



Pourquoi choisir une filière S ?

et

pour qui ?



Pour qui ?

Abstraction, rigueur,

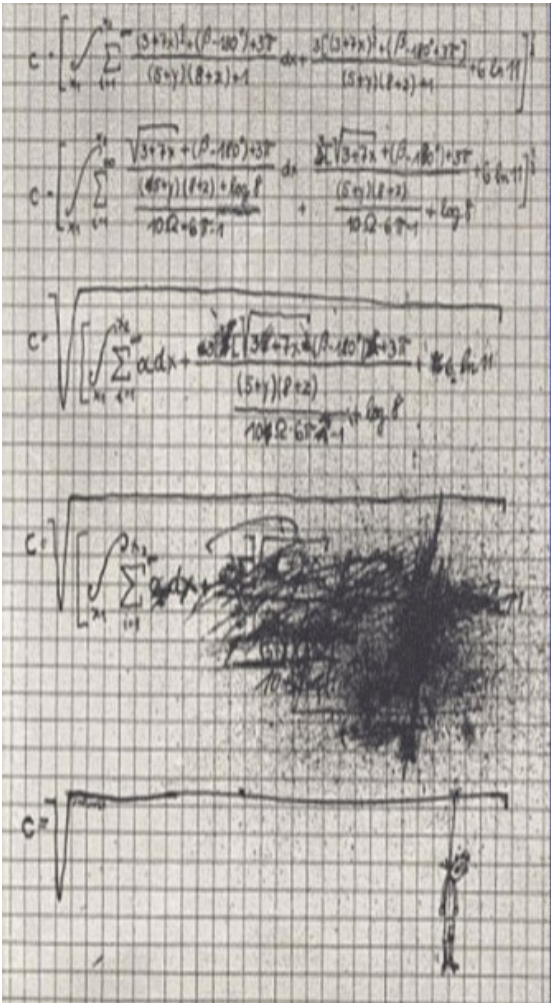
avoir les moyens de comprendre le monde
technologique qui nous entoure



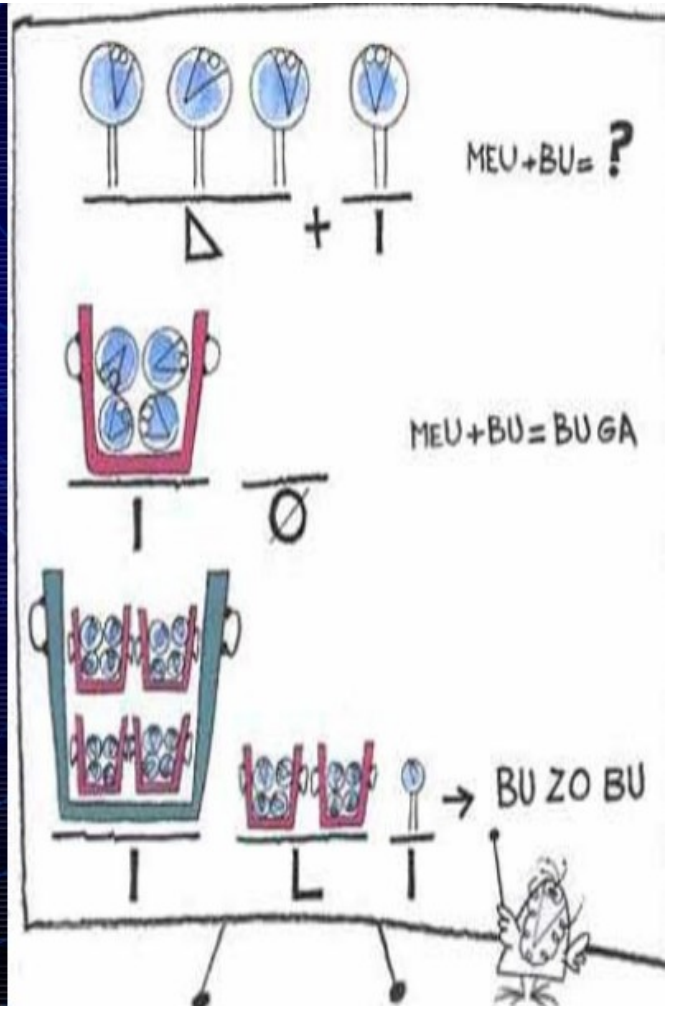
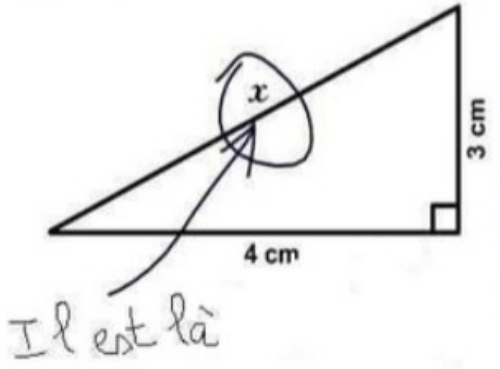
Pourquoi ?

Google : les maths c'est très utile

Ce n'est pas ...



3. Trouver X.



Arithmétique

De l'Antiquité à nos jours

Code Barre, ISBN

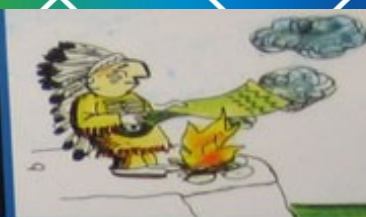


123456789012



Code Secret , Carte Bancaire

Des codes secrets rendus publics ?



Grâce aux codes à clé publique, vous pourrez bientôt faire sans risque des achats sur Internet et transmettre vos références de carte bancaire.

La méthode : le codage est rendu public, mais le message ne peut être déchiffré que par le destinataire autorisé, car la procédure de décodage reste secrète ! C'est vrai par exemple pour la méthode RSA conçue en 1978 par Rivest, Shamir et Adleman.

L'astuce ?

Si un nombre est le produit de deux autres, il peut être très difficile de retrouver les deux nombres le composant, surtout si les nombres sont très grands.

Le codage, qui est public, utilise seulement le nombre produit ; les deux nombres composant, eux, restent secrets. Ils sont nécessaires pour décoder.

C'est pour cette raison que la recherche mathématique s'intéresse aux très grands nombres premiers, de plusieurs centaines de chiffres.

$$\begin{array}{r} \text{RSA155} \\ 1094173864157052742180970733 \\ 732945449205990913842131476 \\ 847179972578912673324976257 \\ 707653724402714674353155 \\ = \\ 10263959282974110577205419 \\ 165678080380668033419335 \\ \times \\ 1066034883801684548209272 \\ 079585759892915222706082 \end{array}$$

Des grands nombres premiers

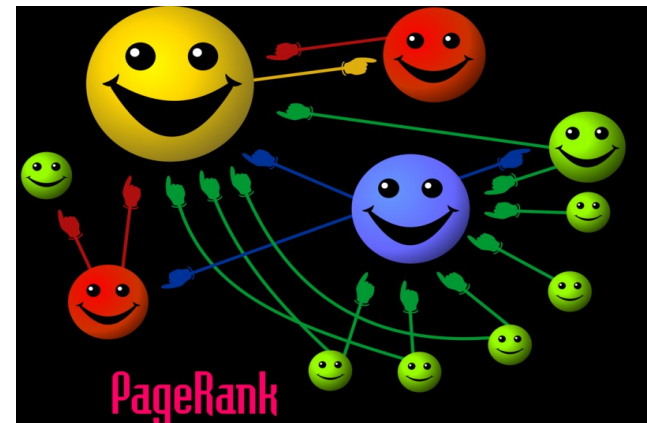
D'un autre côté, certains mathématiciens trouvent - des algorithmes de factoring rapides pour constituer une menace - cela oblige à augmenter, avec les années, des nombres premiers utilisés. Les recherches mathématiques très récentes sur les nombres premiers et la factorisation sont devenues d'une importance cruciale. Et les nombres premiers ne sont pas seulement mathématiquement intéressants pour la cryptographie. Des spécialistes élaborent aussi des algorithmes basés sur les propriétés arithmétiques des courbes elliptiques, d'autres recherchent de nouvelles preuves des lois étranges de la physique.

Matrices et Suites

Les Fractales



Les Maths,
un pas vers le succès : Google



Ecouter un CD rayé !?!

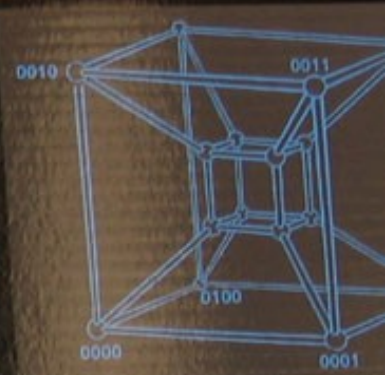


Sur un disque compact, comme sur un ordinateur, chaque son est codé par une suite de 0 et de 1, regroupés par paquets (les octets).
Pour garantir la fidélité de l'enregistrement, on ajoute d'autres octets qui permettent de repérer et corriger les petites erreurs dues aux poussières ou aux rayures.

La théorie mathématique des codes correcteurs d'erreurs étudie comment augmenter la fiabilité tout en diminuant le coût du codage. Elle a aujourd'hui de nombreuses applications : fabrication des disques compacts, transmission des informations par Internet ou par satellites...


100100110111001010110111
1011101101011010110011
10101100111000011

Chaque sommet de cet hypercube est codé par 4 chiffres.
Quel est le code de celui qui est le plus "éloigné" de 0000 ?



Distance entre deux mots

Plus l'écriture des "mots" est différente, le risque de confusion diminue. Pour réduire le nombre d'octets ajoutés, on utilise un type important des codes correcteurs, la "dite de Hamming" - entre deux mots. C'est le nombre de symboles qui sont différents entre 10100111 et 10111111 la distance. Il est facile d'améliorer la correction en augmentant la longueur des mots. Les codes correcteurs permettent des compromis entre la longueur des mots et la capacité à mieux les erreurs en augmentant la longueur des mots.



Les Mathématiques
au lycée Queneau

www.netvibes.com/mathqueneau