Institut de Mathématiques de Luminy | IREM | LUMINY

Laboratoire Pytheas

HIPPOCAMPE-MATHS

Centre d'initiation à la démarche de chercheur en mathématique

Le contexte

- Désaffection des étudiants pour les études scientifiques
- Nécessité d'élargir la diffusion de la culture scientifique
  - Présentation du travail du chercheur au grand public.
  - Expliquer les objectifs, les enjeux de la recherche
  - Difficultés pour les mathématiques.

Hippocampe-maths = Mettre les lycéens en situation dans un laboratoire de recherche

- Les lycéens viennent à l'université (3 jours),
  rencontrent des chercheurs.

- Sont confrontés à de vrais problèmes
  - qui illustrent la démarche scientifique en mathématique,
  - d'énoncés compréhensibles par les élèves,

- Ils appliquent la méthodologie d'un chercheur :
  - Poser le problème, expérimenter et conjecturer
  - Démontrer
  - Communiquer ses résultats : exposé oral, posters (argumentation avec les chercheurs)

Stage (3 jours sous la responsabilité de chercheurs) :

- le responsable propose des problèmes liés à son thème de recherche
- les jeunes chercheurs (moniteurs, ATER) encadrent les élèves
- Poster : rencontre lycéens-chercheurs
- Visite de l'IML et si possible du CIRM

Thèmes (déjà expérimentés) :

- Création de nouvelles mathématiques (C. Mauduit)
- La géométrie en action (J-L. Maltret)
- Codes correcteurs et cryptographie (R. Rolland)
- Tresses et noeuds (X. Bressaud)
- Logique (en projet)
- Mathématiques et Médecine (D. Barbolosi)

Historique :

- "Hippocampe" en biologie

créé en 2004 par Constance Hammond, Directeur de recherche à l'Inserm (INMED)

- "Hippocampe-Maths"

- Premier atelier pilote : juin 2005,
- 10 stages effectués en 2006-07

dont deux avec des lycées en ZEP et une classe de troisième

la logistique :

- dans les locaux de l'IREM.
- Classes accueillies : (troisième), seconde, Premières et Terminales
- Subventions de la Faculté des Sciences (service de moniteurs) , de l'Université (Plan quadriennal), du ministère (projet « Egalités des chances »)

Les institutions

- IREM (Institut de Recherche de l'Enseignement des Mathématiques)
- les laboratoires : IML, LSIS, ...
- Le département de Mathématiques, la Faculté des Sciences de Luminy de Université de la Méditerranée
- APMEP, « Maths pour Tous », SMF

L'équipe

- Les responsables : des enseignants-chercheurs

Jean-Louis MALTRET (MCF, LSIS)
jlm@lumimath.univ-mrs.fr

Robert ROLLAND (MCF, IML)
rolland@iml.univ-mrs.fr

Christian MAUDUIT (PR, IML)
mauduit@iml.univ-mrs.fr

Marie-Renée FLEURY (MCF, IML)
mrd@lumimath.univ-mrs.fr

Site internet

http://www.irem.univ-mrs.fr/


IRRATIONNEL
ou
IRRATIONNEL?
QUESTION: √2 est irRationnel ?
hypothèse : √2 = a/b avec a/b une fraction irréductible
2 = a²/b² ⟺ a² = 2b²
a² est divisible par 2 DONC a est divisible par 2
(a = 2K avec K ∈ ℕ)
b² = 2K d'où b divisible par 2.
CONTRADICTION:
a et b ont un diviseur commun : 2
DONC √2 est irRationnel
Continuons √3 est t'il aussi Irrationnel ?
La démonstration est similaire
DONC √3 est irRationnel
CONJECTURE
CONTRADICTION
CONJECTURE
CONJECTURE FAUSSE
√2+√3 ?

Crypter Decrypter :

RUIZ-HUIDOBRO TRICARD
MOULINAS
VENTURA

INTRODUCTION

EXEMPLES SCRABBLE

CODE DE CESAR

Choix des Clefs :

- On choisit p et q premiers (assez grands)
- On pose $n = pq$
- On pose $\varphi = (p-1)(q-1)$
- On choisit d tel que $PGCD(d, \varphi) = 1$ avec $d < \varphi$
- On trouve le couple (e, r) tel que $ed = 1 + r\varphi$

Exemple de Clefs

- $p = 2$, $q = 5$ donc $n = 10$, $\varphi = 4$
- $PGCD(3, 4) = 1$ donc $d = 3$

CAR $ed \equiv 1 [\varphi]$

Exemple détaillé :

Donc $e = 7$

DECRYPTAGE

A envoi le message crypté m^e, et B doit le décrypter pour retrouver le message original. Alors, on doit avoir $m^{ed} \equiv m\ [n]$.

$m^{ed} \equiv m\ [p.q] \Rightarrow \begin{cases} m^{ed} \equiv m\ [p] \\ m^{ed} \equiv m\ [q] \end{cases}$

* $ed = 1 + k(q-1)(p-1)$.

$m^{1+k(q-1)(p-1)} \equiv m\ [p]$

$\underbrace{(m^k)^{(q-1)}}_{1\ (\text{Thm. de Fermat})}{}^{p-1} \equiv m\ [p]$

$((m^k)^{p-1})^{q-1}_{\times m} \equiv m\ [q]$.

On a $\begin{cases} m^{ed} \equiv m\ [p] \\ m^{ed} \equiv m\ [q] \end{cases}$

p et q sont premiers, donc $ppcm(p, q) = p.q = n$.

$\Rightarrow m^{ed} \equiv m\ [pq]$

$m^{ed} \equiv m\ [n]$

On retrouve alors le message m, décrypté.

Exemple :

* Alice envoie un message à Bob donc :
  - Message : BAC | Traduction : 2, 1, 3
  - $\Rightarrow 2^e = 2^7 = 8 \quad 8 \equiv 8\ [10]$
    $1^e = 1^7 = 1 \quad 1 \equiv 1\ [10]$
    $3^e = 3^7 = 27 \quad 27 \equiv 7\ [10]$
  - Message crypté : 8, 1, 7

* Bob reçoit le message crypté 8, 1, 7
  - Il va le décrypter avec la clef privée : d
    $8^d = 8^3 = 512 \quad 512 \equiv 2\ [10]$
    $1^d = 1^3 = 1 \quad 1 \equiv 1\ [10]$
    $7^d = 7^3 = 343 \quad 343 \equiv 3\ [10]$
  - Le message décrypté est donc : 2, 1, 3
  - $\Rightarrow$ BAC

CODAGE ALEATOIRE

* Si on doit avoir $m^{ed} \equiv m\ [n]$

- On peut prendre un m' tel que :

$(m.m')^{ed} \equiv m\ [n]$ (1)

Cherchons m' tel que $(m.m')^{ed} \equiv m\ [n]$.

Si $m^{ed} \equiv m\ [n]$, alors pour avoir (1), il faut $m'^{ed} \equiv 1\ [n]$

donc $m' \equiv 1\ [n] \Leftrightarrow m' = 1$ donc inutile

- On peut prendre un φ tel que : $m^{(e+\varphi)^d} \equiv m\ [n]$, et on sait $ed \equiv 1 \bmod (p-1)(q-1)$

$ed = 1 + k(q-1)(p-1)$

$\Rightarrow \begin{cases} ed \equiv 1\ [p-1] \\ ed \equiv 1\ [q-1] \end{cases} \Rightarrow \begin{matrix} (p-1) \nmid d \\ (q-1) \nmid d \end{matrix}$

$\Rightarrow \begin{matrix} (p-1) \mid \varphi \\ (q-1) \mid \varphi \end{matrix} \gg ppcm(p-1, q-1) \mid \varphi$

* THEOREMES UTILISES :

THEOREME DE BEZOUT :

$\exists \alpha, \beta \in \mathbb{Z}$ tq $\alpha a + \beta b = 1$ avec a et b sont premiers entre eux

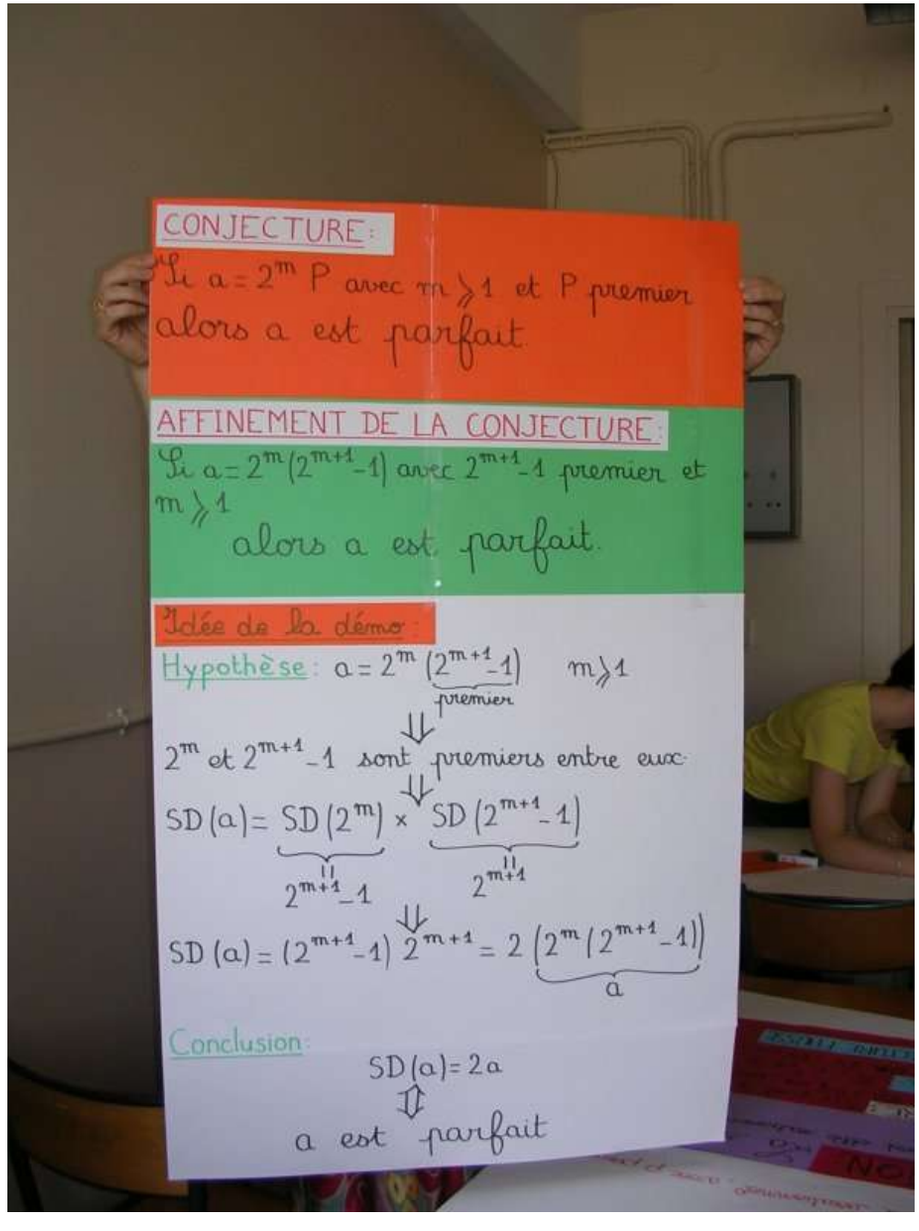
PETIT THEOREME DE FERMAT :

$a^{p-1} \equiv 1\ [p]$, avec p premier

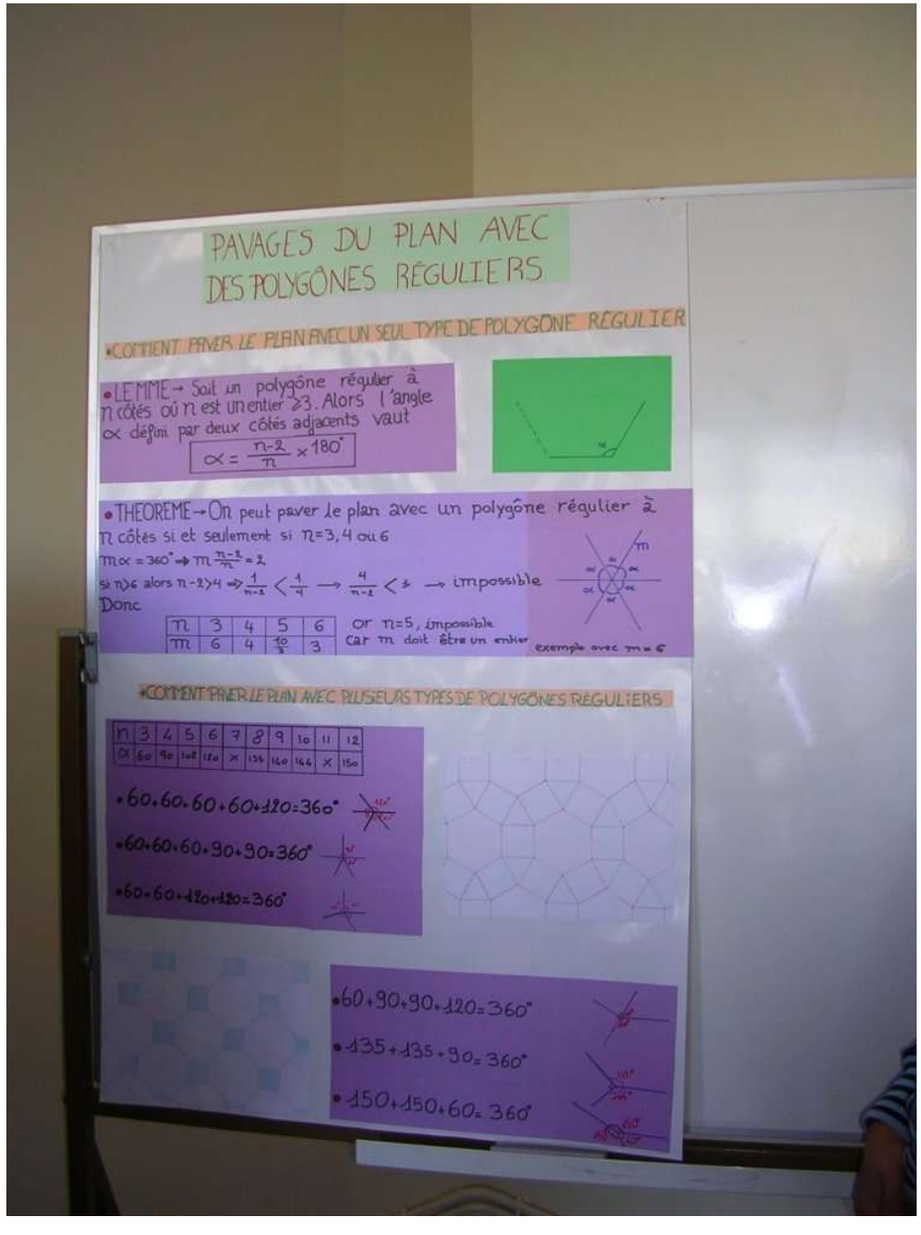
THEOREME DES RESTES CHINOIS

$\begin{cases} x \equiv a\ [p] \\ x \equiv b\ [q] \end{cases}$ p et q sont premiers entre eux $\Rightarrow$ un unique x tq $0 \leq x \leq pq - 1$ vérifiant le système


LES EMBOUTEILLAGES.
Introduction


CONJECTURE :
Si $a = 2^m P$ avec $m \geqslant 1$ et P premier
alors a est parfait
AFFINEMENT DE LA CONJECTURE :
Si $a = 2^m (2^{m+1} - 1)$ avec $2^{m+1} - 1$ premier et $m \geqslant 1$
alors a est parfait
Idée de la démo :
Hypothèse : $a = 2^m \underbrace{(2^{m+1} - 1)}_{\text{premier}}$ $m \geqslant 1$
$\Downarrow$
2^m et $2^{m+1} - 1$ sont premiers entre eux
$\Downarrow$
$SD(a) = \underbrace{SD(2^m)}_{= 2^{m+1} - 1} \times \underbrace{SD(2^{m+1} - 1)}_{= 2^{m+1}}$
$\Downarrow$
$SD(a) = (2^{m+1} - 1) 2^{m+1} = 2 \underbrace{(2^m (2^{m+1} - 1))}_{a}$
Conclusion :
$SD(a) = 2a$
$\Updownarrow$
a est parfait


evian


PAVAGES DU PLAN AVEC DES POLYGÔNES RÉGULIERS
•COMMENT PAVER LE PLAN AVEC UN SEUL TYPE DE POLYGONE RÉGULIER
•LEMME→ Soit un polygône régulier à n côtés où n est un entier ≥3. Alors l'angle α défini par deux côtés adjacents vaut
$\alpha = \frac{n-2}{n} \times 180°$
•THEOREME→ On peut paver le plan avec un polygône régulier à n côtés si et seulement si n=3,4 ou 6
$m\alpha = 360° \Rightarrow m\frac{n-2}{n} = 2$
si n≥6 alors $n-2 > 4 \Rightarrow \frac{1}{n-2} < \frac{1}{4} \rightarrow \frac{4}{n-2} < 1$ → impossible
Donc
n | 3 | 4 | 5 | 6
m | 6 | 4 | 10/3 | 3
or n=5, impossible
car m doit être un entier
exemple avec m = 6
•COMMENT PAVER LE PLAN AVEC PLUSIEURS TYPES DE POLYGÔNES RÉGULIERS
n | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12
α | 60 | 90 | 108 | 120 | x | 135 | 140 | 144 | x | 150
•60+60+60+60+120=360°
•60+60+60+90+90=360°
•60+60+120+120=360°
•60+90+90+120=360°
•135+135+90=360°
•150+150+60=360°


Degrés
ESEL

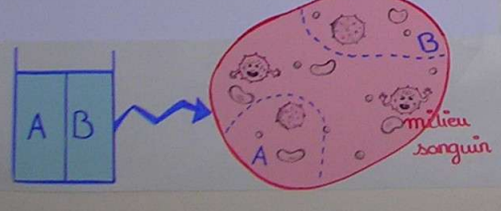
La Recherche d'associations médicamenteuses à l'aide des Mathématiques

Par :
Emma Laurie
Jessica Sarah

PROBLEMATIQUE

Quelle est la procédure à suivre pour éradiquer les cellules cancéreuses de catégories A et B ?

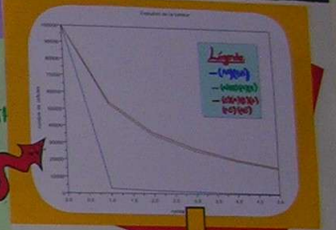
Introduction : Nous allons déterminer Quelle est la procédure à suivre pour éradiquer les cellules cancereuses de catégorie A et B. Cela revient en Mathématiques à montrer que la somme des cellules A et B composant la Tumeur après le n_ième Traitement Tend vers 0. Donc aboutir à la destruction Totale des cellules Cancéreuses.

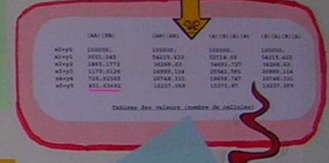


Pour modéliser ce problème, on appelle x_n le nombre de cellules sensibles au produit A, et y_n le nombre de cellules sensibles au produit B, après la n_ième traitement.

Soient (x_n) et (y_n), $n \in \mathbb{N}$, deux suites numériques réelles telles que $\begin{cases} x_{n+1} = \alpha x_n \\ y_{n+1} = \beta y_n + \alpha x_n \end{cases}$

Si $|\alpha| < 1$ et $|\beta| < 1$ alors $(x_n + y_n)$, $n \in \mathbb{N}$, converge vers 0 quand n tend vers $+\infty$.





Conclusion : Afin d'éradiquer les cellules de catégories A et B il est nécessaire d'établir un traitement à l'aide de produits A et B. Le problème était de savoir comment l'établir pour qu'il soit le plus efficace. Nous avons donc constaté que le traitement le plus efficace est le (AA) (BB), administré avec 14 jours d'intervalle, après avoir essayé plusieurs possibilités.

On constate que le traitement (AA)(BB) est le plus efficace. En effet, le nombre de cellules cancéreuses est passé de 100 000 à 452. A ce stade le patient est quasiment guéri car il est impossible d'éradiquer complètement la tumeur.