

## Problème 1 : matrices d'ordre fini

### Partie A : préliminaires

1.

1.1.  $P$  est nécessairement de degré supérieur ou égal à 1.

i) On sait que  $A$  est trigonalisable dans  $\mathcal{M}_n(\mathbb{R})$  si et seulement si  $P$  est scindé sur  $\mathbb{R}$ .

ii) On sait que si  $P$  est scindé sur  $\mathbb{R}$  à racines simples, alors  $A$  est diagonalisable dans  $\mathcal{M}_n(\mathbb{R})$ .

1.2. D'après le théorème de d'ALEMBERT-GAUSS, tout élément de  $\mathbb{C}[X]$  de degré supérieur ou égal à 1 est scindé sur  $\mathbb{C}$ . En conséquence,  $A$  est toujours trigonalisable.

D'autre part, la condition suffisante de diagonalisabilité s'écrit plus simplement : si  $P$  est à racines simples dans  $\mathbb{C}$ .

2.

2.1. Par hypothèse,  $B^b = I_n$  avec  $b \in \mathbb{N}^*$ . Par suite,  $B \times B^{b-1} = B^{b-1} \times B = I_n$ . On en déduit que  $B$  est inversible et que  $B^{-1} = B^{b-1}$ .

2.2. Soit  $k \in \mathbb{Z}$ .  $b$  est un entier naturel non nul. La division euclidienne de  $k$  par  $b$  s'écrit  $k = bq + r$  où  $q$  et  $r$  sont des entiers relatifs tels que  $0 \leq r \leq b - 1$ .

$$\begin{aligned} B^k = I_n &\Leftrightarrow B^{qb+r} = I_n \Leftrightarrow (B^b)^q \times B^r = I_n \Leftrightarrow (I_n)^q \times B^r = I_n \\ &\Leftrightarrow B^r = I_n. \end{aligned}$$

Maintenant,  $r$  est élément de  $\llbracket 0, b - 1 \rrbracket$  et par définition de  $b$ , il existe un et un seul entier  $p$  élément de  $\llbracket 0, b - 1 \rrbracket$  tel que  $B^p = I_n$  à savoir  $p = 0$ . Donc

$$B^k = I_n \Leftrightarrow B^r = I_n \Leftrightarrow r = 0 \Leftrightarrow b \text{ divise } k.$$

2.3. On sait que les valeurs propres dans  $\mathbb{C}$  d'une matrice sont à choisir parmi les racines d'un polynôme annulateur. Puisque  $B^b = I_n$ , le polynôme  $P = X^b - 1$  est annulateur de  $B$ . Les racines de  $P$  sont les racines  $b$ -èmes de l'unité dans  $\mathbb{C}$  et donc les valeurs propres de  $B$  sont des racines  $b$ -èmes de l'unité dans  $\mathbb{C}$ .

2.4.  $P' = bX^{b-1}$ .  $P'$  a une seule racine dans  $\mathbb{C}$  à savoir 0. 0 n'est pas racine de  $P$  et donc  $P$  et  $P'$  n'ont pas de racine commune dans  $\mathbb{C}$ . On sait alors que  $P$  est à racines simples dans  $\mathbb{C}$ .

Ainsi, le polynôme  $P$  est à racines simples dans  $\mathbb{C}$  et annulateur de  $B$ . On en déduit que  $B$  est diagonalisable dans  $\mathbb{C}$ .

3. Posons  $m = \text{PPCM}(k_1, \dots, k_n)$ .  $m$  est un entier naturel non nul. De plus, pour chaque  $i \in \llbracket 1, n \rrbracket$ ,  $m$  est multiple de  $k_i$  et donc  $\lambda_i^m = 1$ .

3.1.  $C$  est diagonalisable. Donc il existe  $P \in \text{GL}_n(\mathbb{C})$  telle que  $C = PDP^{-1}$  avec  $D = \text{diag}(\lambda_i)_{1 \leq i \leq n}$ .

$$C^m = (PDP^{-1})^m = PD^m P^{-1} = P \text{diag}(\lambda_i^m)_{1 \leq i \leq n} P^{-1} = P \times I_n \times P^{-1} = I_n.$$

Donc,  $C$  est d'ordre fini. De plus, d'après la question 2)b),  $o(C)$  divise  $m$ .

3.2. Plus précisément, pour  $k \in \mathbb{Z}$ ,

$$\begin{aligned}
C^k = I_n &\Leftrightarrow (PDP^{-1})^k = I_n \Leftrightarrow PD^kP^{-1} = I_n \\
&\Leftrightarrow D^k = I_n \text{ (P et } P^{-1} \text{ sont inversibles et donc simplifiables)} \\
&\Leftrightarrow \text{diag}(\lambda_i^k)_{1 \leq i \leq n} = I_n \Leftrightarrow \forall i \in \llbracket 1, n \rrbracket, \lambda_i^k = 1 \\
&\Leftrightarrow \forall i \in \llbracket 1, n \rrbracket, k \text{ est multiple de } k_i \\
&\Leftrightarrow k \text{ est multiple de } m \Leftrightarrow k \in m\mathbb{Z}.
\end{aligned}$$

Par suite, l'ordre de  $C$  est le plus petit élément strictement positif de  $m\mathbb{Z}$  et donc  $o(C) = m$ .

## Partie B : matrices d'ordre fini à coefficients réels

1. Puisque  $A$  est d'ordre fini, d'après la question 2)b) de la partie A, les valeurs propres de  $A$  sont des racines de l'unité et en particulier, les valeurs propres de  $A$  sont de module égal à 1. Si de plus, toute valeur propre de  $A$  dans  $\mathbb{C}$  est réelle, une telle valeur propre est nécessairement égale à 1 ou  $-1$ . Donc,  $\text{Sp}(A) \subset \{-1, 1\}$ .

2.

2.1. Par hypothèse, le polynôme caractéristique de  $A$  est  $\chi_A = (1-X)^3$ . Il est scindé sur  $\mathbb{R}$  et donc  $A$  est trigonalisable dans  $\mathcal{M}_3(\mathbb{R})$ . Donc, il existe une matrice  $P$  inversible à coefficients réels et une matrice triangulaire supérieure  $B$  à coefficients réels telle que  $P^{-1}AP = B$ . On sait que  $A$  et  $B$  ont même polynôme caractéristique et que les valeurs propres de  $B$  sont les coefficients diagonaux de  $B$ . Donc  $B$  est de la forme

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

En résumé, il existe  $P \in \text{GL}_3(\mathbb{R})$  et  $(a, b, c) \in \mathbb{R}^3$  tels que  $P^{-1}AP = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$ .

2.2. Soit  $k \in \mathbb{Z}$ .  $B^k = (P^{-1}AP)^k = P^{-1}A^kP$ . Donc

$$B^k = I_n \Leftrightarrow P^{-1}A^kP = I_n \Leftrightarrow A^k = I_n.$$

En particulier,  $B$  est d'ordre fini et  $o(B) = o(A)$ .

2.3. Montrons par récurrence que :  $\forall k \in \mathbb{N}$ ,  $B^k = \begin{pmatrix} 1 & ka & \frac{k(k-1)}{2}ac + kb \\ 0 & 1 & kc \\ 0 & 0 & 1 \end{pmatrix}$ .

• Si  $k = 0$ ,  $\begin{pmatrix} 1 & ka & \frac{k(k-1)}{2}ac + kb \\ 0 & 1 & kc \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = I_3 = B^0$ . La formule est donc vraie quand  $k = 0$ .

• Soit  $k \geq 0$ . Supposons que  $B^k = \begin{pmatrix} 1 & ka & \frac{k(k-1)}{2}ac + kb \\ 0 & 1 & kc \\ 0 & 0 & 1 \end{pmatrix}$ .

$$\begin{aligned}
B^{k+1} = B^k \times B &= \begin{pmatrix} 1 & ka & \frac{k(k-1)}{2}ac + kb \\ 0 & 1 & kc \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a + ka & b + kac + \frac{k(k-1)}{2}ac + kb \\ 0 & 1 & c + kc \\ 0 & 0 & 1 \end{pmatrix} \\
&= \begin{pmatrix} 1 & (k+1)a & \frac{k(k-1+2)}{2}ac + (k+1)b \\ 0 & 1 & (k+1)c \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & (k+1)a & \frac{(k+1)((k+1)-1)}{2}ac + (k+1)b \\ 0 & 1 & (k+1)c \\ 0 & 0 & 1 \end{pmatrix}.
\end{aligned}$$

On a montré par récurrence que  $\forall k \in \mathbb{N}$ ,  $B^k = \begin{pmatrix} 1 & ka & \frac{k(k-1)}{2}ac + kb \\ 0 & 1 & kc \\ 0 & 0 & 1 \end{pmatrix}$ .

**2.4.** Il existe  $k \in \mathbb{N}^*$  tel que  $B^k = I_n$ . Pour cet entier  $k$ , on a  $ka = kc = \frac{k(k-1)}{2}ac + kb = 0$  et donc  $a = b = c = 0$  puisque  $k$  n'est pas nul. On en déduit que  $B = I_3$  puis que  $A = PI_3P^{-1} = I_3$ .

**3.** Si  $A$  admet  $-1$  pour valeur propre triple, alors  $-A$  admet  $1$  pour valeur propre triple. De plus,  $-A$  est d'ordre fini car si pour un entier non nul  $k$ , on a  $A^k = I_3$ , alors  $(-A)^{2k} = +(A^k)^2 = I_3$ . D'après la question précédente, on a nécessairement  $-A = I_3$  ou encore  $A = -I_3$ .

Réciproquement, la matrice  $-I_3$  est d'ordre fini égal à 2.

**4.**

**4.1.** De nouveau, le polynôme caractéristique de  $A$  est scindé sur  $\mathbb{R}$  et donc  $A$  est trigonalisable dans  $\mathbb{R}$ , les valeurs propres de  $A$  se retrouvant sur la diagonale de la matrice triangulaire supérieure avec le même ordre de multiplicité. Donc, il existe

$$Q \in GL_3(\mathbb{R}) \text{ et trois réels } a, b \text{ et } c \text{ tels que la matrice } Q^{-1}AQ = \begin{pmatrix} -1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}.$$

**4.2.** Montrons par récurrence que pour tout  $k \in \mathbb{N}$ , il existe trois réels  $\alpha_k, \beta_k$  et  $\gamma_k$  tels que

$$C^k = \begin{pmatrix} (-1)^k & \alpha_k & \beta_k \\ 0 & 1 & \gamma_k \\ 0 & 0 & 1 \end{pmatrix}.$$

• Le résultat est vrai pour  $k = 0$  avec  $\alpha_0 = \beta_0 = \gamma_0 = 0$ .

• Soit  $k \geq 0$ . Supposons qu'il existe trois réels  $\alpha_k, \beta_k$  et  $\gamma_k$  tels que  $C^k = \begin{pmatrix} (-1)^k & \alpha_k & \beta_k \\ 0 & 1 & \gamma_k \\ 0 & 0 & 1 \end{pmatrix}$ .

$$\begin{aligned} C^{k+1} &= C^k \times C = \begin{pmatrix} (-1)^k & \alpha_k & \beta_k \\ 0 & 1 & \gamma_k \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} -1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} (-1)^{k+1} & \alpha_k + (-1)^k a & c\alpha_k + \beta_k + (-1)^k b \\ 0 & 1 & \gamma_k + c \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} (-1)^{k+1} & \alpha_{k+1} & \beta_{k+1} \\ 0 & 1 & \gamma_{k+1} \\ 0 & 0 & 1 \end{pmatrix} \end{aligned}$$

avec  $\alpha_{k+1} = \alpha_k + (-1)^k a$ ,  $\beta_{k+1} = c\alpha_k + \beta_k + (-1)^k b$  et  $\gamma_{k+1} = \gamma_k + c$ .

Le résultat est démontré par récurrence.

**4.3.** La suite  $(\gamma_k)_{k \in \mathbb{N}}$  est arithmétique de premier terme  $\gamma_0 = 0$  et de raison  $r = c$ . Donc, pour tout entier naturel  $k$ ,  $\gamma_k = \gamma_0 + kr = kc$ .

**4.4.** Comme à la question 2)d), il existe un entier non nul  $k$  tel que  $kc = 0$  et donc  $c = 0$ .

**4.5.** La dimension du sous-espace propre de  $A$  ou de  $C$  associé à la valeur propre simple  $-1$  est 1. D'autre part,

$$\text{rg}(A - I_3) = \text{rg}(C - I_3) = \text{rg} \begin{pmatrix} -1 & a & b \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} = \text{rg} \begin{pmatrix} -1 & a & b \\ & & \end{pmatrix} = 1.$$

D'après le théorème du rang, la dimension du sous-espace propre  $\text{Ker}(A - I_3)$  ou du sous-espace propre  $\text{Ker}(C - I_3)$  est  $3 - 1 = 2$  qui est l'ordre de multiplicité de la valeur propre 1.

En résumé, le polynôme caractéristique de  $C$  ou de  $A$  est scindé sur  $\mathbb{R}$  et l'ordre de multiplicité de chaque valeur propre est égal à la dimension du sous-espace propre correspondant. On en déduit que  $A$  et  $C$  sont diagonalisables dans  $\mathcal{M}_3(\mathbb{R})$ .

**5.** Si  $-1$  est valeur propre double de  $A$  et  $1$  est valeur propre simple de  $A$ , alors  $-1$  est valeur propre simple de  $-A$  et  $1$  est valeur propre double de  $-A$ .  $-A$  étant d'autre part d'ordre fini, la question précédente permet d'affirmer que  $-A$  est diagonalisable dans  $\mathcal{M}_3(\mathbb{R})$ . Il en est de même de la matrice  $A$  car si  $-A$  est semblable à une matrice diagonale réelle  $D$ ,  $A$  est semblable à la matrice diagonale réelle  $-D$ .

Réciproquement, comme à la question précédente, une telle matrice est d'ordre fini.

**6.**

**6.1.** On a vu à la question 1) que toute valeur propre de  $A$  dans  $\mathbb{C}$  est de module 1. Puisque  $A$  admet une valeur propre non réelle, l'une des valeurs propres de  $A$  est de la forme  $e^{i\theta}$  avec  $\theta \in \mathbb{R} \setminus \pi\mathbb{Z}$ . D'après la question 2)c) de la partie A,  $e^{i\theta}$  est une racine  $b$ -ème de l'unité où  $b = o(A)$ . Donc,  $e^{ib\theta} = 1$  puis  $b\theta \in 2\pi\mathbb{Z}$  puis  $\theta \in \frac{2\pi}{b}\mathbb{Z}$  et en particulier,  $\theta \in 2\pi\mathbb{Q}$ . Finalement, l'une des valeurs propres de  $A$  est de la forme  $e^{i\theta}$  avec  $\theta \in 2\pi\mathbb{Q} \setminus \pi\mathbb{Z}$ .

Puisque  $A$  est à coefficients réels, on sait que puisque  $e^{i\theta}$  est une valeur propre non réelle de  $A$ ,  $\overline{e^{i\theta}} = e^{-i\theta}$  est valeur propre de  $A$  avec le même ordre de multiplicité. Donc,  $A$  admet déjà deux valeurs propres distinctes  $e^{i\theta}$  et  $e^{-i\theta}$ . Notons  $\lambda$  la dernière valeur propre.

La trace de  $A$  est un réel et est égale à  $e^{i\theta} + e^{-i\theta} + \lambda$  ou encore  $2 \cos \theta + \lambda$ . On en déduit que  $\lambda$  est un réel, toujours de module 1 et donc  $\lambda = 1$  ou  $\lambda = -1$ . Finalement,  $\text{Sp}(A) = \{e^{i\theta}, e^{-i\theta}, 1\}$  ou  $\text{Sp}(A) = \{e^{i\theta}, e^{-i\theta}, -1\}$ .

**6.2.** En particulier, le polynôme caractéristique de  $A$  est à racines simples dans  $\mathbb{C}$  et on sait que  $A$  est diagonalisable dans  $\mathcal{M}_3(\mathbb{C})$ .

**7. •** Supposons  $A$  d'ordre fini. D'après la question 1), les trois valeurs propres de  $A$  dans  $\mathbb{C}$  sont de module 1. Puisque  $\chi_A$  est de degré 3 à coefficients réels,  $A$  admet au moins une valeur propre réelle qui ne peut être que 1 ou  $-1$ . Si l'une des deux autres valeurs propres n'est pas réelle, elle est de la forme  $e^{i\theta}$ ,  $\theta \in \mathbb{R} \setminus \pi\mathbb{Z}$  et on a vu que l'autre valeur propre est sa conjuguée  $e^{-i\theta}$ . Sinon, toutes les valeurs propres sont réelles.

Si les trois valeurs propres sont réelles, la famille des valeurs propres de  $A$  est nécessairement  $(1, 1, 1)$  ou  $(-1, 1, 1)$  ou  $(-1, -1, 1)$ . Nous sommes donc dans la situation des questions 2), 3), 4) ou 5). La matrice  $A$  est soit égale à  $I_3$ , soit égale à  $-I_3$ , soit diagonalisable et dans tous les cas diagonalisable. D'autre part, le spectre de  $A$  est bien de la forme  $(e^{i\theta}, e^{-i\theta}, 1)$  ou  $(e^{i\theta}, e^{-i\theta}, -1)$  avec  $\theta = 0$  ou  $\theta = \pi$  de sorte que  $\theta \in 2\pi\mathbb{Q}$ .

Si  $A$  admet une valeur propre réelle et deux valeurs propres non réelles conjuguées, on est dans le cas de la question 6) et on a vu que  $A$  est diagonalisable et que le spectre de  $A$  a la forme voulue.

• Réciproquement, supposons que  $A$  soit diagonalisable dans  $\mathcal{M}_3(\mathbb{C})$  et que le spectre de  $A$  soit de la forme  $(e^{i\theta}, e^{-i\theta}, 1)$  ou  $(e^{i\theta}, e^{-i\theta}, -1)$  avec  $\theta \in 2\pi\mathbb{Q}$ .

Posons  $\theta = \frac{2\pi a}{b}$  où  $a \in \mathbb{Z}$  et  $b \in \mathbb{N}^*$ .  $A$  est semblable à la matrice  $D = \text{diag}(e^{i\theta}, e^{-i\theta}, \pm 1)$ . Donc,  $A^{2b}$  est semblable à la matrice

$$D^{2b} = \text{diag}(e^{4\pi a}, e^{-4\pi a}, (\pm 1)^{2b}) = \text{diag}(1, 1, 1) = I_3,$$

et donc  $A^{2b}$  est égale à la matrice  $I_3$ . On a trouvé un entier non nul  $k$ , à savoir  $k = 2b$ , tel que  $A^k = I_3$  et donc  $A$  est d'ordre fini.

## Partie C : matrices d'ordre fini à coefficients entiers

**1.** La trace  $t$  de  $A$  est la somme des coefficients diagonaux de  $A$  et est donc un entier relatif.  $t$  est d'autre part la somme des trois valeurs propres de  $A$  et donc

$$t = e^{i\theta} + e^{-i\theta} + 1 = 2 \cos \theta + 1.$$

Donc  $2 \cos \theta = t - 1$  est un entier relatif.

**2.**  $2 \cos \theta \in [-2, 2] \cap \mathbb{Z} = \{-2, -1, 0, 1, 2\}$  et donc  $\cos \theta \in \left\{-1, -\frac{1}{2}, 0, \frac{1}{2}, 1\right\}$ . On en déduit que

$$\theta \in (\pi\mathbb{Z}) \cup \left(\frac{\pi}{2} + \pi\mathbb{Z}\right) \cup \left(\pm\frac{\pi}{3} + 2\pi\mathbb{Z}\right) \cup \left(\pm\frac{2\pi}{3} + 2\pi\mathbb{Z}\right).$$

On note que dans chacun de ces cas,  $\theta \in 2\pi\mathbb{Q}$ .

**3. Premier cas.** Si  $\cos \theta = 1$ ,  $\text{Sp}(A) = (1, 1, \pm 1)$ .  $A$  est semblable à  $\text{diag}(1, 1, \pm 1)$ . Dans ce cas,  $A$  est d'ordre 1 ou 2.

**Deuxième cas.** Si  $\cos \theta = -1$ ,  $\text{Sp}(A) = (-1, -1, \pm 1)$ .  $A$  est semblable à  $\text{diag}(-1, -1, \pm 1)$ . Dans ce cas,  $A$  est d'ordre 2.

**Troisième cas.** Si  $\cos \theta = 0$ , le spectre de  $A$  est  $(i, -i, \pm 1)$ .  $A$  est semblable à  $\text{diag}(i, -i, \pm 1)$ . Dans ce cas,  $A$  est d'ordre 4.

**Quatrième cas.** Si  $\cos \theta = -\frac{1}{2}$ , le spectre de  $A$  est  $(j, j^2, \pm 1)$  où  $j = e^{\frac{2i\pi}{3}}$ .  $A$  est semblable à  $\text{diag}(j, j^2, \pm 1)$ . Dans ce cas,  $A$  est d'ordre 3 ou 6.

**Cinquième cas.** Si  $\cos \theta = \frac{1}{2}$ , le spectre de  $A$  est  $(-j, -j^2, \pm 1)$ .  $A$  est semblable à  $\text{diag}(-j, -j^2, \pm 1)$ . Dans ce cas,  $A$  est d'ordre 6.

En résumé,  $o(A) \in \{1, 2, 3, 4, 6\}$ .

**4.**

**4.1.**  $I_3$  est un élément de  $\mathcal{M}_3(\mathbb{Z})$  d'ordre 1 et  $-I_3$  est un élément de  $\mathcal{M}_3(\mathbb{Z})$  d'ordre 2.

**4.2. i.** Notons  $A$  la matrice considérée. En développant suivant la dernière colonne, on obtient

$$\begin{aligned}\chi_A &= \det(A - XI_3) = \begin{vmatrix} -X & 0 & -a \\ 1 & -X & -b \\ 0 & 1 & -X-c \end{vmatrix} \\ &= (-X-c)(-X)^2 + b(-X) - a = -X^3 - cX^2 - bX - a.\end{aligned}$$

ii.  $(1-X)(j-X)(j^2-X) = -X^3 + 1$ . Donc, si on prend  $a = -1$ ,  $b = c = 0$ , on obtient une matrice  $A$  à coefficients entiers relatifs dont le spectre est  $(1, j, j^2)$  à savoir

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

On note alors que  $A^2 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$  puis

$$A^3 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = I_3.$$

La matrice  $A$  est d'ordre 3.

iii. •  $(1-X)(i-X)(-i-X) = (1-X)(X^2+1) = -X^3 + X^2 - X + 1$ . Donc, si on prend  $a = -1$ ,  $b = 1$  et  $c = -1$ , on obtient une matrice  $A$  à coefficients entiers relatifs dont le spectre est  $(1, i, -i)$  à savoir

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

$A$  est à valeurs propres simples et est donc diagonalisable dans  $\mathbb{C}$ .  $A$  est semblable à  $D = \text{diag}(1, i, -i)$ .  $D$  est d'ordre 4 et donc  $A$  est d'ordre 4.

•  $(1-X)(-j-X)(-j^2-X) = (1-X)(X^2-X+1) = -X^3 + 2X^2 - 2X + 1$ . Donc, si on prend  $a = -1$ ,  $b = 2$  et  $c = -2$ , on obtient une matrice  $A$  à coefficients entiers relatifs dont le spectre est  $(1, -j, -j^2)$  à savoir

$$A = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & -2 \\ 0 & 1 & 2 \end{pmatrix}.$$

$A$  est à valeurs propres simples et est donc diagonalisable dans  $\mathbb{C}$ .  $A$  est semblable à  $D = \text{diag}(1, -j, -j^2)$ .  $D$  est d'ordre 6 (car  $-j$  et  $-j^2$  sont des racines sixièmes de 1 et pas moins) et donc  $A$  est d'ordre 6.

# Problème 2 : décimales des nombres rationnels

## Partie A : nombres décimaux

1. • Soit  $x \in \mathbb{Z}$ .  $10^0 x \in \mathbb{Z}$  et donc  $x \in \mathbb{D}$ . Ceci montre que  $\mathbb{Z} \subset \mathbb{D}$ . De plus,  $0,1 = \frac{1}{10}$  est un nombre décimal qui n'est pas un entier. Donc,

$$\mathbb{Z} \subsetneq \mathbb{D}.$$

• Soit  $x \in \mathbb{D}$ . Il existe  $(n, p) \in \mathbb{N} \times \mathbb{Z}$  tel que  $10^n x = p$ . Mais alors,  $x = \frac{p}{10^n}$  et donc  $x \in \mathbb{Q}$ . Ceci montre que  $\mathbb{D} \subset \mathbb{Q}$ .

Montrons alors que  $\frac{1}{3}$  est un nombre rationnel qui n'est pas un nombre décimal. Dans le cas contraire, il existe  $(n, p) \in \mathbb{N} \times \mathbb{Z}$  tel que  $10^n \times \frac{1}{3} = p$  et donc  $3p = 10^n$ . Mais  $n = 0$  est impossible car 1 n'est pas un multiple de 3 et  $n \geq 1$  est impossible car le nombre premier 3 n'est pas un facteur premier de  $10^n = 2^n 5^n$ . On a montré par l'absurde que  $\frac{1}{3}$  est un nombre rationnel qui n'est pas un nombre décimal. Donc,

$$\mathbb{D} \subsetneq \mathbb{Q}.$$

2. Soit  $(x, y) \in \mathbb{D}^2$ . Il existe  $(n, p, m, q) \in \mathbb{N} \times \mathbb{Z} \times \mathbb{N} \times \mathbb{Z}$  tel que  $10^n x = p$  et  $10^m y = q$ . Mais alors

$$10^{n+m}(x+y) = 10^m \times 10^n x + 10^n \times 10^m y = 10^m p + 10^n q \in \mathbb{Z},$$

et donc  $x+y \in \mathbb{D}$ . De même,

$$10^{n+m}xy = 10^n x 10^m y = pq \in \mathbb{Z},$$

et donc  $xy \in \mathbb{D}$ . On a montré que  $\mathbb{D}$  est stable pour l'addition et pour la multiplication.

3.

3.1. Soit  $n = \text{Max}\{\alpha, \beta\}$ .  $n$  est un entier naturel supérieur ou égal à  $\alpha$  et à  $\beta$  puis

$$10^n x = \frac{2^n 5^n a}{2^\alpha 5^\beta} = 2^{n-\alpha} 5^{n-\beta} a \in \mathbb{Z}.$$

Donc,  $x$  est un nombre décimal.

3.2.  $x$  n'est pas entier et donc  $b \geq 2$ . Soit  $p$  un facteur premier de  $b$ .

Puisque  $x$  est un décimal positif non entier, il existe deux entiers naturels non nuls  $n$  et  $k$  tels que  $\frac{a}{b} = \frac{k}{10^n}$  et donc  $kb = 10^n a$ .  $b$  divise  $10^n a$  et  $b$  est premier à  $a$ . D'après le théorème de GAUSS,  $b$  divise  $10^n$  puis  $p$  divise  $10^n$ .  $p$  est un donc facteur premier de  $10^n = 2^n 5^n$  (avec  $n \geq 1$ ). Donc,  $p \in \{2, 5\}$ .

3.3. Ainsi, si  $x$  est un décimal non entier, il existe  $(\alpha, \beta) \in \mathbb{N}^2 \setminus \{(0, 0)\}$  tel que  $b = 2^\alpha 5^\beta$ . Si  $x$  est entier,  $b$  divise  $a$  et est premier à  $a$  et donc  $b = 1 = 2^0 5^0$ . Dans tous les cas, il existe  $(\alpha, \beta) \in \mathbb{N}^2$  tel que  $b = 2^\alpha 5^\beta$ .

La réciproque a été établie à la question a) et donc

$$x \text{ est décimal si et seulement si il existe } (\alpha, \beta) \in \mathbb{N}^2 \text{ tel que } b = 2^\alpha 5^\beta.$$

4.

4.1. Pour tout entier naturel  $n$ ,  $0 \leq \frac{d_n}{10^n} \leq \frac{9}{10^n} = 9 \left(\frac{1}{10}\right)^n$ . Puisque  $\frac{1}{10} \in ]-1, 1[$ , la série géométrique de terme général  $9 \left(\frac{1}{10}\right)^n$ ,  $n \in \mathbb{N}$ , converge et il en est de même de la série de terme général  $\frac{d_n}{10^n}$ ,  $n \in \mathbb{N}$ .

4.2. • Si la suite  $(d_n)$  est finie, il existe  $N \in \mathbb{N}^*$  tel que pour  $n \geq N$ ,  $d_n = 0$ . Mais alors,

$$10^N x = 10^N \sum_{n=0}^{+\infty} \frac{d_n}{10^n} = 10^N \sum_{n=0}^N \frac{d_n}{10^n} = \sum_{n=0}^N d_n 10^{N-n} \in \mathbb{Z}.$$

$x$  est donc un nombre décimal.

• Supposons que  $x$  admette un développement décimal impropre. Donc, il existe un rang  $N \in \mathbb{N}^*$  tel que pour  $n \geq N$ ,  $d_n = 9$ . D'après l'étude précédente,  $x$  est la somme d'un nombre décimal  $y$  et de

$$z = \sum_{n=N}^{+\infty} \frac{9}{10^n} = \frac{9}{10^N} \times \frac{1}{1 - \frac{1}{10}} = \frac{1}{10^{N-1}}.$$

Ainsi,  $x = y + z$  est la somme de deux nombres décimaux et est donc un nombre décimal d'après la question 2).

**4.3.** Soit  $N \geq 0$ . Pour tout  $k \geq N + 1$ , on a  $d_k \leq 9$ . D'après le calcul de la question précédente,

$$\sum_{k=N}^{+\infty} \frac{d_k}{10^k} = \frac{d_N}{10^N} + \sum_{k=N+1}^{+\infty} \frac{d_k}{10^k} \leq \frac{d_N}{10^N} + \sum_{k=N+1}^{+\infty} \frac{9}{10^k} = \frac{d_N}{10^N} + \frac{1}{10^N} = \frac{1 + d_N}{10^N}.$$

Si toutes les inégalités  $d_k \leq 9$ ,  $k \geq N + 1$ , sont des égalités, alors  $\sum_{k=N+1}^{+\infty} \frac{9}{10^k} = \frac{1}{10^N}$ . Si l'une des inégalités  $d_k \leq 9$ ,  $k \geq N + 1$ , est stricte, alors

$$\sum_{k=N+1}^{+\infty} \frac{d_k}{10^k} < \sum_{k=N+1}^{+\infty} \frac{9}{10^k} = \frac{1}{10^N},$$

et donc  $\sum_{k=N}^{+\infty} \frac{d_k}{10^k} < \frac{1 + d_N}{10^N}$ . Finalement,  $\sum_{k=N}^{+\infty} \frac{d_k}{10^k} = \frac{1 + d_N}{10^N}$  si et seulement si pour tout  $k \geq N + 1$ ,  $d_k = 9$ .

**4.4.** Considérons deux suites décimales propres distinctes  $(d_n)_{n \in \mathbb{N}}$  et  $(d'_n)_{n \in \mathbb{N}}$ . Soient  $x = \sum_{n=0}^{+\infty} \frac{d_n}{10^n}$  et  $x' = \sum_{n=0}^{+\infty} \frac{d'_n}{10^n}$ .

$\{n \in \mathbb{N} / d_n \neq d'_n\}$  est une partie non vide de  $\mathbb{N}$ . On peut considérer  $N = \text{Min}\{n \in \mathbb{N} / d_n \neq d'_n\}$ . Par définition  $d_N \neq d'_N$ . On peut supposer sans perte de généralité que  $d_N < d'_N$  ou encore que  $d'_N \geq d_N + 1$ . Puisque la suite  $(d_n)_{n \in \mathbb{N}}$  est propre, la question précédente permet d'écrire

$$\sum_{n=N}^{+\infty} \frac{d_n}{10^n} < \frac{1 + d_N}{10^N} \leq \frac{d'_N}{10^N} \leq \sum_{n=N}^{+\infty} \frac{d'_n}{10^n}.$$

Comme d'autre part, les éventuelles décimales de  $x$  et  $x'$  d'indices strictement inférieurs à  $N$  sont égales, on en déduit que  $x < x'$ . On a ainsi montré l'unicité d'un développement décimal propre.

**5.** Soit  $x$  un décimal positif. Posons  $d_0 = E(x)$ .  $x - d_0$  est un décimal de  $[0, 1[$ . Par suite, il existe un entier naturel  $N$  tel que  $10^N(x - d_0) \in \mathbb{N}$ . Mais alors  $10^N(x - d_0)$  est un entier élément de  $[[0, 10^N - 1]]$ . La décomposition de cet entier en base 10 s'écrit

$$10^N(x - d_0) = d_1 \times 10^{N-1} + \dots + d_{n-1} \times 10 + d_N$$

où les chiffres  $d_1, \dots, d_{n-1}$  sont éléments de  $[[0, 9]]$ . On en déduit que

$$x = d_0 + d_1 \times 10^{-1} + \dots + \frac{d_N}{10^N}.$$

Ceci montre l'existence d'un développement décimal fini et en particulier propre de  $x$ . L'unicité de ce développement a été montré à la question précédente.

## Partie B : périodicité des décimales d'un rationnel positif non décimal

**1.** Soit  $N \geq 1$ .

**1.1. Algorithme.**

<b>Variables</b>	a et b sont des entiers naturels non nuls N est un entier naturel non nul k est un entier naturel d et r sont des entiers naturels
<b>Initialisation</b>	Demander a, b et N Affecter à d la valeur E(a/b) Affecter à r la valeur a - db
<b>Traitement</b>	Afficher d Afficher r Tant que k < N Affecter à d la valeur E(10r/b) Affecter à r la valeur 10r - db Afficher d Afficher r Affecter à k la valeur k + 1 Fin du Tant que Fin

1.2. On donne les résultats successifs dans un tableau.

n	0	1	2	3	4	5	6	7
d <sub>n</sub>	0	3	8	4	6	1	5	3
r <sub>n</sub>	5	11	6	8	2	7	5	11
10r <sub>n</sub>	50	110	60	80	20	70	50	110

2.

2.1. Montrons par récurrence que :  $\forall n \in \mathbb{N}, x = \sum_{k=0}^n \frac{d_k}{10^k} + \frac{r_n}{10^n b}$ .

- d<sub>0</sub> et r<sub>0</sub> sont respectivement le quotient et le reste de la division euclidienne de a par b. Donc, a = bd<sub>0</sub> + r<sub>0</sub> puis

$$x = \frac{a}{b} = d_0 + \frac{r_0}{b} = \sum_{k=0}^0 \frac{d_k}{10^k} + \frac{r_0}{10^0 b}.$$

La formule proposée est vraie quand n = 0.

- Soit n ≥ 0. Supposons que  $x = \sum_{k=0}^n \frac{d_k}{10^k} + \frac{r_n}{10^n b}$ . d<sub>n+1</sub> et r<sub>n+1</sub> sont respectivement le quotient et le reste de la division euclidienne de 10r<sub>n</sub> par b. Donc, 10r<sub>n</sub> = bd<sub>n+1</sub> + r<sub>n+1</sub> puis, après division des deux membres par 10<sup>n+1</sup>b,

$$\frac{r_n}{10^n b} = \frac{d_{n+1}}{10^{n+1}} + \frac{r_{n+1}}{10^{n+1} b},$$

puis  $x = \sum_{k=0}^{n+1} \frac{d_k}{10^k} + \frac{r_{n+1}}{10^{n+1} b}$ .

Le résultat est démontré par récurrence.

2.2. Soit n ∈ ℕ. En multipliant les deux membres de l'égalité précédente par 10<sup>n</sup>b, on obtient 10<sup>n</sup>a = q<sub>n</sub>b + r<sub>n</sub> où q<sub>n</sub> =  $\sum_{k=0}^n d_k 10^{n-k}$  est un entier et r<sub>n</sub> est un entier tel que 0 ≤ r<sub>n</sub> < b. Donc r<sub>n</sub> est le reste de la division euclidienne de 10<sup>n</sup>a par b.

2.3. • Pour tout entier naturel n, 0 ≤ r<sub>n</sub> < b puis 0 ≤ 10r<sub>n</sub> < 10b puis

$$0 \leq d_{n+1} = E\left(\frac{10r_n}{b}\right) \leq \frac{10r_n}{b} < 10,$$



ou encore  $0 \leq d_{n+1} \leq 9$ . Ainsi, pour tout entier naturel non nul,  $d_n \in \llbracket 0, 9 \rrbracket$ . D'autre  $d_0 = E\left(\frac{a}{b}\right)$  est un entier.

• Soit  $n \in \mathbb{N}$ .  $0 \leq \frac{r_n}{10^n b} < \frac{b}{10^n b} = \frac{1}{10^n}$ . Puisque  $\frac{1}{10^n}$  tend vers 0 quand  $n$  tend vers  $+\infty$ , le théorème des gendarmes permet d'affirmer que la suite  $\left(\frac{r_n}{10^n b}\right)_{n \in \mathbb{N}}$  converge et que  $\lim_{n \rightarrow +\infty} \frac{r_n}{10^n b} = 0$ .

On en déduit encore que la série de terme général  $\frac{d_k}{10^k}$ ,  $k \in \mathbb{N}$  converge et que

$$x = \sum_{k=0}^{+\infty} \frac{d_k}{10^k}.$$

• Ce développement décimal est nécessairement propre. Dans le cas contraire, d'après la question 4.2, de la partie A,  $x$  serait un nombre décimal ce qui n'est pas.

**3.**

**3.1.** S'il existe  $n \in \mathbb{N}$  tel que  $r_n = 0$ , alors pour cet entier  $n$ ,  $x = \sum_{k=0}^n \frac{d_k}{10^k}$  et en particulier,  $x$  est un nombre décimal, ce qui est faux. Donc,  $\forall n \in \mathbb{N}$ ,  $r_n \neq 0$ .

**3.2.** D'après la question précédente,  $\forall n \in \mathbb{N}$ ,  $1 \leq r_n \leq b-1$ . Les  $b$  nombres  $r_0, \dots, r_{b-1}$  sont éléments de  $\llbracket 1, b-1 \rrbracket$  qui est de cardinal  $b-1 < b$ . D'après le principe des tiroirs, les  $b$  nombres  $r_0, \dots, r_{b-1}$  ne peuvent être deux à deux distincts.

**3.3.** Montrons par récurrence que  $\forall n \geq q$ ,  $r_{n+p} = r_n$ .

• Le résultat est vrai pour  $n = q$  car par définition de  $q$ ,  $r_{q+p} = r_q$ .

• Soit  $n \geq q$ . Supposons que  $r_{n+p} = r_n$ .  $r_{n+1+p}$  est le reste de la division euclidienne de  $10r_{n+p} = 10r_n$  par  $b$ . Le reste de la division euclidienne de  $10r_n$  par  $b$  est aussi  $r_{n+1}$ . Donc,  $r_{n+1+p} = r_{n+1}$ .

Le résultat est démontré par récurrence. La suite  $(r_n)_{n \in \mathbb{N}}$  est  $p$ -périodique à partir du rang  $q$ .

Soit  $n \geq q$ .  $10r_n = d_{n+1}b + r_{n+1}$  et donc  $d_{n+1} = \frac{10r_n - r_{n+1}}{b}$ . On en déduit que la suite  $(d_{n+1})_{n \in \mathbb{N}}$  est  $p$ -périodique à partir du rang  $q$  ou encore que la suite  $(d_n)_{n \in \mathbb{N}}$  est  $p$ -périodique à partir du rang  $q+1$ .

**4.**

**4.1. i.** Tout d'abord, si l'un des entiers  $10^k$ ,  $0 \leq k \leq b-1$  est congru à 0 modulo  $b$ , alors  $b$  est un diviseur de  $10^k$  et est donc de la forme  $2^\alpha 5^\beta$ ,  $(\alpha, \beta) \in \mathbb{N}^2$ . D'après la question 3.1 de la partie A,  $x$  est décimal ce qui est faux. Donc, aucun des  $10^k$ ,  $0 \leq k \leq b-1$ , n'est congru à 0 modulo  $b$ . Par suite, les  $b$  restes des divisions euclidiennes de  $10^0, 10^1, \dots, 10^{b-1}$  sont éléments de  $\llbracket 1, b-1 \rrbracket$ . Comme à la question 3.2, deux d'entre eux sont égaux ou encore deux au moins des nombres  $10^0, 10^1, \dots, 10^{b-1}$  sont congrus modulo  $b$ .

ii. Soit  $(n, m) \in \mathbb{N}^2$ .

$$\begin{aligned} r_n = r_m &\Leftrightarrow 10^n a \equiv 10^m a \pmod{b} \text{ (d'après la question 2.2)} \\ &\Leftrightarrow 10^n \equiv 10^m \pmod{b} \text{ (car } a \text{ et } b \text{ sont premiers entre eux et donc } a \text{ est simplifiable modulo } b\text{)}. \end{aligned}$$

Ceci montre que  $q$  est le plus petit exposant d'un nombre de la liste qui est congru à un autre nombre de la liste modulo  $b$  puis que  $q+p$  est l'exposant du premier nombre de la liste congru à  $10^q$  modulo  $b$  et distinct de  $10^q$ .

**4.2.** Le résultat de la question 4.1. de dépend pas du choix de l'entier non nul  $a$ , premier à  $b$ . Puisque l'entier 1 est premier à  $b$ , les rationnels  $\frac{a}{b}$  et  $\frac{1}{b}$  ont même période et même pré-période.

**5.** •  $10^0 \equiv 1 \pmod{7}$ ,  $10^1 \equiv 3 \pmod{7}$ ,  $10^2 \equiv 2 \pmod{7}$ ,  $10^3 \equiv 6 \pmod{7}$ ,  $10^4 \equiv 4 \pmod{7}$ ,  $10^5 \equiv 5 \pmod{7}$  et  $10^6 \equiv 1 \pmod{7}$ . Donc la pré-période de 7 est 0 et la période de 7 est 6.

•  $10^0 \equiv 1 \pmod{12}$ ,  $10^1 \equiv 10 \pmod{12}$ ,  $10^2 \equiv 4 \pmod{12}$ ,  $10^3 \equiv 4 \pmod{12}$ . Donc la pré-période de 12 est 2 et la période de 12 est 1.

•  $10^0 \equiv 1 \pmod{112}$ ,  $10^1 \equiv 10 \pmod{112}$ ,  $10^2 \equiv 100 \pmod{112}$ ,  $10^3 \equiv 104 \pmod{112}$ ,  $10^4 \equiv 32 \pmod{112}$ ,  $10^5 \equiv 96 \pmod{112}$ ,  $10^6 \equiv 64 \pmod{112}$ ,  $10^7 \equiv 80 \pmod{112}$ ,  $10^8 \equiv 16 \pmod{112}$ ,  $10^9 \equiv 48 \pmod{112}$ ,  $10^{10} \equiv 32 \pmod{112}$ . Donc la pré-période de 112 est 4 et la période de 112 est 6.

## Partie C : détermination de la pré-période

**1.**

**1.1.**  $b$  et 10 sont premiers entre eux et il en est de même de  $b$  et  $10^q$ . Par suite,  $10^q$  est simplifiable modulo  $b$  ou encore  $10^q \equiv 10^{p+q} \pmod{b} \Leftrightarrow 10^p \equiv 10^0 \pmod{b}$ .

**1.2.** Par définition de  $q$ , on a  $10^q \equiv 10^{p+q} \pmod{b}$ . D'après la question précédente, on a donc  $10^p \equiv 10^0 \pmod{b}$ . Puisque  $1 \leq p \leq b-1$ , par définition de  $q$ , on a  $q = 0$  ou encore  $\omega(b) = 0$ .

**2.** Si  $10^q$  est un multiple de  $2^j \times 5^k$  et si  $10^p - 1$  est un multiple de  $c$ , alors  $10^q (10^p - 1)$  est un multiple de  $2^j \times 5^k \times c = b$ . Réciproquement, supposons que  $10^q (10^p - 1)$  soit un multiple de  $b = 2^j \times 5^k \times c$ . Il existe un entier  $K$  tel que

$$10^q (10^p - 1) = K \times 2^j \times 5^k \times c (*).$$

$c$  est premier avec  $10$  et donc avec  $10^q$ . D'autre part, d'après l'égalité (\*), l'entier  $c$  divise  $10^q (10^p - 1)$ . D'après le théorème de GAUSS,  $c$  divise  $10^p - 1$ .

D'après le théorème de BÉZOUT, les entiers  $10^p - 1$  et  $10^p$  sont premiers entre eux car  $1 \times 10^p + (-1) \times (10^p - 1) = 1$ . On en déduit que l'entier naturel  $10^p - 1$  supérieur ou égal à  $2$ , n'admet ni  $2$ , ni  $5$  pour facteur premier et donc premier avec  $2^j \times 5^k$  (même si  $j = k = 0$ ).

D'après l'égalité (\*), l'entier  $2^j \times 5^k$  divise  $10^q (10^p - 1)$  et est d'autre part premier avec  $10^p - 1$ . D'après le théorème de GAUSS,  $2^j \times 5^k$  divise  $10^q$ .

On a ainsi montré que :  $10^q (10^p - 1)$  multiple de  $b \Leftrightarrow 10^q$  multiple de  $2^j \times 5^k$  et  $10^p - 1$  multiple de  $c$ . Maintenant,  $10^q (10^p - 1)$  multiple de  $b \Leftrightarrow 10^{q+p} \equiv 10^p \pmod{b}$ .

D'après la question 4.1 de la partie B et d'après ce qui précède,  $q$  est la pré-période de  $b$  et  $p$  est la période de  $b$  si et seulement si  $q$  est le plus petit entier naturel tel que  $10^q$  soit un multiple de  $2^j \times 5^k$  et  $p$  est le plus petit entier naturel non nul tel que  $10^p \equiv 1 \pmod{c}$ .

Or,  $10^q = 2^q \times 5^q$  est un multiple de  $2^j \times 5^k$  si et seulement si  $q \geq \text{Max}\{j, k\}$ . Ceci montre que

$$\omega(b) = \text{Max}\{j, k\}.$$

D'autre part, le plus petit entier naturel non nul  $p$  tel que  $10^p \equiv 1 \pmod{c}$  est la période de  $c$  d'après la question 1 et donc

$$\pi(b) = \pi(c).$$

**3. •**  $150 = 2 \times 3 \times 5^2$ . Ici,  $c = 3$ ,  $j = 1$  et  $k = 2$ . D'après ce qui précède,  $\pi(150) = \pi(3) = 1$  et  $\omega(150) = \text{Max}\{1, 2\} = 2$ . La pré-période de  $150$  est  $2$  et la période de  $150$  est  $1$ .

**•**  $1120 = 2^5 \times 5 \times 7$ . Donc  $\omega(1120) = \text{Max}\{5, 1\} = 5$  et  $\pi(1120) = \pi(7) = 6$ . La pré-période de  $1120$  est  $5$  et la période de  $1120$  est  $6$ .

## Partie D : détermination de la période

**1.**

**1.1. •** Vérifions tout d'abord que pour tout élément  $\bar{a}$  de  $(\mathbb{Z}/b\mathbb{Z})^*$ ,  $\overline{10} \times \bar{a} \in (\mathbb{Z}/b\mathbb{Z})^*$ .

Soit  $\bar{a}$  de  $(\mathbb{Z}/b\mathbb{Z})^*$ . Puisque  $10$  est premier avec  $b$ , on sait que  $\overline{10}$  est un inversible de l'anneau  $(\mathbb{Z}/b\mathbb{Z}, +, \times)$ . En particulier,  $\overline{10}$  est simplifiable pour  $\times$  dans  $\mathbb{Z}/b\mathbb{Z}$  et donc si  $\overline{10} \times \bar{a} = \bar{0}$ , alors  $\bar{a} = \bar{0}$ . Par contraposition,  $\bar{a} \neq \bar{0} \Rightarrow \overline{10} \times \bar{a} \neq \bar{0}$ .

Ceci montre que  $f$  est effectivement une application de  $(\mathbb{Z}/b\mathbb{Z})^*$  dans lui-même.

**•** Soient  $\bar{a}$  et  $\bar{a}'$  deux éléments de  $(\mathbb{Z}/b\mathbb{Z})^*$  tels que  $f(\bar{a}) = f(\bar{a}')$ . Alors  $\overline{10} \times \bar{a} = \overline{10} \times \bar{a}'$  puis  $\bar{a} = \bar{a}'$  car  $\overline{10}$  est simplifiable pour  $\times$  dans  $\mathbb{Z}/b\mathbb{Z}$ .

On a montré que  $f$  est une application injective de  $(\mathbb{Z}/b\mathbb{Z})^*$  dans lui-même.

**1.2.** Puisque l'ensemble  $(\mathbb{Z}/b\mathbb{Z})^*$  est fini de cardinal  $b-1$ , on sait que  $f$  est une permutation de  $(\mathbb{Z}/b\mathbb{Z})^*$ . On en déduit que

$$\prod_{a=1}^{b-1} \bar{a} = \prod_{a=1}^{b-1} f(\bar{a}) = \prod_{a=1}^{b-1} (\overline{10} \times \bar{a}) = \overline{10}^{b-1} \times \prod_{a=1}^{b-1} \bar{a}.$$

Puisque  $b$  est un nombre premier, on sait que toutes les classes non nulles sont inversibles et donc simplifiables dans  $\mathbb{Z}/b\mathbb{Z}$ .

Après simplification par  $\prod_{a=1}^{b-1} \bar{a}$ , on obtient  $\overline{10}^{b-1} = \bar{1}$  ou encore  $10^{b-1} \equiv 1 \pmod{b}$ .

**1.3.** Soient  $n$  un entier naturel et  $m$  un entier naturel non nul. La division euclidienne de  $n$  par  $m$  s'écrit  $n = qm + r$  où  $q$  et  $r$  sont deux entiers naturels tels que  $0 \leq r < m$ .

$$\begin{aligned} 10^n - 1 &= 10^{qm+r} - 1 = 10^{qm+r} - 10^r + 10^r - 1 = 10^r ((10^m)^q - 1) + (10^r - 1) \\ &= 10^r \left( (10^m)^{m-1} + (10^m)^{m-2} + \dots + 10^m + 1 \right) (10^m - 1) + (10^r - 1) \end{aligned}$$

Tout d'abord,  $10^r \left( (10^m)^{m-1} + (10^m)^{m-2} + \dots + 10^m + 1 \right)$  est un entier. Ensuite,

$$0 \leq r < m \Rightarrow 10^0 \leq 10^r < 10^m \Rightarrow 0 \leq 10^r - 1 < 10^m - 1.$$

Donc, le reste de la division euclidienne de  $10^n - 1$  par  $10^m - 1$  est  $10^r - 1$ .

**1.4.** • Soit  $k$  un entier naturel tel que  $10^k \equiv 1 \pmod{b}$ . D'après la question précédente, il existe un entier  $Q$  tel que  $10^k - 1 = Q \times (10^{\pi(b)} - 1) + (10^r - 1)$  où  $r$  est le reste de la division euclidienne de  $k$  par  $\pi(b)$ .

Les deux entiers  $10^k - 1$  et  $10^{\pi(b)} - 1$  sont congrus à 0 modulo  $b$  et donc  $10^r - 1$  est congru à 0 modulo  $b$ . Ainsi,  $r$  est un entier vérifiant  $10^r \equiv 1 \pmod{b}$  et  $0 \leq r < \pi(b)$ . Puisque  $\pi(b)$  est le plus petit entier naturel non nul vérifiant  $10^n \equiv 1 \pmod{b}$ , il ne reste que la possibilité  $r = 0$ . Ceci montre que  $\pi(b)$  divise  $k$ .

On a montré que pour tout entier naturel  $k$ , si  $10^k \equiv 1 \pmod{b}$ , alors  $\pi(b)$  divise  $k$ . On peut noter que la réciproque est vraie puisque  $10^{\pi(b)} \equiv 1 \pmod{b}$ .

• D'après la question 1.2,  $10^{b-1} \equiv 1 \pmod{b}$  et donc, d'après la question précédente,  $\pi(b)$  divise  $b - 1$ .

## 2.

**2.1.** Soit  $n$  un entier naturel. Si  $10^n - 1$  est multiple de  $bc$ , alors  $10^n - 1$  est multiple de  $b$  et de  $c$ . Réciproquement, si  $10^n - 1$  est multiple de  $b$  et de  $c$ , alors  $10^n - 1$  est multiple du PPCM de  $b$  et de  $c$  à savoir  $bc$  puisque  $b$  et  $c$  sont premiers entre eux. En résumé,

$$10^n \equiv 1 \pmod{bc} \Leftrightarrow 10^n \equiv 1 \pmod{b} \text{ et } 10^n \equiv 1 \pmod{c}.$$

Ensuite, le raisonnement de la question 1.4 n'a pas fait intervenir le fait que  $b$  soit un nombre premier et donc

$$10^n \equiv 1 \Leftrightarrow n \text{ est un multiple de } \pi(b).$$

En résumé,

$$10^n \equiv 1 \pmod{bc} \Leftrightarrow n \text{ est un multiple de } \pi(b) \text{ et } \pi(c).$$

**2.2.** Les multiples communs à deux entiers sont les multiples de leur PPCM et donc

$$10^n \equiv 1 \pmod{bc} \Leftrightarrow n \text{ est un multiple de PPCM}(\pi(b), \pi(c)).$$

En particulier,  $\pi(bc) = \text{PPCM}(\pi(b), \pi(c))$ .

## 3.

**3.1.** Puisque  $\ell\pi(p)$ ,  $10^\ell \equiv 1 \pmod{p}$  ou encore il existe un entier  $K$  tel que  $10^\ell - 1 = Kp$ . Soit  $k$  la valuation  $p$ -adique de  $K$ . On peut écrire  $K$  sous la forme  $K = p^k \times q$  où  $k$  est un entier naturel et  $q$  est un entier naturel non nul premier à  $p$ . On a alors  $10^\ell - 1 = p^{k+1} \times q$  ou encore  $10^\ell - 1 = p^r \times q$  où  $r = k + 1$  de sorte que  $r \geq 1$ .

**3.2.** Supposons que  $n \leq r$ . Alors,  $p^r \times q = 10^\ell - 1$  est un multiple de  $p^n$  et donc  $10^\ell \equiv 1 \pmod{p^n}$ . On sait alors que  $\pi(p^n) \leq \ell$ . Mais d'autre part, puisque  $10^{\pi(p^n)} \equiv 1 \pmod{p^n}$ , alors en particulier  $10^{\pi(p^n)} \equiv 1 \pmod{p}$  et donc  $\pi(p^n) \geq \ell$ . Finalement,  $\pi(p^n) = \ell$ .

**3.3.** Supposons que  $n > r$ .

Montrons par récurrence que pour tout  $k \in \mathbb{N}$ , il existe un entier naturel  $Q_k$  premier avec  $p$  tel que  $10^{\ell \times p^k} - 1 = p^{r+k} \times Q_k$  et que  $\pi(p^{r+k}) = \ell \times p^k$ .

• La proposition est vraie quand  $k = 0$  avec  $Q_0 = q$  (qui est premier avec  $p$ ) puisque d'autre part  $\pi(p^r) = \ell$  d'après la question précédente.

• Soit  $k \geq 0$ . Supposons qu'il existe un entier naturel  $Q_k$  premier avec  $p$  tel que  $10^{\ell \times p^k} - 1 = p^{r+k} \times Q_k$  et que  $\pi(p^{r+k}) = \ell \times p^k$ . Alors

$$\begin{aligned} 10^{\ell \times p^{k+1}} - 1 &= \left( 10^{\ell \times p^k} \right)^p - 1 \\ &= (p^{r+k} \times Q_k + 1)^p - 1 \text{ par hypothèse de récurrence} \\ &= \sum_{j=1}^p \binom{p}{j} (p^{r+k} Q_k)^j = p^{r+k+1} Q_k + \sum_{j=2}^p \binom{p}{j} p^{j(r+k)} Q_k^j \end{aligned}$$

$$\text{Posons } Q_{k+1} = Q_k + \sum_{j=2}^p \binom{p}{j} p^{j(r+k)-r-k-1} Q_k^j = Q_k + \sum_{j=2}^p \binom{p}{j} p^{(j-1)(r+k)-1} Q_k^j.$$

Pour  $j \geq 2$ ,  $(j-1)(r+k) - 1 \geq r+k-1 \geq 1+0-1 = 0$  car  $r \geq 1$ . Donc  $Q_{k+1}$  est un entier naturel non nul tel que

$$10^{\ell \times p^{k+1}} - 1 = p^{r+k+1} Q_{k+1}.$$

Vérifions que  $Q_{k+1}$  est premier avec  $p$ . Pour  $j \geq 3$ ,  $(j-1)(r+k) - 1 \geq 2(r+k) - 1 \geq 2 - 1 = 1$ . Donc,

$\sum_{j=3}^p \binom{p}{j} p^{(j-1)(r+k)-1} Q_k^j$  est un entier divisible par  $p$ . D'autre part,  $\binom{p}{2} p^{(2-1)(r+k)-1} Q_k^2 = p \times \frac{p-1}{2} p^{r+k-1} Q_k^2$  est

un entier divisible par  $p$  puisque  $\frac{p-1}{2}$  est un entier,  $p$  étant impair. Finalement,  $\sum_{j=2}^p \binom{p}{j} p^{(j-1)(r+k)-1} Q_k^j$  est

un entier divisible par  $p$ . On en déduit que  $Q_{k+1} \equiv Q_k [p]$ . Par hypothèse de récurrence,  $Q_k$  est premier au nombre premier  $p$ . Il en est de même de  $Q_{k+1}$ .

Montrons alors que  $\pi(p^{r+k+1}) = \ell \times p^{k+1}$ . Puisque  $10^{\ell \times p^{k+1}} - 1$  est divisible par  $p^{r+k+1}$ , on a  $10^{\ell \times p^{k+1}} \equiv 1 [p^{r+k+1}]$ . On en déduit que  $\pi(p^{r+k+1})$  est un diviseur de  $\ell \times p^{r+k+1}$ .

Mais d'autre part,  $10^{\pi(p^{r+k+1})} - 1$  est divisible par  $p^{r+k+1}$  et donc par  $p^{r+k}$  et donc  $\pi(p^{r+k+1})$  est un multiple de  $\pi(p^{r+k})$  ou encore de  $\ell \times p^{r+k}$  par hypothèse de récurrence. Donc, il existe un entier naturel non nul  $K$  tel que  $\pi(p^{r+k+1}) = K \times \ell \times p^{r+k}$ . Puisque  $K \times \ell \times p^{r+k}$  divise  $\ell \times p^{r+k+1}$ ,  $K$  est un diviseur de  $p$  et donc  $K = 1$  ou  $K = p$  puisque  $p$  est premier.

Ceci ne laisse plus comme possibilités que  $\pi(p^{r+k+1}) = \ell \times p^{r+k+1}$  ou  $\pi(p^{r+k+1}) = \ell \times p^{r+k}$ .

Mais si  $\pi(p^{r+k+1}) = \ell \times p^{r+k}$ , alors  $10^{\ell \times p^{r+k}} - 1 \equiv 0 [p^{r+k+1}]$  ou encore  $p^{r+k} Q_k \equiv 0 [p^{r+k+1}]$  ou enfin  $Q_k \equiv 0 [p]$  ce qui est faux. Donc,  $\pi(p^{r+k+1}) = \ell \times p^{r+k+1}$ .

Le résultat est démontré par récurrence.

En particulier, pour  $k = n - r \in \mathbb{N}$  de sorte que  $n = r + k$ , on obtient  $\pi(p^n) = \ell \times p^{n-r}$ .

#### 4.

**4.1.** •  $10^1 \equiv 1 [3]$ . Donc si  $p = 3$ , alors  $\ell = 1$ . De plus,  $10^\ell - 1 = 9 = 3^2$  et donc  $r = 2$  si  $p = 3$ . Par suite,  $\pi(3) = \pi(3^2) = 1$  puis  $\pi(3^3) = 1 \times 3^1 = 3$  et  $\pi(3^4) = 1 \times 3^2 = 9$ .

• On a vu à la question 5 de la partie B que  $\pi(7) = 6$ . De plus,  $10^6 - 1 = 999\,999 = 7^1 \times 142\,857$  avec  $142857$  premier à  $7$ . Donc, si  $p = 7$ , alors  $r = 1$ . D'après la question précédente,  $\pi(7) = 6$  puis  $\pi(7^2) = 6 \times 7 = 42$  puis  $\pi(7^3) = 6 \times 7^2 = 294$ .

**4.2.**  $27783 = 3^4 \times 7^3$ . D'après ce qui précède,  $\pi(27783) = \pi(3^4) \times \pi(7^3) = 9 \times 294 = 2646$ .

$$\pi(27783) = 2646.$$