DEVOIR SURVEILLÉ

1

1) Montrer pour tous $a, b \in \mathbb{N}$ premiers entre eux, $2a^2 - b^2$ n'est pas divisible par 3.

2) En déduire que pour tous $(a,b) \in \mathbb{N}^2 \setminus \{(0,0)\}$, $v_3\big(2a^2 - b^2\big)$ est pair.

3) Résoudre l'équation diophantienne : $x^2 + 3y^2 = 2z^2$ d'inconnue $(x,y,z) \in \mathbb{N}^3$.

2

On pose : $A = \begin{pmatrix} 3 & 1 & -3 \\ 2 & 4 & -6 \\ 1 & 1 & -1 \end{pmatrix}$. On souhaite calculer les puissances de A de deux façons différentes.

1) a) Déterminer deux réels λ et μ pour lesquels : $A^2 = \lambda A + \mu I_3$.

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

c) Montrer l'existence de deux suites $(\lambda_n)_{n\in\mathbb{N}}$ et $(\mu_n)_{n\in\mathbb{N}}$ de réels pour lesquelles pour tout $n \in \mathbb{N}$: $A^n = \lambda_n A + \mu_n I_3$.

d) Déterminer une expression explicite de λ_n et μ_n en fonction de n pour tout $n \in \mathbb{N}$.

e) En déduire une expression explicite coefficient par coefficient de A^n pour tout $n \in \mathbb{N}$.

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

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

On pose : $X_1 = \begin{pmatrix} -1 \\ 1 \\ 0 \end{pmatrix}$, $X_2 = \begin{pmatrix} 3 \\ 0 \\ 1 \end{pmatrix}$ et $X_3 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$ et on note P la matrice de $\mathcal{M}_3(\mathbb{R})$ de colonnes X_1, X_2, X_3.

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

d) Montrer que pour une certaine matrice triangulaire $T \in \mathcal{M}_3(\mathbb{R})$ à préciser : $AP = PT$.

e) Pourquoi T est-elle inversible ? Calculer T^n pour tout $n \in \mathbb{N}$.

f) Retrouver enfin le résultat de la question **1)e)**.

g) Avez-vous compris de quelle manière les colonnes X_1 et X_2 ont été choisies et quel impact cela a eu dans les calculs qui ont suivi ?

3

On note $\mathbb{H}$ l'ensemble des matrices $\begin{pmatrix} \overline{u} & -\overline{v} \\ v & u \end{pmatrix}$ de $\mathcal{M}_2(\mathbb{C})$, u et v décrivant $\mathbb{C}$. Les éléments de $\mathbb{H}$ sont appelés les *quaternions*.
On introduit également quatre matrices importantes : $E = I_2$, $I = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, $J = \begin{pmatrix} 0 & \mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix}$ et $K = \begin{pmatrix} -\mathrm{i} & 0 \\ 0 & \mathrm{i} \end{pmatrix}$.
On pose enfin : $\mathcal{Q} = \{ \pm E, \pm I, \pm J, \pm K \}$ — où la lettre « $\mathcal{Q}$ » est un « Q » cursif.

1) a) Montrer que $\mathbb{H}$ est un sous-anneau de $\mathcal{M}_2(\mathbb{C})$.

b) Déterminer l'ensemble $\mathrm{U}(\mathbb{H})$ des éléments inversibles de $\mathbb{H}$.

2) a) Montrer que $\mathcal{Q}$ est stable par produit.

b) Montrer que $\mathcal{Q}$ est un sous-groupe de $\mathrm{U}(\mathbb{H})$.

c) L'anneau $\mathbb{H}$ est-il un corps ?

3) a) Montrer que tout quaternion s'écrit d'une et une seule manière sous la forme $xE + yI + zJ + tK$ avec $x, y, z, t \in \mathbb{R}$.

b) Montrer que l'ensemble $\mathscr{C}$ des matrices $xE + yI$, x et y décrivant $\mathbb{R}$, est un sous-anneau commutatif de $\mathbb{H}$.

L'ensemble $\mathscr{C}$ peut être vu comme une copie de $\mathbb{C}$ à l'intérieur de $\mathbb{H}$ de même que l'ensemble des matrices scalaires xE, x décrivant $\mathbb{R}$, peut y être vu comme une copie de $\mathbb{R}$. Les quaternions, en ce sens, sont une généralisation des nombres complexes.

4) Pour tout $M = xE + yI + zJ + tK \in \mathbb{H}$ avec $x, y, z, t \in \mathbb{R}$, on appelle *norme de* M et on note $\|M\|$ le réel positif $\sqrt{x^2+y^2+z^2+t^2}$, et on dit que M est *unitaire* si : $\|M\| = 1$.

a) Simplifier $\det(M)$ pour tout $M \in \mathbb{H}$, puis montrer que pour tous $M, N \in \mathscr{M}_2(\mathbb{C})$: $\det(MN) = \det(M)\det(N)$.

b) Montrer que l'ensemble $\mathscr{U}$ des quaternions unitaires est un sous-groupe de $\mathrm{GL}_2(\mathbb{C})$.

5) On note $\mathrm{Z}(\mathbb{H})$ le *centre de* $\mathbb{H}$, i.e. l'ensemble des éléments de $\mathbb{H}$ qui commutent à tout élément de $\mathbb{H}$. Montrer que : $\mathrm{Z}(\mathbb{H}) = \left\{xE\right\}_{x\in\mathbb{R}}$.

Les quaternions, création du mathématicien Hamilton au XIX$^{\text{ème}}$ siècle, sont à l'espace ce que les nombres complexes sont au plan. De même qu'on peut voir les objets naturels de la géométrie plane comme des nombres et faire de la géométrie plane une théorie du calcul dans $\mathbb{C}$, on peut voir les objets naturels de la géométrie dans l'espace comme des quaternions et faire de la géométrie dans l'espace une théorie du calcul dans $\mathbb{H}$. Le groupe $\mathscr{U}$ est par exemple à l'espace ce que le groupe $\mathbb{U}$ est au plan. Alors que $\mathbb{U}$ décrit les rotations du plan, $\mathscr{U}$ décrit celles de l'espace, mais vos connaissances actuelles ne nous permettent pas d'approfondir cette idée.

4

1) Ordre d'un entier modulo un autre entier : Soient $b \in \mathbb{N}^*$ et $a \in \mathbb{Z}$ premiers entre eux.

On pose : $E = \left\{k \in \mathbb{N}^* / \quad a^k \equiv 1\ [b]\right\}$.

a) Montrer que E possède un plus petit élément e appelé l'*ordre de* a *modulo* b.

b) Montrer l'égalité : $E = e\mathbb{N}^*$. On pourra notamment étudier la division euclidienne de k par e pour tout $k \in E$.

c) Montrer que si b est un nombre premier : $b \equiv 1\ [e]$.

En résumé, l'ordre de a modulo b divise tout entier $k \in \mathbb{N}$ pour lequel : $a^k \equiv 1\ [b]$.

2) Exemples : Calculer l'ordre de 2 modulo 7 et celui de 5 modulo 13.

3) Une première application : On souhaite résoudre l'équation diophantienne : $3^m - 2^n = 1$ ★ d'inconnue $(m,n) \in \mathbb{N}^2$.

a) Déterminer toutes les solutions d'★ pour lesquelles : $n \leqslant 3$.

On se donne à présent un couple (m,n) solution d'★ pour lequel : $n \geqslant 4$.

b) Calculer l'ordre de 3 modulo 16. Qu'en déduit-on sur m ?

c) Conclure en raisonnant modulo 5.

4) Une deuxième application : On souhaite montrer à présent qu'un entier $n \geqslant 2$ ne divise jamais $2^n - 1$.

Raisonnant par l'absurde, on se donne un entier $n \geqslant 2$ pour lequel $2^n - 1$ est divisible par n. On note p le plus petit diviseur premier de n et e l'ordre de 2 modulo p.

Montrer que : $e = 1$, puis conclure.

5) Une troisième application : On fixe enfin un nombre premier p et on pose pour tout $n \in \mathbb{N}$: $x_n = 2^{p^n} - 1$.

a) Exprimer x_{n+1} en fonction de x_n pour tout $n \in \mathbb{N}$, puis montrer que x_n divise x_{n+1}.

b) Montrer que pour tout $n \in \mathbb{N}$ et pour tout diviseur d de x_n : $\dfrac{x_{n+1}}{x_n} \equiv p\ [d]$.

c) Montrer que pour tout $n \in \mathbb{N}$: $x_n \equiv 1\ [p]$.

d) En déduire que x_n et $\dfrac{x_{n+1}}{x_n}$ sont premiers entre eux pour tout $n \in \mathbb{N}$.

e) Montrer que pour tout $n \in \mathbb{N}$ et pour tout diviseur d de $\dfrac{x_{n+1}}{x_n}$, l'ordre de 2 modulo d vaut p^{n+1}.

f) En déduire que pour tout $n \in \mathbb{N}^*$, il existe une infinité de nombres premiers congrus à 1 modulo p^n.
