MINISTÈRE
DE L'ÉDUCATION
NATIONALE, DE
L'ENSEIGNEMENT
SUPÉRIEUR ET DE
LA RECHERCHE

EBE MAT 2

SESSION 2015

CAPES
CONCOURS EXTERNE
TROISIÈME CONCOURS
ET CAFEP CORRESPONDANTS

Section : MATHÉMATIQUES

SECONDE ÉPREUVE D'ADMISSIBILITÉ

Durée : 5 heures

Calculatrice électronique de poche – y compris calculatrice programmable, alphanumérique ou à écran graphique – à fonctionnement autonome, non imprimante, autorisée conformément à la circulaire n° 99-186 du 16 novembre 1999.

L'usage de tout ouvrage de référence, de tout dictionnaire et de tout autre matériel électronique est rigoureusement interdit.

Dans le cas où un(e) candidat(e) repère ce qui lui semble être une erreur d'énoncé, il (elle) le signale très lisiblement sur sa copie, propose la correction et poursuit l'épreuve en conséquence.
De même, si cela vous conduit à formuler une ou plusieurs hypothèses, il vous est demandé de la (ou les) mentionner explicitement.

NB : La copie que vous rendrez ne devra, conformément au principe d'anonymat, comporter aucun signe distinctif, tel que nom, signature, origine, etc. Si le travail qui vous est demandé comporte notamment la rédaction d'un projet ou d'une note, vous devrez impérativement vous abstenir de signer ou de l'identifier.

A

Tournez la page S.V.P.

Problème n° 1

Notations

On note $\mathbb{N}$ l'ensemble des entiers naturels, $\mathbb{N}^*$ l'ensemble des entiers naturels non nuls et $\mathbb{Z}$ l'ensemble des entiers relatifs.

Soient p et q deux entiers relatifs tels que $p \leqslant q$, on note $[\![p,q]\!]$ l'ensemble des entiers relatifs k tels que $p \leqslant k \leqslant q$.

Préambule

Ce problème a pour objet l'étude de deux méthodes de chiffrement.

À chaque lettre de l'alphabet est associé un unique entier compris entre 0 et 25 de la façon suivante : à la lettre A est associé 0, à la lettre B est associé 1, ..., à la lettre Z est associé 25. Cet entier est appelé **rang de la lettre**.

Partie A. – Un chiffrement monographique

L'objectif de cette partie est de démontrer les théorèmes de Bézout, puis de Gauss, et de mettre en œuvre ces théorèmes dans le chiffrement proposé.

I. Soient a et b des entiers relatifs non nuls.

1. Montrer que s'il existe des entiers relatifs u et v tels que $au + bv = 1$, alors a et b sont premiers entre eux.

2. On veut à présent prouver que la réciproque de cette propriété est vraie. On suppose que a et b sont premiers entre eux et on considère l'ensemble $\mathscr{E}$ des entiers relatifs de la forme $au + bv$ où u et v sont des entiers relatifs.

a. Montrer que l'ensemble $\mathscr{E} \cap \mathbb{N}^*$ admet un plus petit élément, que l'on notera n_0.

b. Démontrer que le reste de la division euclidienne de a (respectivement b) par n_0 vaut 0.

c. Conclure.

3. Énoncer le théorème ainsi démontré.

II. À l'aide du théorème précédent, démontrer que, pour tous les entiers relatifs non nuls a, b et c, si a divise bc et si a et b sont premiers entre eux, alors a divise c.

III. Chiffrement lettre à lettre

1. Un exemple. — Dans cette question, on décide de coder chaque lettre d'un mot par un nombre y défini comme suit : *si x est le rang de la lettre à coder, y est le reste de la division euclidienne de* $58x$ *par* 369.

a. Coder le mot GAUSS.

b. Proposer une activité de classe sur tableur permettant, à partir du codage des 26 lettres de l'alphabet de décoder le mot de 6 lettres qui se cache derrière la suite de nombres :

$$290 \quad 232 \quad 248 \quad 327 \quad 0 \quad 364$$

(Dans cette question, le décodage effectif n'est pas demandé ; il le sera à la question III.3.c.)

2. Principe général du chiffrement lettre à lettre. — On se donne un couple d'entiers naturels (n,e) vérifiant les conditions suivantes :

- L'entier n est supérieur ou égal à 26.
- Les entiers n et e sont premiers entre eux.

Chaque lettre est alors codée de la façon suivante : *si x est le rang de la lettre à coder, y est le reste de la division euclidienne de ex par n.*

a. Démontrer qu'il existe un entier naturel f tel que $fe \equiv 1 \pmod{n}$.

b. Démontrer que la connaissance de f permet de retrouver x à partir de y. On dit que f est une *clé de décodage* associée à la clé de codage (n,e).

3. Un procédé de construction d'une clé de codage et d'une clé de décodage associée :

- On choisit quatre entiers naturels a, b, c, et d supérieurs ou égaux à 3.
- On pose : $M = ab - 1$, $e = cM + a$, $f = dM + b$ et $n = \dfrac{ef-1}{M}$.

a. Vérifier que (n,e) est une clé de codage et que f est une clé de décodage associée.

b. Calculer n, e, et f lorsque $a = 3$, $b = 4$, $c = 5$ et $d = 6$.

c. Un mot de 6 lettres a été codé à l'aide de la clé définie à la question précédente :

290 232 248 327 0 364

Décoder ce mot.

4. Ensemble des clés de décodage associées à une clé de codage donnée. — On revient au cas général où n est un entier naturel supérieur ou égal à 26 et e un entier naturel premier avec n et on se propose de déterminer l'ensemble des couples (u,v) d'entiers relatifs tels que $nu + ev = 1$.

L'algorithme d'Euclide, qui permet de déterminer le PGCD de deux entiers naturels non nuls, assure l'existence d'un entier naturel N strictement supérieur à 1 et de deux suites finies $(r_k)_{k\in[\![0,N+1]\!]}$ et $(q_k)_{k\in[\![1,N]\!]}$ telles que :

- La suite $(r_k)_{k\in[\![0,N+1]\!]}$ est strictement décroissante.
- $r_0 = n, \quad r_1 = e \quad$ et $\quad r_{N+1} = 0$.
- $\forall k \in [\![1,N]\!], \quad r_{k-1} = r_k q_k + r_{k+1}$.

a. Que vaut r_N ?

b. Démontrer qu'il existe deux suites d'entiers relatifs $(u_k)_{k\in[\![0,N]\!]}$ et $(v_k)_{k\in[\![0,N]\!]}$ vérifiant, pour tout $k \in [\![0,N]\!]$,

$$r_k = nu_k + ev_k.$$

c. En déduire une clé de décodage associée à la clé de codage (n,e).

d. On met en œuvre cette méthode à l'aide d'un tableur à partir de la clé de codage $(369,58)$:

	A	B	C	D
1	r	q	u	v
2	369		1	0
3	58	6	0	1
4	21	2	1	-6
5	16	1	-2	13

Quelle formule a-t-on saisie dans la cellule C4 pour que, tirée en bas et à droite, elle permette de déterminer les valeurs des termes des deux suites (u_k) et (v_k) ?

e. Déterminer un couple (u,v) d'entiers relatifs tels que $369u+58v=1$ et une clé de décodage associée à la clé de codage $(369,58)$.

f. Déterminer l'ensemble des couples (u,v) d'entiers relatifs tels que $369u+58v=1$ et l'ensemble des clés de décodage associées à la clé de codage $(369,58)$.

Partie B. – Chiffrement de Hill

L'objectif de cette partie est de retrouver quelques résultats sur les matrices carrées d'ordre 2 à coefficients réels, puis de les appliquer au chiffrement de Hill.

La matrice nulle d'ordre 2 est notée O_2 et la matrice unité d'ordre 2 est notée I_2.

Pour tout entier naturel n non nul, si P et Q sont deux matrices carrées d'ordre 2 dont les coefficients respectifs $p_{i,j}$ et $q_{i,j}$ appartiennent à $\mathbb{Z}$, on dit qu'elles sont congrues modulo n et on note $P \equiv Q \pmod{n}$ lorsque

$$\forall (i,j) \in \{1,2\}, \quad p_{i,j} \equiv q_{i,j} \pmod{n}.$$

De même, on dit que les vecteurs colonnes à coefficients dans $\mathbb{Z}$

$$X = \begin{pmatrix} x \\ y \end{pmatrix} \quad \text{et} \quad X' = \begin{pmatrix} x' \\ y' \end{pmatrix}$$

sont congrus modulo n et on note $X \equiv X' \pmod{n}$ lorsque $x \equiv x' \pmod{n}$ et $y \equiv y' \pmod{n}$.

Dans toute cette partie, la matrice A est définie par

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

où a, b, c et d désignent quatre réels.

I. Questions de cours

1. Donner la définition d'une matrice inversible et démontrer l'unicité de son inverse.
2. Établir que $A^2-(a+d)A+(ad-bc)I_2 = O_2$.
3. Démontrer que la matrice A est inversible si et seulement si $ad-bc \neq 0$.

II. Dans cette question, on suppose que a, b, c et d sont des entiers relatifs.

1. Donner un exemple de matrice inversible à coefficients dans $\mathbb{Z}$, mais dont l'inverse n'a pas tous ses coefficients dans $\mathbb{Z}$.
2. Énoncer une condition suffisante pour que la matrice A soit inversible et que son inverse A^{-1} soit à coefficients dans $\mathbb{Z}$.
3. Quelle notion mathématique (qui ne figure pas dans les programmes de lycée) permet de prouver que cette condition est nécessaire ? Proposer une démonstration du résultat.

III. La méthode étudiée ci-après utilise un chiffrement par blocs de 2 lettres pour coder un mot comportant un nombre pair de lettres :

- On choisit quatre entiers naturels non nuls a, b, c et d.
- On note x le rang de la première lettre du bloc et y le rang de la deuxième lettre du bloc.

- On définit les entiers x' et y' de la manière suivante :

$$(S) \qquad \begin{cases} x' = ax + by \\ y' = cx + dy \end{cases}$$

- Le rang de la première lettre du bloc codé est le reste modulo 26 de x' ; le rang de la deuxième lettre du bloc codé est le reste modulo 26 de y'.

Un tel chiffrement est dit digraphique.

1. Traduire le système (S) par une relation matricielle à l'aide de la matrice A qui est appelée **matrice de codage**.
2. On donne : $a = 4$, $b = 3$, $c = 5$ et $d = 4$.
   a. Coder le mot BEZOUT.
   b. En détaillant les étapes, décoder le mot suivant :

   S F X M O J

3. On donne à présent $a = 3$, $b = 2$, $c = 1$ et $d = 3$. On souhaite décoder le mot suivant :

   A K X O U E V H D L

   a. Démontrer qu'il existe un unique entier u compris entre 0 et 25 tel que

   $$7u \equiv 1 \pmod{26}.$$

   b. On note A la matrice de codage associée aux entiers a, b, c et d. Déterminer une matrice B, à coefficients entiers relatifs, telle que $uBA \equiv I_2 \pmod{26}$.
   c. Décoder le mot en détaillant la démarche pour le premier bloc de deux lettres.
4. À quelle condition sur a, b, c et d peut-on décoder tout mot comportant un nombre pair de lettres ?

Problème n° 2

Notations

On note $\mathbb{N}$ l'ensemble des entiers naturels et $\mathbb{N}^*$ l'ensemble des entiers naturels non nuls.

Soient p et q deux entiers relatifs tels que $p \leqslant q$, on note $[\![p, q]\!]$ l'ensemble des entiers relatifs k tels que $p \leqslant k \leqslant q$.

Partie A

Une urne contient des boules rouges et des boules noires. On désigne par n un entier naturel non nul et on considère l'expérience aléatoire consistant à effectuer n tirages avec remise. On attribue à chaque tirage d'une boule noire (échec) la valeur 0 et à chaque tirage d'une boule rouge (succès) la valeur 1. On peut modéliser cette expérience à l'aide d'un arbre comportant 2^n chemins. Ces chemins sont des n-uplets dont chaque composante appartient à l'ensemble $\{0, 1\}$. Par exemple, si $n = 4$, un des $2^4 = 16$ chemins est $(0, 0, 1, 0)$.

I. On suppose dans cette question que $n = 4$.

1. Écrire la liste des 16 chemins.
2. Parmi ces chemins, combien y en a-t-il qui contiennent exactement 2 fois l'élément 1 ?
3. Parmi les chemins contenant exactement 2 fois l'élément 1, combien y en a-t-il contenant 1 à la première place ? À la deuxième place ? À la troisième place ? À la quatrième place ?

II. On revient au cas général où $n \in \mathbb{N}^*$ et on se donne $k \in [\![0, n]\!]$.

Dans les questions II.1, II.2 et II.3, pour tout entier $p \in [\![0, n]\!]$, l'entier $\binom{n}{p}$ est défini comme au lycée : il s'agit donc du nombre de chemins de l'arbre correspondant à n tirages et réalisant exactement p succès. En particulier, on n'aura pas recours dans ces trois questions à l'expression des coefficients binomiaux à l'aide de factorielles.

1. Démontrer que $\binom{n}{k} = \binom{n}{n-k}$.
2. On suppose dans cette question que $k \neq 0$. En exprimant de deux manières différentes le nombre de $(n+1)$-uplets contenant k fois l'élément 1, démontrer que
$$\binom{n}{k-1} + \binom{n}{k} = \binom{n+1}{k}.$$
3. Pour $1 \leqslant k \leqslant n$, on se propose de démontrer l'égalité
$$k\binom{n}{k} = n\binom{n-1}{k-1}.$$
On considère une matrice A à n colonnes dont chacune des $\binom{n}{k}$ lignes est l'un des chemins conduisant à k succès et $n-k$ échecs.
   - **a.** Calculer la somme des éléments d'une ligne de la matrice.
   - **b.** Soit $j \in [\![1, n]\!]$. Que représente la somme des éléments de la j-ème colonne de la matrice A ?
   - **c.** Conclure.

4. Dans l'enseignement supérieur, on définit, pour tout entier $p \in [\![0, n]\!]$, l'entier $\binom{n}{p}$ comme étant le nombre de parties à p éléments d'un ensemble à n éléments.

   a. Justifier la cohérence de cette définition avec celle qui est donnée au lycée.

   b. Démontrer que $\binom{n}{k} = \dfrac{n!}{k!(n-k)!}$.

   c. Retrouver par le calcul les résultats des questions II.2 et II.3.

III. On note θ la proportion de boules rouges dans l'urne et X la variable aléatoire égale au nombre de boules rouges (succès) obtenues à l'issue des n tirages. Identifier la loi de X et, en utilisant la question II.3 ainsi que la formule du binôme, calculer son espérance.

Partie B

Un point se déplace sur un axe gradué. Il se trouve au départ à l'origine et son déplacement à chaque étape est déterminé par le résultat du lancer d'une pièce équilibrée :

- Si on obtient pile, son abscisse augmente de 1.
- Si on obtient face, son abscisse diminue de 1.

On note D_n le nombre de fois où la pièce est tombée sur pile au cours des n premiers lancers et X_n l'abscisse du point à l'issue du n-ième lancer.

I. **1.** Donner la loi de la variable aléatoire X_4.

2. Reconnaître la loi de la variable aléatoire D_n.

3. Exprimer X_n à l'aide de D_n.

4. Calculer l'espérance de X_n. Interpréter le résultat.

II. **1.** Que vaut la probabilité $P(X_n = 0)$ lorsque n est impair ?

2. Calculer la probabilité $P(X_{2n} = 0)$.

III. **1.** L'algorithme suivant utilise une fonction `alea()` qui renvoie à chaque appel un nombre aléatoire selon la loi uniforme sur l'intervalle $]0, 1[$:

```
entrer(n)
x ← 0
pour k allant de 1 à n
      si alea() > 0,5 alors
           x ← x + 1
      sinon
           x ← x − 1
      finsi
finpour
retourner(x)
```

À quoi correspond la valeur renvoyée par cet algorithme ?

2. Écrire un deuxième algorithme, obtenu en modifiant l'algorithme donné, de façon à ce qu'il renvoie le nombre de passages à l'origine à l'issue de n lancers.

Tournez la page S.V.P.

3. Écrire un troisième algorithme, obtenu en modifiant l'algorithme donné, de façon à ce qu'il renvoie la fréquence d'apparition de l'événement $X_n = 0$ au cours de la répétition de 1 000 séries de n lancers.

4. Comment un professeur peut-il exploiter ces algorithmes devant une classe ?

IV. Soit $n \in \mathbb{N}^*$. Dans cette question, on s'intéresse à la position du point à l'issue de $2n$ lancers et au nombre de passages à l'origine entre le premier et le $2n$-ième lancer.

1. Expliquer pourquoi, à l'issue de ces $2n$ lancers, l'abscisse du point ne peut être qu'un entier relatif pair compris entre $-2n$ et $2n$.

2. Soit $k \in [\![0, n]\!]$. Calculer la probabilité qu'à l'issue de ces $2n$ lancers, l'abscisse du point soit égale à $2k$.

3. On note C_n la variable aléatoire égale au nombre de passages à l'origine entre le premier et le $2n$-ième lancer.

   Calculer l'espérance $E(C_n)$ de la variable aléatoire C_n et montrer par récurrence sur n que, pour tout entier $n \geqslant 1$,
$$E(C_n) = \frac{2n+1}{4^n}\binom{2n}{n} - 1.$$

   On pourra utiliser la variable aléatoire Ω_k égale à 1 si l'abscisse du point à l'issue du k-ième lancer est nulle et égale à 0 sinon.