

## ***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

Christian MAUDUIT (PR, IML)

mauduit@iml.univ-mrs.fr

Robert ROLLAND (MCF, IML)

rolland@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?**

Un nombre est irrationnel s'il ne peut pas s'écrire sous la forme d'une fraction irréductible de nombre entier.

**QUESTION:  $\sqrt{2}$  est-il rationnel?**

hypothèse:  $\sqrt{2} = \frac{a}{b}$  avec  $\frac{a}{b}$  une fraction irréductible

$2 = \frac{a^2}{b^2} \iff a^2 = 2b^2$

$a^2$  est divisible par 2  $\implies$   $a$  est divisible par 2  
( $a = 2k$  avec  $k \in \mathbb{N}$ )

$b^2 = 2k^2$  d'où  $b$  divisible par 2.

**CONTRADICTION:**  
 $a$  et  $b$  ont un diviseur commun: 2.  
**DONC  $\sqrt{2}$  est irrationnel!**

Continuons  $\sqrt{3}$  est-il aussi Irrationnel?  
 la démonstration est similaire  
**DONC  $\sqrt{3}$  est irrationnel**

**CONJECTURE** Si  $p$  est un nombre premier, alors  $\sqrt{p}$  est irrationnel.

**Démonstration:** Par le même raisonnement on a  $a^2 = pb^2$   
 donc  $a^2$  divisible par  $p$   
 donc  $a$  divisible par  $p$  ( $a = pk$ )  
 donc  $b^2$  divisible par  $p$   
 donc  $b$  divisible par  $p$

**CONTRADICTION**  
 donc  $a$  et  $b$  ont un diviseur commun  $p$  premier.

**CONJECTURE:** Si  $n$  est un nombre premier, alors  $\sqrt{n}$  est irrationnel.

**CONJECTURE FAUSSE**



**INTRODUCTION**

EXEMPLES SCRIBBLE

A	10
B	11
C	12
D	13
E	14
F	15
G	16
H	17
I	18
J	19
K	20
L	21
M	22
N	23
O	24
P	25
Q	26
R	27
S	28
T	29
U	30
V	31
W	32
X	33
Y	34
Z	35

CODE DE CIPHER

1. Message: ...

2. ...

# Crypter Decrypter:

RUIZ-HUIDOBARO TRICARD  
MOULINAS  
VENTURA

**Choix des Clés:**

- On choisit  $p, q$  premiers (très grands)
- $n = pq$
- $\phi(n) = (p-1)(q-1)$
- On choisit  $e$  tel que  $\gcd(e, \phi(n)) = 1$
- On trouve le  $d$  tel que  $ed \equiv 1 \pmod{\phi(n)}$

**Exemple de Clés:**

$p=11, q=13, \phi(n)=120$

On choisit  $e=7$

On trouve  $d=17$  car  $7 \cdot 17 = 119 \equiv -1 \pmod{120}$

**DECRYPTAGE**  $((m^e)^d)^{1/n} \equiv m \pmod{n}$

A envoie le message crypté  $m^e$ , et B doit le decrypter pour récupérer le message original. Alors, on doit avoir  $m^{ed} \equiv m \pmod{n}$ .

$m^{ed} \equiv m \pmod{p} \Rightarrow \begin{cases} m^{ed} \equiv m \pmod{p} \\ m^{ed} \equiv m \pmod{q} \end{cases} \Rightarrow m^{ed} \equiv m \pmod{pq}$

$\Rightarrow m^{ed} \equiv m \pmod{p}$   
 $\Rightarrow m^{ed} \equiv m \pmod{q}$

On retrouve alors le message  $m$ , decrypté.

$m^{ed} \equiv m \pmod{p} \Rightarrow m^{k(q-1)(p-1)} \equiv m \pmod{p}$   
 $(m^k)^{1/n} \equiv m \pmod{p}$   
 $\uparrow$  (théorème de Fermat)



**Exemple:**

\* Alice envoie un message  $m$

Bob donc:

Message: BAC

Exécution: 2, 3, 3

$\Rightarrow 2^2 = 2^2 = 8 \pmod{11}$   
 $1^3 = 1^3 = 1 \pmod{13}$   
 $3^3 = 3^3 = 27 \pmod{13} = 10$

Message crypté:  $[8, 1, 10]$

\* Bob reçoit le message crypté  $[8, 1, 10]$

Il va le decrypter avec les clés privées  $d$

$8^d = 8^3 = 512 \pmod{11} = 2 \pmod{11}$   
 $1^d = 1^3 = 1 \pmod{13} = 1 \pmod{13}$   
 $10^d = 10^3 = 1000 \pmod{13} = 10 \pmod{13}$

Le message decrypté est donc:  $[2, 1, 10]$

ce qui donne:  $[B, A, C]$

**CODAGE A LEATOIRE**

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

On peut prendre un  $m'$  tel que:

$(m \cdot m')^d \equiv m \pmod{n}$

Cherchons  $m'$  tel que  $(m \cdot m')^d \equiv m \pmod{n}$

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

donc  $m' \equiv 1 \pmod{n} \Leftrightarrow m' = 1$  donc inutile

On peut prendre un  $\varphi$  tel que  $(m \cdot \varphi)^d \equiv m \pmod{n}$ , alors on a  $e \equiv 1 \pmod{(p-1)(q-1)}$

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

$\Rightarrow ed \equiv 1 \pmod{p-1} \Rightarrow (p-1) \nmid d$   
 $ed \equiv 1 \pmod{q-1} \Rightarrow (q-1) \nmid d$

$\Rightarrow (p-1) \mid \varphi$   
 $(q-1) \mid \varphi \Rightarrow \text{ppcm}(p-1, q-1) \mid \varphi$

\* THEOREMES UTILISES:

**THEOREME DE BEZOUT:**  
 $ax + by = 1$  avec  $a, b$  entiers premiers entre eux  $a, b \in \mathbb{Z}$

**PETIT THEOREME DE FERMAT:**  
 $a^{p-1} \equiv 1 \pmod{p}$ , avec  $p$  premier

**THEOREME DES RESTES CHINOIS:**  
 $\begin{cases} x \equiv a \pmod{p} \\ x \equiv b \pmod{q} \end{cases}$  si  $p$  et  $q$  sont premiers entre eux  $\Leftrightarrow$  toujours une solution unique modulo  $p \cdot q$





### CONJECTURE:

Si  $a = 2^m P$  avec  $m \geq 1$  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  
 $m \geq 1$   
alors  $a$  est parfait.

### Idee de la demo:

Hypothèse:  $a = 2^m \underbrace{(2^{m+1} - 1)}_{\text{premier}} \quad m \geq 1$

$\Downarrow$   
 $2^m$  et  $2^{m+1} - 1$  sont premiers entre eux

$$SD(a) = \underbrace{SD(2^m)}_{2^{m+1} - 1} \times \underbrace{SD(2^{m+1} - 1)}_{2^{m+1}}$$

$$SD(a) = (2^{m+1} - 1) \underbrace{2^{m+1}}_a = 2 (2^m (2^{m+1} - 1))$$

### Conclusion:

$$SD(a) = 2a$$
$$\Downarrow$$

$a$  est parfait



# PAVAGES DU PLAN AVEC DES POLYÈNES RÉGULIERS

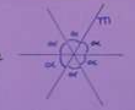
## COMMENT PAVER LE PLAN AVEC UN SEUL TYPE DE POLYÈNE RÉGULIER

• LEMME → Soit un polygone régulier à  $n$  côtés où  $n$  est un entier  $\geq 3$ . Alors l'angle  $\alpha$  défini par deux côtés adjacents vaut

$$\alpha = \frac{n-2}{n} \times 180^\circ$$



• THEOREME → On peut paver le plan avec un polygone régulier à  $n$  côtés si et seulement si  $n=3, 4$  ou  $6$   
 $m\alpha = 360^\circ \Rightarrow m \frac{n-2}{n} = 2$   
 si  $n \neq 4$  alors  $n-2 > 4 \Rightarrow \frac{1}{n-2} < \frac{1}{4} \Rightarrow \frac{4}{n-2} < 2 \rightarrow$  impossible



Donc

$n$	3	4	5	6
$m$	6	4	$\frac{10}{3}$	3

Or  $n=5$ , impossible car  $m$  doit être un entier

exemple avec  $m=6$

## COMMENT PAVER LE PLAN AVEC PLUSIEURS TYPES DE POLYÈNES RÉGULIERS

$n$	3	4	5	6	7	8	9	10	11	12
$\alpha$	60	90	108	120	128.57	135	144	144	150	150

- $60 \cdot 60 \cdot 60 \cdot 60 + 120 = 360^\circ$
- $60 \cdot 60 \cdot 60 \cdot 90 + 90 = 360^\circ$
- $60 \cdot 60 + 120 + 120 = 360^\circ$



- $60 \cdot 90 + 90 + 120 = 360^\circ$
- $135 + 135 + 90 = 360^\circ$
- $150 + 150 + 60 = 360^\circ$

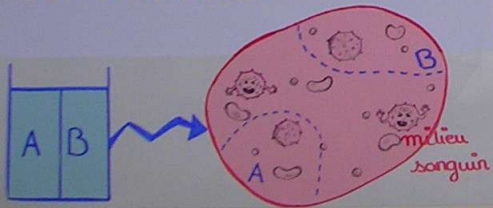




# La Recherche d'associations médicamenteuses à l'aide des Mathématiques

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

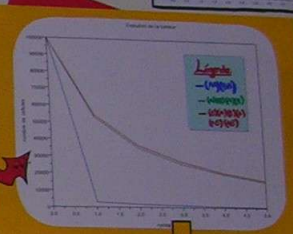
**Introduction:** Nous allons déterminer quelle est la procédure à suivre pour éradiquer les cellules cancéreuses de catégorie A et B. Cela revient en Mathématiques à montrer que la somme des cellules A et B composant la tumeur après le n-ième traitement tend vers 0. Donc aboutir à la destruction totale 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 le n-ième traitement. Soient  $(x_n)$  et  $(y_n)$ ,  $n \in \mathbb{N}$ , deux suites numériques réelles telles que

Par: Emma Louie Jessica Sarah

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



(AA) (BB)	(AA) (AB)	(AB) (BB)	(AB) (AB)
100000	100000	100000	100000
99999	99999	99999	99999
99998	99998	99998	99998
99997	99997	99997	99997
99996	99996	99996	99996
99995	99995	99995	99995
99994	99994	99994	99994
99993	99993	99993	99993
99992	99992	99992	99992
99991	99991	99991	99991
99990	99990	99990	99990
99989	99989	99989	99989
99988	99988	99988	99988
99987	99987	99987	99987
99986	99986	99986	99986
99985	99985	99985	99985
99984	99984	99984	99984
99983	99983	99983	99983
99982	99982	99982	99982
99981	99981	99981	99981
99980	99980	99980	99980
99979	99979	99979	99979
99978	99978	99978	99978
99977	99977	99977	99977
99976	99976	99976	99976
99975	99975	99975	99975
99974	99974	99974	99974
99973	99973	99973	99973
99972	99972	99972	99972
99971	99971	99971	99971
99970	99970	99970	99970
99969	99969	99969	99969
99968	99968	99968	99968
99967	99967	99967	99967
99966	99966	99966	99966
99965	99965	99965	99965
99964	99964	99964	99964
99963	99963	99963	99963
99962	99962	99962	99962
99961	99961	99961	99961
99960	99960	99960	99960
99959	99959	99959	99959
99958	99958	99958	99958
99957	99957	99957	99957
99956	99956	99956	99956
99955	99955	99955	99955
99954	99954	99954	99954
99953	99953	99953	99953
99952	99952	99952	99952
99951	99951	99951	99951
99950	99950	99950	99950
99949	99949	99949	99949
99948	99948	99948	99948
99947	99947	99947	99947
99946	99946	99946	99946
99945	99945	99945	99945
99944	99944	99944	99944
99943	99943	99943	99943
99942	99942	99942	99942
99941	99941	99941	99941
99940	99940	99940	99940
99939	99939	99939	99939
99938	99938	99938	99938
99937	99937	99937	99937
99936	99936	99936	99936
99935	99935	99935	99935
99934	99934	99934	99934
99933	99933	99933	99933
99932	99932	99932	99932
99931	99931	99931	99931
99930	99930	99930	99930
99929	99929	99929	99929
99928	99928	99928	99928
99927	99927	99927	99927
99926	99926	99926	99926
99925	99925	99925	99925
99924	99924	99924	99924
99923	99923	99923	99923
99922	99922	99922	99922
99921	99921	99921	99921
99920	99920	99920	99920
99919	99919	99919	99919
99918	99918	99918	99918
99917	99917	99917	99917
99916	99916	99916	99916
99915	99915	99915	99915
99914	99914	99914	99914
99913	99913	99913	99913
99912	99912	99912	99912
99911	99911	99911	99911
99910	99910	99910	99910
99909	99909	99909	99909
99908	99908	99908	99908
99907	99907	99907	99907
99906	99906	99906	99906
99905	99905	99905	99905
99904	99904	99904	99904
99903	99903	99903	99903
99902	99902	99902	99902
99901	99901	99901	99901
99900	99900	99900	99900

**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.