BTS SIO

Mathématiques pour l'informatique

Épreuve U21

Annales 2013 - 2021

<u>Remarque :</u> Les exercices sur les suites n'entrent pas dans le programme de l'épreuve U2 du nouveau BTS. Ils sont utiles pour l'option UF2.

2021 Métropole

Exercice 1 (10 points) **: Un problème de routage**

Les parties A et B sont indépendantes.

Partie A

On considère un réseau de commutation de paquets constitués de 6 routeurs A, B, C, D, E et F. Chaque paquet reçu par l'un des routeurs doit être acheminé vers un autre routeur, jusqu'à atteindre sa destination finale.

Dans le tableau ci-dessous, on a résumé les règles de routage d'un routeur à un autre routeur.

Peut transmettre à	A	B	C	D	E	F
A			■	■	■	
B	■		■		■	■
C					■	
D						
E				■		■
F				■		

On considère le graphe simple orienté **G** constitué des sommets A, B, C, D, E et F. Les sommets représentent les routeurs. Si un sommet X peut transmettre un paquet vers un sommet Y alors on a l'arc X → Y.

1.
   a. Recopier et compléter le tableau des successeurs et des prédécesseurs du graphe **G** :

Sommets	Prédécesseurs	Successeurs
A		
B		
C		
D		
E		
F		

   b. Déterminer la matrice d'adjacence M du graphe **G,** les sommets étant rangés par ordre alphabétique.

2.
   a. Calculer M^3.
   b. Combien existe-t-il de chemins de longueur 3 allant du sommet B au sommet D ?

3.
   a. Déterminer la matrice $\widehat{M}$ de la fermeture transitive du graphe **G**.
   b. Que signifie le nombre 1 à l'intersection de la troisième ligne et la sixième colonne de $\widehat{M}$?

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

Partie B

Dans un parc informatique, chaque machine connectée à un réseau peut être identifiée à l'aide d'une adresse IPv4.

1.
   a. Dans la base 2, un octet est constitué de 8 chiffres.
      Déterminer le plus grand entier noté en base 10 qu'on peut écrire sous la forme d'un octet.
   b. Une adresse IPv4 étant constituée de 4 octets notés en base 10 et séparés par un point, quel nombre maximal d'adresses IPv4 peuvent être attribuées ?

Le routeur C de la partie A gère les connexions réseaux d'un parc informatique de 8 machines étiquetées de 1 à 8.
Le DHCP de ce routeur est paramétré de telle façon qu'il attribue une plage de 49 adresses IPv4 allant de 192.168.1.2 jusqu'à 192.168.1.50.
Les 8 machines sont identifiées grâce aux adresses IPv4 suivantes :

Etiquette de la machine	Adresse IPv4 de la machine
1	192.168.1.2
2	192.168.1.4
3	192.168.1.12
4	192.168.1.49
5	192.168.1.48
6	192.168.1.50
7	192.168.1.5
8	192.168.1.6

2. Écrire le premier octet commun aux adresses de ces machines sous forme binaire puis sous forme hexadécimale.

Exercice 2 (5 points)

Le spam, courriel indésirable ou pourriel, est une communication électronique non sollicitée, en premier lieu via le courrier électronique. Il s'agit en général d'envois en grande quantité effectués à des fins publicitaires.
Un étudiant en BTS SIO a développé un logiciel anti spam. Le filtre mis en place par l'étudiant se base sur les trois variables booléennes suivantes :

- a l'objet du message contient au moins un terme douteux (gratuit, offre, promotion, gagner ...), $\bar{a}$ l'objet du message ne contient aucun terme douteux ;
- b le corps du message contient des images ou des hyperliens, $\bar{b}$ le corps du message ne contient ni images, ni hyperliens ;
- c les messages de l'expéditeur sont rarement lus, $\bar{c}$ les messages de l'expéditeur sont lus fréquemment.

Avec ce logiciel, un courriel est considéré comme indésirable si :

- l'objet du message contient au moins un terme douteux avec un corps du message contenant des images ou des hyperliens ;
  ou
- l'objet du message ne contient aucun terme douteux et les messages de l'expéditeur sont rarement lus ;
  ou
- les messages de l'expéditeur sont rarement lus et le corps du message ne contient ni images, ni d'hyperliens ;

1. Traduire chaque condition par une expression booléenne en fonction des variables a, b et c puis déterminer l'expression booléenne E traduisant les conditions pour qu'un courriel soit considéré comme indésirable.
   Pour la suite de l'exercice, on admet que $E = ab + c\bar{a} + \bar{b}c$.

2.
   a. Présenter E dans une table de Karnaugh.
   b. Un courriel, ayant comme objet « promotion : une réduction de 50 % ...» et dont les messages de l'expéditeur sont lus fréquemment, peut-il être considéré comme indésirable ? Justifier.
   c. En utilisant la table de Karnaugh, déduire l'expression simplifiée de E sous la forme d'une somme de deux termes dont l'un est éventuellement un produit.

3. Traduire, en français, la règle pour considérer un courriel comme indésirable.

4. Donner une expression de $\bar{E}$.

Exercice 3 (5 points) : **Codage de Hill**

Dans le tableau suivant, on associe à chaque lettre de l'alphabet, en majuscule, son rang dans l'alphabet en commençant par 0.

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

La procédure pour chiffrer un message est décrite dans l'exemple ci-dessous :

Pour chiffrer le message « **CARTES** » avec la clé de chiffrement $W = \begin{pmatrix} 1 & 2 & 1 \\ 2 & 1 & 3 \\ 2 & 4 & 2 \end{pmatrix}$:

- On remplace chaque lettre par son rang : C par 2, A par 0, R par 17, T par 19, E par 4 et S par 18. On obtient ainsi une matrice à 3 colonnes $M = \begin{pmatrix} 2 & 0 & 17 \\ 19 & 4 & 18 \end{pmatrix}$;
- On effectue le produit matriciel $M \times W$; on a $M \times W = \begin{pmatrix} 36 & 72 & 36 \\ 63 & 114 & 67 \end{pmatrix}$;
- On remplace chaque coefficient de la matrice $M \times W$ par le reste de sa division euclidienne par 26. Ce qui revient à trouver, pour chaque coefficient, l'unique entier compris entre 0 et 25 qui lui est congru modulo 26.
  On a $36 \equiv 10\ [26]$, $72 \equiv 20\ [26]$, $63 \equiv 11\ [26]$, $114 \equiv 10\ [26]$, $67 \equiv 15\ [26]$;
  Ainsi on obtient la matrice $\begin{pmatrix} 10 & 20 & 10 \\ 11 & 10 & 15 \end{pmatrix}$
- On remplace chaque nouveau coefficient de $M \times W$ par la lettre correspondante ; on obtient donc $\begin{pmatrix} KUK \\ LKP \end{pmatrix}$;
- Donc le message chiffré est « **KUKLKP** ».

Partie A :

Dans cette partie, on considère la clé de chiffrement $W = \begin{pmatrix} 1 & 2 & 1 \\ 2 & 1 & 3 \\ 2 & 4 & 2 \end{pmatrix}$.

Cette clé permet de chiffrer le mot « **BUR** » en « **XMR** »

1. On considère le message « **JUA** ». Déterminer le message chiffré.

2. Que peut-on remarquer ? Que pensez-vous de cette clé de chiffrement ?

Partie B :

Dans cette partie, on considère la clé de chiffrement $W = \begin{pmatrix} 11 & n & 14 \\ 7 & 9 & 21 \\ 17 & 0 & 3 \end{pmatrix}$, où n est un entier naturel compris entre 15 et 25.

On sait que cette clé permet de chiffrer le mot « **GEL** » en « **VMT** ».

1. Vérifier que $6n + 36 \equiv 12 \pmod{26}$.

2. Déterminer la valeur de l'entier naturel n.

2021 Nouvelle Calédonie

Pas d'épreuve écrite….

2020 Métropole (Session spéciale)

Exercice 1 (5 points)

Une entreprise fabrique des manettes pour consoles de jeux vidéo. Elle en propose de deux tailles différentes : grandes ou bien petites ; qui sont de couleur soit noires, soit argentées pour chaque taille ; et qui sont sans fil ou bien à brancher pour chaque taille également.

On introduit les variables booléennes suivantes :

- g signifie que la manette est grande, $\bar{g}$ que la manette est petite ;
- n signifie que la manette est de couleur noire, $\bar{n}$ que la manette est de couleur argentée ;
- b signifie que la manette est à brancher, $\bar{b}$ que la manette est sans fil.

Cette entreprise fournit plusieurs fabricants qui lui en achètent des quantités analogues. Après plusieurs mois de vente, l'entreprise constate que les manettes vendues sont de l'un au moins des 4 types suivants :

- les grandes manettes sans fil ;
- les petites manettes de couleur noires ;
- les petites manettes de couleur argentées et sans fil ;
- les petites manettes qui sont à brancher.

On note E l'expression booléenne correspondant aux types de manettes les plus vendues par l'entreprise. On admet que **E =** $\boldsymbol{g.\bar{b}+\bar{g}.n+\bar{g}.\bar{n}.\bar{b}+\bar{g}.b}$.

1. Traduire par une phrase l'expression booléenne $\bar{g}.b$.
2. Représenter E par un tableau de Karnaugh, puis déterminer une forme simplifiée, à deux termes, de l'expression booléenne E.
3. Traduire par une phrase l'expression simplifiée E.
4. L'entreprise souhaite réduire sa production en supprimant les types de manettes non vendues. Lesquelles doit-elle supprimer ? Justifier votre réponse.

Exercice 2 (8 points)

Dans le modèle RGB (Red, Green, Blue), datant de 1931, la couleur et l'intensité de la lumière peuvent être représentées par la matrice colonne $C=\begin{pmatrix}R\\G\\B\end{pmatrix}$, où R représente l'intensité de la composante rouge, G l'intensité de la composante verte et B l'intensité de la composante bleue. L'intensité de chaque composante est, dans le système décimal, un entier compris entre 0 et 255 : 0 désigne l'absence de celle-ci et 255 désigne l'intensité maximale de celle-ci.

Partie A - Codage de couleurs.

La couleur « saumon » est codée par $\begin{pmatrix}248\\142\\85\end{pmatrix}$ en décimal, l'intensité du rouge est donc 248, celle du vert est 142 et celle du bleu est 85. Dans certains logiciels comme Photoshop par exemple, les couleurs sont codées par 3 nombres hexadécimaux à deux chiffres représentant les valeurs de Rouge, Vert et Bleu. En hexadécimal, cette couleur « saumon » est codée $(F8\ ;\ 8E\ ;\ 55)$ que l'on notera par la matrice $\begin{pmatrix}F8\\8E\\55\end{pmatrix}$.

1. La couleur « vert tilleul » est codée en écriture décimale par $\begin{pmatrix} 165 \\ 209 \\ 82 \end{pmatrix}$.

   Déterminer son codage en hexadécimal, on détaillera la démarche pour la valeur 165.

2. La couleur « mauve » est codée en hexadécimal par $\begin{pmatrix} D4 \\ 73 \\ D4 \end{pmatrix}$.

   Déterminer son codage en écriture décimale, on détaillera la démarche pour la valeur D4.

3. Combien de couleurs différentes peut-on représenter avec ce mode de représentation ? Combien de bits utilise ce codage ?

Partie B - De la lumière vers l'œil.

La rétine d'un œil humain est composée de deux types de récepteurs : les cônes et les bâtonnets. Les bâtonnets sont responsables de la vision à faible niveau d'énergie (vision nocturne dite « scotopique » et vision à niveaux de gris) et ne perçoivent pas les couleurs. Ils mesurent l'intensité de la lumière visible. Les cônes sont responsables de la vision diurne colorée. La vision des couleurs n'est pas toutefois directe, elle est envoyée au cerveau au moyen d'un signal S = $\begin{pmatrix} i \\ l \\ c \end{pmatrix}$, où :

- L'intensité i de la lumière est $i = \frac{1}{3}(R + G + B)$;
- L'intensité l des ondes longues est $l = R - G$;
- L'intensité c des ondes courtes est $c = B - \frac{R+G}{2}$

Par exemple, pour la couleur « vert tilleul » codée en décimal par $\begin{pmatrix} 165 \\ 209 \\ 82 \end{pmatrix}$, l'intensité i de la lumière est $i = \frac{1}{3}(165 + 209 + 82) = 152$; l'intensité l des ondes longues est

$l = 165 - 209 = -44$; et l'intensité c des ondes courtes est $c = 82 - \frac{165+209}{2} = -105.$

On note les matrices : $C = \begin{pmatrix} R \\ G \\ B \end{pmatrix}$ et $M = \begin{pmatrix} \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \\ 1 & -1 & 0 \\ -\frac{1}{2} & -\frac{1}{2} & 1 \end{pmatrix}$.

1. a. Donner une égalité reliant les matrices S, C et M.
   b. Calculer les différentes intensités i, l et c du signal lorsque $R = 150$, $G = 90$ et $B = 210$.

2. Soit N la matrice définie par : $N = \begin{pmatrix} 1 & \frac{1}{2} & -\frac{1}{3} \\ 1 & -\frac{1}{2} & -\frac{1}{3} \\ 1 & 0 & \frac{2}{3} \end{pmatrix}$.

   a. Calculer le produit $N \times M$.
   b. Que peut-on en déduire pour les matrices N et M ?

3. a. Prouver que si $M \times C = S$ alors $C = N \times S$.
   b. Le cerveau reçoit comme signal : $i = 120$; $l = 100$ et $c = -90$.
   Quelles sont les intensités R, G et B de la lumière reçue par l'œil ?

Exercice 3 (7 points)

En informatique, le code ASCII associe à certains caractères (lettre, chiffre, signe de ponctuation ...) un entier compris entre 0 et 255 que l'on appelle son code ASCII. La fonction code du tableur renvoie le code ASCII du caractère. L'extrait de tableur ci-dessous donne le codage de quelques caractères.

Lettre	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
Code ASCII:n	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90
$p=f(n)$	199	206																								

On décide de chiffrer (crypter) une lettre à partir de son code ASCII en utilisant la fonction f définie pour tout entier n tel que $0 \leq n < 256$ par : $f(n)$ est le reste de la division euclidienne de $7n$ par 256, c'est-à-dire que si on note $p = f(n)$, alors $p \equiv 7n$ (mod 256) où $p = f(n)$, avec p entier tel que $0 \leq p < 256$.

Par exemple, le code ASCII de la lettre A est 65. On a $7 \times 65 \equiv 199$ (mod 256) et $0 \leq 199 < 256$ donc la lettre A est chiffrée par 199.

Partie A - Chiffrement

1. Vérifier que la lettre « B » est chiffrée par le nombre 206.
2. Déterminer le cryptage du mot « BTS ». (On séparera chaque code de lettre par un espace).

Partie B - Déchiffrement.

Pour déchiffrer un entier p compris entre 0 et 255 (inclus), on calcule le reste de la division euclidienne de $183 \times p$ par 256 ; autrement dit $n \equiv 183 \times p$ (mod 256) avec n entier tel que $0 \leq n < 256$.

Par exemple, pour $p = 20$, on a $183 \times 20 \equiv 76$ (mod 256) et donc la valeur chiffrée correspond à la lettre L.

1. Déterminer la lettre correspondant à la valeur chiffrée 27. On détaillera la réponse.
2. Donner le mot de trois lettres correspondant au code chiffré des trois entiers : 234 255 34

Partie C - Justification

1. Prouver que $183 \times 7 \equiv 1$ (mod 256).
2. On souhaite justifier comment obtenir l'entier n à partir de l'entier $p = f(n)$.
   On rappelle que $f(n) \equiv 7n$ (mod 256).
   En déduire que $183 \times f(n) \equiv n$ (mod 256).

2020 Nouvelle Calédonie

Exercice 1 (6 points)

Pour constituer des groupes de travail en informatique dans une classe, un professeur définit trois variables booléennes $r, p, g,$ de la façon suivante :

- $r = 1$ si le groupe comprend au maximum un élève redoublant, $r = 0$ sinon ;
- $p = 1$ si le groupe comprend au moins un élève ayant déjà travaillé sur Python, $p = 0$ sinon ;
- $g = 1$ si le groupe ne comprend que des garçons, $g = 0$ sinon.

Les deux questions suivantes sont à choix multiple. Pour chacune d'elles, recopier la seule bonne réponse. Une réponse fausse ou une absence de réponse ne rapporte ni ne retire aucun point.

1. Parmi les phrases suivantes, recopier celle qui traduit le fait que $r = 0$:
- phrase A : « le groupe comprend au minimum un élève redoublant » ;
- phrase B : « le groupe ne comprend aucun élève redoublant » ;
- phrase C : « le groupe comprend au minimum deux élèves redoublants ».

2. Parmi les phrases suivantes, recopier celle qui traduit le fait que $p = 0$:
- phrase A : « le groupe comprend au plus un élève ayant déjà travaillé sur Python » ;
- phrase B : « le groupe ne comprend aucun élève ayant déjà travaillé sur Python » ;
- phrase C : « le groupe comprend au plus deux élèves ayant déjà travaillé sur Python ».

3. Le professeur impose à chaque groupe de respecter au moins une des contraintes suivantes :
- le groupe comprend au maximum un élève redoublant, et comprend au moins un élève ayant déjà travaillé sur Python, et ne comprend que des garçons,
  ou
- le groupe comprend au moins un élève ayant déjà travaillé sur Python et comprend au moins une fille,
  ou
- le groupe comprend au maximum un élève redoublant, et ne comprend aucun élève ayant déjà travaillé sur Python.

a) Traduire par une expression booléenne E les contraintes imposées à chaque groupe.

b) À l'aide d'un tableau de Karnaugh, déterminer une écriture simplifiée de E sous forme d'une somme de deux termes.

c) Interpréter cette écriture simplifiée par une phrase.

4. Les redoublants de la classe s'estiment désavantagés ; ils affirment : « *tous les groupes interdits contiennent au moins deux redoublants* ».

Cette affirmation est-elle vraie ? Justifier la réponse.

Exercice 2 (8 points)

Un groupe d'étudiants de BTS a planifié la réalisation d'un jeu dans le cadre du projet de fin d'année.

Le tableau suivant regroupe l'ensemble des informations.

Tâche à réaliser	Repère	Durée en heures	Tâches précédentes
Cahier des charges	A	4	
Recherches sur les interfaces graphiques	B	8	
Jeu en mode console	C	2	A
Page d'accueil	D	4	A, B
Interface graphique	E	12	A, B
Rapport	F	4	C, D, E
Extension (jeu en réseau)	G	8	C, D

On considère le graphe orienté correspondant aux conditions d'antériorité données par le tableau précédent. Les repères A, B, …, G sont les sept sommets de ce graphe.

1. Déterminer le niveau de chacun des sommets du graphe.
2. Construire le tableau des successeurs du graphe.
3. Construire le graphe d'ordonnancement du projet (selon la méthode P.E.R.T. ou M.P.M.). Déterminer pour chaque tâche les dates au plus tôt et au plus tard.
4. Déterminer le chemin critique et la durée minimale de réalisation du projet.
5. Déterminer la marge totale des sommets A et C.
6. Justifier le fait que, si la tâche A prend un retard de 4 h et la tâche C prend un retard de 8 h, alors le projet prendra du retard par rapport à la durée minimale de réalisation prévue.

Exercice 3 (6 points)

Une petite entreprise de la zone euro, créée le 1[er] janvier 2018, vend des ordinateurs destinés à des professionnels.

Les ordinateurs sont de trois types K, L et M. Le tableau suivant détaille les différents coûts, en euro, relatifs aux ordinateurs de chaque type, durant l'année 2018.

Type d'ordinateur	Type K	Type L	Type M
Coût des éléments matériels	100	150	250
Coût de la main d'œuvre	100	150	200
Coût de la livraison	50	50	50

On note $A = \begin{pmatrix} 100 & 150 & 250 \\ 100 & 150 & 200 \\ 50 & 50 & 50 \end{pmatrix}$ la matrice correspondant au tableau précédent et $X = \begin{pmatrix} x \\ y \\ z \end{pmatrix}$ la matrice colonne correspondant à x ordinateurs de type K, y ordinateurs de type L et z ordinateurs de type M vendus durant un mois de l'année 2018. Enfin, $Y = \begin{pmatrix} e \\ m \\ l \end{pmatrix}$ est la matrice colonne dont les trois nombres e, m et l sont les coûts totaux respectifs, en euro, des éléments matériels, de la main d'œuvre et de la livraison de tous ces ordinateurs, durant ce même mois.

1. a) Écrire une égalité matricielle reliant les matrices A, X et Y.

b) Durant le mois de janvier 2018, l'entreprise a vendu 25 ordinateurs de type K, 40 ordinateurs de type L et 15 ordinateurs de type M.
À l'aide du calcul matriciel, calculer le coût total des éléments matériels, celui de la main d'œuvre et celui de la livraison durant ce mois.

2. On considère la matrice $B = \begin{pmatrix} \frac{1}{50} & -\frac{1}{25} & \frac{3}{50} \\ -\frac{1}{25} & \frac{3}{50} & -\frac{1}{25} \\ \frac{1}{50} & -\frac{1}{50} & 0 \end{pmatrix}$.

a) Calculer le produit matriciel $B \times A$.

b) Démontrer que, si $A \times X = Y$, alors $X = B \times Y$.

c) Durant le mois de février 2016, le coût total relatif à tous les ordinateurs vendus s'est élevé à 13 500 € pour les éléments matériels, 12 350 € pour la main d'œuvre et 4 150 € pour la livraison.
Déterminer le nombre d'ordinateurs de chaque type qui ont été vendus durant ce mois.

2019 Métropole

Exercice 1 **9 points**

Les parties A et B de cet exercice sont relatives aux pages d'un site web. Elles peuvent être traitées de manière indépendante.

Partie A

Le site comporte 6 pages notées A, B, C. D. E et F. Les pages ainsi que les liens hypertextes d'une page vers une autre sont représentés par un graphe orienté de sommets A, B, C, D. E, F, en convenant qu'un lien hypertexte d'une page X vers une page Y est représenté par une flèche orientée du sommet X vers le sommet Y.
Le tableau ci-après récapitule tous les liens entre les sommets.

Sommet	Prédécesseurs
A	–
B	A
C	A
D	B
E	C, D
F	D, E

1. Donner la matrice d'adjacence du graphe que l'on peut construire à partir de ce tableau, les sommets étant rangés par ordre alphabétique.
2. Donner le niveau de chaque sommet puis dessiner ce graphe ordonné par niveaux.
3. Déterminer la matrice de la fermeture transitive de ce graphe.
4. Montrer que ce graphe ne contient pas de circuit.

Partie B

Chaque page du site comprend 4 questions, qui peuvent rapporter des points ou en faire perdre.
Un utilisateur peut accéder à une page suivante lorsque l'une au moins des conditions suivantes est satisfaite :

— l'utilisateur a répondu correctement à 3 questions au minimum,
ou
— l'utilisateur a répondu correctement à strictement moins de 3 questions et a marqué 5 points au minimum sur la page,
ou
— l'utilisateur a marqué strictement moins de 5 points sur la page et il est titulaire du BTS SIO

On définit les variables booléennes suivantes :

- $a = 1$ si l'utilisateur a répondu correctement à 3 questions au minimum, $a = 0$ sinon ;
- $b = 1$ si l'utilisateur a marqué 5 points au minimum, $b = 0$ sinon ;
- $c = 1$ si l'utilisateur est titulaire du BTS SIO, $c = 0$ sinon.

1. Écrire une expression booléenne F traduisant les conditions permettant à un utilisateur de passer à une page suivante.
2. À l'aide d'un tableau de Karnaugh ou d'un calcul booléen, déterminer une écriture simplifiée de F sous la forme d'une somme de trois variables booléennes élémentaires.
   Écrire sous forme d'une phrase, les conditions pour lesquelles un utilisateur ne peut pas accéder à une page suivante,

Exercice 2 **6 points**

Cet exercice met en œuvre sur de petits nombres le premier système de cryptage asymétrique. Dans ce système, une personne destinataire qui veut recevoir des informations confidentielles publie une clé permettant à quiconque de lui envoyer des messages sous forme cryptée. Cependant seule la personne destinataire peut décrypter les messages à l'aide d'une autre clé connue d'elle seule.

Partie A - Détermination de la clé publique servant au cryptage

1. On choisit deux nombres premiers entre eux : $p = 78$ et $q = 95$.
   Justifier que les entiers p et q sont premiers entre eux.
2. La personne destinataire choisit 5 entiers $b_1 = 45, b_2 = 22, b_3 = 13, b_4 = 4, b_5 = 2$.
   La clé de cryptage est formée des 5 nombres entiers $(a_1,\ a_2,\ a_3,\ a_4,\ a_5)$ ainsi calculés :
   pour tout i de l'ensemble $\{1, 2, 3, 4, 5\}$, $0 \leqslant a_i \leqslant 77$ et $b_i \times q = a_i$, mod p.
   Exemple : pour le calcul de a_1 on calcule $b_1 \times q = 45 \times 95 = 4275$.
   Or $4275 \equiv 63$ mod p, et 63 est bien compris entre 0 et 77. Donc $a_1 = 63$.

Question : en détaillant le calcul, montrer que $a_3 = 62$.

Partie B - Cryptage d'un message

On admet dans la suite de l'exercice que $a_3 = 65$, $a_4 = 68$ et $a_5 = 34$.
La clé de cryptage est donc $(a_1,\ a_2,\ a_3,\ a_4,\ a_5) = (63, 62, 65, 68, 34)$.
Cette clé, publiée par la personne destinataire, permet à quiconque de lui envoyer un message crypté.
Cette partie va expliquer comment on crypte le message.
On associe d'abord à chaque lettre son rang dans l'alphabet, selon la correspondance suivante :

Lettre	A	B	C	D	E	F	G	H	I	J	K	L	M
Rang	1	2	3	4	5	6	7	8	9	10	11	12	13
Lettre	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Rang	14	15	16	17	18	19	20	21	22	23	24	25	26

Pour crypter une lettre :

— on détermine son rang à l'aide du tableau de correspondance précédent;

— on écrit ce nombre en base 2 sur 5 bits; on ainsi obtient 5 chiffres $(m_1, m_2, m_3, m_4, m_5)$, chaque chiffre étant égal à 0 ou à 1;

— on détermine alors la valeur cryptée, égale à la somme $\sigma = a_1 m_1 + a_2 m_2 + a_3 m_3 + a_4 m_4 + a_5 m_5$.

On remarque qu'une lettre est ainsi cryptée par un nombre entier.
Exemple : on veut crypter la lettre « I ».

— Le rang de I est 9_{10} ;

— on écrit ce nombre en base deux sur 5 bits : $9_{10} = 8 + 1 = 01001$,

— on calcule la somme $\sigma = 0 \times 63 + 1 \times 62 + 0 \times 65 + 0 \times 68 + 1 \times 34 = 96$.

La lettre « I » est donc cryptée par l'entier 96.
Question : crypter la lettre « W ».

Exercice 3 **5 points**

Cet exercice étudie la suite (u_n) dont les termes sont définis par leur écriture en base deux : $u_0 = 1$, et, pour tout entier $n \geqslant 1$, $u_n = 1,1\dots1$ où sont écrits n chiffres 1 à droite de la virgule.

1. Vérifier que, écrit en base dix, $u_1 = 1,5$.
   Donner l'écriture en base dix de u_2.
2. Justifier le fait que la suite (u_n) n'est ni arithmétique ni géométrique.
3. On pose $A = 1 + \dfrac{1}{2} + \dfrac{1}{4} + \dfrac{1}{8} + \dfrac{1}{16}$.
   a. Vérifier que le nombre A est l'un des termes de la suite (u_n). Donner son rang.
   b. Déterminer l'écriture décimale du nombre A.
4. On admet dans cette question que, pour tout $n \geqslant 1$: $u_n = 1 + \dfrac{1}{2} + \left(\dfrac{1}{2}\right)^2 + \dots + \left(\dfrac{1}{2}\right)^n$

   Démontrer que, pour tout $n \geqslant 1$, on a $u_n = 2 - \left(\dfrac{1}{2}\right)^n$.

   On pourra utiliser le formulaire ci-après.
5. Déterminer la plus petite valeur de n telle que $u_n > 1,999$.

Formulaire

Si q est un réel différent de 1 et n un entier naturel non nul, on a : $1 + q + \dots + q^n = \dfrac{1 - q^{n+1}}{1 - q}$.

2019 Nouvelle Calédonie

Exercice 1 **4 points**

Une Box possède huit diodes électroluminescentes alignées en façade. Chaque diode possède deux états qui traduisent les chiffres binaires : 1 pour une diode allumée et 0 pour une diode éteinte.
L'alignement des huit chiffres binaires reflétant l'état de la Box donne l'écriture binaire d'un nombre N.
Exemple :
Si la Box est éteinte, les huit diodes le sont aussi et le nombre N associé est $0000\ 0000_2$, soit 0_{10}.
Si les huit diodes sont allumées, le nombre N associé est $1111\ 1111_2$, soit 255_{10}.

1. **a.** Quel est le nombre N exprimé en base 10 correspondant au nombre $0001\ 0101_2$?
   b. Quel sera le nombre N exprimé en base 2 correspondant au nombre 57_{10} ?
   c. Montrer qu'il y a 256 valeurs différentes possibles du nombre N.
2. L'affichage des huit diodes, éteintes ou allumées, peut aussi signaler un problème particulier (absence de réseau, saturation, panne, ...). On suppose dans cette question qu'il n'y a que 57 problèmes différents possibles.
   a. On considère l'ensemble E des nombres entiers entre 1 et 57, c'est-à-dire $E = \{1\ ;\ 2\ ;\ \cdots\ ;\ 57\}$. et l'ensemble $*E'$ des écritures binaires du nombre N : $E' = \{0000\ 0000\ ;\ 0000\ 0001\ ;\cdots;\ 1111\ 1111\}$. L'application qui à tout élément de E associe l'écriture binaire dans E' est-elle injective ? Surjective ? Bijective ?
   b. Pour traduire 57 problèmes différents, combien de diodes auraient été suffisantes ?
3. Le fournisseur de la Box envisage de remplacer les diodes par l'affichage de deux symboles correspondant à un code hexadécimal.
   a. Quelle serait l'écriture du nombre N exprimé en base hexadécimale correspondant au problème (numéroté en base 10) : 43 ?
   b. Que signifierait dans le contexte de l'exercice l'écriture en base hexadécimale FF du nombre N ?

Exercice 2 **8 points**

Un site internet permet de partager des commentaires sur des mangas.

Partie A : étude du nombre de commentaires

Au début de l'étude, au moins numéro 0, il y avait 550 commentaires proposés. Les modérateurs constatent que 80 % des commentaires donnent lieu à un autre commentaire que l'on comptabilise le mois suivant. De plus, 240 commentaires sur de nouveaux sujets apparaissent d'un mois à l'autre.

Pour tout $n \in \mathbb{N}$, on note u_n le nombre de nouveaux commentaires émis au mois numéro n.

1. Justifier que la suite (u_n) est définie par $u_0 = 550$ et pour tout $n \in \mathbb{N}$, $u_{n+1} = 0{,}8u_n + 240$.
2. Calculer u_1 et u_2. Interpréter les résultats obtenus dans le contexte de l'exercice.
3. On admet que pour tout $n \in \mathbb{N}$, $u_n = 1\,200 - 650 \times (0{,}8)^n$. Pour quelle valeur de n, $u_n \geqslant 1\,000$?
4. Peut-on dépasser 1 200 nouveaux commentaires avec ce modèle ? Justifier.

Partie B : archivage des commentaires

Afin de limiter l'espace de stockage nécessaire, un commentaires n'est conservé que s'il répond au moins à l'un des critères suivants :

- le commentaire a eu strictement moins de 100 vues et est daté de strictement moins de 6 mois,
- ou le commentaire a été écrit par un anonyme et a eu 100 vues ou plus,
- ou le commentaire est daté de 6 mois ou plus et a eu 100 vues ou plus,
- ou le commentaire est daté de strictement moins de 6 mois et n'a pas été écrit par un anonyme.

On définit les variables booléennes a, b et c de la façon suivante :

- $a = 1$ si le commentaire a strictement moins de 6 mois ; $a = 0$ sinon ;
- $b = 1$ si le commentaire comptabilise strictement moins de 100 vues ; $b = 0$ sinon ;
- $c = 1$ si l'auteur du commentaire est anonyme ; $c = 0$ sinon.

On admet qu'une expression booléenne E traduisant qu'un commentaire est conservé est donnée par :

$$E = ab + \bar{b}c + \bar{a}\bar{b} + a\bar{c}$$

1. À quel critère correspond l'expression $\bar{b}c$?
2. Déterminer une écriture simplifiée de E sous la forme d'une somme de deux termes. En déduire une interprétation des conditions pour que le commentaire soit conservé.
3. Un commentaire date de 6 mois ou plus et son auteur est anonyme. Est-il toujours conservé ?
4. Donner une expression simple de $\overline{E}$. À quelle condition un commentaire est-il supprimé ?

Exercice 3 **8 points**

Partie A

Une entreprise fabrique 28 produits différents. Elle dispose d'un site internet pour les présenter au grand public. On suppose que les 28 produits sont référencés par un nombre entier compris entre 0 et 27.
Sur la page d'accueil de son site, l'entreprise souhaiterait mettre en avant chaque jour un produit différent, sans l'afficher nécessairement dans l'ordre de référencement, mais en étant certaine que tous les produits soient affichés un jour ou l'autre.

1. **a.** Décomposer 28 en produit de facteurs premiers.
   b. Calculer le PGCD de 12 et 28.
   c. Les nombres 15 et 28 sont-ils premiers entre eux ?

L'entreprise choisit de commencer par présenter le produit référencé numéro 0.
À partir du deuxième jour, pour obtenir le numéro du produit mis en avant, on ajoute un nombre entier positif a au numéro précédent et on calcule le reste de cette somme dans la division par 28. Le nombre obtenu est le numéro du produit mis en avant.
Par exemple, en choisissant $a = 12$, la liste des numéros des produits mis en avant sur le site dans l'ordre est : 0 – 12 – 24 – 8 – 20.

2. Compléter la liste des numéros des 11 premiers produits mis en avant pour $a = 12$.
3. Ce choix du nombre a permet-il de présenter tous les produits ?
4. Parmi les valeurs suivantes de a : 1 ; 2 ; 17 ; 24 ; 25, dire lesquelles permettent de mettre en avant tous les produits ? On ne demande pas de justification.

Partie B

Le site internet de cette entreprise est composé de 4 pages WEB : une page d'accueil A, une page de présentation des produits B, une page de commande C et une page de facturation D.

- La page A permet d'aller sur les pages B et C.
- La page B permet d'allée sur la page C.
- Seule la page C permet d'aller sur la page D.
- Les pages B et D permettent d'aller sur la page A.

1. Représenter l'ensemble de ces liens par un graphe orienté de sommets A, B, C, D.
2. Donner la matrice M d'adjacence de ce graphe.
3. Vérifier que $M^2 = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix}$. Combien existe-t-il de circuits de longueur 2 ? Les citer.
4. Existe-t-il un ou des chemin(s) de longueur 2 allant de la page A vers la page D ? Si oui, le(s) citer.
5. Calculer M^3. Existe-t-il au moins un chemin de longueur 3 allant de B vers A ? Si oui, en citer au moins un.
6. Déterminer la matrice $\widehat{M}$ de fermeture transitive du graphe. Interpréter ce résultat dans le contexte de l'exercice.

2019 Polynésie

Exercice 1 **7 points**

Après l'obtention de leur BTS SIO, trois amis décident de créer un jeu vidéo nommé « escape game ». Les différentes tâches de la réalisation de ce projet sont décrites dans le tableau suivant.

Nom simplifié de la tâche	Description de la tâche	Durée en jour	Tâches précédentes
A	Choix du matériel et achats	1	F
B	Fabrication du matériel	5	A
C	Inauguration	1	E
D	Livraison du matériel	1	B, A, G
E	Mise en place du matériel et essais	5	D, H
F	Recherche des énigmes	4	-
G	Recherche des locaux	9	-
H	Rédaction du scénario complet	5	F

1. Déterminer le niveau de chacun des sommets.
2. Donner le tableau des successeurs de chaque sommet.
3. Construire le graphe d'ordonnancement du projet (méthode M. P. M. ou P. E. R. T.) en incluant les dates au plus tôt et au plus tard.
4. Donner le chemin critique et la durée minimale du projet.
5. Calculer la marge totale de la tâche H et donner une interprétation de ce résultat.
6. Un célèbre animateur accepte d'assister à l'inauguration si elle a lieu 15 jours après le lancement du projet. Les tâches A, B, C, D, E ont une durée incompressible. De quelle(s) tâche(s) doit-on réduire la durée pour que l'inauguration puisse avoir lieu le jour fixé ?

Exercice 2 **9 points**

Les parties A et B étudient deux éléments d'un jeu vidéo nommé « escape game ». Elles sont indépendantes.

Partie A

Le jeu vidéo comprend un coffre-fort. Son ouverture dépend de trois paramètres : une clé que doit trouver le joueur, une énigme à résoudre, la durée de ces deux tâches (donnée par un chronomètre). Le coffre s'ouvre si l'une au moins des conditions suivantes est réalisée :

- le joueur a trouvé la clé et le chronomètre marque 30 minutes ou plus, ou
- l'énigme est résolue et le chronomètre marque strictement moins de 30 minutes, ou
- le joueur a trouvé la clé et l'énigme n'est pas résolue.

On définit trois variables booléennes a, b, c de la manière suivante :

- $a = 1$ si le joueur a trouvé la clé, $a = 0$ sinon ;
- $b = 1$ si l'énigme est résolue, $b = 0$ sinon ;
- $c = 1$ si le chronomètre marque strictement moins de 30 minutes, $c = 0$ sinon.

1. Écrire une expression booléenne E qui traduit les critères d'ouverture du coffre-fort.

2. **a.** Représenter l'expression E dans un tableau de Karnaugh.

b. En déduire une écriture simplifiée de l'expression booléenne E sous la forme d'une somme de deux termes.

c. Interpréter cette expression simplifiée dans le contexte de l'exercice.

3. Donner une écriture simplifiée de E et interpréter ce résultat dans le contexte de l'exercice.

Partie B

Pour passer un niveau dans le jeu, il faut taper sur un clavier un code de 6 caractères comprenant des lettres et des chiffres. Le joueur peut trouver ces chiffres en résolvant trois énigmes numériques, qui sont décrites dans les questions 1, 2, 3.

1. Le caractère de gauche du code est le nombre de diviseurs positifs de 2019. Cette question détaille la détermination de ce nombre.

a. Justifier le fait que 673 est un nombre premier.

b. Donner la décomposition en produit de facteurs premiers du nombre 2019.

c. Déterminer tous les diviseurs positifs de 2019. En déduire le nombre cherché.

2. Les 2^{e}, 3^{e} et 4^{e} caractères du code en partant de la gauche sont, dans cet ordre, les chiffres de l'écriture hexadécimale du nombre 2019.

Trouver ces caractères en détaillant les calculs.

3. Cette question détaille la détermination des deux derniers caractères du code, ce qui demande d'abord de résoudre l'équation $n^2 + n + 1 \equiv 0 \mod 7$.

a. Déterminer les restes possibles de la division de $n^2 + n + 1$ par 7 en fonction des restes possibles de la division de n par 7.

On pourra pour cela recopier et compléter le tableau suivant :

Reste possible de la division de n par 7	0	1	2	3	4	5	6
Reste possible de la division de n^2 par 7							
Reste possible de la division de $n^2 + n + 1$ par 7							

b. On peut lire dans le tableau ci-dessus, après l'avoir complété, que les entiers de la forme $7k + 2$, avec k entier naturel, sont des solutions de l'équation $n^2 + n + 1 \equiv 0 \mod 7$.

Donner les autres solutions sous une forme analogue.

c. En déduire le nombre de solutions de l'équation $n^2 + n + 1 \equiv 0 \mod 7$ qui sont comprises entre 0 et 101.

d. Les deux derniers caractères à droite sont, dans cet ordre, les chiffres en base dix du nombre trouvé en **c**. Donner ces deux caractères.

4. Choisir sans justification la bonne réponse.

Le code à taper pour passer le niveau du jeu est :

Réponse A : 43E730	Réponse B : 47E329
Réponse C : 33E729	Réponse D : 27E330

Exercice 3 **4 points**

Pour un jeu vidéo nommé « escape game », il est prévu des abonnements pour une durée de deux ans. Lors de la mise en service du jeu, 40 personnes se sont abonnées. Les dirigeants estiment qu'à partir du jour suivant l'inauguration, le nombre de nouveaux abonnés va augmenter de 5 % chaque mois.

1. Pour tout entier naturel n, on note u_n le nombre estimé de nouveaux abonnés n mois après l'ouverture. Ainsi $u_0 = 40$.

a. Calculer u_1 et u_2. Arrondir à l'entier le plus proche.

b. Pour tout entier naturel n, exprimer u_{n+1} en fonction de u_n.

c. Déterminer la nature de la suite (u_n) puis, pour tout entier naturel n, exprimer u_n en fonction de n.

2. Pour tout entier naturel n, on note S_n le nombre total d'abonnés n mois après l'ouverture du jeu.

Ainsi $S_0 = 40$.

a. Justifier l'égalité $S_1 = 82$.

b. Combien de mois après l'ouverture du jeu le nombre estimé d'abonnés sera-t-il supérieur à 200 ?

c. Estimer le nombre total d'abonnés un an après l'ouverture du jeu.

2018 Métropole

Exercice 1 (5 points)

Sur une plateforme de vidéos en ligne, les vidéos sont notées de 0 à 5 par les utilisateurs.
Après une période d'observation, les administrateurs de la plateforme décident de mettre une vidéo sur la page d'accueil lorsqu'elle satisfait à l'un au moins des critères suivants :

- la vidéo a obtenu la note 5 et comptabilise un nombre de vues supérieur ou égal à 200 ;
- la vidéo a obtenu la note 5 et elle est récente ;
- la vidéo comptabilise un nombre de vues strictement inférieur à 200 et elle est récente ;
- la vidéo n'a pas obtenu la note 5 et comptabilise un nombre de vues supérieur ou égal à 200.

On définit les trois variables booléennes a, b, c de la façon suivante :

- $a=1$ si la vidéo a obtenu la note 5, $a=0$ sinon ;
- $b=1$ si la vidéo comptabilise un nombre de vues supérieur ou égal à 200, $b=0$ sinon ;
- $c=1$ si la vidéo est récente, $c=0$ sinon.

1. L'administrateur de la plateforme a traduit les conditions pour qu'une vidéo soit mise sur la page d'accueil par l'expression booléenne $E=ab+ac+\overline{b}c+\overline{a}b$.
Justifier chacun des termes de cette somme.

2. **a)** Représenter l'expression E dans un diagramme de Karnaugh.
b) En déduire une expression simplifiée de E sous la forme d'une somme de deux termes.
c) Interpréter cette expression simplifiée de E dans le contexte de l'exercice.

3. Une vidéo qui n'est pas récente, qui n'a pas obtenu la note 5 et qui comptabilise un nombre de vues strictement inférieur à 200 sera-t-elle mise sur la page d'accueil ?

4. Donner une expression de $\overline{E}$ à l'aide des variables booléennes précédemment définies.
En déduire une définition des vidéos qui ne seront pas mises sur la page d'accueil.

Exercice 2 (10 points)

Partie A

Quatre sites internet traitent les changements climatiques et leurs conséquences sur la planète. On considère une page web sur chacun de ces sites, et on note ces quatre pages A, B, C et D. Les liens hypertextes respectifs entre ces quatre pages sont tous récapitulés dans l'énumération suivante :

- A reçoit un unique lien de B et un unique lien de C ;
- B reçoit un unique lien de D ;
- C reçoit un unique lien de B, un unique lien de D et un unique lien de A ;
- D reçoit un unique lien de A.

1. Représenter l'ensemble de ces liens par un graphe orienté G de sommets A, B, C, D, dans lequel, si une page Y reçoit un lien d'une page X, on représente un arc du sommet X vers le sommet Y.

2. **a)** Donner la matrice d'adjacence M du graphe G.
b) Interpréter les valeurs des termes situés sur la diagonale de la matrice M.

3. **a)** Calculer la matrice M^4.

   b) Le graphe contient-il des circuits ? Justifier la réponse.

   c) Interpréter le terme de la 1re ligne et 3e colonne de la matrice M^4 en termes de chemins, puis donner la liste de ces chemins.

4. Calculer $\hat{M}$, la matrice de la fermeture transitive du graphe G.
   Interpréter le résultat obtenu dans le contexte de l'exercice.

Partie B

Un étudiant du BTS SIO a mis en place un moteur de recherche avec lequel les pages affichées sont ordonnées par pertinence, selon le nombre de liens hypertextes pointant vers chaque page.
Cette partie étudie un exemple simplifié, en limitant ce moteur de recherche aux quatre pages web A, B, C et D définies dans la partie **A**, et en considérant le graphe associé G.
La méthode mise en place par l'étudiant consiste à associer un score à chaque sommet du graphe.
Les scores a, b, c, d de chacun des sommets A, B, C, D, sont calculés à partir des instructions suivantes :

- on liste les prédécesseurs du sommet considéré dans le graphe G ;
- on divise le score de chaque prédécesseur par le nombre de ses successeurs ;
- le score d'un sommet est obtenu en ajoutant les quotients obtenus.

Exemple : le sommet A possède deux prédécesseurs B et C ; B a 2 successeurs et C a 1 successeur.
D'où $a = \frac{b}{2} + \frac{c}{1}$.

1. Justifier l'égalité : $c = \frac{a}{2} + \frac{b}{2} + \frac{d}{2}$.

2. En établissant les quatre égalités vérifiées par les scores a, b, c, d, on obtient un système de quatre équations linéaires aux inconnues a, b, c, d. Ce système ayant une infinité de solutions, toutes proportionnelles entre elles, on pose $a = 1$ et on admet que la résolution se ramène à celle du système :

$$(S)\begin{cases} 0,5b + c = 1 \\ b - 0,5d = 0 \\ 0,5b - c + 0,5d = -0,5 \end{cases}.$$

   On définit les matrices $X = \begin{pmatrix} b \\ c \\ d \end{pmatrix}$, $A = \begin{pmatrix} 0,5 & 1 & 0 \\ 1 & 0 & -0,5 \\ 0,5 & -1 & 0,5 \end{pmatrix}$ et $B = \begin{pmatrix} 0,5 & 0,5 & 0,5 \\ 0,75 & -0,25 & -0,25 \\ 1 & -1 & 1 \end{pmatrix}$.

   a) Exprimer le système (S) sous la forme $A \times X = Y$, où Y est une matrice à préciser.

   b) Calculer le produit $B \times A$.

   c) En déduire que $X = B \times Y$, puis donner la solution du système (S).

3. Donner, en justifiant, le classement des pages web A, B, C et D selon la méthode mise en place.

Exercice 3 (5 points)

Les publications en série, comme les journaux et les périodiques, sont toutes identifiées par un numéro ISSN (*International Standard Serial Number*). En France, ce numéro est attribué par le Centre national d'enregistrement des publications en série.
L'ISSN comporte huit caractères répartis en deux groupes de quatre, ces groupes étant séparés par un tiret. Le tableau ci-après donne les numéros ISSN de quelques journaux ou périodiques français.

Journal ou périodique	Numéro ISSN
Le Monde	1950-6244
Le Figaro	1241-1248
Le Nouvel Observateur	0029-4713
Les Échos	0153-4831
Libération	0335-1793
Le Canard Enchaîné	0008-5405
Courrier International	1154-516X

Les sept premiers caractères d'un numéro ISSN sont des chiffres qui caractérisent la publication. Le dernier caractère, situé en huitième position, sert de clé de contrôle et est pris dans l'ensemble $E=\{0,1,2,3,4,5,6,7,8,9,\mathrm{X}\}$ où les chiffres de 0 à 9 représentent le nombre correspondant et le caractère X représente le nombre 10.

Pour déterminer la clé de contrôle d'un numéro ISSN dont les sept premiers chiffres correspondent aux nombres a, b, c, d, e, f, g :

- on calcule le nombre $N=8a+7b+6c+5d+4e+3f+2g$;
- on détermine le reste r de $-N$ dans la division euclidienne par 11 ;
- la clé de contrôle est le caractère de l'ensemble E correspondant au nombre r.

Par exemple, pour *Le Monde*, on a $N=8\times1+7\times9+6\times5+5\times0+4\times6+3\times2+2\times4=139$.
D'où $-N\equiv-139\equiv4 \mod 11$. La clé de contrôle est donc bien égale à 4.

1. En détaillant les étapes, retrouver la clé de contrôle du périodique *Courrier International*.

2. On considère l'application $f:F\to E$ où F est l'ensemble des 7 numéros ISSN du tableau ci-dessus. L'application f associe à tout élément de numéro ISSN sa clé de contrôle.

a) L'application f est-elle injective ? Justifier.

b) L'application f est-elle surjective ? Justifier.

3. Le deuxième caractère du numéro ISSN d'un journal est illisible. Si l'on note n ce caractère, le numéro ISSN est 3n08-2138.

a) Montrer que $81+7n\equiv3 \mod 11$.

b) En déduire la valeur de n.

2018 Nouvelle Calédonie

Exercice 1 (5 points)

Une société de création de jeux vidéo souhaite développer un nouveau jeu composé d'un certain nombre d'étapes de construction, de cycles de déplacement et de scènes cinématiques.
Chacune nécessite un temps d'infographie, de programmation et de réalisation musicale.

Le tableau suivant donne la durée, en heure, de chaque traitement :

	Étapes de construction	Cycles de déplacement	Scènes cinématiques
Infographie	100	70	50
Programmation	200	60	80
Réalisation musicale	30	6	20

1. Un projet comporte 8 étapes de construction, 17 cycles de déplacement et 2 scènes cinématiques.

On considère les matrices suivantes : $M = \begin{pmatrix} 100 & 70 & 50 \\ 200 & 60 & 80 \\ 30 & 6 & 20 \end{pmatrix}$ et $A = \begin{pmatrix} 8 \\ 17 \\ 2 \end{pmatrix}$.

a) Calculer le produit matriciel $M \times A$

b) Interpréter les lignes de ce produit matriciel.

2. Le projet retenu nécessite 2100 heures d'infographie, 2940 heures de programmation et 420 heures de réalisation musicale.
Soit a, b et c les nombres respectifs d'étapes de construction, de cycles de déplacement et de scènes cinématiques. La suite détaille une méthode pour déterminer ces trois nombres.

On considère les matrices $B = \begin{pmatrix} 2100 \\ 2940 \\ 420 \end{pmatrix}$ et $X = \begin{pmatrix} a \\ b \\ c \end{pmatrix}$.

a) Traduire les contraintes de réalisation du projet par une égalité matricielle.

b) On considère la matrice : $T = \dfrac{1}{7000}\begin{pmatrix} -72 & 110 & -260 \\ 160 & -50 & -200 \\ 60 & -150 & 800 \end{pmatrix}$.

Calculer le produit matriciel $T \times M$.

c) Montrer que l'égalité matricielle $M \times X = B$ implique l'égalité matricielle $X = T \times B$.

d) En déduire les nombres d'étapes de construction, de cycles de déplacement et de scènes cinématiques pour le jeu.

Exercice 2 (7 points)

Partie A

Une entreprise décide de produire un jeu vidéo. À cette fin, elle doit recruter du personnel.
Un candidat, femme ou homme, est recruté lorsqu'il remplit l'une au moins des conditions suivantes :

- il possède un BTS, maîtrise l'infographie 3D et possède des compétences en scénographie ;
- il ne possède pas de BTS et maîtrise l'infographie 3D ;
- il ne maîtrise pas l'infographie 3D et possède des compétences en scénographie.

On définit les variables booléennes a, b, c suivantes :

- $a = 1$ si le candidat possède un BTS, $a = 0$ sinon ;
- $b = 1$ si le candidat maîtrise l'infographie 3D, $b = 0$ sinon ;
- $c = 1$ si le candidat possède des compétences en scénographie, $c = 0$ sinon.

1. Écrire une expression booléenne E traduisant les critères du recrutement.

2. Représenter l'expression booléenne E par un tableau de Karnaugh.

3. Simplifier E sous la forme d'une somme de deux expressions.

4. En déduire une version simplifiée des critères du recrutement.

Partie B

Le jeu étant commercialisé en ligne, l'entreprise doit prévoir un espace de stockage des données personnelles des acheteurs.
La direction commerciale estime que 1600 jeux seront achetés le premier mois.
Les études statistiques réalisées sur les autres jeux commercialisés ont montré que le nombre d'achats augmente de 25 % par mois.

1. Quel est, selon ce modèle d'augmentation, le nombre prévisible d'achats le deuxième mois ?

2. Est-il vrai que, selon ce modèle, le nombre d'achats aura doublé le cinquième mois ?

3. Le nombre d'achats du jeu est modélisé par une suite (u_n) où, pour tout entier n non nul, le terme u_n représente le nombre d'achats lors du n-ième mois. Ainsi $u_1 = 1600$.

a) Justifier que (u_n) est une suite géométrique dont on donnera la raison.

b) Pour tout entier n non nul, exprimer u_n en fonction de n.

c) Calculer le nombre total cumulé d'achats pour la première année, en arrondissant ce nombre à la dizaine.

4. Les serveurs de l'entreprise peuvent stocker les données relatives à un total cumulé de 300 000 achats en ligne.
Quel est le rang n du mois où les serveurs de l'entreprise seront saturés ?

Exercice 3 (8 points)

Le but de cet exercice est d'envisager le codage ASCII de fichiers texte, et leur cryptage en utilisant des congruences modulo 128.

Partie A : codage ASCII des lettres de l'alphabet standard

On veut coder le mot « HELLO » et enregistrer son codage ASCII en système binaire sur un fichier, chaque lettre tenant sur 8 bits, celui écrit à gauche étant un 0. On utilise le code ASCII dont l'extrait de la table de correspondance figure en annexe page 5/5.

1. À l'aide de cette table de correspondance, donner le code ASCII en système décimal, puis en système binaire (sur 8 bits) de la lettre L.

2. En déduire son code ASCII en système hexadécimal.

Partie B : cryptage

On souhaite crypter les fichiers et utiliser pour cela une clé de cryptage notée a. Soit x le code ASCII en système décimal d'un caractère et y le code ASCII en système décimal du caractère crypté. Ainsi y est l'entier compris entre 0 et 127 défini par la relation $y \equiv a x$ modulo 128 .

1. Dans cette question, on pose $a = 25$.

a) Vérifier que $25 \times 69 \equiv 61$ modulo 128. En déduire le code ASCII du cryptage de la lettre E, d'abord en système binaire (sur 8 bits), puis en système hexadécimal.

b) Déterminer en système hexadécimal le code ASCII du cryptage de la lettre L.

c) Crypter le mot « HELLO » en système hexadécimal, sachant que la lettre O est cryptée, en système hexadécimal, par 37 et la lettre H par 08.

2. Dans cette question, on pose $a = 96$.

a) Déterminer les codes ASCII en système décimal cryptant les lettres H et L.

b) La fonction de l'ensemble $\{0 ; 1 ; ... ; 127\}$ dans lui-même qui, à x associe y, est-elle injective ? Que peut-on en conclure ?

Partie C : quelques propriétés arithmétiques de l'entier 128

1. Décomposer 128 en un produit de facteurs premiers.

2. Établir la liste des diviseurs positifs de 128.

3. a) Les entiers 128 et 96 sont-ils premiers entre eux ? Justifier.

b) Les entiers 128 et 25 sont-ils premiers entre eux ? Justifier.

*Remarque : le résultat de la question 3a) explique celui de la question **B.2.b)**.*

Annexe

Extrait de la table de correspondance entre code ASCII et lettres majuscules

Caractère	Code ASCII	
	Décimal	Binaire
A	65	0100 0001
B	66	0100 0010
C	67	0100 0011
D	68	0100 0100
E	69	0100 0101
F	70	0100 0110
G	71	0100 0111
H	72	0100 1000
I	73	0100 1001
J	74	0100 1010
K	75	0100 1011
L	76	0100 1100
M	77	0100 1101
N	78	0100 1110
O	79	0100 1111
P	80	0101 0000
Q	81	0101 0001
R	82	0101 0010
S	83	0101 0011
T	84	0101 0100
U	85	0101 0101
V	86	0101 0110
W	87	0101 0111
X	88	0101 1000
Y	89	0101 1001
Z	90	0101 1010

2018 Polynésie

Exercice 1 (4 points)

Cet exercice est un questionnaire à choix multiple. Pour chaque question, une seule affirmation est exacte. Recopier sur la copie le numéro de la question et l'affirmation exacte. On ne demande pas de justification. Une réponse exacte vaut 1 point. Une absence de réponse n'est pas pénalisée.

Question1

On définit l'application $f : \mathbf{N} \to \{0,1,2,3,4,5,6,7,8,9\}$ qui, à un entier n, associe son chiffre des unités en base 10.

Affirmation A : l'application f est bijective.
Affirmation B : l'application f est injective mais non surjective.
Affirmation C : l'application f est surjective mais non injective.
Affirmation D : l'application f n'est ni injective ni surjective.

Question 2

On considère un graphe orienté de sommets E, F, G, H, dont la matrice d'adjacence est :

$$M = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}.$$

Affirmation A : le sommet F a exactement 2 successeurs.
Affirmation B : le sommet F a exactement 2 prédécesseurs.
Affirmation C : le graphe comprend exactement 11 chemins de longueur 2.
Affirmation D : le graphe ne contient aucun circuit.

Question 3

Les chiffres en base seize sont notés : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F.
On considère un entier X dont l'écriture en base seize est : $X = \mathrm{BC7}_{16}$.

Affirmation A : en base dix, l'entier X s'écrit $X = 3015_{10}$.
Affirmation B : en base dix, l'entier X s'écrit $X = 2018_{10}$.
Affirmation C : en base dix, l'entier X s'écrit $X = 11127_{10}$.
Affirmation D : en base dix, l'entier X s'écrit $X = 1995_{10}$.

Question 4

On considère la relation $\mathcal{R}$ définie sur $\mathbf{N}^*$ par : « $m \ \mathcal{R} \ n \Leftrightarrow m$ divise n ».

Affirmation A : la relation $\mathcal{R}$ est réflexive et transitive.
Affirmation B : la relation $\mathcal{R}$ est symétrique et transitive.
Affirmation C : la relation $\mathcal{R}$ est réflexive et symétrique.
Affirmation D : la relation $\mathcal{R}$ est une relation d'équivalence.

Exercice 2 (11 points)

Partie A

Une société de fabrication et d'installation de fibre optique a besoin de recruter un informaticien, femme ou homme. La direction des ressources humaines considère qu'une candidature est recevable lorsqu'elle satisfait à l'une au moins des conditions suivantes :

- le candidat est âgé de 25 ans ou moins et est titulaire du BTS SIO ;
- le candidat est âgé de 25 ans ou moins, n'est pas titulaire du BTS SIO et possède de l'expérience ;
- le candidat est âgé de strictement plus de 25 ans et est titulaire du BTS SIO.

On définit les variables booléennes a, b, c de la façon suivante :

- $a=1$ si le candidat est âgé de strictement plus de 25 ans, $a=0$ sinon ;
- $b=1$ si le candidat est titulaire du BTS SIO, $b=0$ sinon ;
- $c=1$ si le candidat a de l'expérience, $c=0$ sinon.

1. Écrire une expression booléenne E traduisant qu'une candidature est recevable, à l'aide des variables booléennes a, b, c.
2. À l'aide d'un tableau de Karnaugh, déterminer une écriture simplifiée de E sous la forme d'une somme de deux termes. En déduire une interprétation simplifiée des conditions pour qu'une candidature soit recevable.
3. Une candidate a 21 ans, aucune expérience, mais est titulaire du BTS SIO. Remplit-elle les critères de recrutement ?
4. Donner une expression simple de $\overline{E}$.

Partie B

La société produit trois types de fibres optiques à partir de silice, forme naturelle du dioxyde de silicium (SiO_2) qui entre dans la composition de nombreux minéraux. Elle produit :

- x pièces du type A, dont le débit supporté vaut 1 gigabit par seconde ;
- y pièces du type B, dont le débit supporté vaut 10 gigabits par seconde ;
- z pièces du type C, dont le débit supporté vaut 100 gigabits par seconde.

Pour une pièce, la masse de silice utilisée et le temps de production de chacun de ces types de fibres sont récapitulés dans le tableau suivant.

Type de fibre	A	B	C
Masse de silice en kg (par pièce)	3	4	7
Temps de production en h (par pièce)	2	3	5

La société modélise cette fabrication afin d'envisager différents scénarios sur une période donnée. Pour cette période, on note N le nombre total de pièces produites, S la masse totale en kg de silice utilisée et H le temps total de production, exprimé en heure.

1. Justifier le fait que x, y, z vérifient le système $\begin{cases} x+y+z=N \\ 3x+4y+7z=S \\ 2x+3y+5z=H \end{cases}$.

2. On considère les matrices colonnes $X = \begin{pmatrix} x \\ y \\ z \end{pmatrix}$ et $Y = \begin{pmatrix} N \\ S \\ H \end{pmatrix}$. Déterminer la matrice carrée M qui traduit le système ci-dessus par l'équation matricielle $M \times X = Y$.

3. Calculer Y lorsque $X = \begin{pmatrix} 20 \\ 10 \\ 30 \end{pmatrix}$. Interpréter les résultats obtenus dans le contexte de l'exercice.

4. On considère la matrice carrée $P = \begin{pmatrix} 1 & 2 & -3 \\ 1 & -3 & 4 \\ -1 & 1 & -1 \end{pmatrix}$.

   a) Calculer le produit matriciel $P \times M$.
   b) Montrer que si $M \times X = Y$, alors $X = P \times Y$.
   c) Pour une période donnée, l'entreprise dispose de 94 kg de silice et de 67 heures de production. Elle souhaite fabriquer 21 pièces de fibres.
   Combien de pièces de chaque type peut-t-elle fabriquer ?

Partie C

Pour une informaticienne recrutée en janvier 2018, le salaire mensuel initial est de 1500 euros. Pendant les dix premières années, son contrat prévoit une augmentation de 3 % du salaire mensuel au début de chaque nouvelle année.

On note u_n le salaire mensuel en euro, lors de la n-ième année de recrutement. Ainsi $u_1 = 1500$.

La direction des ressources humaines utilise un tableur afin d'évaluer les salaires mensuels versés chaque année à l'informaticienne (voir ci-contre).

	A	B
1	n	$u(n)$
2	1	1500
3	2	
4	3	
5	4	
6	5	
7	6	
8	7	
9	8	
10	9	
11	10	

1. Donner la nature de la suite (u_n).

2. Proposer une formule à saisir dans la cellule B3, permettant par recopie vers le bas de compléter les valeurs de la suite (u_n).

3. Exprimer u_n en fonction de n.

4. Calculer u_9, en arrondissant au centième.
   Interprétez ce résultat dans le contexte de l'exercice.

Exercice 3 (5 points)

Une start-up conçoit un petit jeu gratuit pour smartphones. Dans ce jeu, un personnage est généré à chaque début de partie avec un équipement choisi dans une liste de 40 objets, vêtements et accessoires, qui sont numérotés de 0 à 39.
Le concepteur du jeu envisage différents algorithmes pour attribuer automatiquement ces objets à chaque début de partie. Le but de cet exercice est d'étudier certains d'entre eux.

1. Décomposer 40 et 12 en produits de facteurs premiers.

2. Calculer le PGCD de 12 et 40.

3. Le concepteur du jeu envisage d'attribuer les objets à chaque début de partie en parcourant la liste de leurs numéros par des sauts d'amplitude constante a, où a est un nombre entier strictement positif :

- lors de la première partie, le personnage se voit attribuer l'objet numéro 0 ;
- pour obtenir le numéro de l'objet à partir de la deuxième partie, on ajoute a au numéro précédent et on calcule le reste de cette somme dans la division euclidienne par 40. Le reste obtenu est alors le numéro attribué à l'objet.

Par exemple, en choisissant la valeur $a = 12$, la liste des numéros des objets dans l'ordre est :

$$0 ; 12 ; 24 ; 36 ; 8 ; \ldots$$

a) Compléter la liste des numéros des objets attribués lors des 11 premières parties, pour une amplitude de saut égale à 12.

b) Ce choix d'amplitude permet-il d'utiliser tous les objets au cours des parties successives ?

4. On admet le résultat suivant :
« Le nombre a choisi permet de former une liste complète comportant tous les numéros de 0 à 39 dans le cas où le PGCD de 40 et de a est égal à 1, et dans ce cas seulement ».

Ainsi, les nombres a permettant d'utiliser tous les objets au cours des parties successives sont les entiers a qui sont premiers avec 40.

Donner la liste de tous les entiers a compris entre 1 et 39 pour lesquels, au cours des parties successives, tous les objets seront utilisés.

2017 Métropole

Exercice 1 **8 points**

Cet exercice envisage deux. problèmes relatifs à l'équipement d'une salle informatique d'une entreprise. Les deux parties sont indépendantes.

Partie 1 : Choix d'un réseau

Le réseau informatique qui équipera la salle doit satisfaire au moins l'une des conditions suivantes :

- le réseau compte 5 postes ou plus et il existe un poste qui ne reçoit pas de données en entrée
- il existe un poste qui ne reçoit pas de données en entrée, et le réseau compte strictement moins de 5 postes, et il comporte strictement plus de 12 connexions ;
- le réseau comporte 12 connexions ou moins.

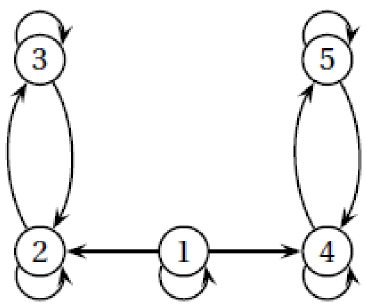
On définit les variables booléennes suivantes :

- $a = 1$ si le réseau compte 5 postes ou plus, $a = 0$ sinon ;
- $b = 1$ s'il existe un poste qui ne reçoit pas de données en entrée, $b = 0$ sinon ;
- $c = 1$ si le réseau comporte 12 connexions ou moins, $c = 0$ sinon.

1. Cette question est une question à choix multiple. Une seule réponse est correcte. Recopier sur la copie seulement la réponse correcte. On ne demande pas de justification.
   Parmi les quatre phrases suivantes, donner celle qui traduit la variable $\overline{b}$:
   — réponse A : « il existe un poste qui reçoit des données en entrée » ;
   — réponse B : « tout poste reçoit des données en entrée » ;
   — réponse C : « il existe un poste qui envoie des données en sortie » ;
   — réponse D : « aucun poste ne reçoit des données en entrée ».
2. Donner l'expression booléenne E traduisant les critères voulus pour un réseau informatique.
3. À l'aide d'un tableau de Karnaugh ou par des calculs, exprimer E comme somme de deux variables booléennes.
4. Traduire les critères de sélection simplifiés, à partir de l'expression obtenue à la question 3.
5. Un réseau dans lequel 2 postes ne reçoivent pas de données en entrée et qui comporte 15 connexions répond-il aux critères voulus ? Justifier la réponse.

Partie 2 : Étude des connexions

La salle informatique doit comprendre cinq postes numérotés de 1 à 5 et branchés en réseau selon le graphe orienté ci-contre.
Dans ce graphe, une flèche d'un poste A vers un poste B traduit le fait que l'on peut envoyer des données de A vers B.



1. Donner la matrice d'adjacence M de ce graphe en prenant les numéros des postes dans l'ordre croissant.

6. Déterminer la matrice $\hat{M}$ de la fermeture transitive de ce graphe.
7. Pour permettre l'envoi de données entre les postes, même en cas de défaillance d'une connexion on utilise la fermeture transitive du graphe.
   Dessiner sur la copie le graphe correspondant à cette fermeture transitive.

Exercice 2 **7 points**

Le but de cet exercice est d'étudier, sur des exemples numériques simples, deux variantes d'une méthode de cryptage inventée par Gilbert Vernam en 1917, et appelée « masque jetable ».
Dans tout l'exercice, on note respectivement M le mot initial, K la clé de cryptage et Y le mot crypté.
Les trois nombres M, K, Y sont des entiers naturels.
Les deux parties de cet exercice sont indépendantes

Partie 1 : Masque jetable

La méthode décrite dans cette partie utilise le connecteur logique « *xor* », appelé « ou exclusif », qui est défini par la table de vérité suivante :

P	Q	$P\ xor\ Q$
0	0	0
0	1	1
1	0	1
1	1	0

Par exemple les deux premières lignes signifient que $0\ xor\ 0 = 0$ et que $0\ xor\ 1 = 1$.

1. Recopier intégralement la table de vérité ci-après et compléter la dernière colonne.

P	Q	$P xor Q$	$(P\ xor\ Q)\ xor\ Q$
0	0	0	
0	1	1	
1	0	1	
1	1	0	

2. Parmi les quatre propositions P, Q, $(P\ xor\ Q)$ et $((P\ xor\ Q)\ xor\ Q)$, deux sont équivalentes.
   À l'aide de la table 2 complétée, déterminer lesquelles, en expliquant la réponse.

Dans la suite de l'exercice, on note ab l'écriture du nombre entier a en base b.

3. Donner la représentation binaire de l'entier qui s'écrit 26_{10} en décimal.
4. Soit M et K deux entiers naturels écrits en binaire, tels que la longueur de l'écriture de K est supérieure ou égale à celle de M.
   Pour crypter le mot M avec la clé K, on procède comme suit : pour chaque chiffre m du mot initial M, on considère le chiffre k de la clé K qui a la même position que m dans l'écriture.
   On obtient alors le chiffre y du mot crypté Y qui a la même position que m dans l'écriture du mot initial M, par la relation : $y = m\ xor\ k$.
   L'écriture binaire du mot crypté Y est la juxtaposition dans le même ordre des chiffres y calculés pour chaque chiffre m du mot M.

Exemple : avec $M = 01_2$ et $K = 10_2$

— Avec le chiffre de rang 1 en partant de la droite : $m = 1$ et $k = 0$

— avec le chiffre de rang 2 : $m = 0$ et $k = 1$; donc $y = 0\, xor\, 1 = 1$.

Donc le mot crypté est $Y = 11_2$

Question : avec le mot initial $M = 011_2$ et la clé $K = 101_2$, déterminer le mot crypté Y.

Remarque : d'après la question 2, le décryptage s'effectue de la même manière que le cryptage.

Partie 2 : Masque jetable hexadécimal

Cette partie envisage le cryptage de nombres entiers écrits dans le système hexadécimal.
Les chiffres hexadécimaux sont notés 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F.

1. Questions préliminaires
   - **a.** Donner la représentation en hexadécimal de l'entier binaire 1011101_2.
   - **b.** Calculer en travaillant dans le système hexadécimal les sommes $7_{16} + 4_{16}$ et $A_{16} + C_{16}$.
2. Soit M et K deux entiers naturels écrits en hexadécimal, tels que la longueur de l'écriture de K est supérieure ou égale à celle de M, et tels que l'écriture de K ne comporte aucun chiffre 0.

   Pour crypter le mot M avec la clé K, on procède comme suit : pour chaque chiffre m du mot initial M, on considère le chiffre k de la clé K qui a la même position que m dans l'écriture.

   On obtient alors le chiffre y du mot crypté Y qui a la même position que m dans l'écriture du mot initial M, de la façon suivante : y est le chiffre hexadécimal des unités de la somme $m + k$.

   Le mot crypté Y est déterminé en hexadécimal par la juxtaposition dans le même ordre des chiffres y calculés pour chaque chiffre m du mot M.

   Exemple : avec $M = 49_{16}$ et $K = 19_{16}$

   — Avec le chiffre de rang 1 en partant de la droite : $m = 9$ et $k = 9$; donc $m + k = 12_{16}$ et par suite $y = 2$;

   — avec le chiffre de rang 2 : $m = 4$ et $k = 1$; donc $m + k = 5_{16}$ et par suite $y = 5$.

   Donc le mot crypté est $Y = 52_{16}$.

   Question : avec le mot initial $M = 7A_{16}$ et la clé $K = 4C_6$, déterminer le mot crypté Y.
3. Par cette méthode, on admet que le décryptage suit les mêmes étapes en remplaçant la clé K par une autre clé K'. Lorsque l'écriture de K comporte au maximum deux chiffres hexadécimaux, la clé K' est l'écriture en hexadécimal de la différence (écrite en décimal) $272_{10} - K_{10}$.

   Cette question est une question à choix multiple. Une seule réponse est exacte. Recopier sur la copie seulement la réponse exacte. On ne demande pas de justification.

   Avec la clé de cryptage $K = 19_{16}$, la clé de décryptage K' est égale à :

Réponse A : 253_{16} **Réponse B** : 247_{16}
Réponse C : FD_{16} **Réponse D** : $F7_{16}$

Exercice 3 **5 points**

Pour effectuer des calculs, un ordinateur représente les nombres en binaire. Cet exercice étudie l'effet d'une perte de précision initiale sur une suite de calculs.
Dans tout l'exercice, on note a_b l'écriture du nombre a en base b.

1. Représentation binaire de quelques nombres décimaux
   a. Cette question est une question à choix multiple. Une seule réponse la copie seulement la réponse exacte. On ne demande pas de justification.

   La représentation binaire du nombre qui s'écrit en décimal $15,5_{10}$ est :

   Réponse A : $10101,101_2$ **Réponse B** : $1111,1_2$
   Réponse C : $1111,0101_2$ **Réponse D** : $10101,1_2$

   b. Justifier que le nombre décimal $15,625_{10}$ a pour représentation binaire $1111,101_2$.
2. On considère la suite géométrique (u_n) de terme initial $u_0 = 32$ et de raison $15,625$.
   a. Calculer la valeur exacte de u_1.
   b. Donner l'expression de u_n en fonction de n.
3. Pour calculer les termes de la suite (u_n), on utilise un logiciel qui arrondit le nombre $15,62$ et le transforme en $15,5$. L'arrondi se répercute sur tous les termes calculés. qui sont alors ceux de la suite géométrique (v_n) qui a le même terme initial que la suite (u_n) c'est-à-dire $v_0 = u_0 = 32$, et dont la raison est égale à $15,5$.
   Ainsi, par exemple, $v_1 = 496$.
   Pour tout entier naturel n, on définit la perte de précision relative e_n sur le n-ième terme par la relation :

$$e_n = \frac{v_n}{u_n}.$$

   a. Démontrer que la suite (e_n) est la suite géométrique de terme initial $e_0 = 1$ et de raison $0,992$.
   b. Déterminer le plus petit entier naturel n tel que $e_n < 0,9$.

2017 Nouvelle Calédonie

Exercice 1 **5 points**

Un opérateur de téléphonie mobile propose trois offres de forfait mensuel sans engagement à ses clients. Chaque offre met à disposition du client une durée de communication mensuelle ainsi qu'un accès à l'Internet 4G avec un volume prédéfini de données.
Le descriptif de chacune de ces offres est détaillé dans le tableau suivant :

	Offre n° 1	Offre n° 2	Offre n° 3
Montant mensuel du forfait (en euro)	6	10	18
Durée de communication (en heure)	2	2	6
Données internet (en Go)	0,2	2	20

1. On considère les matrices $M = \begin{pmatrix} 6 & 10 & 18 \\ 2 & 2 & 6 \\ 0,2 & 2 & 20 \end{pmatrix}$, $A = \begin{pmatrix} 350 \\ 120 \\ 70 \end{pmatrix}$ et $B = \begin{pmatrix} 350 & 120 & 70 \end{pmatrix}$.

- **a.** Lequel de ces deux produits de matrices est-il défini : $M \times A$ ou $M \times B$? Justifier.
- **b.** Effectuer ce produit de matrices à la calculatrice et interpréter le résultat obtenu.

2. On donne P la matrice inverse de M dont les coefficients sont arrondis à la quatrième décimale :

$$P = \begin{pmatrix} -0,1804 & 1,0567 & -0,1546 \\ 0,25 & -0,75 & 0 \\ -0,0232 & 0,0644 & 0,0515 \end{pmatrix}.$$

Pour un mois donné, l'opérateur a obtenu un chiffre d'affaires de 26 540 € pour l'ensemble de ces trois offres. On sait que cela correspond à la mise à disposition de 7 780 h de communications et à un volume de données internet de 14 440 Go.

On définit les matrices $C = \begin{pmatrix} 26540 \\ 7780 \\ 14440 \end{pmatrix}$ et $X = \begin{pmatrix} x \\ y \\ z \end{pmatrix}$ où x désigne le nombre de clients ayant choisi l'offre n° 1, y le nombre de clients pour l'offre n° 2 et z le nombre de clients pour l'offre n° 3.

- **a.** Écrire une égalité matricielle représentant la situation en utilisant les matrices M, C et X.
- **b.** Montrer l'égalité matricielle $X = P \times C$.
- **c.** En déduire le nombre de clients ayant choisi chacune des trois offres.
  Les valeurs seront arrondies à la dizaine.

Exercice 2 **9 points**

En France, chaque entreprise est identifiée par un numéro unique appelé **SIREN** (Système d'**I**dentification du **R**épertoire des **EN**treprises) composé de 9 chiffres. Chaque établissement d'une même entreprise se voit attribuer un numéro de SIRET à 14 chiffres composé de trois parties :

$$\underbrace{\text{SIREN}}_{9\text{ chiffres}}\ \underbrace{\text{NIC}}_{4\text{ chiffres}}\ \underbrace{\text{Clé}}_{1\text{ chiffre}}$$

- la première partie est le numéro SIREN de l'entreprise ;
- la deuxième partie, appelée NIC (Numéro Interne de Classement), est un numéro d'ordre séquentiel à quatre chiffres attribué à l'établissement ;
- la troisième partie est une clé de contrôle qui permet de vérifier la validité de l'ensemble du numéro SIRET.

Exemple 1 : 478 333 495 25518 est le numéro de SIRET du 2551^{e} établissement de l'entreprise de numéro de SIREN 478 333 495. La clé de contrôle est le dernier chiffre : 8.

On définit :

- E : l'ensemble de toutes les entreprises ;
- S : l'ensemble de tous les numéros de SIREN attribués ;
- T : l'ensemble de tous les numéros de SIRET attribués.

1. Indiquer si chacune des propositions suivantes est vraie ou fausse :

a. Q : « Deux établissements différents d'une même entreprise ont les 9 premiers chiffres de leur numéro de SIRET identiques. »

b. R : « Deux établissements différents d'une même entreprise ont le même numéro NIC. »

2. a. Peut-on définir une application de l'ensemble S de tous les numéros de SIREN attribués vers l'ensemble T de tous les numéros de SIRET attribués ? Justifier.

b. L'application qui, à chaque entreprise de l'ensemble E, associe un numéro de SIREN de l'ensemble S, est-elle injective, surjective, bijective ? Justifier chaque réponse.

c. Quel nombre maximum d'entreprises différentes la numérotation SIREN permet-elle d'identifier ?

3. Le calcul de la clé de contrôle (14^{e} chiffre du code SIRET) se fait selon l'algorithme ci-dessous.

1re étape : on calcule la somme pondérée des 13 chiffres constituant le numéro de SIRET sans la clé.

- On détermine le rang de chacun des 13 chiffres (le premier. en partant de la gauche, étant de rang 0).
- On associe à chaque chiffre une pondération de 2 pour les chiffres de rang pair et 1 pour les chiffres de rang impair.
- On calcule le produit de chaque chiffre par sa pondération. Si le résultat obtenu est supérieur ou égal à 10, on enlève 9.
- On effectue la somme de tous les chiffres ainsi obtenus.

Exemple 2 : on considère le numéro de SIRET (sans clé) suivant : 732 829 320 0007.

Rang	0	1	2	3	4	5	6	7	8	9	10	11	12
Chiffres	7	3	2	8	2	9	3	2	0	0	0	0	7
Pondération	2	1	2	1	2	1	2	1	2	1	2	1	2
Chiffres × Pondération	14	3	4	8	4	9	6	2	0	0	0	0	14
On enlève 9 si le produit précédent est supérieur ou égal à 10	5	3	4	8	4	9	6	2	0	0	0	0	5

- La somme pondérée est $5+3+4+8+4+9+6+2+0+0+0+0+5=46$.

2^{e} étape : on détermine la clé de contrôle.

- Si la somme pondérée est un multiple de 10, la clé est 0. Sinon, la clé est égale à $10-a$ où a est le reste de la division de la somme pondérée par 10.

a. Déterminer la clé du numéro de SIRET de l'exemple 2.

b. Vérifier si le numéro de SIRET 321 654 980 12312 est valide, c'est-à-dire si la clé de contrôle est correcte.

4. Soit $A = \{478333496 ; 732829320\}$ et $B = \{0001 ; 0002 ; 0003\}$.

a. Indiquer le cardinal de A, de B et du produit cartésien $A \times B$.

b. Déterminer deux éléments de $A \times B$.

c. Interpréter le contenu de l'ensemble $A \times B$ dans le contexte de l'exercice.

Exercice 3 **6 points**

Sous l'effet des phénomènes climatiques, de la houle et des marées, l'érosion provoque le recul des falaises. Actuellement, la vitesse de recul est élevée et selon les secteurs géographiques, elle peut varier de $0,08$ à $0,28$ mètre par an. Ce phénomène provoque l'affaiblissement de la base des falaises et entraîne des éboulements. Les constructions en bordure de falaises sont alors menacées et leurs habitants doivent être relogés.

Une maison est construite à 15 mètres du bord de la falaise. On considère que le danger est trop important pour que les occupants puissent l'habiter lorsqu'elle se trouvera à moins de 10 m du bord.

1. On suppose que dans ce secteur géographique, l'érosion se fait à raison de $0,21$ m par an.
On note u_n la distance en mètre entre le bord de la falaise et la maison après n années d'érosion.
On a donc $u_0 = 15$.

a. Déterminer la nature de la suite (u_n) puis exprimer u_n en fonction de n.

b. Déterminer dans combien d'années les occupants devront quitter cette maison en raison du danger.

2. Les scientifiques considèrent à présent un autre modèle mathématique dans lequel la distance restante entre la maison et le bord de la falaise diminue de 2,5 % chaque année.
On note alors v_n la distance en mètres restante après n années d'érosion, avec $v_0 = 15$.

a. Déterminer la nature de la suite (v_n) puis exprimer v_n en fonction de n.

b. Déterminer avec ce modèle mathématique, dans combien d'années les occupants devront quitter cette maison.

3. Lorsque la distance restante avec le modèle (u_n) est de $11,85$ m, déterminer par un calcul la distance restante obtenue avec le modèle (v_n).
Le résultat sera arrondi au cm.

2017 Polynésie

Exercice 1 **11 points**

Cinq joueurs, notés A, B, C, 0 et E, jouent régulièrement à un jeu en ligne.
Chaque partie de ce jeu oppose deux adversaires.
Le tableau suivant donne, pour chacun des cinq joueurs, la liste des adversaires qu'il a déjà battus.

Le joueur	a déjà battu
A	B, D
B	C
C	B, D
D	E
E	D

Ainsi, par exemple, le joueur C a déjà battu les joueurs B et D.

1. Graphe orienté associé à la situation

a. En considérant le tableau précédent comme un tableau de successeurs, représenter la situation par un graphe orienté G, dans lequel un arc relie un sommet x à un sommet y si le joueur x a déjà battu le joueur y.

b. Écrire la matrice d'adjacence M du graphe G.

c. Recopier et compléter le tableau des prédécesseurs dans le graphe G.

Le joueur	**a déjà ......**
A	
B	
C	
D	
E	

d. Le graphe G contient-il un circuit ? Contient-il un chemin hamiltonien ? Justifier les réponses.

2. Dans cette question, on note $J = \{A, B, C, D, E\}$ l'ensemble des cinq joueurs.
On note $V(x\,;\ y)$ le prédicat : « le joueur x a déjà battu le joueur y ».
Ainsi, la valeur $V(A\,;B)$ est VRAI, et la valeur de V(B ; A) est FAUX.

On définit trois prédicats :

P1 : $\forall x \in J, \exists y \in J$, $x \neq y$ et $V(x\,;\ y)$

P2 : $\exists x \in J, \exists y \in J$, $x \neq y$ et $V(x\,;\ y)$

P3 : $\exists y \in J, \forall x \in J$, $x \neq y$ et $V(x\,;\ y)$

Associer à chaque prédicat **P1**, **P2**, **P3**, celle des trois phrases suivantes qui lui correspond parmi les phrases suivantes. Aucune justification n'est demandée.

- « Il existe un joueur qui a été battu par tous les autres joueurs ».
- « Tous les joueurs ont battu au moins un autre joueur ».
- « Il existe un joueur qui a battu tous les autres joueurs ».

3. Un joueur reçoit un bonus lorsqu'il vérifie l'un au moins des trois critères suivants :

- le joueur a participé à 20 parties ou davantage, et il a affronté plusieurs adversaires différents ;
- le joueur n'a pas affronté plusieurs adversaires différents, et il a obtenu strictement plus de victoires que de défaites ;
- le joueur n'a pas obtenu strictement plus de victoires que de défaites, et il a participé à 20 parties ou davantage.

On définit les variables booléennes a, b, c de la façon suivante :

— $a = 1$ si le joueur a participé à 20 parties ou davantage ; $a = 0$ sinon ;
— $b = 1$ si le joueur a affronté plusieurs adversaires différents ; $b = 0$ sinon ;
— $c = 1$ si le joueur a obtenu strictement plus de victoires que de défaites ; $c = 0$ sinon.

a. Écrire une expression booléenne F traduisant les conditions permettant à un joueur d'obtenir le bonus.

b. À l'aide d'un tableau de Karnaugh ou d'un calcul booléen, déterminer une écriture simplifiée de F sous forme d'une somme de deux termes.

c. En déduire une formulation simplifiée des critères permettant à un joueur d'obtenir le bonus.

4. On note S la relation « successeur »dans le graphe G.
Ainsi, l'écriture « xSy » signifie que x a pour successeur y dans ce graphe.
On rappelle les définitions suivantes.

- Une relation binaire R sur un ensemble E est symétrique si pour tous x et y dans E :

$$x\,R\,y \Rightarrow y\,R\,x.$$

- Une relation binaire sur un ensemble E est transitive si pour tous x, y et z dans E :

$$x\,R\,y \text{ et } y\,R\,z \Rightarrow x\,R\,z.$$

a. La relation S est-elle transitive ? Justifier.

b. Quel(s) arc(s) faut-il ajouter au graphe pour rendre la relation S symétrique ?

Exercice 2 **9 points**

Le but de cet exercice est d'étudier une façon de parcourir un fichier de 195 clients, dont les fiches sont numérotées de 0 à 194.

Les deux parties peuvent être traitées de manière indépendante

Partie A - Étude d'une suite

On considère la suite (u_n) définie par

$$u_0 = 5 \text{ et, pour tout entier naturel } n : u_{n+1} = 3u_n + 4.$$

1. Déterminer u_1 et u_2.

2. Justifier que la suite (u_n) n'est ni arithmétique ni géométrique.

3. On considère la suite (v_n) définie pour tout entier naturel n par : $v_n = u_n + 2$.

a. Déterminer v_0, v_1 et v_2.

b. Justifier que (v_n) est une suite géométrique dont on précisera la raison.

c. Déterminer une expression de v_n en fonction de n.

4. En déduire, que pour tout entier naturel n, on a : $u_n = 7 \times 3^n - 2$.

Partie B - Étude d'un mode de parcours du fichier

Pour tout entier naturel n, on note w_n le reste de la division euclidienne de $7 \times 3^n - 2$ par 195.
On a ainsi, en particulier : $w_n \equiv 7 \times 3^n - 2 \text{ modulo } 195$.
On parcourt le fichier à l'aide de la suite (w_n) en déplaçant un curseur de la façon suivante :

- initialement, le curseur est positionné sur la fiche numéro 5, qui correspond à la valeur w_0 ;
- le curseur se déplace ensuite sur la fiche numéro 19, qui correspond à la valeur w_1 ;
- plus généralement, après n déplacements, le curseur est positionné sur la fiche dont le numéro correspond à la valeur de w_n.

1. Justifier que $w_5 = 139$.

2. Justifier que $3^{13} \equiv 3$ modulo 195. En déduire que $w_{13} = 19$.

3. Soit n un entier naturel quelconque.

   a. Démontrer que $w_{n+13} - w_{n+1} \equiv 7 \times 3^n \left(3^{13} - 3\right)$ modulo 195.

   b. En déduire, en utilisant la question 2., que $w_{n+13} = w_{n+1}$.

   c. Interpréter le résultat précédent concernant le positionnement du curseur.

4. On donne la liste des 15 premières valeurs de w_n :

$$5 - 19 - 61 - 187 - 175 - 139 - 31 - 97 - 100 - 109 - 136 - 22 - 70 - 19 - 61.$$

On considère l'ensemble $E = \{0,\ 1,\ 2,\ 3,\ \ldots, 193\ , 194\}$ et l'application f de E dans E, définie pour tout entier n de l'ensemble E par : $f(n) = w_n$.

   a. L'application f est-elle injective ? Justifier la réponse.

   b. L'application f est-elle surjective ? Justifier la réponse.

2016 Métropole

Exercice 1 (9 points)

La planification d'un projet de création d'un robot requiert les sept tâches listées ci-dessous.

Description de la tâche	Tâche	Durée (en jour)	Prédécesseurs
Achat de la structure	A	1	–
Modélisation numérique	B	5	A
Montage de la maquette	C	1	A, D
Achat des capteurs	D	3	–
Développement du programme	E	1	D
Test du programme sur la maquette et ajustements	F	4	C, E
Négociation des frais de fabrication	G	1	B, F

1. Déterminer le niveau de chacun des sommets.

2. Donner le tableau des successeurs de chaque sommet.

3. Construire le graphe d'ordonnancement du projet (méthode M.P.M. ou P.E.R.T.) en incluant les dates au plus tôt et au plus tard.

4. Donner un chemin critique et la durée minimale du projet.

5. Calculer la marge libre et la marge totale de la tâche A.

6. La tâche A commence avec un jour de retard.

a) Ce retard aura-t-il une incidence sur le début des tâches suivantes ? Justifier.

b) Ce retard aura-t-il une incidence sur la date de fin du projet ? Justifier.

Exercice 2 (5 points)

Dans un jeu vidéo de stratégie, le but est de franchir des niveaux successifs pour augmenter la résistance d'un bâtiment. Au début du jeu, le joueur commence au niveau 0 avec un bâtiment de résistance 5000. Au cours de la partie, le joueur gagne des pièces d'or qui lui permettent de passer des niveaux tout en augmentant la résistance du bâtiment. Par exemple, il en coûte 450 pièces d'or pour passer au niveau 1.

L'entier naturel n désigne le niveau du jeu atteint. On note r_n la résistance du bâtiment au niveau n et u_n le coût en pièce d'or pour passer du niveau n au niveau $n+1$.
On a donc $r_0 = 5\,000$ et $u_0 = 450$.

1. Dans la programmation du jeu, la suite (r_n) est une suite arithmétique de raison 1000.

a) Donner une expression de son terme général.

b) Calculer la résistance d'un bâtiment de niveau 20.

2. Le jeu est programmé pour que la suite (u_n) soit une suite géométrique de raison 1,5.

a) Donner une expression du terme général u_n de cette suite.

b) Calculer le coût en pièce d'or pour améliorer un bâtiment du niveau 19 au niveau 20. *Le résultat sera arrondi à l'unité.*

3. On s'intéresse à plusieurs améliorations successives d'un bâtiment.

a) Le coût total en pièce d'or pour améliorer successivement un bâtiment du niveau 0 au niveau 20 est égal à la somme des 20 premiers termes de la suite (u_n), c'est-à-dire la somme

$$u_0 + u_1 + \cdots + u_{19}$$

Calculer ce coût total en pièce d'or, arrondi à l'unité.

b) En récoltant 500 000 pièces d'or au cours de la partie, quel est le niveau atteint par le joueur ? Justifier la réponse.

Exercice 3 (6 points)

Lors de la transmission d'un message entre un émetteur et un récepteur, il est possible que le message soit altéré par des erreurs. On utilisera le vocabulaire suivant :

- un *mot* est une suite de 4 bits ;
- le *code initial* est le code envoyé par l'émetteur, il est constitué de 7 bits ;
- le *code reçu* est le code reçu par le récepteur, il est constitué de 7 bits.

On s'intéresse dans cet exercice à un code correcteur dit code de Hamming dont l'intérêt est de permettre de retrouver le code initial si une erreur intervient dans la transmission du code.

1. Travail préliminaire

On appelle « réduction d'un entier modulo 2 » le reste de la division euclidienne de cet entier par 2. Par exemple $11 = 2 \times 5 + 1$ donc la réduction de 11 modulo 2 est égale à 1.

a) Donner les 3 plus petits entiers naturels dont la réduction modulo 2 est égale à 1.

b) Quelle est la réduction modulo 2 d'un entier pair ?

Dans la suite de cet exercice, tous les produits de matrices seront calculés de façon habituelle, puis on donnera la réduction modulo 2 de tous les coefficients.

2. Codage d'un mot

On veut transmettre un mot de 4 bits. On le représente par une matrice à 1 ligne et 4 colonnes, par exemple le mot 0100 est représenté par la matrice :

$$m = \begin{pmatrix} 0 & 1 & 0 & 0 \end{pmatrix}.$$

Pour calculer son codage, on définit la matrice G suivante :

$$G = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{pmatrix}.$$

La fonction de codage C, qui donne le code c, est la fonction injective définie pour tout mot m de longueur 4 par le produit de matrices :

$$c = C(m) = m \times G.$$

Par exemple pour le mot $m = \begin{pmatrix} 1 & 1 & 0 & 0 \end{pmatrix}$, on a le code $c = \begin{pmatrix} 0 & 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$ car :

$$\begin{pmatrix} 1 & 1 & 0 & 0 \end{pmatrix} \times \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 2 & 2 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

et, après réduction modulo 2, on obtient bien : $c = C(m) = \begin{pmatrix} 0 & 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$.

a) Calculer le code du mot $m = (0 \quad 1 \quad 1 \quad 0)$.

On rappelle que les coefficients de la matrice obtenue doivent être réduits modulo 2.

b) Parmi les réponses suivantes, laquelle traduit le fait que la fonction de codage C est injective ?

Recopier sur la copie la seule bonne réponse.

- Le code d'un mot contient 7 bits différents.
- Il existe un code de 7 bits.
- Deux mots différents ont des codes différents.
- Tout code de 7 bits est l'image d'un mot de 4 bits.

3. Décodage

La fonction de décodage D est la fonction surjective qui associe à tout code c le mot $m = D(c)$ tel que $c = C(m)$. Le processus de codage-décodage permet donc de coder un mot avant sa transmission et de retrouver ce mot après sa transmission.

a) Soit H la matrice à 7 lignes et 4 colonnes définie par : $H = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$.

On remarque que l'on a $G \times H = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$.

Montrer que l'égalité $c = m \times G$ implique l'égalité $m = c \times H$.

b) On reçoit le code $c = (1 \quad 1 \quad 0 \quad 1 \quad 1 \quad 1 \quad 0)$. Il n'y a pas eu d'erreur de transmission. Retrouver le mot m qui a été codé par l'émetteur.

4. Vérification de la présence d'une erreur et correction

Dans la suite, on appelle erreur le remplacement d'un seul bit du code initial (0 au lieu de 1, ou 1 au lieu de 0). Pour vérifier l'apparition d'une telle erreur dans le code reçu c et la corriger, on utilise une matrice dite de parité P définie par :

$$P = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}.$$

On calcule le produit matriciel $c \times P$. Les coefficients résultants sont réduits modulo 2.

- Si le résultat est $(0 \quad 0 \quad 0)$ alors il n'y a pas eu d'erreur au sens défini ci-dessus.
  Par exemple, si le code reçu est $c = (1 \quad 1 \quad 0 \quad 1 \quad 0 \quad 0 \quad 1)$ alors $c \times P = (0 \quad 0 \quad 0)$, il n'y a pas eu d'erreur au sens défini ci-dessus.

- Sinon, le résultat obtenu correspond à la décomposition binaire de la position de l'erreur.
  Par exemple, si le code reçu est $c = (1 \quad 1 \quad 0 \quad 0 \quad 0 \quad 0 \quad 1)$ on a $c \times P = (1 \quad 0 \quad 0)$, donc il y a eu une erreur. Comme $100_2 = 4$, l'erreur porte sur le 4[e] bit en partant de la droite, on en déduit que le code initial était $(1 \quad 1 \quad 0 \quad 1 \quad 0 \quad 0 \quad 1)$.

Parmi les deux codes suivants, déterminer celui qui contient une erreur puis la corriger. Justifier (on ne demande pas le mot m correspondant à ce code).

- $(1 \quad 1 \quad 1 \quad 0 \quad 1 \quad 1 \quad 0)$;
- $(0 \quad 0 \quad 1 \quad 0 \quad 1 \quad 1 \quad 0)$.

2016 Nouvelle Calédonie

Exercice 1 (9 points)

Pour s'inscrire en BTS SIO, les étudiants doivent passer par la chaîne d'inscription mise en place dans leur établissement d'accueil. Cette chaîne d'inscription est composée de cinq postes :

- *photo* (P) : réalisation d'une photo d'identité numérique de l'étudiant ;
- *service médical* (M) : entretien avec l'infirmière de l'établissement (vaccinations et adaptation de la scolarité) ;
- *transport* (T) : mise à disposition des formulaires et justificatifs destinés aux sociétés de transports en commun ;
- *administration* (A) : constitution du dossier administratif ;
- *scolarité* (S) : constitution du dossier scolaire et choix des options.

Un étudiant qui s'inscrit doit passer par ces différents postes en respectant les contraintes suivantes :

- après le poste *photo*, l'étudiant peut se rendre au *service médical*, au *transport* ou à l'*administration* ;
- après le *service médical*, l'étudiant peut se rendre au *transport* ou à l'*administration* ;
- après le *transport*, l'étudiant peut se rendre au *service médical* ou à l'*administration* ;
- après l'*administration*, l'étudiant peut se rendre à la *scolarité*.

On définit le graphe orienté correspondant à cette situation. Les sommets associés aux différents postes de la chaîne sont nommés P, M, T, A, S dans cet ordre.
On donne la matrice d'adjacence B de ce graphe :

$$B=\begin{pmatrix} 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

1. Donner la représentation géométrique de ce graphe.

2. Dans le contexte de l'exercice, que signifient :
   a) les zéros de la première colonne ?
   b) les zéros de la dernière ligne ?

3. a) Citer un chemin hamiltonien de ce graphe.
   b) Comment peut-on interpréter l'existence d'un tel chemin dans le contexte de l'exercice ?

4. a) Recopier et compléter les coefficients de la matrice B^3 :

$$B^3=\begin{pmatrix} 0 & 1 & 1 & 2 & 2 \\ \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots \end{pmatrix}.$$

   b) Interpréter le coefficient de la première ligne et quatrième colonne de la matrice B^3, dans le contexte de l'exercice.

5. On définit la matrice :

$$\hat{B} = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

a) Vérifier, par une méthode au choix, que $\hat{B}$ est la matrice d'adjacence de la fermeture transitive du graphe associé à la matrice B.

b) Interpréter, dans le contexte de l'exercice, le coefficient de la deuxième ligne et cinquième colonne de la matrice $\hat{B}$.

Exercice 2 (5 points)

Dans le cadre d'une campagne publicitaire, une agence de publicité a décidé d'augmenter régulièrement le nombre de spots publicitaires diffusés, et ce pendant une période de 30 jours.
Le premier jour de la campagne, 15 spots sont diffusés. Chacun des jours suivants, on diffuse 7 spots de plus que la veille.

On note u_n le nombre de spots publicitaires diffusés le n-ième jour de la campagne. Ainsi $u_1 = 15$.

1. Déterminer la nature de la suite (u_n). Justifier et préciser le terme initial et la raison.

2. Pour tout entier n supérieur ou égal à 1, exprimer u_n en fonction de n.

3. Combien de spots ont-ils été diffusés le 30^{e} jour de la campagne ?

4. Combien de spots au total ont-ils été diffusés à la fin du 30^{e} jour de la campagne ?

Formulaire :

Si (u_n) est une suite arithmétique : $u_1 + ... + u_n = n \times \left(\dfrac{u_1 + u_n}{2} \right)$.

Si (u_n) est une suite géométrique de raison q ($q \neq 1$) : $u_1 + ... + u_n = u_1 \times \left(\dfrac{1-q^n}{1-q} \right)$.

Exercice 3 (6 points)

L'acheminement des messages sur un réseau informatique s'appuie sur des adresses IP (*Internet Protocol*). Une adresse IP est un numéro d'identification attribué, de manière provisoire ou définitive, à chaque équipement connecté à un réseau informatique.

Deux formats sont disponibles pour représenter une adresse IP. Le plus utilisé aujourd'hui est le format IP version 4 (IP V4). Mais le nombre d'adresses IP disponibles en version 4 tendant à s'épuiser, les adresses IP peuvent désormais être définies au format IP version 6 (IP V6).

Format d'une adresse IP V4

Une adresse IP V4 est codée sur 4 octets. Elle est représentée par 4 nombres séparés par des points, chacun de ces nombres étant en notation décimale.

Exemple : 192.168.1.231

Format d'une adresse IP V6

Une adresse IP V6 est codée sur 16 octets. Elle est représentée par 8 groupes de 4 chiffres hexadécimaux séparés par le symbole « *deux points* » (« : »).

Exemple : 8000:0000:0000:0000:0123:4567:89AB:CDEF

Représentation d'une adresse IP V4 au format IP V6

Il peut s'avérer nécessaire de coder une adresse IP V4 au format IP V6.
Dans ce cas, on convient, que :

- les dix octets situés à gauche contiennent des 0 ;
- les deux octets suivants contiennent chacun la valeur FF en hexadécimal ;
- les quatre octets situés à droite contiennent l'adresse IP V4 selon deux formats possibles ;
  - **le format IP V6-A :** 4 nombres décimaux séparés par des points ;
  - **le format IP V6-B :** deux groupes de 4 chiffres hexadécimaux.

Exemple

L'adresse IP V4 : 192.168.1.231 s'écrit de la manière suivante :

au format IP V6-A :	0000:0000:0000:0000:0000:FFFF:192.168.1.231
au format IP V6-B :	0000:0000:0000:0000:0000:FFFF:C0A8:01E7

Partie A - Format des adresses IP

1. Chacun des quatre nombres composant une adresse IP V4 est représenté sur un octet.
   Rappeler combien d'entiers différents on peut représenter sur un octet.

2. Justifier que l'écriture décimale 192.168.1.231 correspond bien à C0A8:01E7 en hexadécimal.

3. Déterminer l'adresse IP V4 correspondant à l'adresse IP V6-B suivante :

   0000:0000:0000:0000:0000:FFFF:C000:0783.

Partie B - Relations binaires

Dans cette partie, on suppose que les adresses IP V4 ne peuvent être codées qu'au format IP V6-B.

On considère les ensembles suivants :

- E_{V4} est l'ensemble de toutes les adresses IP pouvant être codées dans le format V4 ;
- E_{V6} est l'ensemble de toutes les adresses IP pouvant être codées dans le format V6 ;
- $E_{V4\text{-}V6}$ est l'ensemble de toutes les adresses IP V4 écrites dans le format V6.

On définit les applications f et g par les conditions suivantes :

- f est l'application de E_{V4} dans E_{V6} qui, à toute adresse IP V4, associe son adresse correspondante dans le format V6 ;
- g est l'application de E_{V4} dans $E_{V4\text{-}V6}$ qui, à toute adresse IP V4, associe son adresse correspondante dans le format V6.

1. L'application f est-elle surjective ? Justifier.

2. L'application g est-elle bijective ? Justifier.

2016 Polynésie

Exercice 1 (8 points)

Un administrateur réseau met en place une stratégie logique de maintenance en cinq étapes : A, B, C, D et E. Il a noté dans un tableau la dépendance immédiate des étapes les unes par rapport aux autres, en fonction de la logique d'enchainement des étapes.

Par exemple, selon lui, il est logique d'enchainer immédiatement l'étape B après l'étape A, ou de répéter l'étape A si nécessaire, mais il n'est pas logique d'effectuer immédiatement les étapes C, D et E après l'étape A.

Étapes	A	B	C	D	E
Étapes qui peuvent suivre immédiatement	A, B	B, C	D	C	A, D, E

1. Dessiner le graphe orienté G de sommets A, B, C, D, E, dont les arêtes orientées sont données par le tableau des successeurs ci-dessus.
2. Donner la matrice d'adjacence M associée au graphe orienté G.
3. Combien y a-t-il de chemins de longueur 2 d'origine E dans le graphe orienté G ? Justifier.
4. Combien y a-t-il de chemins de longueur 2 d'extrémité finale C dans le graphe orienté G ? Justifier.

On donne les matrices suivantes :

$$M^3 = \begin{pmatrix} 1 & 3 & 2 & 1 & 0 \\ 0 & 1 & 2 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 3 & 3 & 2 & 2 & 1 \end{pmatrix} \quad M^4 = \begin{pmatrix} 1 & 4 & 4 & 2 & 0 \\ 0 & 1 & 2 & 2 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 4 & 6 & 5 & 3 & 1 \end{pmatrix} \quad \text{et} \quad M^5 = \begin{pmatrix} 1 & 5 & 6 & 4 & 0 \\ 0 & 1 & 3 & 2 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 5 & 10 & 9 & 6 & 1 \end{pmatrix}.$$

5. Combien y a-t-il de circuits de longueur 4 dans le graphe ? Justifier.
6. On désigne par $\widehat{M}$ la matrice d'adjacence de la fermeture transitive du graphe orienté G.
   - **a)** Déterminer $\widehat{M}$.
   - **b)** Dans la matrice $\widehat{M}$, interpréter la valeur du coefficient de la ligne 1 et colonne 4, et celui de la ligne 1 et colonne 5.

Exercice 2 (5 points)

Un administrateur réseau gère le parc d'une petite entreprise qui comprend 9 ordinateurs. Chaque ordinateur possède une adresse de carte réseau, dite adresse MAC (Media Access Control) unique. Cette adresse est composée de 6 nombres entiers compris entre 0 et 255 séparés par des « : ». Chacun des 6 nombres est codé en hexadécimal.

Partie A

1. Pourquoi un nombre de 0 à 255 est-il codé en binaire sur un octet ?
2. En hexadécimal, avec combien de chiffres au maximun peut-on coder un entier de 0 à 255 ? Justifier.

3. Un ordinateur a l'adresse MAC suivante : $00\colon FF\colon B4\colon A9\colon 96\colon 11$.
Traduire en binaire et en décimal le nombre d'écriture hexadécimale $(B4)_{16}$.

Partie B

L'administrateur a assigné une adresse IP (Internet Protocol) à chaque ordinateur à l'aide d'un logiciel installé sur le serveur. Il obtient le tableau suivant :

Adresse MAC	N° de l'ordinateur	Adresse IP
00: FF: B4: A9: 96: 11	1	172.16.0.21
00: FF: B4: B0: 45: 1A	2	172.16.0.22
00: FF: B4: 00: C5: DE	3	172.16.0.23
00: EE: B5: 01: 32: C4	4	172.16.0.24
00: EE: B5: 01: 32: C5	5	172.16.0.25
00: EE: B5: 01: 32: C6	6	172.16.0.26
00: FF: B4: 00: C5: DF	7	172.16.0.27
00: FF: B4: 00: 02: 98	8	172.16.0.28
00: EE: B5: 01: 34: CA	9	172.16.0.29

On considère l'application f qui, à un numéro d'ordinateur, associe la dernière partie de l'adresse IP. Cette dernière partie est un entier variant de 2 à 255.

$$f : \{1; 2; 3; 4; 5; 6; 7; 8; 9\} \longrightarrow \{2; 3; ...; 255\}.$$

Par exemple, $f(1) = 21$.

1. Justifier le fait que cette application est injective.
2. Cette application est-elle surjective ? Justifier.
3. À la suite d'une opération informatique, le poste dont l'adresse MAC est $00\colon FF\colon B4\colon 00\colon C5\colon DF$ obtient l'adresse IP suivante : 172.16.0.23. Les autres postes gardent leur adresse IP précédente.
On a alors une nouvelle application $g : \{1; 2; 3; 4; 5; 6; 7; 8; 9\} \longrightarrow \{2; 3; ...; 255\}$.
L'application g est-elle injective ? Justifier.

Exercice 3 (7 points)

Le jeu du Juniper Green ou jeu des diviseurs et multiples a été créé par Richard Porteous, enseignant à l'école de Juniper Green. Il se joue à deux. Une fois qu'on a fixé un entier $N > 1$, les deux joueurs choisissent alternativement un entier entre 1 et N compris selon les règles suivantes :

- le joueur 1 choisit un entier n_1 compris entre 1 et N ;
- le joueur 2 choisit un entier n_2 compris entre 1 et N, multiple ou diviseur de n_1, qui n'a pas encore été joué ;
- le joueur 1 choisit un entier n_3 compris entre 1 et N, multiple ou diviseur de n_2, qui n'a pas encore été joué ;
- etc.

Chaque entier entre 1 et N ne peut apparaître au plus qu'une fois. Le perdant est celui qui ne peut plus jouer.

Exemple avec $N = 20$:

Joueur 1	6		9		2		4		1		perdu
Joueur 2		3		18		8		16		17	

- le joueur 1 choisit 6 ;
- le joueur 2 choisit 3 qui divise 6 ;
- le joueur 1 choisit 9 qui est bien un multiple de 3 ;
- etc.

À partir d'une partie, on crée un identifiant. L'identifiant est la suite d'entiers joués alternativement par les deux joueurs. Par exemple avec $N = 20$ et à partir de 6, l'identifiant créé peut être (6, 3, 9, 18, 2, 8, 4, 16, 1, 17).

1. a) On choisit $N = 14$. Reproduire et compléter le tableau suivant avec une solution possible.

Joueur 1	1		6		...		perdu
Joueur 2		2		12		...	

b) Donner l'identifiant qui correspond à cette solution.

2. Pour gagner la partie, les joueurs ont besoin de connaître les diviseurs et les multiples des différents nombres. Ils utilisent pour cela les décompositions en facteurs premiers.

a) Donner la décomposition en produit de facteurs premiers de 2262 en faisant apparaître la démarche.

b) En déduire tous les diviseurs de 2262.

3. Lorsqu'un nombre premier apparaît dans la liste des nombres composant l'identifiant, quelles sont les possibilités pour le nombre suivant ?

4. On suppose que $N = 14$. Montrer que si la liste commence par 11, alors il est possible que cette liste ne contienne que trois nombres.

5. Pour que la partie dure plus longtemps, il faut éviter que l'identifiant soit trop court. On impose alors que le premier entier q de la liste vérifie :

• q n'est pas un nombre premier   ou   • q vérifie $q \leq \sqrt{N}$.

Sous ces conditions et pour $N = 14$, donner les valeurs possibles du premier entier q de la liste.

2015 Métropole

Exercice 1 (7 points)

Une société de services et d'ingénierie informatiques planifie la mise en place d'un nouveau système d'information interne dans une entreprise. Les tâches nécessaires à la réalisation de ce projet sont répertoriées dans le tableau suivant.

Tâche à réaliser	Repère	Durée en jours	Tâche(s) précédente(s)	Nombre d'intervenants nécessaires
Établissement du cahier des charges	A	2		2
Rédaction du cahier technique	B	2	A	2
Définition des droits d'accès aux données	C	1	B	1
Choix, achat du matériel	D	4	B	3
Installation du matériel	E	1	D	2
Formation des responsables techniques	F	2	C, D	1
Installation et paramétrage du système	G	2	C, E	2
Rédaction de la notice d'utilisation et information des salariés	H	1	F, G	2

On souhaite ordonner la réalisation de ces tâches de façon à ce que le nouveau système soit fonctionnel le plus tôt possible.
Pour cela, on considère le graphe orienté correspondant aux conditions d'antériorité données par le tableau précédent.

1. Déterminer le niveau de chacun des sommets de ce graphe.

2. Donner le tableau des successeurs de chaque sommet.

3. Construire le graphe d'ordonnancement du projet (selon la méthode P.E.R.T. ou M.P.M.). Déterminer pour chaque tâche les dates au plus tôt et au plus tard. En déduire le chemin critique et la durée minimale de réalisation du projet.

4. Pour des questions de gestion du personnel, la société de services et d'ingénierie informatiques ne souhaite pas mobiliser plus de trois intervenants par jour. Peut-on planifier les tâches avec cette contrainte, sans modifier la durée totale du projet ?

Exercice 2 (5 points)

Une association sportive souhaite recruter une personne pour animer son site internet et dynamiser son image. Le candidat recruté devra remplir l'une au moins des quatre conditions suivantes :

- avoir des connaissances en informatique et être sous contrat avec la mairie ;
- ne pas avoir de connaissances particulières en informatique, mais être membre de l'association et être sous contrat avec la mairie ;
- ne pas être membre de l'association mais être sous contrat avec la mairie ;
- ne pas être sous contrat avec la mairie, mais être membre de l'association.

On définit les trois variables booléennes a, b et c de la manière suivante :
- $a = 1$ si la personne est membre de l'association, et $a = 0$ sinon ;
- $b = 1$ si la personne a des connaissances en informatique, et $b = 0$ sinon ;
- $c = 1$ si la personne est en contrat avec la mairie, et $c = 0$ sinon.

1. Écrire une expression booléenne E traduisant globalement les conditions de recrutement.

2. À l'aide d'un calcul booléen ou d'un tableau de Karnaugh, simplifier l'expression E sous la forme d'une somme de deux termes, puis interpréter cela à l'aide d'une phrase.

3. Un candidat ayant des connaissances en informatique se présente, mais il est écarté car il ne correspond pas aux critères de recrutement. Que peut-on en déduire sur le profil de ce candidat ?

Exercice 3 (8 points)

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

Le but de cet exercice est de décrire un procédé de codage d'un *mot* de deux lettres (partie **A**) à l'aide de la matrice A, puis de détailler une méthode de décodage de ce *mot* (partie **C**) en s'appuyant sur des résultats mathématiques établis dans la partie **B**.

Un *mot* de deux lettres est assimilé à une matrice colonne $X = \begin{pmatrix} x \\ y \end{pmatrix}$, où x est le nombre correspondant à la première lettre du *mot*, et y le nombre correspondant à la deuxième lettre du *mot*, selon le tableau de correspondance ci-après :

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Ainsi, par exemple, le *mot* « SI » est assimilé à la matrice $X = \begin{pmatrix} 18 \\ 8 \end{pmatrix}$.

Partie A : codage d'un *mot* de deux lettres

Pour coder le *mot* assimilé à la matrice $X=\begin{pmatrix} x \\ y \end{pmatrix}$, on calcule la matrice $U=\begin{pmatrix} u \\ v \end{pmatrix}$ telle que $AX=U$,

puis la matrice $C=\begin{pmatrix} c \\ d \end{pmatrix}$, où les nombres c et d sont les restes respectifs de la division euclidienne par 26 des nombres u et v. Le *mot* codé est alors le *mot* de deux lettres assimilé à la matrice $C=\begin{pmatrix} c \\ d \end{pmatrix}$, selon le tableau de correspondance précédent, c'est-à-dire que c et d sont les deux lettres du *mot* codé.

Déterminer le *mot* codé correspondant au *mot* « SI ».

Partie B : deux résultats mathématiques

On considère les matrices $B=\begin{pmatrix} 2 & -1 \\ -3 & 4 \end{pmatrix}$ et $I=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

1. Justifier la congruence : $5\times 21 \equiv 1$ modulo 26.

2. **a)** Calculer le produit matriciel $B\times A$, puis exprimer ce produit en fonction de la matrice I.

b) Soit $U=\begin{pmatrix} u \\ v \end{pmatrix}$ et $X=\begin{pmatrix} x \\ y \end{pmatrix}$ deux matrices quelconques à deux lignes et une colonne.

Justifier que, si $AX=U$, alors $5X=BU$.

Partie C : décodage d'un *mot*

On souhaite décoder le *mot* « BE », associé à la matrice $C=\begin{pmatrix} 1 \\ 4 \end{pmatrix}$.

Si $X=\begin{pmatrix} x \\ y \end{pmatrix}$ est la matrice associée au *mot* de départ, la matrice $U=\begin{pmatrix} u \\ v \end{pmatrix}$ définie par l'égalité $AX=U$ a ses coefficients qui vérifient : $\begin{cases} u\equiv 1 \text{ modulo } 26 \\ v\equiv 4 \text{ modulo } 26 \end{cases}$ d'après la partie **A**.

1. En utilisant la question **B 2.**, démontrer que $\begin{cases} 5x=2u-v \\ 5y=-3u+4v \end{cases}$.

En déduire que $\begin{cases} 5x\equiv -2 \text{ modulo } 26 \\ 5y\equiv 13 \text{ modulo } 26 \end{cases}$.

2. En utilisant la question **B 1.**, démontrer que $\begin{cases} x\equiv 10 \text{ modulo } 26 \\ y\equiv 13 \text{ modulo } 26 \end{cases}$ puis décoder le *mot* « BE ».

2015 Nouvelle Calédonie

Exercice 1 (5 points)

Cet exercice est un questionnaire à choix multiples.
Pour chacune des cinq questions, quatre réponses sont proposées, dont une seule est exacte.

Recopier sur la copie le numéro de la question et la réponse exacte.

Aucune justification n'est attendue.
Une bonne réponse rapporte 1 point.
Une réponse inexacte ou une absence de réponse n'enlèvent aucun point.

Questions		Réponses proposées
1.	a et b étant deux variables booléennes, l'expression $\overline{a+b}$ est toujours égale à :	• $\overline{a}+\overline{b}$ • $\overline{a}.\overline{b}$ • $\overline{a.b}$ • $\overline{a}+\overline{b}+\overline{a.b}$
2.	a, b et c étant des variables booléennes, une écriture simplifiée de l'expression $E = ab+\overline{b}\,\overline{c}+bc+\overline{a}\,\overline{c}$ est :	• $b+\overline{c}$ • $b\overline{c}$ • $b+c$ • $a+b+c$
3.	Les nombres 63 et 91 :	• sont premiers entre eux • sont premiers l'un et l'autre • ont un diviseur commun autre que 1 • sont divisibles par 3
4.	À chaque nombre entier naturel, on associe son double, ce qui définit une application f de **N** dans **N**. Cette application f est :	• injective • surjective • ni injective, ni surjective • bijective
5.	Soit P la proposition : « Tout étudiant en STS SIO connaît le langage Python ». La négation de la proposition P est :	• « Aucun étudiant en STS SIO ne connaît le langage Python » • « Exactement un étudiant en STS SIO ne connaît pas le langage Python » • « Les étudiants en STS SIO ne connaissent pas tous le langage Python » • « Tout étudiant en STS SIO connaît le langage JAVA »

Exercice 2 (8 points)

Partie A

Le tableau suivant donne la durée en heure des traversées entre différentes villes portuaires.
Par exemple, la case contenant le nombre 4 s'interprète ainsi : la durée de la traversée au départ de la ville B et à destination de la ville E est égale à 4 h.

Ville	A	B	C	D	E	F
A		3		8		
B				6	4	
C						
D			12			
E			8			6
F			3			

À ce tableau est associé un graphe orienté dont les sommets sont A, B, C, D, E et F.

1. Dresser le tableau des prédécesseurs de chacun des sommets de ce graphe, et déterminer le niveau de chaque sommet.
2. Dessiner le graphe en ordonnant les sommets par niveaux et en marquant la longueur de chaque arc.
3. Déterminer le (ou les) trajet(s) de durée minimale permettant d'aller de A à C.

Partie B

Une agence de voyage de la zone euro propose un circuit touristique pour visiter les 3 villes A, B et C. Le client peut choisir la durée du séjour dans chaque ville. L'agence distingue deux périodes, la haute et la basse saison, et différencie ses tarifs selon la période.

Les tarifs journaliers dans les différentes villes, en centaines d'euro par personne, sont donnés dans le tableau suivant. L'euro est noté €.

	Ville A	Ville B	Ville C
Nombre de jours	1	1	1
Tarif haute saison	2	2,5	1,5
Tarif basse saison	1	2	1

On note P la matrice $\begin{pmatrix} 1 & 1 & 1 \\ 2 & 2,5 & 1,5 \\ 1 & 2 & 1 \end{pmatrix}$.

1. Monsieur Martin a choisi un circuit qui comprend 3 jours dans la ville A, 2 jours dans la ville B et 5 jours dans la ville C. On associe à ce choix la matrice $M = \begin{pmatrix} 3 \\ 2 \\ 5 \end{pmatrix}$.

a) Calculer le produit matriciel $P \times M$. Que représentent les termes de la matrice obtenue ?

b) Monsieur Martin dispose de 1 500 €. Pourra-t-il réaliser son voyage ?

2. On considère la matrice $Q = \begin{pmatrix} -1 & 2 & -2 \\ -1 & 0 & 1 \\ 3 & -2 & 1 \end{pmatrix}$, et on note I la matrice unité : $I = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$.

a) Calculer le produit matriciel $Q \times P$.

b) Soient X et Y deux matrices colonnes quelconques à 3 lignes et 1 colonne.
Montrer que, si $P \times X = Y$, alors $X = Q \times Y$.

3. Dans une publicité, l'agence de voyage affirme qu'un circuit complet de 12 jours est possible au tarif de 2250 € en haute saison et 1400 € en basse saison.
Comment se compose ce circuit, en nombre de jours dans chacune des villes ?

Exercice 3 (7 points)

Après l'obtention de leur BTS SIO, Aurélien et Barbara sont employés dans deux entreprises différentes le 1er janvier 2015. Ces deux entreprises sont situées dans la zone euro ; l'euro est l'unité monétaire utilisée (notation €).

L'entreprise A propose à Aurélien un salaire annuel de 18 000 € en 2015, avec une augmentation annuelle de 380 €.
L'entreprise B propose à Barbara un salaire de 18 000 € en 2015, avec une augmentation annuelle de 2 %.

Pour tout entier naturel n, on note a_n et b_n les montants respectifs, en euro, des salaires annuels d'Aurélien et de Barbara, pour l'année $(2015 + n)$.

1. Étude du salaire d'Aurélien

a) Calculer le salaire annuel d'Aurélien en 2016 puis en 2017.
b) Déterminer la nature de la suite (a_n) et, pour tout entier naturel n, exprimer le nombre a_n en fonction de l'entier n.
c) Quel sera le salaire annuel d'Aurélien en 2025 ?
d) On rappelle que la somme des premiers termes d'une suite arithmétique (u_n) peut être obtenue à l'aide de la formule : $u_0 + u_1 + ... + u_n = \frac{(u_0 + u_n)}{2} \times (n+1)$.
Par une méthode au choix, calculer le montant total que doit percevoir Aurélien, du 1er janvier 2015 au 31 décembre 2025.

2. Étude du salaire de Barbara

a) Calculer le salaire annuel de Barbara en 2016 puis en 2017.
b) Déterminer la nature de la suite de la suite (b_n).
c) Justifier que, pour tout entier naturel n, on a : $b_n = 18000 \times 1{,}02^n$.
d) Quel sera, arrondi au centime d'euro, le salaire annuel de Barbara en 2025 ?
Expliquer la démarche.

3. Comparaison des deux salaires

À l'aide de la calculatrice, comparer, pour les années allant de 2015 à 2030, les salaires de Barbara et Aurélien.

2015 Polynésie

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.

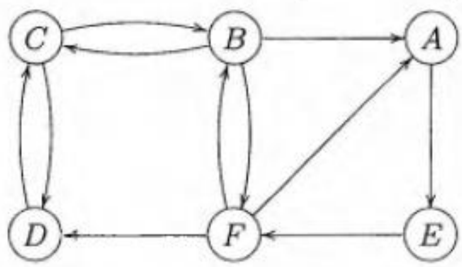
4. L'entreprise et le fournisseur conviennent que le contrat sera rompu lorsque le prix unitaire d'un clavier souple sera inférieur à 5 euros.
Déterminer le nombre d'années qui engagent l'entreprise et son fournisseur. Justifier.

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 :
> $$p \text{ divise } a^p - a.$$

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 $a = 3$.

2014 Métropole

Exercice 1 **7 points**

Un lycée a été doté de postes informatiques et de logiciels.
Le proviseur envisage de transformer une salle de cours en salle informatique. Pour cela, le responsable du projet définit les tâches à réaliser avec leur durée.
Le tableau suivant regroupe l'ensemble de ces données.

Tâche à réaliser	Repère	Durée en jours	Tâches précé-dentes
Vider la salle de cours et démonter le matériel inutilisé.	A	2	–
Nettoyer et repeindre la salle.	B	4	A
Installer les tables et fixer un tableau.	C	1	B
Commander et réceptionner le matériel de câblage.	D	10	–
Déballer et contrôler le matériel de câblage livré.	E	1	D
Câbler la salle.	F	3	B, E
Installer et brancher les postes informatiques.	G	1	C, F
Installer les logiciels, configurer les postes et tester leur fonctionnement.	H	7	G

Le but de cet exercice est d'ordonner la réalisation de ces tâches de façon à ce que la salle soit disponible le plus rapidement possible.
On considère le graphe orienté correspondant aux conditions d'antériorité données par le tableau précédent.

1. Déterminer le niveau de chacun des sommets du graphe.
2. Donner le tableau des successeurs.
3. **a.** Construire le graphe d'ordonnancement du projet (selon la méthode P.E.R.T. ou M.P.M.)
   Déterminer pour chaque tâche les dates au plus tôt et au plus tard.
   b. En déduire le chemin critique et la durée minimale de réalisation du projet.
4. En fait, la réalisation de la tâche B a nécessité 10 jours au lieu de 4 car il a fallu enduire un mur et le laisser sécher avant de le peindre.
   Ce changement a-t-il une incidence sur la durée du projet ? Expliquer pourquoi.

Exercice 2 **5 points**

La loi de Moore, énoncée en 1975 par Gordon Moore, co-fondateur de la société Intel, prévoit que le nombre de transistors des micro-processeurs proposés à la vente au grand public double tous les 2 ans. Les micro-processeurs fabriqués en 1975 comportaient 9 000 transistors.

Pour modéliser cette loi de Moore, on considère la suite (u_n) définie par $u_0 = 9000$ et $u_{n+1} = 2u_n$ pour tout entier naturel n.

Un terme u_n de cette suite correspond au nombre de transistors prévus par la loi de Moore pour un micro-processeur fabriqué lors de l'année $1975 + 2n$.

1. Calculer u_1 et u_2 puis interpréter ces nombres.
2. Quelle est la nature de la suite (u_n) ?
   Donner l'expression de u_n en fonction de n.
3. Déterminer le nombre de transistors prévus par la loi de Moore pour un micro-processeur fabriqué en 2001.
4. Selon ce modèle, à partir de quelle année les micro-processeurs intégreront-ils plus de 100 milliards de transistors ?

Exercice 3 **8 points**

Partie A

1. **a.** Décomposer le nombre 2014 en produit de facteurs premiers.
   b. En déduire la liste des diviseurs positifs de 2014.
2. Calculer le PGCD des nombres 2014 et 212. On note d ce PGCD.
   Déterminer l'entier p tel que : $2014 = p \times d$.

Partie B

Un jury de concours doit établir l'ordre de passage des 2014 candidats qui doivent passer une épreuve orale. Le président du jury envisage la procédure automatique décrite ci-après.
Tout d'abord, il classe les 2014 candidats par ordre alphabétique et attribue à chacun, en suivant cet ordre, un numéro allant de 1 à 2014. Ainsi, pour définir un ordre de passage à l'oral des candidats il suffit de dresser la liste des numéros des candidats qui seront appelés l'un après l'autre à passer l'épreuve orale.
Pour établir cette liste, le président du jury choisit un entier n compris entre 1 et 400, puis procède de la manière suivante :

- le premier numéro inscrit sur la liste est le nombre n ;
- le deuxième numéro inscrit sur la liste est le nombre $2n$;
- le troisième numéro inscrit est le nombre $3n$;
- de façon générale, pour obtenir chaque numéro inscrit à partir du deuxième, on ajoute n au numéro précédent et :
  — si la somme s obtenue est inférieure ou égale à 2014, le numéro inscrit est égal à cette somme s ;
  — sinon, le numéro inscrit est égal à $s - 2014$.

Par exemple, en choisissant la valeur $n = 257$, les premiers numéros inscrits sur la liste sont, dans l'ordre :

257–514–771–1028–1285–1542–1799–42–299–556–...– etc.

En effet :

- le premier numéro inscrit est $n = 257$;
- du 2e numéro (égal à 514) au 7e numéro (égal à 1799), on a ajouté 257 au numéro précédent puisque la somme ne dépassait pas 2014 ;
- le 8e numéro inscrit est le numéro 42 car $1799 + 257 = 2056$ et, comme 2056 dépasse 2014, le numéro à inscrire est $2056 - 2014 = 42$.

Ainsi le candidat 257 passera en premier l'oral ; il sera suivi du candidat 514 et ainsi de suite.
Le président du jury se demande si cette procédure permet de convoquer tous les candidats, c'est-à-dire si la liste obtenue, en 2 014 étapes, contient tous les nombres de 1 à 2 014.

1. Dans cette question, le président du jury choisit $n = 212$.
   a. Les 9 premiers numéros inscrits sont donc :

   $$212–424–636–848–1\,060–1\,272–1\,484–1\,696–1\,908.$$

   Donner la liste des 15 numéros suivants.
   La valeur $n = 212$ permet-elle de convoquer tous les candidats ?
   b. Avec cette valeur de n, combien de numéros différents la liste comporte-t-elle ?
2. Dans cette question, le président du jury choisit $n = 38$.
   Déterminer combien de numéros différents comporte la liste. Justifier la réponse. On pourra remarquer que 38 est un diviseur de 2 014.

Partie C

D'après la partie B, il apparaît que, pour certaines valeurs de n, la procédure utilisée ne permet pas de convoquer tous les candidats, c'est-à-dire de constituer une liste comportant tous les nombres de 1 à 2 014.
On admet le résultat suivant :
« Le nombre n choisi permet de former une liste complète comportant tous les numéros de 1 à 2 014 dans le cas où le PGCD de 2 014 et de n est égal à 1, et dans ce cas seulement ».
Ainsi, les nombres n permettant de convoquer tous les candidats sont les entiers n compris entre 1 et 400 qui sont premiers avec 2 014.

1. Si $n = 15$, la procédure utilisée permet-elle de convoquer tous les candidats ?
2. Dans cette question, on cherche à déterminer le nombre d'entiers n, parmi ceux compris entre 1 et 400, qui permettent par la procédure utilisée de convoquer tous les candidats.
   a. Donner le nombre de multiples de 2 non nuls, inférieurs ou égaux à 400.
   b. Donner la liste des multiples **impairs** de 19, inférieurs ou égaux à 400.
   c. Donner la liste des multiples **impairs** de 53, inférieurs ou égaux à 400.
   d. En déduire le nombre d'entiers n qui ne permettent pas de convoquer tous les candidats, puis le nombre d'entiers n qui le permettent.

2014 Nouvelle Calédonie

Exercice 1 (6 points)

Les questions 1, 2, 3 sont indépendantes.

1. En informatique, pour coder les lettres de l'alphabet, l'un des premiers codes utilisés a été le code ASCII.
Par exemple le caractère « a » est codé en ASCII par le nombre 97 (en écriture décimale), qui correspond dans le système binaire (ou base deux) au nombre 1100001.

On donne ci-dessous un extrait de la table ASCII, le code étant donné en écriture décimale :

lettre	a	b	c	d	e	f	g	h	i	j	k	l	m
code	97	98	99	100	101	102	103	104	105	106	107	108	109

lettre	n	o	p	q	r	s	t	u	v	w	x	y	z
code	110	111	112	113	114	115	116	117	118	119	120	121	122

a) Déterminer la lettre qui est codée, en ASCII, par le nombre 1101101 écrit en binaire.

b) Écrire en binaire le codage ASCII de la lettre « j ».

2. Pour coder une couleur, on utilise souvent le code RVB. Le principe est de donner pour cette couleur l'intensité de ses trois composantes Rouge, Vert, Bleu en hexadécimal (base seize) ou en écriture décimale (base dix).
Pour l'intensité, on utilise une échelle allant de 00 à FF en hexadécimal, c'est-à-dire de 0 à 255 en écriture décimale.

Par exemple : la couleur « lilas » est codée (A5 ; 44 ; B9) en hexadécimal ou $(165\,;68\,;185)$ en écriture décimale. Ceci signifie qu'en hexadécimal, l'intensité du rouge est A5, celle du vert est 44 et celle du bleu est B9.

a) La couleur « or » est codée en écriture décimale $(255\,;215\,;0)$.
Déterminer son codage en hexadécimal.

b) La couleur « brun » est codée en hexadécimal (5B ; 3C ; 11).
Déterminer son codage en écriture décimale.

3. Pour réaliser certaines applications en assembleur, il faut effectuer des opérations sur les nombres entiers en base deux. Deux telles opérations sont proposées ci-après.

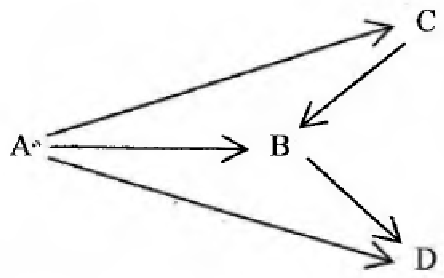
a) 10111 et 1101 sont deux nombres écrits en base deux.
Calculer leur somme en base deux.

b) Le nombre $R = 101\ 1101\ 0101$ est écrit en base deux.
Écrire le nombre décimal 8 en base deux. Le résultat est noté S.
Déterminer en base deux le produit $R \times S$.

Exercice 2 (6 points)

Au cours d'un stage, un étudiant en BTS SIO a développé un jeu pour téléphone portable.
Le jeu comprend quatre étapes, notées A, B, C, D.

Le joueur commence à l'étape A puis, selon l'indice découvert, passe à une autre étape. Les possibilités de passage d'une étape à l'autre sont données par le graphe orienté G ci-contre, dont les sommets A, B, C, D modélisent les étapes, et les flèches les possibilités de passage d'une étape à une autre.



1. Donner la matrice d'adjacence M de ce graphe orienté, en considérant les quatre sommets A, B, C, D dans cet ordre.

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

a) Citer tous les chemins de longueur 2.

b) Déterminer la matrice M^4 ; cette matrice peut être obtenue à la calculatrice.
Interpréter le résultat dans le contexte du jeu.

3. Existe-t-il un chemin hamiltonien ? Si oui, le donner.

4. On note $M^{[n]}$ la n-ième puissance booléenne de la matrice M, et $\oplus$ l'addition booléenne de deux matrices.

a) Déterminer la matrice $M' = M \oplus M^{[2]} \oplus M^{[3]} \oplus M^{[4]}$.

b) Donner la représentation géométrique du graphe G' dont la matrice d'adjacence est M'.

c) Interpréter dans le contexte du jeu la dernière ligne de la matrice M'.

Exercice 3 (8 points)

Les trois parties A, B et C sont indépendantes.

Partie A

Dans une société de service informatique, chaque client possède un numéro noté n, où n est un entier naturel non nul.

La notation $a \equiv b\ [k]$ signifie que le nombre a est congru au nombre b modulo k.

- Si $n \equiv 0\ [6]$, alors le client est suivi par le technicien A ;
- si $n \equiv 1\ [6]$ alors le client est suivi par le technicien B ;
- si $n \equiv 2\ [6]$ alors le client est suivi par le technicien C ;
- si $n \equiv 3\ [6]$ alors le client est suivi par le technicien D ;
- dans les autres cas, le client est suivi par le technicien E.

1. Par quel technicien est suivi le client numéro 51 ? Justifier la réponse.

2. Le client numéro 23 est-il suivi par technicien E ? Justifier la réponse.

Partie B

Pour permettre aux clients de la société d'accéder à leurs factures, le service comptable attribue un code à chacun d'entre eux.

Pour tout entier naturel n, le code attribué au client numéro n se calcule avec la formule $x+n\,y+n^2\,z$, où x, y et z sont trois nombres que les questions suivantes vont permettre de déterminer.

1. Sachant que le client numéro 1 a pour code le nombre 12, que le client numéro 2 a pour code le nombre 27 et que le client numéro 3 a pour code le nombre 50, écrire un système de trois équations vérifié par les nombres x, y et z.

2. On donne les matrices $X=\begin{pmatrix} x \\ y \\ z \end{pmatrix}$, $M=\begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 4 \\ 1 & 3 & 9 \end{pmatrix}$ et $Y=\begin{pmatrix} 12 \\ 27 \\ 50 \end{pmatrix}$.

Le système précédent s'écrit alors sous la forme matricielle : $M\times X=Y$.

Résoudre ce système revient à déterminer la matrice X, ce que proposent les questions suivantes.

a) Soit $P=\begin{pmatrix} 3 & -3 & 1 \\ -2{,}5 & 4 & -1{,}5 \\ 0{,}5 & -1 & 0{,}5 \end{pmatrix}$. Calculer le produit matriciel $P\times M$.

b) En déduire que si $M\times X=Y$ alors $X=P\times Y$.

c) Déterminer alors les nombres x, y et z.

Partie C

Dans la société, pour modéliser les critères de recrutement aux postes de conseillers, on définit pour chaque postulant les trois variables booléennes a, b et c, ainsi définies :

- $a=1$ si le postulant a eu un entretien favorable avec le DRH (directeur des ressources humaines), $a=0$ sinon ;
- $b=1$ si le postulant a réussi un concours interne, $b=0$ sinon ;
- $c=1$ si le postulant a été parrainé par un cadre, $c=0$ sinon.

Les critères de recrutement sont définis par l'expression booléenne E suivante :

$$E=a\,c+b\,\overline{c}+a\,b.$$

1. Écrire une phrase traduisant ces critères de recrutement.

2. **a)** À l'aide d'un diagramme de Karnaugh ou à l'aide d'un calcul booléen, donner une écriture simplifiée de l'expression booléenne E sous la forme d'une somme de deux termes.

b) Écrire une phrase correspondant à la simplification précédente de l'expression booléenne E.

2014 Polynésie

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. Quelles 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 SA TA 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 SAT A, $c = 0$ 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 Kanaugh 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 1^er^ 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 $u_1 = 6000$.

1. Vérifier que $u_2 = 6300$ 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 :

$$U_1 + U_2 + \cdots + U_n = U_1 \times \frac{1-q^n}{1-q}.$$

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 $K = 4 \times 22 = 88$, 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 $d \times c \equiv 1 \mod K$. Le couple d'entiers (n, d) est la clé privée. Alice a trouvé $d = 49$.
   Expliquer pourquoi $49 \times 9 \equiv 1 \mod 88$.

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 :

$$2^{33} = 8\,589\,934\,592 \quad \text{et} \quad 8\,589\,934\,592 \equiv 47 \mod 115,$$
$$2^{16} = 65\,536 \quad \text{et} \quad 65\,536 \equiv 101 \mod 115.$$

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

2013 Métropole

Exercice 1 (6 points)

Le directeur des ressources humaines (DRH) d'une mairie doit recruter une personne pour un travail concernant la circulation des voitures dans le centre ville.

Partie A

Pour faire son choix, le DRH met en place trois critères de sélection concernant les connaissances en informatique, l'expérience dans le domaine concerné et le suivi d'un stage de formation spécifique.
La personne recrutée devra :

- avoir des connaissances informatiques et de l'expérience dans le domaine concerné ;
- ou ne pas avoir de connaissances informatiques mais avoir suivi un stage de formation spécifique ;
- ou ne pas avoir d'expérience dans le domaine concerné, mais avoir suivi un stage de formation spécifique.

On définit les trois variables booléennes a, b et c suivantes :

- $a=1$ si la personne possède des connaissances informatiques, $a=0$ sinon ;
- $b=1$ si la personne possède de l'expérience dans le domaine concerné, $b=0$ sinon ;
- $c=1$ si la personne a suivi un stage de formation spécifique, $c=0$ sinon.

1. Décrire la situation correspondant au produit $a\,b\,\overline{c}$.

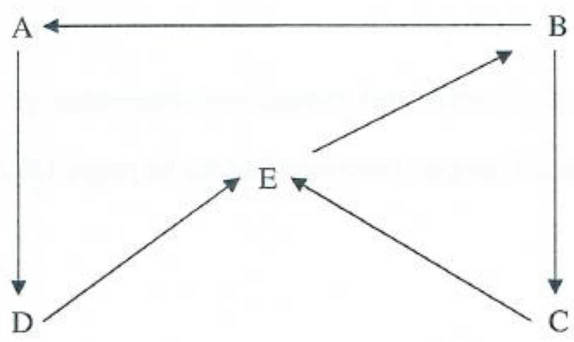
2. Définir l'expression booléenne E correspondant aux critères de sélection du DRH.

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

4. Écrire une phrase donnant les conditions de recrutement correspondant à la simplification précédente de l'expression booléenne E.

Partie B

Le plan de circulation du centre ville peut être représenté par le graphe orienté suivant où les sommets A, B, C, D et E sont les carrefours et où les arcs indiquent les rues et leur sens de circulation.



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

2. On donne le carré de la matrice M : $M^2 = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \end{pmatrix}$.

   Interpréter les chiffres « 1 » de la deuxième ligne et donner les chemins correspondants.

3. Calculer la somme booléenne $M \oplus M^{[2]}$ et donner la signification des termes de cette somme.

Exercice 2 (7 points)

Le but de cet exercice est d'étudier la dépréciation d'un modèle d'ordinateur en fonction du temps écoulé, exprimé en trimestre, depuis sa mise sur le marché.
L'entreprise conceptrice de ce modèle souhaite déterminer l'évolution trimestrielle du prix de vente de cet ordinateur, exprimé en euro. On appelle n le nombre de trimestres écoulés depuis la mise sur le marché de ce produit. Ainsi, à la mise sur le marché, on a $n=0$.
Deux modélisations ont été retenues par cette entreprise.

Partie A : 1$^{\text{re}}$ modélisation

Le prix de vente initial à la mise sur le marché de ce modèle d'ordinateur est de 795 €. Chaque trimestre, le prix de vente de ce modèle diminue de 10 % en raison des progrès technologiques.
On note (u_n) la suite telle que, pour tout entier naturel n, u_n désigne le prix de vente, exprimé en euro, de ce modèle d'ordinateur, n trimestres après sa mise sur le marché.

1. Donner u_0, puis calculer u_1 et u_2.
2. Déterminer la nature de la suite (u_n) et préciser sa raison.
3. En déduire que, pour tout entier n, on a : $u_n = 795\times 0{,}9^n$.
4. À partir de combien de trimestres le prix de vente d'un tel ordinateur devient-il strictement inférieur à 300 € ?

Partie B : 2$^{\text{e}}$ modélisation

Le prix de vente, exprimé en euro, de ce modèle d'ordinateur au bout de n trimestres écoulés depuis sa mise sur le marché, noté v_n, est donné par : $v_n = 525\mathrm{e}^{-0{,}25n}+270$.

1. Vérifier que le prix de vente de ce modèle d'ordinateur à sa mise sur le marché est de 795 €.
2. Déterminer le nombre minimal de trimestres écoulés depuis sa mise sur le marché à partir duquel le prix de vente de ce modèle d'ordinateur deviendra inférieur ou égal à 300 €.

Partie C : comparaison des deux modèles

1. Déterminer les prix de vente, dans chacune des modélisations, 5 trimestres après la mise sur le marché du modèle d'ordinateur.
2. À long terme, laquelle des deux modélisations donne le prix de vente le plus bas ? Justifier la réponse.

Exercice 3 (7 points)

Un jeu classique consiste à coder des messages. Pour cela, on utilise la correspondance entre les lettres de l'alphabet et un nombre entier x compris entre 0 et 25.
Le tableau ci-dessous donne cette correspondance :

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Le codage consiste à choisir une clé formée de deux nombres entiers a et b compris entre 0 et 25 et à remplacer une lettre par une autre selon le principe suivant :

- on lit sur le tableau le nombre x correspondant à la lettre ;
- on calcule le reste r de la division de $ax+b$ par 26 ;
- on lit sur le tableau la lettre correspondant au nombre r qui est donc la lettre codée.

Exemple : avec la clé $(a;b)=(7;12)$, pour coder la lettre T, on calcule $7\times19+12=145$, puis le reste de la division euclidienne de 145 par 26, soit 15. La lettre codée est ainsi la lettre P.

1. Coder les lettres A, K et W avec la clé $(a;b)=(5;17)$.

2. Que se passe-t-il si on prend $a=0$ et $b=17$?

3. On considère un entier x compris entre 0 et 25.

a) Donner, sans justification, les restes obtenus dans la division euclidienne de $13x+6$ par 26 pour x compris entre 0 et 25.

b) Coder le mot PREMIER avec la clé $(13;6)$.

Commenter le résultat obtenu.

4. Un codage est dit acceptable lorsque deux lettres distinctes quelconques sont toujours codées différemment.

On admet que les clés $(a;b)$ donnant un codage acceptable sont celles pour lesquelles a est un entier premier avec 26, quel que soit l'entier b compris entre 0 et 25.

a) Donner la liste des nombres entiers compris entre 0 et 25 et premiers avec 26.

b) Déterminer le nombre de clés donnant un codage acceptable.

5. Le mot ABSURDE a été codé à l'aide d'une clé $(a;b)$ selon le principe décrit ci-dessus et l'on a obtenu VOZLGAT. Déterminer cette clé.

2013 Nouvelle Calédonie

Exercice 1 **5 points**

Pour obtenir un diplôme, des étudiants doivent valider quatre modules différents notés A, B, C et D.
Les modules nécessitent certaines connaissances et doivent donc être validés en respectant les règles suivantes :

— une fois le module A validé, on peut valider les modules B, C ou D ;
— une fois le module B validé, on peut valider le module D ;
— une fois le module C validé, on peut valider les modules B ou D ;
— aucun module ne peut être validé après le module D.

On définit ainsi un graphe orienté de sommets A, B, C et D, pris dans cet ordre, et dont la matrice d'adjacence est la matrice M :

$$M = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Ainsi $m_{12} = 1$ signifie que l'on peut valider le module B, le module A ayant été validé.

1. Reproduire et compléter le tableau des prédécesseurs :

Sommets	Prédécesseurs
A	
B	
C	A
D	

2. Déterminer le niveau des sommets de ce graphe. Expliquer la démarche suivie.
3. Donner une représentation géométrique du graphe ordonné par niveaux.
4. Existe-t-il un chemin de longueur 4 entre deux sommets du graphe ? Justifier.
   a. Déterminer la longueur de chemin maximale qui peut exister entre deux sommets de ce graphe.
   b. Donner un tel chemin. Un étudiant qui a suivi un tel parcours a-t-il validé tous les modules ?

Exercice 2 **6 points**

Un petit fournisseur de matériel informatique propose trois formules de vente à ses clients :

— une formule F1 « clavier + souris » à 12 euros ;
— une formule F2 « clavier + souris + clé USB » à 16 euros ;
— une formule F3 « clavier » à 10 euros.

Pour chacune de ces formules, dans le tableau suivant sont indiqués le coût d'achat du matériel, le temps moyen nécessaire au conditionnement de chaque formule et le prix demandé :

	Formule F1	Formule F2	Formule F3
Coût d'achat en euro	3	4	2
Temps en minute	8	10	6
Prix de vente en euro	12	16	10

1. a. On considère la matrice $M = \begin{pmatrix} 3 & 4 & 2 \\ 8 & 10 & 16 \\ 12 & 16 & 10 \end{pmatrix}$ et la matrice colonne $C = \begin{pmatrix} 10 \\ 8 \\ 14 \end{pmatrix}$.

Effectuer le produit matriciel MC.

b. On considère le cas où 10 clients optent pour la formule F1, 8 pour la formule F2 et 14 pour la formule F3.

Donner la signification de chacun des coefficients du produit matriciel MC en termes de coût d'achat, de temps et de prix de vente.

2. On considère la matrice $P = \begin{pmatrix} a & 2 & -1 \\ 2 & -1,5 & 0,5 \\ -2 & 0 & 0,5 \end{pmatrix}$.

a. Calculer les coefficients de la première ligne du produit matriciel PM.

b. Déterminer le réel a tel que le produit matriciel PM soit égal à la matrice unité $I = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$.

3. Dans la suite de l'exercice on prend $a = -1$ et l'on admet que, dans ce cas, $PM = I$.

Soient X et Y deux matrices à une colonne et trois lignes. Démontrer que si $MX = Y$ alors $X = PY$.

4. On sait que le fournisseur a dépensé 100 euros pour l'achat du matériel, que le conditionnement a nécessité 270 minutes et que la recette pour ces trois formules a été de 430 euros.

Déterminer, pour chacune des formules, le nombre de clients l'ayant choisie.

Exercice 3 **9 points**

Des étudiants en informatique étudient la propagation de virus sur le disque d'un ordinateur non connecté à un réseau.

Partie A : un premier virus

À chaque allumage de l'ordinateur, le virus se répand et le nombre de fichiers infectés est déterminé par le terme général de la suite (U_n) définie par son premier terme $U_1 = 1$ et, pour tout entier naturel n non nul : $U_{n+1} = 1 + 2U_n$ où n est le nombre d'allumages de l'ordinateur.

1. Calculer U_2, U_3 et U_4.
   Justifier que la suite (U_n) n'est ni arithmétique ni géométrique.
2. On considère la suite (V_n) définie pour tout entier naturel $n \geqslant 1$ par : $V_n = U_n + 1$.
   Calculer V_1, V_2, V_3 et V_4.
   Quelle conjecture sur la nature de la suite (V_n) peut-on formuler ?
3. **a.** Démontrer que, pour tout entier naturel $n \geqslant 1$: $V_{n+1} = 2V_n$.
   b. En déduire une expression de V_n en fonction de n.
4. **a.** En déduire que, pour tout entier naturel n, $n \geqslant 1 : U_n = 2^n - 1$.
   b. À partir de combien d'allumages de l'ordinateur, le nombre de fichiers infectés sera-t-il supérieur à 1 000 ?

Partie B : un deuxième virus

L'équipe d'étudiants implante maintenant un virus sur un autre ordinateur. Le nombre de fichiers infectés en fonction du nombre n d'allumages de l'ordinateur est $3^n - 1$.
Par ailleurs, chaque fois que le nombre de fichiers infectés est un multiple de 11, un message d'avertissement s'affiche à l'écran.
Le reste de la division euclidienne de $3^n - 1$ par 11 est noté W_n.

1. Reproduire et compléter le tableau suivant :

n	$3^n - 1$	W_n
1		
2		
3		
4		
5		

2. Démontrer que si n est un multiple de 5, alors $3^n - 1 \equiv 0$ (modulo11).
   Quelle information peut-on en déduire sur l'apparition du message d'avertissement ?

2013 Polynésie

Exercice 1 **5 points**

Un professeur de BTS SIO souhaite sélectionner un langage de programmation.
Pour cette sélection, il s'impose les critères suivants : le langage doit :

— exister depuis plus de 3 ans et être utilisé en entreprise, ou
— ne pas exister depuis plus de 3 ans et être gratuit, ou
— être gratuit et être utilisé en entreprise.

Pour un langage donné, on définit trois variables booléennes a, b et c de la manière suivante :

— $a = 1$ si le langage existe depuis plus de 3 ans, et $a = 0$ sinon ;
— $b = 1$ si le langage est utilisé en entreprise, et $b = 0$ sinon ;
— $c = 1$ si le langage est gratuit, et $c = 0$ sinon.

1. …crire une expression booléenne E qui traduit les critères de sélection du professeur.
2. Dans cette question seulement, on considère un langage existant depuis plus de 3 ans qui a été sélectionné par le professeur.
   a. Traduire cette sélection par une égalité booléenne.
   b. À l'aide d'un calcul booléen, que peut-on en déduire concernant le langage sélectionné ?
3. À l'aide d'un tableau de Karnaugh, trouver une écriture simplifiée de l'expression booléenne E sous la forme d'une somme de deux termes.
4. Un langage de programmation payant a été écarté par le professeur car il ne correspondait pas à ses critères de sélection. Que peut-on en déduire ?

Exercice 2 **7 points**

Une société de services techniques en informatique doit mettre en place un réseau interne de 50 ordinateurs pour une entreprise. Les tâches nécessaires à la réalisation de ce projet ont été reproduites dans le tableau suivant.

Description de la tâche	Abréviation	T,ches antérieures	Durée (en jours)
Identification des besoins matériels/logiciels et commandes	COM		1
Acheminement/Livraison des OS/logiciels	LOG	COM	3
Achat du matériel pour les UC + C,bles réseau	MAT	COM	1
Acheminement/Livraison des écrans	ECR	COM	6
Assemblage des UC	ASS	MAT	1,5
Installation des OS/logiciels	INST	LOG, ASS	2
Pose des c,bles réseau dans l'entreprise	CABL	MAT	4
Mise en place des postes dans l'entreprise	POST	INST,ECR	1
Configuration du réseau interne	CONF	POST,CABL	1

On considère le graphe orienté de sommets COM, LOG, MAT, ECR, ASS, INST, CABL, POST, CONF correspondant aux conditions d'antériorités données par le tableau précédent.

1. **a.** Quels sont les prédécesseurs du sommet POST ?
   b. Quels sont les successeurs du sommet COM ?
2. Déterminer le niveau de chacun des sommets du graphe en expliquant la méthode utilisée.
3. Construire le graphe d'ordonnancement du projet (selon la méthode MPM ou PERT) et établir les dates au plus tôt et au plus tard de chaque tâche.
4. Déterminer le chemin critique et la durée de réalisation du projet.
5. **a.** Calculer la marge totale de la tâche ASS. À quoi correspond-elle ?
   b. Calculer la marge libre de la tâche ASS. À quoi correspond-elle ?

Exercice 3 **8 points**

Le but de cet exercice est l'étude d'un procédé de cryptage des lettres majuscules de l'alphabet français. Chacune des 26 lettres est associée à l'un des entiers de 0 à 25, selon le tableau de correspondance suivant.

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Le cryptage se fait à l'aide d'une clé, qui est un nombre entier k fixé, compris entre 0 et 25.

Pour crypter une lettre donnée :

— on repère le nombre x associé à la lettre, dans le tableau de correspondance précédent ;
— on multiplie ce nombre x par la clé k ;
— on détermine le reste r de la division euclidienne de $k \times x$ par 26 ;
— on repère la lettre associée au nombre r dans le tableau de correspondance ; c'est la lettre cryptée.

Par exemple, pour crypter la lettre « P » avec la clé $k = 11$:

— le nombre x associé à la lettre « P » est le nombre 15 ;
— on multiplie 15 par la clé k, ce qui donne $11 \times 15 = 165$;
— on détermine le reste de 165 dans la division par 26 : on trouve 9 ;
— on repère enfin la lettre associée à 9 dans le tableau : c'est « J ».

Ainsi, avec la clé $k = 11$, la lettre « P » est cryptée en la lettre « J ».
On crypte un mot en cryptant chacune des lettres de ce mot.

Partie A - Cryptage d'un mot avec la clé $k = 11$

Dans cette partie, la clé de cryptage est $k = 11$. Le but de cette partie est de crypter le mot « BTS ».

1. Déterminer en quelle lettre est cryptée la lettre « S ». On détaillera les différentes étapes du processus de cryptage.
2. Crypter le mot « BTS ». On ne demande pas le détail du cryptage.

Partie B - Décryptage avec la clé $k = 11$

Dans cette partie, la clé de cryptage est toujours $k = 11$.
Le but de cette partie est de retrouver une lettre initiale connaissant la lettre cryptée.

1. Prouver que $19 \times 11 \equiv 1 \quad \text{modulo } 26$.
2. Une lettre associée à un nombre x a été cryptée. Le nombre associé à la lettre cryptée est noté y.
   a. Justifier que $11 \times x \equiv y \quad \text{modulo } 26$.
   b. Montrer que $19 \times y \equiv x \text{modulo } 26$.

   Ces propriétés montrent que pour décrypter une lettre codée y avec la clé $k = 11$, il suffit de crypter cette lettre avec la clé de cryptage $k' = 19$.
   Exemple : si une lettre est codée par $y = 22$, on multiplie 22 par 19 et on prend le reste du résultat dans la division euclidienne par 26 ; on obtient $x = 2$. Donc la lettre de départ est C.
3. Utiliser les résultats précédents pour décrypter le mot « WGA ».

Partie C - Recherche des bonnes clés de cryptage

Une clé k ne possède pas forcément une clé de décryptage associée.
On dit qu'une clé est une bonne clé de cryptage si elle possède une clé de décryptage associée.
On admet qu'une clé k est une bonne clé de cryptage si et seulement si les nombres k et 26 sont premiers entre eux.
Le but de cette partie est de trouver les bonnes clés de cryptage, parmi les nombres entiers compris entre 0 et 25.

1. Décomposer 26 en un produit de facteurs premiers.
2. En déduire la liste des nombres k compris entre 0 et 25 qui sont de bonnes clés de cryptage.