# BREVET DE TECHNICIEN SUPÉRIEUR
# SERVICES INFORMATIQUES
# AUX ORGANISATIONS

## SESSION 2015

## SUJET

## ÉPREUVE E2 – MATHÉMATIQUES POUR L'INFORMATIQUE

**Sous épreuve E21 – Mathématiques**
**Épreuve obligatoire**

**Durée : 2 heures** **coefficient : 2**

***Calculatrice autorisée,*** *conformément à la circulaire n° 99-186 du 16 novembre 1999 :*
« Toutes les calculatrices de poche, y compris les calculatrices programmables, alphanumériques ou à écran graphique, à condition que leur fonctionnement soit autonome et qu'il ne soit pas fait usage d'imprimante, sont autorisées.
Les échanges de machines entre candidats, la consultation des notices fournies par les constructeurs ainsi que les échanges d'informations par l'intermédiaire des fonctions de transmission des calculatrices sont interdits ».

**Dès que le sujet vous est remis, assurez-vous qu'il est complet.**

**Il comprend 5 pages numérotées de la page 1/5 à 5/5.**

# Exercice 1 (10 points)

## Partie 1

Une entreprise européenne de vente de matériel informatique anticipe l'évolution des ventes de claviers souples dans les années à venir. Elle souscrit le contrat suivant avec son fournisseur :

- l'entreprise s'engage à commander initialement 500 claviers, et à augmenter sa commande de 100 unités par semestre (un semestre dure 6 mois) ;
- de son côté, le fournisseur s'engage à vendre chaque clavier souple 9 euros au début du contrat, et à multiplier ce prix par 0,95 chaque semestre.

Au bout de $n$ semestres, $n$ étant un entier naturel quelconque, on note $u_n$ le nombre de claviers souples achetés par l'entreprise, et $p_n$ le prix unitaire d'un clavier souple, exprimé en euro.

Ainsi, $u_0 = 500$ et $p_0 = 9$.

1. **a)** Calculer $u_1$ et $u_2$.
   **b)** Déterminer la nature de la suite $(u_n)$ et exprimer $u_n$ en fonction de $n$.

2. **a)** Calculer $p_1$ et $p_2$, en arrondissant les résultats au centième.
   **b)** Déterminer la nature de la suite $(p_n)$ et exprimer $p_n$ en fonction de $n$.

3. Déterminer le prix unitaire $p_n$ d'un clavier, arrondi au centime d'euro, lorsque l'entreprise en commandera 1000.

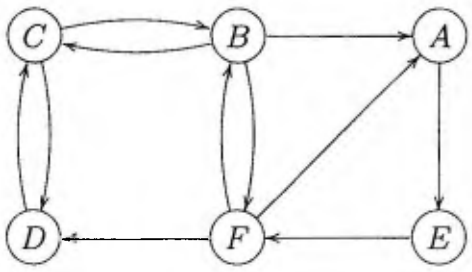
4. L'entreprise et le fournisseur conviennent que le contrat sera rompu lorsque le prix unitaire d'un clavier souple sera inférieur à 5 euros.
   Déterminer le nombre d'années qui engagent l'entreprise et son fournisseur. Justifier.

5. En honorant le contrat, l'entreprise dépense chaque semestre une somme, en euro, égale au produit du nombre de claviers commandés par leur prix unitaire.

   Déterminer la dépense de l'entreprise pour les 5 premières années, c'est-à-dire pour les semestres numérotés de 0 à 9.

## Partie 2

Le fournisseur doit livrer 5 entreprises. Le réseau de transport est représenté par le graphe orienté donné ci-dessous où l'entrepôt du fournisseur est noté $F$, et les entreprises sont notées $A$, $B$, $C$, $D$, $E$.



1. Écrire la matrice d'adjacence $M$ de ce graphe en considérant les sommets notés $A$, $B$, $C$, $D$, $E$, et $F$ dans cet ordre.

2. Le fournisseur souhaite livrer chacune des entreprises. Il part de son entrepôt.

   a) Existe-t-il un chemin hamiltonien d'origine $F$ dans ce graphe ? Si oui, citer un tel chemin.
   b) Interpréter le résultat relativement aux possibilités de livraison.

3. On donne la matrice $M^3 = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 2 & 0 & 4 & 0 & 1 & 3 \\ 1 & 3 & 0 & 3 & 1 & 0 \\ 1 & 0 & 2 & 0 & 0 & 1 \\ 1 & 0 & 2 & 0 & 1 & 1 \\ 1 & 3 & 0 & 3 & 1 & 1 \end{pmatrix}$.

   **a)** Dans le contexte de l'exercice, interpréter le coefficient 2 situé sur la quatrième ligne et la troisième colonne de la matrice $M^3$.

   **b)** Combien existe-t-il de chemins de longueur 3 issus du sommet $D$ dans ce graphe ? Justifier puis citer ces chemins.

   **c)** Le fournisseur doit maintenant effectuer une livraison, depuis l'entrepôt, dans quatre entreprises en commençant par l'entreprise $D$.

   Montrer que, pour effectuer cette livraison sans repasser par une entreprise déjà livrée, le fournisseur n'a qu'un seul chemin possible.
   Expliquer la démarche et préciser ce chemin.

## Exercice 2 (5 points)

Dans cet exercice on note $\Rightarrow$ le connecteur binaire d'implication.
Étant donnée une proposition $P$, on note $\overline{P}$ sa négation.

On admet la propriété suivante, démontrée par le mathématicien du XVII$^{e}$ siècle Pierre de Fermat.

**Propriété (1) :**
Soit $p$ un entier naturel.
Si $p$ est un nombre premier alors pour tout entier naturel $a$ :

$p$ divise $a^p - a$.

Dans la suite de l'exercice, $p$ est un entier naturel. On définit les prédicats suivants :

- $P(p)$ : $p$ est un nombre premier.
- $Q(p)$ : $\forall a \in \mathbf{N}, p$ divise $a^p - a$.

Les négations des prédicats $P(p)$ et $Q(p)$ sont notées respectivement $\overline{P(p)}$ et $\overline{Q(p)}$.

**1.** Les trois questions suivantes sont à choix multiple. Pour chacune d'elles, recopier la seule bonne réponse. Une réponse fausse ou une absence de réponse n'ôte pas de point.

**a)** Soit $a$ et $b$ deux entiers naturels, avec $b$ différent de 0.
Si le reste de la division euclidienne de $a$ par $b$ est égal à 0 alors :
- $b$ divise $a$ ;
- $b$ est un multiple de $a$ ;
- $a$ divise $b$ ;
- $a$ est un diviseur de $b$.

**b)** Le prédicat $\overline{Q(p)}$ peut être exprimé par :
- $\forall a \notin \mathbf{N}, p$ divise $a^p - a$ ;
- $\forall a \in \mathbf{N}, p$ ne divise pas $a^p - a$ ;
- $\exists a \in \mathbf{N}, p$ divise $a^p - a$ ;
- $\exists a \in \mathbf{N}, p$ ne divise pas $a^p - a$.

**c)** Soient $P$ et $Q$ deux propositions. Une proposition équivalente à $P \Rightarrow Q$ est :
- $\overline{Q} \Rightarrow \overline{P}$ ;
- $\overline{Q} \Rightarrow P$ ;
- $\overline{P} \Rightarrow \overline{Q}$ ;
- $\overline{P} \Rightarrow Q$.

**2.** La propriété (1) permet d'affirmer que la proposition « $\forall p \in \mathbf{N}$, $P(p) \Rightarrow Q(p)$ » est vraie.
On s'intéresse dans cette question à l'entier $p = 2701$. On donne les résultats suivants :

| $a$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| Reste de la division euclidienne de $a^{2701} - a$ par 2701 | 0 | 0 | 0 | 0 | 0 | 1961 | 0 | 1965 |

**a)** Donner la valeur de vérité de $Q(2701)$. Justifier à l'aide du tableau ci-dessus.

**b)** 2701 est-il un nombre premier ? Justifier.

## Exercice 3 (5 points)

Alice et Bob veulent échanger des messages privés sur un canal public qui peut être espionné. Pour cela ils choisissent un nombre premier $p$ qu'ils se communiquent par le canal public, puis calculent une clé secrète commune $K$ par un protocole nommé « protocole de Diffie-Hellman ». Cette clé secrète, qui est un entier naturel, leur permettra ensuite de coder les messages qu'ils s'enverront.

Pour le calcul de cette clé secrète, Alice et Bob commencent par échanger un nombre entier $g$ par le canal public.
Ensuite Alice choisit pour elle-même un entier naturel $a$, et Bob choisit pour lui-même un entier naturel $b$.

Les entiers $g$, $a$ et $b$ seront utilisés par Alice et par Bob pour déterminer la valeur de l'entier $K$, selon un protocole qui utilise des congruences modulo l'entier premier $p$.
Ce protocole est décrit dans les questions qui suivent, d'abord de façon générale avec des écritures littérales, puis avec des calculs numériques qui seront effectués avec les valeurs :

$$p = 2741,\ g = 14,\ a = 3 \text{ et } b = 12.$$

**1.** Calcul d'un entier $x$ par Alice

Alice doit déterminer l'unique entier $x$ vérifiant $0 \leq x \leq p-1$ et $g^a \equiv x \pmod{p}$.

Déterminer cet entier $x$ en prenant $p = 2741$, $g = 14$ et $a = 3$, c'est-à-dire déterminer l'entier $x$ vérifiant les conditions : $0 \leq x \leq 2740$ et $14^3 \equiv x \pmod{2741}$.

**2.** Calcul d'un entier $y$ par Bob

Bob doit déterminer l'unique entier $y$ vérifiant $0 \leq y \leq p-1$ et $g^b \equiv y \pmod{p}$.

Déterminer cet entier $y$, en prenant $p = 2741$, $g = 14$ et $b = 12$, c'est-à-dire déterminer l'entier $y$ vérifiant les conditions : $0 \leq y \leq 2740$ et $14^{12} \equiv y \pmod{2741}$.

(Pour le calcul de la puissance douzième, on pourra utiliser l'égalité $14^{12} = 14^6 \times 14^6$ et remarquer que $14^6 \equiv 9 \pmod{2741}$.)

À ce niveau, en utilisant un canal public, Alice transmet à Bob le nombre $x$ qu'elle a calculé, et Bob transmet à Alice le nombre $y$ qu'il a calculé.

**3.** Calcul de la clé $K$ par Bob

Bob peut calculer l'entier $K$ en utilisant les conditions $0 \leq K \leq p-1$ et $x^b \equiv K \pmod{p}$.

Déterminer cet entier $K$, avec les valeurs $p = 2741$ et $b = 12$.

*On admet qu'Alice peut retrouver le même entier $K$ en utilisant les conditions $0 \leq K \leq p-1$ et $y^a \equiv K \pmod{p}$, avec les valeurs $p = 2741$ et $a = 3$.*