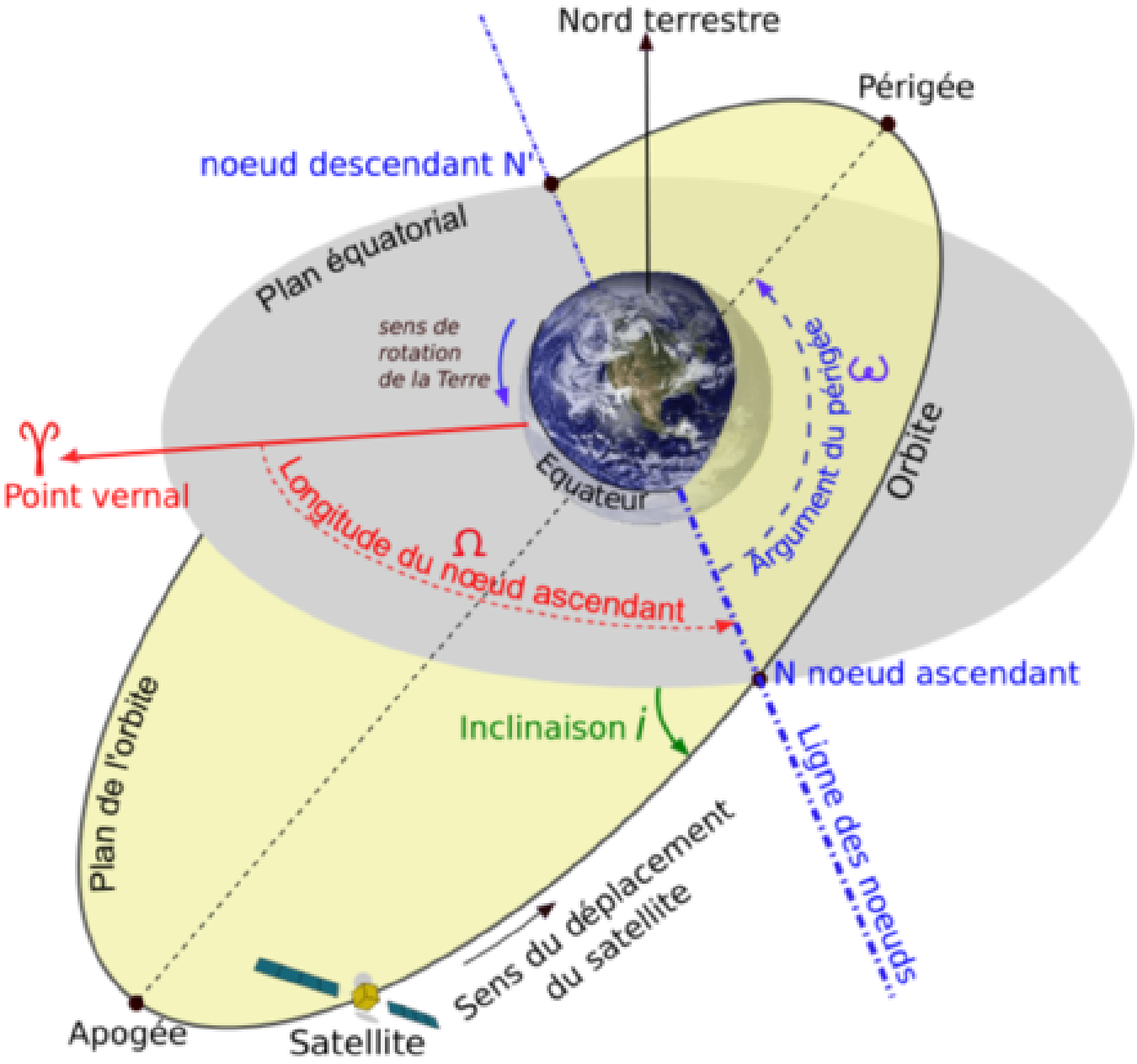
Les mathématiques qui ne servent pas aujourd'hui serviront peut-être demain

exemple 1 : les coniques

Lorsque les Grecs étudiaient les coniques (c'est-à-dire les sections des cônes par des plans, voir figure Cabri), il s'agissait de mathématiques "pures ", c'est-à-dire qui n'avaient pas d'applications.

Depuis, Kepler ($\sim$ 1610) est arrivé ...

À quoi servent les coniques ?



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

exemple 2 : l'arithmétique

Si en 1970 vous m'aviez posé la question :

à quoi servent les nombres premiers ?

Je vous aurais répondu : à rien, on les étudie *pour l'honneur de l'esprit humain* (comme disait Jacobi vers 1850) et j'aurais peut-être ajouté, comme R. Godement :

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

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

TCLG TGBG TGAG

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.

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/stuart3.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 ?

SALCFCFVHLCNEANVHHPLGNZIPUUA
NAKNRNHHLBNCFVHNYOANEGLYHK
NZKVSOANHUNARNGNHZLHHNVAHGN
ZFGNHHNZANOHUALYZLPHKNHNHMP
FYHYFYOMKVHTVLSPNYHNONYPAUN
KPZPOLOPFYH

sachant que les lettres les plus fréquentes
en français sont : E S A R I N T U O L

Vérification des fréquences

Un voisin compatissant l'accompagna à la consultation à l'hôpital Cochin. Il donna son nom, son rang d'immatriculation à l'Association du travail. On l'invita à subir auscultation, palpation, puis radio. Il fut d'accord. On l'informa : souffrait–il ? Plus ou moins, dit–il. Qu'avait–il ? Il n'arrivait pas à dormir ? Avait–il pris un sirop ? Un cordial ? Oui, il avait, mais ça n'avait pas agi. Avait–il parfois mal à l'iris ? Plutôt pas. Au palais ? Ca pouvait ; Au front ? Oui. Aux conduits auditifs ? Non, mais il y avait, la nuit, un bourdon qui bourdonnait. On voulut savoir : un bourdon ou un faux-bourdon ? Il l'ignorait.

(suite)

Il fut bon pour l'oto-rhino, un gars jovial, au poil ras, aux longs favoris roux, portant lorgnons, papillon gris à pois blancs, fumant un cigarillo qui puait l'alcool. L'oto-rhino prit son pouls, l'ausculta, introduisit un miroir rond sous son palais, tripota son pavillon, farfouilla son tympan, malaxa son larynx, son naso–pharynx, son sinus droit, sa cloison. L'oto-rhino faisait du bon travail, mais il sifflotait durant l'auscultation ; ça finit par aigrir Anton.

Le code RSA :

Rivest, Shamir, Adleman, 1978

L'espion Ernesto doit transmettre des messages codés à son chef Carlos.

Carlos calcule deux grands nombres premiers p et q (disons de 200 chiffres), leur produit pq et il choisit un nombre e premier avec $p-1$ et $q-1$.

Il transmet à Ernesto les nombres pq et e (qui constituent la clé de codage), cette clé est **publique**.

Il garde p et q secrets.

Pour coder un message Ernesto n'a besoin que de pq et de e.

Pour décoder le message, Carlos a besoin de p et de q.

Précisions sur le code RSA

Codage

Le message a est un entier $< pq$. Ernesto calcule le codage r qui est le reste de la division de a^e par pq. On note $a^e \equiv r \pmod{pq}$.

Décodage

Carlos calcule un entier d qui vérifie $de \equiv 1$ modulo $(p-1)(q-1)$ par l'algorithme d'Euclide.

Il retrouve alors a à partir de r en calculant r^d modulo pq.

Pour calculer d il faut $(p-1)(q-1) = pq - p - q + 1$, donc p et q.

Exemple : $pq = 11639$, $e = 3361$, $a = 2511$.

La sécurité du code RSA

Ce qui assure la sécurité du code RSA :

• On sait fabriquer de très grands nombres premiers p et q, disons de 200 chiffres.

• 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.

Fabriquer de grands nombres premiers

c'est facile car on a les nombres

de Fermat $F_n = 2^{2^n} + 1$

Fermat avait affirmé que tous ces nombres étaient premiers. C'est vrai pour :

$F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65537$.

Ensuite, ça se gâte ...

La honte de Fermat !

Euler le premier a montré :

$$2^{32} + 1 = 641 \times 6700417$$

Ensuite, on a :

$$2^{64} + 1 = 274177 \times 67280421310721$$

$$2^{128} + 1 = 59649589127497217 \times 5704689200685129054721$$

On notera que la calculatrice répond beaucoup plus vite à la question de la primalité qu'à celle de la factorisation.

Faute de Fermat, on se contente des nombres de Mersenne $M_n = 2^n - 1$ et de leurs records

$M_{19} = 524287$ (Cataldi 1588)

M_{127} (39 chiffres, Lucas, 1876)

$M_{6972593} = 437075 \cdots 193791$
(plus de 2 millions de chiffres, 1999)

Factoriser les nombres

c'est plus difficile !

Un défi de Mersenne à Fermat (1643)

Le nombre 100895598169 est-il premier ?

À cette question je réponds que ce nombre est composé et se fait du produit des deux : 898423 *et* 112303 *qui sont premiers. Je suis toujours, mon révérend Père, votre très humble et très affectionné serviteur.*

Fermat

Le record de factorisation (1999)

n (155 chiffres) $n = pq$ (78 chiffres chacun)

$$
\begin{aligned}
&10941738641570527421809707322040357612003732945449205990913842131476349984288934784717997257891267332497625752899781833797076537244027146743531593354333897 = \\
&10263959282974110577205419657399167590071656780803806680334193352179071130777 \times \\
&10660348838016845482092722036001287867920795857598929152227060823719306280864 3.
\end{aligned}
$$

Qui veut gagner des sous ?

Il suffit de factoriser le nombre suivant de 212 chiffres :

7403756347956171282804679609742957314259318888923128908493623263897276503402826627689199641962511784399589433050212758537011896809828673317327310893090055250511687706329907239638078671008609696253793465056379635 9

Le prix offert par la société RSA est de 10000 $

En mathématiques il y a beaucoup de questions sans réponse

Nous avons déjà rencontré le problème des nombres de Fermat F_n :

en existe-t-il qui sont premiers en dehors de F_0, F_1, F_2, F_3 *et* F_4 *?*

On ne sait pas répondre à cette question.

Je vais vous donner d'autres exemples de questions ouvertes, choisies en arithmétique parce que c'est l'endroit où l'on trouve les problèmes les plus faciles à formuler, mais il y en a dans tous les domaines des mathématiques.

Combien de nombres premiers dans une dizaine ?

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 ?

Y a-t-il beaucoup de dizaines riches ?

Et des dizaines pauvres ?

Problème : existe-t-il des dizaines sans nombre premier ?

Et des centaines pauvres ?

Peut-on trouver un million de nombres de suite sans aucun nombre premier ?

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.

Exemple $n = 7$.

Conjecture : La suite de Collatz finit toujours par revenir à 1.

Un exemple de Jean-Paul Delahaye

ou pourquoi prouver

quand on a fait

des milliards d'expériences ?

Soit n un entier.

Les nombres $n^{17} + 9$ et $(n+1)^{17} + 9$ sont-ils toujours premiers entre eux ?

Réponse : C'est vrai longtemps, longtemps, mais ...

c'est faux pour :

$n = 8\,424\,432\,925\,592\,889\,329\,288\,197\,322\,308$
$900\,672\,459\,420\,460\,792\,433,$

facteur commun :

$r = 8\,936\,582\,237\,915\,716\,659\,950\,962\,253\,358$
$945\,635\,793\,453\,256\,935\,559.$

Comment travaille un mathématicien ?

Je n'ai pas le temps de traiter avec vous un exemple en direct, mais je vous ai préparé quelques problèmes pour vous exercer à chercher. Je voudrais juste insister sur deux points.

Premier point :

Quand on cherche un problème ouvert, une première phase est quasiment "expérimentale" : étudier des **exemples**, **formuler** ce qu'on y voit, émettre des **conjectures**.

Voici ce que dit à ce propos Alexandre Grothendieck, l'un des plus grands mathématiciens du XX-ième siècle :

Ce que dit Grothendieck

Quand je suis curieux d'une chose, mathématique ou autre, je l'interroge. Je l'interroge, sans me soucier si ma question est peut-être stupide ou si elle va paraître telle ... Souvent la question prend la forme d'une affirmation – une affirmation qui, en vérité est un coup de sonde. ... Souvent, surtout au début d'une recherche, l'affirmation est carrément fausse – encore fallait-il l'écrire pour que ça saute aux yeux que c'est faux, alors qu'avant de l'écrire il y avait un flou, comme un malaise, au lieu de cette évidence. Ça permet maintenant de revenir à la charge avec cette ignorance en moins, avec une question-affirmation peut-être un peu moins "à côté de la plaque".

Deuxième point :

Même si l'on travaille sérieusement, personne n'est à l'abri des erreurs, être un chercheur c'est aussi sécher et se tromper.

Écoutons encore Grothendieck :

Errare humanum est

Grothendieck encore :

Mais il arrive aussi que cette image [de la situation] *est entachée d'une erreur de taille, de nature à la fausser profondément. ... Le travail, parfois laborieux, qui conduit au dépistage d'une telle idée fausse est souvent marqué par une tension croissante au fur et à mesure qu'on approche du nœud de la contradiction, d'abord vague, puis de plus en plus criante jusqu'au moment où elle éclate avec la découverte de l'erreur et l'écroulement d'une certaine vision des choses, survenant comme un soulagement immense.*

Errare humanum est,

une parenthèse :

le schéma de Hilbert

n'est presque jamais connexe ?

Ou l'histoire vraie d'une erreur et ses conséquences.

Déceler une erreur dans une démonstration est un des moments les plus difficiles dans la vie d'un chercheur, mais écoutons une dernière fois Grothendieck :

Errare humanum est

Grothendieck toujours :

La découverte de l'erreur est un des moments cruciaux, un moment créateur entre tous, dans tout travail de découverte.