PROBLÈME 2

Définitions et notations : on désigne par $\mathscr{P}$ l'ensemble des nombres premiers : $\mathscr{P} = \{2,3,5,7,11,\cdots\}$.
Si n et p sont deux entiers naturels, on note $n \mid p$ lorsque n divise p.

On désigne par $\mathscr{M}_3(\mathbb{R})$ l'ensemble des matrices carrées de taille 3 à coefficients réels. On note I_3 la matrice identité de $\mathscr{M}_3(\mathbb{R})$.
Si $M = \begin{pmatrix} a & \star & \star \\ \star & b & \star \\ \star & \star & c \end{pmatrix} \in \mathscr{M}_3(\mathbb{R})$, le réel $a+b+c$ est appelé trace de M et noté $\mathrm{tr}(M)$.

Les parties de ce problème sont dépendantes mais le candidat pourra admettre les résultats qui y sont montrés pour aborder une partie suivante.

Théorème de Fermat

21) Soit $p \in \mathscr{P}$ et soit k entier avec $1 \leq k \leq p-1$. Montrer que :

$$k\binom{p}{k} = p\binom{p-1}{k-1}$$

et en déduire que :

$$p \mid \binom{p}{k}$$

22) Montrer que :

$$\forall a \in \mathbb{N}, \quad \forall p \in \mathscr{P}, \qquad p \mid (a^p - a)$$

On pourra raisonner par récurrence sur a.

On note, pour M dans $\mathscr{M}_3(\mathbb{R})$, $\det(M)$ le déterminant de M et on admettra que si M est à coefficients entiers, $\det(M)$ est un entier.
23) Montrer que les matrices M de $\mathscr{M}_3(\mathbb{R})$ à coefficients entiers qui vérifient

$$\forall p \in \mathscr{P}, \qquad p \mid \det(M^p)$$

sont exactement les matrices non inversibles à coefficients entiers.

Étude d'un ensemble de matrices

On note $\mathscr{A}$ l'ensemble :

$$\mathscr{A} = \left\{ \begin{pmatrix} a & 0 & 0 \\ 0 & b & c \\ 0 & -c & b \end{pmatrix}, \quad (a,b,c) \in \mathbb{R}^3 \right\}$$

24) Montrer que $\mathscr{A}$ est un $\mathbb{R}$-espace vectoriel. Quelle est la dimension de cet espace ?
25) Montrer que $\mathscr{A}$ est un anneau commutatif.

Dans la suite de ce problème, on désigne par M la matrice : $M = \begin{pmatrix} -2 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & -1 & 1 \end{pmatrix}$.

26) Justifier que (I_3, M, M^2) est une base de $\mathscr{A}$.
27) Exprimer M^3 en fonction de I_3 et M.

Étude d'une suite

Dans cette partie, on désigne par u la suite définie par :

$$u_0 = 3, \qquad u_1 = 0, \qquad u_2 = 4, \qquad \forall n \in \mathbb{N},\ u_{n+3} = 2u_{n+1} - 4u_n$$

On se propose de montrer que $\forall p \in \mathscr{P}$, $p \mid u_p$.

On pose, pour $k \in \mathbb{N}$, $M^k = \begin{pmatrix} a_k & 0 & 0 \\ 0 & b_k & c_k \\ 0 & -c_k & b_k \end{pmatrix}$.

28) Justifier, pour $k \in \mathbb{N}$, l'existence de a_k, b_k et c_k.

29) Trouver une relation de récurrence vérifiée par la suite (a_k) seule et deux relations de récurrence liant les suites (b_k) et (c_k).

30) En déduire, pour k dans $\mathbb{N}$, a_k en fonction de k.

31) Pour $k \in \mathbb{N}$, on appelle z_k le nombre complexe $z_k = b_k + ic_k$ avec $i^2 = -1$.
Exprimer z_{k+1} en fonction de z_k et montrer que $b_k = \mathrm{Re}\big((1+i)^k\big)$.

32) Retrouver ce dernier résultat en trouvant une relation de récurrence vérifiée par la suite (b_k).

33) Justifier que :

$$\forall n \in \mathbb{N}, \qquad u_n = \mathrm{tr}(M^n)$$

34) Montrer que :

$$\forall p \in \mathscr{P}, \qquad p \mid u_p$$

Étude d'un coefficient

Dans cette partie, on pose $e_1 = (1,2,-1)$, $e_2 = (2,1,0)$ et $e_3 = (-1,1,2)$.

On munit $\mathbb{R}^3$ de son produit scalaire usuel :
si $X = (x,y,z)$ et $X' = (x',y',z')$ sont dans $\mathbb{R}^3$, on pose $(X|X') = xx' + yy' + zz'$.
Si u est un endomorphisme de $\mathbb{R}^3$, on pose $c(u) = (u(e_1)|e_1) + (u(e_2)|e_2) + (u(e_3)|e_3)$.

35) Montrer que (e_1,e_2,e_3) est une base de $\mathbb{R}^3$ notée $\mathscr{B}$.

Jusqu'à la fin de ce problème, u désigne un endomorphisme de $\mathbb{R}^3$, dont la matrice dans la base $\mathscr{B}$ est :

$$\mathrm{diag}(\lambda_1,\lambda_2,\lambda_3) = \begin{pmatrix} \lambda_1 & 0 & 0 \\ 0 & \lambda_2 & 0 \\ 0 & 0 & \lambda_3 \end{pmatrix}$$

où λ_1, λ_2 et λ_3 sont des entiers naturels.

36) Que vaut $c(u)$ et plus généralement $c(u^k)$ pour $k \in \mathbb{N}$?

37) On suppose que :

$$\forall p \in \mathscr{P}, \qquad p \mid c(u^p)$$

En utilisant la question 22), montrer que u est nul.