Mines d'Albi ...
2010 , épreuve spécifique MPSI
problème 2

rappel sur les nombres premiers:
tous les entiers sont des entiers positifs
un nombre premier est un entier ayant exactement 2 diviseurs 1 et lui même
1 n'est pas premier
Il existe une infinité de nombres premiers
Si p divise mes entiers x et y , p divise $x+y, x-y$ et kx pour tout entier k .
Tout entier $x>1$ se décompose de façon unique en un produit de facteurs premier :

$$x=\prod_{i=1}^{k} p_i^{\alpha_i} \text{ avec pour tout } i \text{ , } p_i \text{ premier et } \alpha_i \in \mathbb{N}^*$$

En regardant la décomposition de xy on constate que si p est un facteur premier de xy , c'est un facteur premier de x ou y .

1. On revient à la définition par factoriels :

$$k\binom{p}{k}=k\frac{p!}{k!(p-k)!}=\frac{p!}{(k-1)!(p-k)!}=p.\frac{(p-1)!}{(k-1)!((p-1)-(k-1))!}=p\binom{p-1}{k-1}$$

la formule est vraie pour tout entier p et $k \in [[1,p]]$
On a de plus que p est premier et $k<p$, donc p n'est pas un facteur de la décomposition en facteurs premiers de k .
Mais p est un facteur de $p\binom{p-1}{k-1}=k\binom{p}{k}$, donc p est un facteur premier de $\binom{p}{k}$

$$\boxed{\forall p \in \mathcal{P}, \forall k \in [[1,p-1]], p|\binom{p}{k}}$$

2. on pose $H_a : \forall p \in \mathcal{P}$, $p|(a^p-a)$
   - vrai si $a=0$ et $a=1$:$p|0$
   - si p divise a^p-a on écrit :

$$\begin{aligned}(a+1)^p-(a+1) &= \sum_{k=0}^{p}\binom{p}{k}a^k-a-1 \\ &= \sum_{k=1}^{p-1}\binom{p}{k}a^k+(a^p-a)+(1-1)\end{aligned}$$

   p divise chaque terme du Σ par la question 21 et le dernier terme par l'hypothèse de récurrence.:$p|\left((a+1)^p-(a+1)\right.$

$$\boxed{\forall p \in \mathcal{P}, \forall a \in \mathbb{N} \text{ , } p|a^p-a}$$

3. Le résultat admis peut se vérifier par le calcul en développant le déterminant 3×3.
   On sait que $\det(M^p)=\det(M)^p$.
   - On peut appliquer la question 22 à $a=|\det(M)|$ et dire que p divise $|\det(M^p)|-|\det(M)|$ .p divise aussi $\det(M)^p$ donc $|\det(M)^p|$ et donc p divise $|\det(M)|$
     $|\det(M)|$ est donc divisible par tous les nombres premiers , donc $|\det(M)|=0$ (si $|\det(M)|\neq 0$, prendre p premier ,$p>|\det(M)|$ on a une absurdité).

   Réciproquement si $\det(M)=0, \det(M)=p.0$ donc est divisible par p.

$$\forall M \in \mathcal{M}_3(\mathbb{Z}), (\forall p \in \mathcal{P} \text{ , } p|\det(M^p)) \Rightarrow M \text{ non inversible}$$

4. On pose $A=\begin{pmatrix}1&0&0\\0&0&0\\0&0&0\end{pmatrix}$, $B=\begin{pmatrix}0&0&0\\0&1&0\\0&0&1\end{pmatrix}$, $C=\begin{pmatrix}0&0&0\\0&0&1\\0&-1&0\end{pmatrix}$, on a $\mathcal{A}=Vect(A,B,C)$ qui est un sous vectoriel.
   On vérifie qua $aA+bB+cC=0 \Rightarrow a=b=c=0$. La famille est libre et génératrice de $\mathcal{A}$, c'est une base

$$\boxed{\mathcal{A} \text{ est un espace vectoriel de dimension 3}}$$

5. $\mathcal{A}$ est un sous ensemble de l'anneau $\mathcal{M}_3(\mathbb{R})$ non vide stable par différence (c'est un espace vectoriel) et stable par produit :

$$\begin{pmatrix} a & 0 & 0 \\ 0 & b & c \\ 0 & -c & b \end{pmatrix}.\begin{pmatrix} a' & 0 & 0 \\ 0 & b' & c' \\ 0 & -c' & b' \end{pmatrix} = \begin{pmatrix} aa' & 0 & 0 \\ 0 & bb'-cc' & bc'+b'c \\ 0 & -(bc'+b'c) & bb'-cc' \end{pmatrix} = \begin{pmatrix} a" & 0 & 0 \\ 0 & b" & c" \\ 0 & -c" & b" \end{pmatrix}$$

avec $a" = aa', b" = bb' - cc', c" = bc' + cb'$.

De plus $\mathcal{A}$ contient I_3 $(a = b = 1, c = 0)$

Enfin la symétrie des formules donne

$$\begin{pmatrix} a & 0 & 0 \\ 0 & b & c \\ 0 & -c & b \end{pmatrix}.\begin{pmatrix} a' & 0 & 0 \\ 0 & b' & c' \\ 0 & -c' & b' \end{pmatrix} = \begin{pmatrix} a' & 0 & 0 \\ 0 & b' & c' \\ 0 & -c' & b' \end{pmatrix}\begin{pmatrix} a & 0 & 0 \\ 0 & b & c \\ 0 & -c & b \end{pmatrix}.$$

$\boxed{\mathcal{A} \text{ est un anneau commutatif.}}$

6. $\mathcal{A}$ contient I_3 $(a = b = 1, c = 0), M(c = b = 1, a = -2)$ et $M^2 = \begin{pmatrix} 4 & 0 & 0 \\ 0 & 0 & 2 \\ 0 & -2 & 0 \end{pmatrix}$. De plus ces 3 matrices forment un système libre : Si

$$xI_3 + yM + zM_2 = 0$$

on a le système linéaire : $\begin{cases} x - 2y + 4z = 0 \\ x + y = 0 \\ y + 2z = 0 \end{cases}$ donc $\begin{cases} x - 2y + 4z = 0 \\ x = -y \\ z = -y/2 \end{cases}$ donc $y = 0, x = 0, z = 0$

On a une famille libre de 3 éléments dans un espace de dimension 3 , c'est une base.

On peut aussi dire $Mat_{(A,B,C)}\left(I_3, M, M^2\right) = \begin{pmatrix} 1 & -2 & 4 \\ 1 & 1 & 0 \\ 0 & 1 & 2 \end{pmatrix}$ *de déterminant non nul.*

7. $M^3 = \begin{pmatrix} -8 & 0 & 0 \\ 0 & -2 & 2 \\ 0 & -2 & -2 \end{pmatrix} = 2M - 4I_3$ (après calcul)

8. On sait que $\mathcal{A}$ est une algèbre donc si $\mathcal{A}$ contient M et M^k , $\mathcal{A}$ contient M^{k+1} . Or $\mathcal{A}$ contient M^0 et M^1 . Donc par récurrence $\mathcal{A}$ contient M^k pour tout entier k . Les coefficients a_k, b_k, c_k sont les coordonnées de M^k dans la base (A, B, C)

9. On pose $M.M^k = M^{k+1}$: $\begin{cases} a_{k+1} = -2a_k \\ b_{k+1} = b_k - c_k \\ c_{k+1} = b_k + c_k \end{cases}$

10. (a_k) est géométrique de raison -2 et $a_0 = 1$ donc :

$$\boxed{\forall k \in \mathbb{N}, a_k = (-2)^k}$$

11. On a $z_{k+1} = (1 + i)z_k$ suite géométrique de premier terme 1 et donc $z_k = (1 + i)^k$. Et donc comme b_k et c_k sont réels :

$$\boxed{b_k = \mathrm{Re}((1 + i)^k), c_k = \mathrm{Im}((1 + i)^k)}$$

12. On peut aussi dire que $c_k = -b_{k+1} + b_k$ et donc $(b_{k+1} - b_{k+2}) = b_k + (b_k - b_{k+1})$ soit

$$b_{k+2} = 2b_{k+1} - 2b_k$$

On a une suite linéaire récurrente double , d'équation caractéristique $r^2 - 2r + 2 = 0$ donc de racine $1 \pm i$. Donc b_k s'écrit $\lambda(1 + i)^k + \mu(1 - i)^k$, comme $b_0 = 1$ et $b_1 = 1$, on a $b_k = \dfrac{(1 + i)^k + (1 - i)^k}{2} = \mathrm{Re}((1 + i)^k)$

13. Comme la trace est linéaire (vérification évidente) et comme $M^3 = 2M - 4I_3$ on a $M^{k+3} = 2M^{k+1} - 4M^k$ donc $Tr(M^{k+3}) = 2Tr(M^{k+1}) - 4Tr(M^k)$.

(u_k) et $(Tr(M_k))$ vérifie la même relation de récurrence et les mêmes conditions initiales pour $k = 0, 1, 2$. les 2 suites sont donc égales..

14. On a donc

$$\forall p \in \mathcal{P}\ ,\ u_p = Tr(M^p) = (-2)^p + 2\,\mathrm{Re}\left((1+i)^p\right)$$

Or

$$\mathrm{Re}\left((1+i)^p\right) = \mathrm{Re}\left(\sum_{k=0}^{p}\binom{p}{k}i^k\right) = \sum_{k=0,k\text{ pair}}^{p}(-1)^{k/2}\binom{p}{k}$$

On sépare en 2 cas :

- si $p = 2$, $u_2 = 4$ est divisible par 2
- si $p > 2$, p est impair donc dans la somme $\sum_{k=0,k\text{ pair}}$, $k = p$ est impossible. D'après la question 21 tous les termes de la somme sauf le premier sont divisibles par p.

On écrit alors comme $(-2)^p = -2^p$:

$$u_p = -2^p + 2 + 2\sum_{k=1,k\text{ pair}}^{p}(-1)^{k/2}\binom{p}{k}$$

le premier terme est alors aussi divisible par p d'après la question 22 pour $a = 2$.

$$\boxed{\forall p \in \mathcal{P}\ ,\ p|u_p}$$

15. On a $\det_{(i,j,k)}(e_i) = \begin{vmatrix} 1 & 2 & -1 \\ 2 & 1 & 1 \\ -1 & 0 & 2 \end{vmatrix} = -9 \neq 0$. on a donc une base

16. On a $u^k(e_i) = \lambda_i^k e_i$ donc

$$c(u^k) = \sum_{i=1}^{3}\lambda_i^k\left\|e_i\right\|^2 = 6\lambda_1^k + 5\lambda_2^k + 6\lambda_3^k$$

17. On suppose que p premier divise $c\left(u^p\right) = 6\lambda_1^p + 5\lambda_2^p + 6\lambda_3^p$. Or d'après la question 22, les λ_i étant entiers positifs, p divise tous les $\lambda_i^p - \lambda_i$. donc p divise $6\lambda_1 + 5\lambda_2 + 6\lambda_3$.

    Comme p est un entier premier quelconque, on en déduit comme à la question 23 que $6\lambda_1 + 5\lambda_2 + 6\lambda = 0$.

18. On a une somme nulle de réels positifs, donc chaque terme est nul : $\lambda_1 = \lambda_2 = \lambda_3 = 0$. Donc $Mat(u) = 0$ et donc $\boxed{u \text{ est nul}}$