DEVOIR SURVEILLÉ

1 Les questions **1)** et **2)** sont indépendantes.

1) Montrer, en raisonnant modulo 5, que l'équation : $x^4 = 3y^2 - 25$ d'inconnue $(x,y) \in \mathbb{N}^2$ n'a pas de solution.

2) a) Calculer le reste de la division euclidienne de 5^n par 3 pour tout $n \in \mathbb{N}$.

b) Résoudre l'équation : $x^2 + 9 = 5^n$ d'inconnue $(n,x) \in \mathbb{N}^2$.

---

2 On pose : $A = \begin{pmatrix} -1 & 3 & 3 \\ 3 & -1 & -3 \\ -3 & 3 & 5 \end{pmatrix}$.

1) a) Résoudre le système linéaire : $AX = -X$ d'inconnue $X \in \mathbb{R}^3$.

b) Résoudre le système linéaire : $AX = 2X$ d'inconnue $X \in \mathbb{R}^3$.

c) Montrer que pour tout $\lambda \in \mathbb{R} \setminus \{-1, 2\}$, le système linéaire : $AX = \lambda X$ d'inconnue $X \in \mathbb{R}^3$ admet $(0,0,0)$ pour seule solution.

2) On pose : $C_1 = \begin{pmatrix} 1 \\ -1 \\ 1 \end{pmatrix}$, $C_2 = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}$ et $C_3 = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}$ et on note P la matrice de $\mathcal{M}_3(\mathbb{R})$ de colonnes C_1, C_2, C_3.

a) Montrer que pour une certaine matrice diagonale $D \in \mathcal{M}_3(\mathbb{R})$ à préciser : $AP = PD$. Quel lien avec la question **1)** ?

b) Montrer que P est inversible et calculer son inverse.

c) Calculer les puissances de D, puis **EN DÉDUIRE** que pour tout $n \in \mathbb{N}$:

$$A^n = \begin{pmatrix} (-1)^n & 2^n - (-1)^n & 2^n - (-1)^n \\ 2^n - (-1)^n & (-1)^n & (-1)^n - 2^n \\ (-1)^n - 2^n & 2^n - (-1)^n & 2 \times 2^n - (-1)^n \end{pmatrix}.$$

3) On note $(u_n)_{n\in\mathbb{N}}$, $(v_n)_{n\in\mathbb{N}}$ et $(w_n)_{n\in\mathbb{N}}$ les suites définies par : $u_0 = v_0 = w_0 = 1$ et pour tout $n \in \mathbb{N}$:

$$\begin{cases} u_{n+1} = -u_n + 3v_n + 3w_n \\ v_{n+1} = 3u_n - v_n - 3w_n \\ w_{n+1} = -3u_n + 3v_n + 5w_n. \end{cases}$$

Déterminer une expression explicite de u_n, v_n et w_n en fonction de n pour tout $n \in \mathbb{N}$.

3

1) On pose pour tous $a,b\in\mathbb{C}$: $\quad M(a,b)=\begin{pmatrix}a-b & b & -a\\ a-b & b & -a\\ 2a-b & -a+b & -a\end{pmatrix}$ et $\quad \mathrm{e}^{M(a,b)}=I_3+M(a,b)+\dfrac{M(a,b)^2}{2}$.

On note en outre $\mathscr{M}$ l'ensemble des matrices $M(a,b)$ et $\mathscr{G}$ l'ensemble des matrices $\mathrm{e}^{M(a,b)}$, a et b décrivant $\mathbb{C}$.

a) Compléter pour tous $a,b,c,d\in\mathbb{C}$: $\quad M(a,b)+M(c,d)=M(\dots\,,\dots)$ $\quad$ et $\quad M(a,b)\times M(c,d)=M(\dots\,,\dots)$. Que vaut $M(a,b)^3$ pour tous $a,b\in\mathbb{C}$?

b) Montrer que pour tous $A,B\in\mathscr{M}$: $\quad \mathrm{e}^{A+B}=\mathrm{e}^A\mathrm{e}^B$.

c) En déduire l'inclusion : $\quad \mathscr{G}\subset \mathrm{GL}_3(\mathbb{C})$.

d) Montrer que $\mathscr{G}$ est un sous-groupe de $\mathrm{GL}_3(\mathbb{C})$.

2) On rappelle qu'une matrice $A\in\mathscr{M}_n(\mathbb{C})$ est *nilpotente* si : $\quad A^p=0$ $\quad$ pour un certain $p\in\mathbb{N}^*$, et que le plus petit de ces entiers p est appelé l'*indice de nilpotence de A*. On appelle dans ce cas *exponentielle de A* la matrice : $\quad \mathrm{e}^A=\displaystyle\sum_{k=0}^{p-1}\frac{A^k}{k!}$.

Soient $A,B\in\mathscr{M}_n(\mathbb{C})$ deux matrices nilpotentes qui commutent d'indices de nilpotence respectifs p et q.

a) Montrer que $A+B$ est nilpotente d'indice inférieur ou égal à $p+q-1$.

b) Montrer l'égalité : $\quad \mathrm{e}^{A+B}=\mathrm{e}^A\mathrm{e}^B$ $\quad$ en calculant de deux façons la somme : $\quad \displaystyle\sum_{k=0}^{p+q-2}\frac{(A+B)^k}{k!}$.

---

4 On s'intéresse dans ce problème à l'*équation de Mordell* : $\quad y^2=x^3-6$ $\quad$ d'inconnue $(x,y)\in\mathbb{Z}^2$. On **admettra** dans la question **1)** le résultat important suivant — démontré dans la question **2)** :

> **Théorème** **(Loi complémentaire de Gauss)** Soit p un nombre premier impair. Si 2 est un carré modulo p, autrement dit si : $\quad \exists\, n\in\mathbb{Z}/\quad 2\equiv n^2\ [p]$, $\quad$ alors p est congru à 1 ou -1 modulo 8.
>
> La réciproque est vraie, mais ne sera ni utilisée ni démontrée dans ce problème.

1) Résolution de l'équation de Mordell étudiée : Soit $(x,y)\in\mathbb{Z}^2$. On fait l'hypothèse que : $\quad y^2=x^3-6$.

a) Montrer que x et y sont impairs.

b) En déduire que : $\quad x\equiv -1\ [8]$.

c) Montrer que tout diviseur premier de y^2-2 est congru à 1 ou -1 modulo 8.

d) Conclure. On pourra commencer par factoriser y^2-2 par $x-2$.

2) Démonstration de la loi complémentaire de Gauss : Soit p un nombre premier impair fixé. On pose : $\quad r=\dfrac{p-1}{2}$.

On note en outre $2\mathbb{Z}$ l'ensemble des entiers relatifs pairs et $2\mathbb{Z}+1$ l'ensemble des entiers relatifs impairs.

a) Montrer que l'application $k\longmapsto p-k$ est bijective de $[\![1,r]\!]\cap(2\mathbb{Z}+1)$ sur $[\![r+1,p-1]\!]\cap 2\mathbb{Z}$.

b) En déduire que : $\quad \displaystyle\prod_{k=1}^{r}\big((-1)^k k\big)\equiv 2^r r!\ [p]$.

c) En déduire que : $\quad 2^r\equiv(-1)^{\frac{r(r+1)}{2}}\ [p]$.

d) On suppose à présent que 2 est un carré modulo p. Montrer, grâce au petit théorème de Fermat, que p est congru à 1 ou -1 modulo 8.

3) Une autre application de la loi complémentaire de Gauss : Montrer que l'ensemble des nombres premiers congrus à -1 modulo 8 est infini. On pourra s'intéresser à un entier de la forme $(p_1\dots p_r)^2-2$ pour certains $p_1,\dots,p_r\in\mathbb{N}^*$.
