

**CORRECTION** – Barème sur 22 points

**Exercice 1** (6 points) - Estimation 30'

1. 0,5pt  $Card(E \times E) = 8 \times 8 = 64$  soit 64 couples possibles.

2. 1,5pt Vérifions que  $\mathcal{R}$  est réflexive, symétrique et transitive.

• Soit  $(x_1, y_1) \in E \times E$ .  $(x_1, y_1)\mathcal{R}(x_1, y_1) \Leftrightarrow \begin{cases} x_1 - x_1 \text{ est pair} \\ y_1 - y_1 \text{ est divisible par 3} \end{cases}$  ce qui est vrai.

• Soient  $(x_1, y_1), (x_2, y_2) \in E \times E$ .

$(x_1, y_1)\mathcal{R}(x_2, y_2) \Leftrightarrow \begin{cases} x_1 - x_2 \text{ est pair,} \\ y_1 - y_2 \text{ est divisible par 3} \end{cases} \Leftrightarrow \begin{cases} x_2 - x_1 \text{ est pair,} \\ y_2 - y_1 \text{ est divisible par 3} \end{cases}$ .

Par conséquent,  $(x_2, y_2)\mathcal{R}(x_1, y_1)$ .

• Soient  $(x_1, y_1), (x_2, y_2), (x_3, y_3) \in E \times E$ .

$\begin{cases} (x_1, y_1)\mathcal{R}(x_2, y_2) \\ (x_2, y_2)\mathcal{R}(x_3, y_3) \end{cases} \Rightarrow \begin{cases} x_1 - x_2 \text{ est pair} \\ y_1 - y_2 \text{ est divisible par 3} \\ x_2 - x_3 \text{ est pair} \\ y_2 - y_3 \text{ est divisible par 3} \end{cases} \Rightarrow \begin{cases} x_1 - x_3 \text{ est pair} \\ y_1 - y_3 \text{ est divisible par 3} \end{cases}$

En effet, la somme de deux nombres pairs est un nombre pair et, si deux nombres sont divisibles par 3, leur somme l'est également. Donc  $(x_1, y_1)\mathcal{R}(x_3, y_3)$ .

Conclusion,  $\mathcal{R}$  est une relation d'équivalence.

3. (a) 1pt  $p - p_0$  est pair si et seulement si  $p$  et  $p_0$  sont pairs ou  $p$  et  $p_0$  sont impairs.  $q - q_0$  est divisible par 3 si et seulement si  $q$  et  $q_0$  sont congrus modulo 3. On dénombre donc  $2 \times 3 = 6$  classes d'équivalence, soit  $\overline{(1, 1)}, \overline{(2, 1)}, \overline{(1, 2)}, \overline{(2, 2)}, \overline{(1, 3)}$  et  $\overline{(2, 3)}$ .

(b) 1pt

$\overline{(1, 1)} = \{(1, 1), (3, 1), (5, 1), (7, 1), (1, 4), (3, 4), (5, 4), (7, 4), (1, 7), (3, 7), (5, 7), (7, 7)\}$   
Donc  $Card(\overline{(1, 1)}) = 12$ .

$\overline{(1, 2)} = \{(1, 2), (3, 2), (5, 2), (7, 2), (1, 5), (3, 5), (5, 5), (7, 5), (1, 8), (3, 8), (5, 8), (7, 8)\}$   
Donc  $Card(\overline{(1, 2)}) = 12$ .

$\overline{(1, 3)} = \{(1, 3), (3, 3), (5, 3), (7, 3), (1, 6), (3, 6), (5, 6), (7, 6)\}$   
Donc  $Card(\overline{(1, 3)}) = 8$ .

(c) 1pt Montrons que  $\forall q \in E$ ,  $f : \overline{(1, q)} \rightarrow \overline{(2, q)}$  est bijective.

$$(x, y) \mapsto (x + 1, y)$$

Soit  $(a, b) \in \overline{(2, q)}$ . Montrons qu'il existe  $(x, y) \in \overline{(1, q)}$  tel que  $f(x, y) = (a, b)$ . Cette égalité est équivalente à  $(x + 1, y) = (a, b)$  et on en déduit que  $\begin{cases} x = a - 1 \\ y = b \end{cases}$ . Comme  $(a, b) \in \overline{(2, q)}$ ,  $a - 2$  est pair (et  $b - q$  est divisible par 3). Donc  $(x + 1) - 2$  est pair ce qui implique que  $x - 1$  est pair. Cela prouve que  $(x, y) \in \overline{(1, q)}$ ,  $f$  est par conséquent surjective.

Soient  $(x_1, y_1), (x_2, y_2) \in \overline{(1, q)}$ .  $f(x_1, y_1) = f(x_2, y_2) \Rightarrow (x_1 + 1, y_1) = (x_2 + 1, y_2) \Rightarrow (x_1, y_1) = (x_2, y_2)$ . On a démontré l'injectivité de  $f$ .

4. 1pt On utilise le caractère bijectif de  $f$  et on démontre simplement que  $Card(\overline{(2, 1)}) = Card(\overline{(1, 1)}) = 12$ ,  $Card(\overline{(2, 2)}) = Card(\overline{(1, 2)}) = 12$  et  $Card(\overline{(2, 3)}) = Card(\overline{(1, 3)}) = 8$ .

On note enfin que  $Card(E \times E) = \sum_{i=1}^2 \sum_{j=1}^3 Card(\overline{(i, j)}) = 64$ .

**Exercice 2** (2 points) - Estimation 15'

1. 1,5pt Montrons que  $\Theta$  est une relation d'ordre.

- Soit  $x \in \mathbb{N}^*$ . On a  $x = x^1$  ce qui est équivalent, d'après la définition de  $\Theta$ , à  $x\Theta x$ .  $\Theta$  est réflexive.
- Soient  $x, y \in \mathbb{N}^*$ ,  $x\Theta y \Leftrightarrow \exists n \in \mathbb{N}^*, y = x^n$ . De même,  $y\Theta x \Leftrightarrow \exists m \in \mathbb{N}^*, x = y^m$ . Par conséquent,  $\begin{cases} x\Theta y \\ y\Theta x \end{cases} \Rightarrow \exists n, m \in \mathbb{N}^*, \begin{cases} y = x^n \\ x = y^m \end{cases} \Rightarrow y = (y^m)^n = y^{mn} \Rightarrow mn = 1$ . Or  $m, n \in \mathbb{N}^*$  donc  $m = n = 1$ . Ainsi,  $x = y$  et  $\Theta$  est antisymétrique.
- Soient  $x, y, z \in \mathbb{N}^*$ ,  $\begin{cases} x\Theta y \\ y\Theta z \end{cases} \Leftrightarrow \exists n, m \in \mathbb{N}^*, \begin{cases} y = x^n \\ z = y^m \end{cases} \Leftrightarrow z = (x^n)^m = x^{mn} = x^N$  où  $N = mn \in \mathbb{N}^*$ . On en déduit que  $x\Theta z$  et que  $\Theta$  est donc transitive.

Conclusion,  $\Theta$  est une relation d'ordre sur  $\mathbb{N}^*$ .

2. 0,5pt L'ordre n'est pas total, il suffit pour s'en convaincre de considérer l'exemple (le contre-exemple) suivant : on n'a ni  $2\Theta 3$  ni  $3\Theta 2$ .

**Exercice 3** (4 points) - Estimation 30'

1. 2,5pts Montrons que  $(\mathcal{F}(E, A), \oplus, \otimes)$  est un groupe abélien.

- Soient  $f, g \in \mathcal{F}(E, A)$ . Soit  $x \in E$  alors  $(f \oplus g)(x) = f(x) + g(x)$  par définition.  $(A, +, \times)$  est un anneau donc « + » est une loi interne pour  $A$ , ce qui signifie que la somme deux éléments de  $A$  est encore dans  $A$ . En conséquence, comme  $f(x) \in A$  et  $g(x) \in A$ ,  $(f \oplus g)(x) \in A$  ce qui induit que  $f \oplus g \in \mathcal{F}(E, A)$ . La loi  $\oplus$  est interne.
- Existe t-il un élément neutre  $e \in \mathcal{F}(E, A)$  pour  $\oplus$ , c'est-à-dire tel que,  $\forall f \in \mathcal{F}(E, A)$ ,  $f \oplus e = e \oplus f = f$  ou encore tel que  $\forall x \in E$ ,  $(f \oplus e)(x) = (e \oplus f)(x) = f(x)$ ?  
 $(f \oplus e)(x) = f(x) \Leftrightarrow f(x) + e(x) = f(x) \Leftrightarrow e(x) = 0$  car  $(A, +, \times)$  est un anneau (on utilise l'élément neutre pour l'addition). On en déduit que  $e$  est l'application de  $E$  dans  $A$  identiquement nulle. On montre aisément que cet élément neutre à droite pour  $\oplus$  l'est aussi à gauche.
- Soient  $f, g, h \in \mathcal{F}(E, A)$ .  $\forall x \in E$ ,  $((f \oplus g) \oplus h)(x) = (f \oplus g)(x) + h(x) = (f(x) + g(x)) + h(x) = f(x) + g(x) + h(x)$  car  $(A, +, \times)$  est un anneau (on utilise l'associativité de « + »). On montre de la même manière que cette quantité est égale à  $(f \oplus (g \oplus h))(x)$ .  $\oplus$  est une loi associative dans  $\mathcal{F}(E, A)$ .
- Existe t-il un élément symétrique  $f^{-1} \in \mathcal{F}(E, A)$  de  $f \in \mathcal{F}(E, A)$  pour  $\oplus$ , c'est-à-dire tel que,  $\forall f \in \mathcal{F}(E, A)$ ,  $f \oplus f^{-1} = f^{-1} \oplus f = 0$  ou encore tel que  $\forall x \in E$ ,  $(f \oplus f^{-1})(x) = (f^{-1} \oplus f)(x) = 0$ ? (on ne confondra pas ici  $f = 0$  et  $f(x) = 0$ ).  
 $(f \oplus f^{-1})(x) = 0 \Leftrightarrow f(x) + f^{-1}(x) = 0 \Leftrightarrow f^{-1}(x) = -f(x)$  car  $(A, +, \times)$  est un anneau (on utilise le symétrique de  $f(x) \in A$  pour l'addition). On en déduit que  $f^{-1}$  est l'application de  $E$  dans  $A$  égale à  $-f$ . On montre aisément que ce symétrique à droite pour  $\oplus$  l'est aussi à gauche.
- Soient  $f, g \in \mathcal{F}(E, A)$ . Soit  $x \in E$  alors  $(f \oplus g)(x) = f(x) + g(x) = g(x) + f(x)$  car  $(A, +, \times)$  est un anneau (on utilise la commutativité de l'addition). Or  $g(x) + f(x) = (g \oplus f)(x)$ , on en déduit que  $\oplus$  est une loi commutative.

2. 1,5pt Il reste à montrer que la loi  $\otimes$  est associative et distributive par rapport à la loi  $\oplus$ .

- Soient  $f, g, h \in \mathcal{F}(E, A)$ .  $\forall x \in E$ ,  $((f \otimes g) \otimes h)(x) = (f \otimes g)(x) \times h(x) = (f(x) \times g(x)) \times h(x) = f(x) \times g(x) \times h(x)$  car  $(A, +, \times)$  est un anneau (on utilise l'associativité de «  $\times$  »). On montre de la même manière que cette quantité est égale à  $(f \otimes (g \otimes h))(x)$ .  $\otimes$  est une loi associative dans  $\mathcal{F}(E, A)$ .
- Soient  $f, g, h \in \mathcal{F}(E, A)$ .  $\forall x \in E$ ,  $(f \otimes (g \oplus h))(x) = f(x) \times (g \oplus h)(x) = f(x) \times (g(x) + h(x)) = f(x) \times g(x) + f(x) \times h(x)$  car  $(A, +, \times)$  est un anneau (on utilise la distributivité de «  $\times$  » par rapport à « + »). Cette quantité est elle-même égale à  $(f \otimes g)(x) + (f \otimes h)(x) = (f \otimes g \oplus f \otimes h)(x)$ . On montre de manière similaire la distributivité à droite.

**Exercice 4** (4 points) - Estimation 15'

1. 1pt On désigne par  $\mathbb{Z}/n\mathbb{Z}$  l'ensemble des classes d'équivalences de la relation de congruence modulo  $n$ .

Soient  $\bar{x}, \bar{y} \in \mathbb{Z}/n\mathbb{Z}$  alors

- $\bar{x} + \bar{y} = \overline{x+y}$ ,
- $\bar{x} \times \bar{y} = \overline{x \times y}$ .

2. 1pt

| $\bar{+}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ |
|-----------|-----------|-----------|-----------|-----------|
| $\bar{0}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ |
| $\bar{1}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ | $\bar{0}$ |
| $\bar{2}$ | $\bar{2}$ | $\bar{3}$ | $\bar{0}$ | $\bar{1}$ |
| $\bar{3}$ | $\bar{3}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ |

3. 1pt

| $\bar{\times}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ |
|----------------|-----------|-----------|-----------|-----------|
| $\bar{0}$      | $\bar{0}$ | $\bar{0}$ | $\bar{0}$ | $\bar{0}$ |
| $\bar{1}$      | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ |
| $\bar{2}$      | $\bar{0}$ | $\bar{2}$ | $\bar{0}$ | $\bar{2}$ |
| $\bar{3}$      | $\bar{0}$ | $\bar{3}$ | $\bar{2}$ | $\bar{1}$ |

4. 1pt On a vu en cours que  $\mathbb{Z}/n\mathbb{Z}$  est un corps (fini) si et seulement si  $n$  est un nombre premier. Ici  $n = 4$  donc  $\mathbb{Z}/4\mathbb{Z}$  n'est pas un corps.  $\mathbb{Z}/n\mathbb{Z}$  est un anneau mais certains éléments non nuls dans cet anneau n'admettent pas de symétrique pour la multiplication, ce qui s'observe grâce à la table de la question précédente, avec la classe  $\bar{2}$ . En effet, il n'existe pas de classe  $\bar{a} \in \mathbb{Z}/4\mathbb{Z}$  telle que  $\bar{2} \times \bar{a} = \bar{a} \times \bar{2} = \bar{1}$ .

**Exercice 5** (6 points) - Estimation 30'

• Partie A

1. 0,5pt  $11 \times (-7) - 26 \times (-3) = -77 + 78 = 1$ , donc le couple  $(-7; -3)$  est solution de  $(E)$ .
2. 1,5pt Soit  $(x; y)$  une solution de  $(E)$ , on a alors  $11x - 26y = 1$  et d'après la question précédente  $11 \times (-7) - 26 \times (-3) = 1$  donc  $11x - 26y = 11 \times (-7) - 26 \times (-3)$ . On en déduit que  $11(x+7) = 26(y+3)$ . Ainsi 26 divise  $11(x+7)$ , or 26 et 11 sont premiers entre eux, le théorème de Gauss implique donc que 26 divise  $x+7$ . Il existe donc un entier relatif  $k$  tel que  $x+7 = 26k$ , c'est-à-dire  $x = -7 + 26k$ . On a alors  $11 \times 26k = 26(y+3)$ , d'où, en divisant par 26 :  $11k = y+3$ , d'où  $y = -3 + 11k$ . Ainsi, si  $(x; y)$  est solution de  $(E)$ , il existe un entier  $k$  tel que  $(x; y) = (-7 + 26k; -3 + 11k)$ .

Réiproquement, on vérifie que ces couples sont bien solutions de  $(E)$  ; en effet

$$11 \times (-7 + 26k) - 26 \times (-3 + 11k) = -77 + 286k + 78 - 286k = 1.$$

En conclusion, les solutions de  $(E)$  sont les couples de la forme  $(-7 + 26k; -3 + 11k)$  où  $k \in \mathbb{Z}$ .

3. 1pt  $(u; v)$  est solution de  $(E)$  avec  $0 \leq u \leq 25$  si et seulement s'il existe un entier relatif  $k$  tel que  $u = -7 + 26k$ ,  $v = -3 + 11k$  et  $0 \leq -7 + 26k \leq 25$ . Cela conduit à  $7 \leq 26k \leq 32$ , et  $k = 1$  est la seule possibilité. L'unique couple répondant à la question est donc  $(19; 8)$ .

• Partie B

4. 0,5pt La lettre  $W$  est chiffrée par  $x = 22$ . Or  $11 \times 22 + 8 = 16$  (modulo 26), donc  $y = 16$ , ce qui correspond à la lettre  $Q$ .

5. (a) 1pt Soient  $x$  et  $j$  deux entiers relatifs tels que  $11x = j$  (modulo 26). Alors, en multipliant par 19, on obtient  $19 \times 11x = 19j$  (modulo 26). Or  $19 \times 11 = 209$  et  $209 \equiv 1$  (modulo 26), donc  $x \equiv 19j$  (modulo 26).

Réiproquement, si  $x \equiv 19j$  (modulo 26), alors, en multipliant par 11, on obtient  $11 = 11 \times 19j$  (modulo 26), d'où  $11x \equiv j$  (modulo 26). L'équivalence est donc démontrée.

- (b) 1pt Soit  $y$  un entier compris entre 0 et 25, il s'agit de trouver un entier  $x$  compris entre 0 et 25 tel que :  $11x + 8 \equiv y \pmod{26}$ . Nécessairement on doit avoir :  $11x \equiv y - 8 \pmod{26}$ , ce qui équivaut, d'après la question précédente, à  $x \equiv 19(y - 8) \pmod{26}$ . Le procédé de décodage est donc le suivant :
- on chiffre la lettre à décoder par un nombre entier  $y$  compris entre 0 et 25 ;
  - on calcule le reste  $x$  de la division euclidienne de  $19(y - 8)$  par 26 ;
  - on déchiffre alors pour obtenir la lettre décodée.
- (c) 0,5pt  $W$  est chiffré par  $y = 22$ . Or  $19 \times (22 - 8) \equiv 6 \pmod{26}$ , donc  $x = 6$ , ce qui correspond à la lettre G.