BTS BLANC

Services **I**nformatiques aux **O**rganisations

Épreuve obligatoire

MATHÉMATIQUES

Durée de l'épreuve : **2 heures**

L'usage de la calculatrice avec mode examen actif est autorisé.

Dès que ce sujet vous est remis, assurez-vous qu'il est complet.
Ce sujet comporte 4 pages numérotées de 1/4 à 4/4.

Le candidat traite les 4 exercices proposés.

Le candidat est invité à faire figurer sur la copie toute trace de recherche, même incomplète ou non fructueuse, qu'il aura développée.

La qualité de la rédaction, la clarté et la précision des raisonnements seront prises en compte dans l'appréciation de la copie. Les traces de recherche, même incomplètes ou infructueuses, seront valorisées.

EXERCICE 1 (9 points)

Répondre aux questions suivantes en **justifiant les réponses**.

1. Le nombre 101 est-il un nombre premier ?
2. Soit f l'application de l'ensemble $E = \{0;1;2;3;4;5\}$ définie de la façon suivante :

   - $f(x)$ est le reste dans la division euclidienne de x^2 par 6

   Par exemple, $f(3) = 3$, car $3^2 = 9 = 6 \times 1 + \mathbf{3}$.

   L'affirmation suivante est-elle vraie ?

   « L'application f est injective et non surjective. »

3. Quelle est la **contraposée** de l'affirmation suivante ?

   « Si la télévision est allumée alors quelqu'un la regarde »

4. Quel est le PGCD des nombres 225 et 415 ?
5. Quelle est l'écriture de 2026 (nombre décimal) en base 16 ?
6. On considère la relation binaire $\mathscr{R}$ définie sur $\mathbb{R}$ par :

   $$x \mathscr{R} y \iff \left(xy \leqslant 0 \wedge x \neq y\right)$$

   3 est-il en relation avec -4 ?
7. Comment s'écrit le nombre décimal 13,375 en binaire à virgule ?
8. Quelle est la valeur décimale du plus petit nombre héxadécimal à 4 chiffres sans 0 que l'on peut écrire ?
9. Soient $E = \{1;2\}$ et $F = \{2;3;4\}$. Quel est le cardinal de l'ensemble $E \times F$?

EXERCICE 2 (4 points)

Un nombre entier est dit **parfait** si la somme de ses diviseurs est égale au double de ce nombre.
Par exemple, les diviseurs de 6 sont $\{1,2,3,6\}$ et leur somme est égale à $1+2+3+6=12=2\times 6$, ce qui prouve que 6 est un nombre parfait.

1. Montrer que 28 est un nombre parfait.
2. Montrer que 15 n'est pas un nombre parfait.
3. Dans le livre IX de ses *Éléments*, Euclide, au IIIe siècle av. J.-C., a démontré que si le nombre $M=2^p-1$ est un nombre premier, alors $\dfrac{M(M+1)}{2}$ est un nombre parfait.
   a) Que vaut M si $p=3$? si $p=5$?
   b) Déterminer deux nombres parfaits autres que 6 et 28.

EXERCICE 3 (4 points)

Un professeur de lycée souhaite aménager une salle de cours en salle vidéo pour l'option cinéma. Le gestionnaire du lycée considère que le projet est envisageable lorsqu'il satisfait à l'une au moins des conditions suivantes :

- Le matériel vidéo est acheté dans un magasin local et est de fabrication française ;
- Le matériel vidéo n'est pas de fabrication française et il coûte moins de 500 euros ;
- Le matériel vidéo n'a pas été acheté dans un magasin local, est de fabrication française et a coûté moins de 500 euros.

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

- a le matériel vidéo coûte moins de 500 euros et $\overline{\text{a}}$ le matériel vidéo coute 500 euros ou plus ;
- b le matériel vidéo est acheté dans un magasin local et $\overline{\text{b}}$ le matériel vidéo n'est pas acheté dans un magasin local.
- c le matériel vidéo est de fabrication française et $\overline{\text{c}}$ le matériel vidéo n'est pas de fabri- cation française.

1. Écrire une expression booléenne E traduisant que le projet est envisageable, à l'aide des variables booléennes a, b, c.
2. **a)** À l'aide d'un tableau de Karnaugh, déterminer une écriture simplifiée de E à deux termes.
   b) En déduire une interprétation simplifiée des conditions pour que le projet soit envisageable.
3. Dans le projet présenté, le matériel vidéo coûte plus de 500 euros, n'est pas de fabrication française mais sera acheté localement.

   Ce projet est-il envisageable ?

EXERCICE 4 (3 points)

Le **protocole de Diffie-Hellman** est une méthode cryptographique permettant à deux parties (souvent appelées Alice et Bob) de **partager une clé secrète à travers un canal de communication non sécurisé**. Le fonctionnement est le suivant :

- Alice et Bob choisissent ensemble un nombre premier p et un entier g inférieur à p
- Ils choisissent chacun une **clé privée secrète** : a pour Alice et b pour Bob
- Ils calculent chacun leur **clé publique** :
  - pour Alice, c'est l'entier A tel que $g^a \equiv A[p]$ (autrement dit, A est le reste dans la division euclidienne de g^a par p)
  - pour Bob, c'est l'entier B tel que $g^b \equiv B[p]$
- Alice et Bob peuvent alors calculer la **clé secrète** K :
  - pour Alice, K est l'entier tel que $B^a \equiv K[p]$
  - pour Bob, K est l'entier tel que $A^b \equiv K[p]$

Avec ce procédé, même si un attaquant voit g, p, A et B, il ne peut pas facilement trouver la clé secrète sans connaître a et b. Pour l'exercice, on considère les paramètres suivants :

$$p = 2207 \qquad g = 47 \qquad a = 10 \qquad b = 16$$

1. Justifier que $47^2 \equiv 2[2207]$. En déduire que $A = 32$.

2. Calculer la valeur de B.

3. Déterminer alors la clé secrète commune K.