BREVET DE TECHNICIEN SUPÉRIEUR
SERVICES INFORMATIQUES
AUX ORGANISATIONS

SESSION 2014

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 4 pages numérotées de la page 1/4 à 4/4.

Exercice 1 (7 points)

Un amateur a publié un site internet avec 5 pages, notées P_1, P_2, P_3, P_4 et P_5.
La page d'accueil du site est la page P_1.
Chaque page contient des liens permettant de naviguer vers d'autres pages.

Pour améliorer la navigation sur son site, il demande conseil à un informaticien, qui modélise le site par un graphe.
Les 5 sommets S_1, S_2, S_3, S_4 et S_5 de ce graphe représentent les 5 pages.
Un lien d'une page vers une autre est représenté par un arc orienté allant du sommet associé à la page de départ vers celui associé à la page d'arrivée.

Le tableau des successeurs obtenu par l'informaticien est le suivant :

Sommet	S_1	S_2	S_3	S_4	S_5
Successeurs	S_2, S_3, S_5	S_3	S_2	S_3	S_1, S_2, S_4

1. a) Déterminer la matrice d'adjacence M de ce graphe.

b) Donner une représentation géométrique de ce graphe orienté.

2. Existe-t-il un chemin hamiltonien dans ce graphe ? Si oui, en indiquer un.

3. Calculer la matrice M^2.

4. a) Combien existe-t-il de chemins de longueur 2 dans le graphe ?

b) Combien existe-t-il de chemins de longueur 2 issus du sommet S_1 ?

5. On rappelle que la matrice M' de fermeture transitive du graphe est donnée par l'addition booléenne : $M' = M \oplus M^{[2]} \oplus M^{[3]} \oplus M^{[4]} \oplus M^{[5]}$.

On admet que $M' = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 \end{pmatrix}$.

a) Quelle sont les pages du site qui sont accessibles depuis toutes les autres pages en quelques clics ? Justifier.

b) Interpréter les 0 de la première colonne de la matrice M' dans le contexte de l'énoncé.

Exercice 2 (6 points)

Une société de création de jeux vidéo commercialise un nouveau produit. Avec les bénéfices escomptés, elle souhaite renouveler son parc informatique.

Partie A : choix des ordinateurs

Les ordinateurs envisagés offrent les composants suivants :
- un processeur quad-core ou dual-core ;
- une carte graphique avec 4 Go ou 2 Go de mémoire ;
- un disque dur SATA ou SSD.

Pour un ordinateur quelconque, on définit les variables booléennes suivantes :
- $a = 1$ s'il possède un processeur quad-core, $a = 0$ sinon ;
- $b = 1$ si la carte graphique a 4 Go de mémoire, $b = 0$ sinon ;
- $c = 1$ si l'ordinateur possède un disque dur SATA, $c = 0$ sinon.

Le responsable informatique a pu tester différentes combinaisons de composants.
Il décide de retenir, pour les équipements informatiques futurs de la société, des ordinateurs satisfaisant aux critères de choix suivants :
- être équipé d'un processeur quad-core et d'un disque dur SSD ;
- ou être équipé d'un processeur dual-core et d'une carte graphique de 4 Go ;
- ou être équipé d'un processeur quad-core, d'une carte graphique de 4 Go et d'un disque dur SATA.

1. Traduire par une expression booléenne E les critères de choix du responsable informatique.

2. À l'aide d'un tableau de Karnaugh ou d'un calcul booléen, trouver une expression simplifiée de E sous la forme d'une somme de deux termes.

3. Traduire par une phrase, dans le contexte de l'énoncé, l'expression simplifiée trouvée à la question précédente.

Partie B : financement du projet

Le renouvèlement du parc informatique est échelonné sur 12 trimestres, pour un coût total de 95 500 €.
Le service comptable propose le financement suivant :
- pour le 1er trimestre, verser un montant de 6 000 € ;
- chaque trimestre, le montant versé augmente de 5 % par rapport à celui du trimestre précédent.

On note u_n le montant, exprimé en euro, versé le n-ième trimestre. On a donc $u_1 = 6\,000$.

1. Vérifier que $u_2 = 6\,300$ et calculer u_3.

2. Montrer que la suite (u_n) est une suite géométrique dont on donnera la raison.

3. **a)** Exprimer u_n en fonction de n.

b) Calculer le montant versé au dernier trimestre, arrondi à l'euro.

4. On rappelle que, pour une suite géométrique (U_n) de raison q différente de 1 et de premier terme U_1, on a la formule : $U_1 + U_2 + \cdots + U_n = U_1 \times \dfrac{1-q^n}{1-q}$.

Le financement prévu permet-il de renouveler le parc informatique ? Justifier.

Exercice 3 (7 points)

Alice souhaite que Bob lui envoie des données confidentielles par Internet. Pour éviter que ces données puissent être exploitées par une tierce personne, ils ont recours à un cryptage de type RSA. Aucune connaissance sur le cryptage RSA n'est attendue dans cet exercice.

Partie A – Création des clés publique et privée par Alice

1. Il faut tout d'abord choisir deux nombres premiers distincts notés p et q, puis calculer leur produit noté n. Alice décide de prendre $p=5$ et $q=23$, ce qui donne $n=115$.

Expliquer pourquoi 23 est un nombre premier.

2. Il faut ensuite calculer $K=(p-1)\times(q-1)$, ce qui donne ici $K=4\times22=88$, puis trouver un entier naturel c, compris entre 2 et K, qui soit premier avec K. Le couple d'entiers (n,c) est la *clé publique*. Alice décide de prendre $c=9$.

a) Donner la décomposition en produit de facteurs premiers de 88.

b) Expliquer pourquoi 9 et 88 sont deux nombres premiers entre eux.

3. Il faut enfin trouver un entier d tel que $d\times c\equiv1$ modulo K. Le couple d'entiers (n,d) est la *clé privée*. Alice a trouvé $d=49$.

Expliquer pourquoi $49\times9\equiv1$ modulo 88.

Partie B – Cryptage du message à envoyer par Bob avec la clé publique d'Alice

Alice envoie sa clé publique à Bob et celui-ci s'en sert pour crypter un nombre a, qui doit être un entier naturel strictement inférieur à n. Le nombre crypté b est alors égal au reste dans la division euclidienne de a^c par n. C'est ce nombre crypté b que Bob envoie à Alice.

Bob veut transmettre à Alice le nombre 12.

Déterminer le nombre crypté b que Bob envoie à Alice.

Partie C – Décryptage d'un message reçu par Alice avec sa clé privée

Cette partie est indépendante de la précédente.

Alice reçoit un nouveau nombre crypté de la part de Bob : le nombre 2. Pour le décrypter, Alice utilise sa clé privée, c'est-à-dire le couple (n,d).

On admet que le nombre non crypté transmis par Bob, noté a, est égal au reste dans la division euclidienne de 2^{49} par n.

Alice doit donc calculer le reste dans la division euclidienne de 2^{49} par 115 pour trouver a.
Mais sa calculatrice ne permet pas de calculer la valeur exacte de 2^{49}. Cependant, elle a pu obtenir les résultats suivants :

$$2^{33}=8\,589\,934\,592 \quad \text{et} \quad 8\,589\,934\,592\equiv47 \quad \text{modulo } 115,$$
$$2^{16}=65\,536 \quad \text{et} \quad 65\,536\equiv101 \quad \text{modulo } 115.$$

À partir de ces résultats, calculer le nombre a transmis par Bob à Alice.