

Formation : **Accompagner les réformes du Lycée en Mathématiques**  
-- Enseignement TS de spécialité ( présentation du nouveau programme 2012) --  
Par Jean-Jacques Castot (professeur au lycée Félix Eboué de Cayenne).

# BACCALAURÉAT GÉNÉRAL

Session 2012

---

**MATHÉMATIQUES**

**Série S**

**Enseignement de spécialité**

*Durée de l'épreuve : 4 heures*

*Coefficient : 9*

**Ce sujet comporte 5 pages numérotées de 1 à 5.**

**L'utilisation d'une calculatrice est autorisée.**

## EXERCICE 4 (5 points)

Candidats ayant suivi l'enseignement de spécialité

### Partie A **Restitution organisée de connaissance**

Soit  $a, b, c, d$  des entiers relatifs et  $n$  un entier naturel non nul.

Montrer que si  $a \equiv b \pmod{n}$  et  $c \equiv d \pmod{n}$  alors  $ac \equiv bd \pmod{n}$ .

### Partie B **Inverse de 23 modulo 26**

On considère l'équation  $(E) : 23x - 26y = 1$ , où  $x$  et  $y$  désignent deux entiers relatifs.

1. Vérifier que le couple  $(-9, -8)$  est solution de l'équation  $(E)$ .
2. Résoudre alors l'équation  $(E)$ .
3. En déduire un entier  $a$  tel que  $0 \leq a \leq 25$  et  $23a \equiv 1 \pmod{26}$ .

## Partie C Chiffrement de Hill

On veut coder un mot de deux lettres selon la procédure suivante :

**Étape 1** Chaque lettre du mot est remplacée par un entier en utilisant le tableau ci-dessous :

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

On obtient un couple d'entiers  $(x_1, x_2)$  où  $x_1$  correspond à la première lettre du mot et  $x_2$  correspond à la deuxième lettre du mot.

**Étape 2**  $(x_1, x_2)$  est transformé en  $(y_1, y_2)$  tel que :

$$(S_1) \begin{cases} y_1 \equiv 11x_1 + 3x_2 \pmod{26} \\ y_2 \equiv 7x_1 + 4x_2 \pmod{26} \end{cases} \text{ avec } 0 \leq y_1 \leq 25 \text{ et } 0 \leq y_2 \leq 25.$$

**Étape 3**  $(y_1, y_2)$  est transformé en un mot de deux lettres en utilisant le tableau de correspondance donné dans l'étape 1.

Exemple :  $\underbrace{\text{TE}}_{\text{mot en clair}} \xrightarrow{\text{étape 1}} (19, 4) \xrightarrow{\text{étape 2}} (13, 19) \xrightarrow{\text{étape 3}} \underbrace{\text{NT}}_{\text{mot codé}}$

1. Coder le mot **ST**.

2. On veut maintenant déterminer la procédure de décodage :

(a) Montrer que tout couple  $(x_1, x_2)$  vérifiant les équations du système  $(S_1)$ , vérifie les équations du système :

$$(S_2) \begin{cases} 23x_1 \equiv 4y_1 + 23y_2 \pmod{26} \\ 23x_2 \equiv 19y_1 + 11y_2 \pmod{26} \end{cases}$$

(b) À l'aide de la **partie B**, montrer que tout couple  $(x_1, x_2)$  vérifiant les équations du système  $(S_2)$ , vérifie les équations du système

$$(S_3) \begin{cases} x_1 \equiv 16y_1 + y_2 \pmod{26} \\ x_2 \equiv 11y_1 + 5y_2 \pmod{26} \end{cases}$$

(c) Montrer que tout couple  $(x_1, x_2)$  vérifiant les équations du système  $(S_3)$ , vérifie les équations du système  $(S_1)$ .

(d) Décoder le mot **YJ**.

# B.O.

Bulletin officiel spécial n° 8 du 13 octobre 2011

---

## **Annexe**

### **Programme de l'enseignement spécifique et de spécialité de mathématiques Classe terminale de la série scientifique**

- Objectif général
- Raisonnement et langage mathématique
- Utilisation d'outils logiciels
- Diversité de l'activité de l'élève

# Enseignement de spécialité

- Résolution de problèmes
- Introduction motivée des notions
- Conduire à un travail de modélisation
- Placer les élèves en position de recherche
- Utilisation des outils informatiques (logiciels de calcul, tableur)
- Mise en œuvre d'algorithmes

# Arithmétique

## Exemples de problèmes

Problèmes de codage (codes barres, code ISBN, clé du Rib, code Insee)

Problèmes de chiffrement (chiffrement affine, chiffrement de Vigenère, chiffrement de Hill).

Questionnement sur les nombres premiers : infinitude, répartition, tests de primalité, nombres premiers particuliers (Fermat, Mersenne, Carmichael).

Sensibilisation au système cryptographique RSA.

## Contenus

- Divisibilité dans  $\mathbb{Z}$ .
- Division euclidienne.
- Congruences dans  $\mathbb{Z}$ .
- PGCD de deux entiers.
- Entiers premiers entre eux.
- Théorème de Bézout.
- Théorème de Gauss.
- Nombres premiers.
- Existence et unicité de la décomposition en produit de facteurs premiers.

**Géométrie plane**

**Similitudes ... directes, indirectes**

# Matrices et suites

## Exemples de problèmes

Marche aléatoire simple sur un graphe à deux ou trois sommets.

Marche aléatoire sur un tétraèdre ou sur un graphe à  $N$  sommets avec saut direct possible d'un sommet à un autre : à chaque instant, le mobile peut suivre les arêtes du graphe probabiliste ou aller directement sur n'importe quel sommet avec une probabilité constante  $p$ .

Etude du principe du calcul de la pertinence d'une page web

Modèle de diffusion d'Ehrenfest :  $N$  particules sont réparties dans deux récipients ; à chaque instant, une particule choisie au hasard change de récipient.

Modèle proie-prédateur discrétisé :

- évolution couplée de deux suites récurrentes ;
- étude du problème linéarisé au voisinage du point d'équilibre.

## Contenus

- Matrices carrées, matrices colonnes : opérations.
- Matrice inverse d'une matrice carrée.
- Exemples de calcul de la puissance  $n$ -ième d'une matrice carrée d'ordre 2 ou 3.
- Écriture matricielle d'un système linéaire.
- Suite de matrices colonnes  $(U_n)$  vérifiant une relation de récurrence du type  $U_{n+1} = AU_n + C$  :
  - recherche d'une suite constante vérifiant la relation de récurrence ;
  - étude de la convergence.
- Étude asymptotique d'une marche aléatoire.