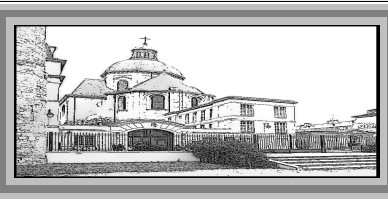
LYCEE CHARLEMAGNE
Vendredi 7 février
M.P.S.I.2



2024 2025

DS06

♡ 0 ♡ Exercice : un élève dit « le produit de deux matrices symétriques est symétrique ». Montrez qu'il a tort. [1 pt.] Maintenant qu'il sait qu'il a tort, il déduit « le carré d'une matrice symétrique n'est donc pas symétrique ». Montrez que là à nouveau, il a tort. [1 pt.]

Rappel : une matrice carrée A est symétrique si elle vérifie $A^T = A$.

♣ 0 ♣ Trouvez le maximum d'entiers n tels que $\sqrt{n^2 + 2025.n}$soit aussi entier ? [4 pt.]

Indication : $(2.n + 2025)^2 - (2025)^2$.

♣ 1 ♣ Le nombre 294001 est premier, mais très particulier.
Si on change un (et un seul) de ses chiffres, on obtient toujours un nombre composé (c'est à dire non premier).

Exemple : $494001 = 3^2.131.419$, $234001 = 29.8069$, $294501 = 3.89.1103$, $294003 = 3^3.10889$.

Première question : combien existe-t-il d'entiers à tester où on change un et un seul de ses chiffres ? [1 pt.]
Oui, ça fait beaucoup. Il faudrait un programme, non ?

Suivant votre niveau : vous disposez d'une fonction est_premier qui retourne un booléen True ou False suivant si le nombre entré est premier ou composé.
Convertir un entier `n` *en string :* `str(n)`.
Convertir un string `s` *en liste :* `list(s)`.
Convertir une liste de `char` *en* `int` *: y'a pas direct, considérez qu'il y a si vous voulez, et sinon recréez la.*

Inspiré de banque concours commune filière PT
Mathématiques A 2011

Les diverses parties sont assez indépendantes les unes des autres.

I∼0) On note $M_2(\mathbb{Z})$ l'ensemble des matrices carrées de taille 2 sur 2 à coefficients entiers relatifs et on note $SL_2(\mathbb{Z})$ l'ensemble des matrices de $M_2(\mathbb{Z})$ inversibles, dont l'inverse est aussi dans $M_2(\mathbb{Z})$.

Montrez que $\begin{pmatrix} 1 & 2 \\ 1 & 3 \end{pmatrix}$ et $\begin{pmatrix} 5 & 2 \\ 8 & 3 \end{pmatrix}$ sont dans $SL_2(\mathbb{Z})$. [1 pt.]

∼0) Montrez que $(SL_2(\mathbb{Z}), .)$ est un groupe, non commutatif. [3 pt.]

∼1) Montrez que si M est dans $SL_2(\mathbb{Z})$, l'ensemble $\{M^k \mid k \in \mathbb{Z}\}$ est un sous-groupe de $(SL_2(\mathbb{Z}), .)$, qu'on notera $< M >$. [2 pt.]

∼2) Montrez qu'une matrice M de $M_2(\mathbb{Z})$ est dans $SL_2(\mathbb{Z})$ si et seulement si son déterminant vaut 1 ou -1. [2 pt.]

∼3) Combien de matrices de la forme $\begin{pmatrix} 5 & \\ & 1 \end{pmatrix}$ sont dans $SL_2(\mathbb{Z})$. [1 pt.]

I∼0) Montrez pour toute matrice carrée M de taille 2 : $M^2 = Tr(M).M - \det(M).I_2$. [1 pt.]

I∼1) Déduisez que pour toute matrice M, l'ensemble$< M >$ est inclus dans $Module(I_2,\ M)$ [1]. [2 pt.]

II∼0) Montrez que $(A, B) \longmapsto Tr(A^T.B)$ est un produit scalaire sur $M_2(\mathbb{R})$, qu'on notera $(A,\ B) \longmapsto \varphi(A, B)$. [2 pt.]

II∼1) Montrez que $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ et $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ sont dans $SL_2(\mathbb{Z})$ et sont orthogonales entre elles. [1 pt.]

---

1. le $\mathbb{Z}-$module engendré par une famille $(A_1, \dots A_k)$ de matrices est l'ensemble des combinaisons linéaires $\sum_{i=1}^{k} \alpha_i.A_i$ quand $(\alpha_1, \dots \alpha_k)$ décrit $\mathbb{Z}^k$

II∼2) Existe-t-il dans $SL_2(\mathbb{Z})$ des éléments orthogonaux à la fois à $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ et $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$? 1 pt.

II∼3) Pouvez vous trouver dans $SL_2(\mathbb{Z})$ une famille de quatre matrices deux à deux orthogonales ? 2 pt.

II∼4) Montrez que l'ensemble $SL_2(\mathbb{Z})$ n'est pas borné pour la norme issue de notre produit scalaire [2]. 1 pt.

III∼0) *On note $C_2(\mathbb{Z})$ l'ensemble des matrices M de $M_2(\mathbb{Z})$ pour lesquelles il existe au moins un entier non nul k vérifiant $M^k = I_2$* [3]. Montrez que $\begin{pmatrix} 3 & -1 \\ 7 & -2 \end{pmatrix}$ est dans $C_2(\mathbb{Z})$ et donnez son ordre. 2 pt.

III∼1) Montrez que tous les éléments de $C_2(\mathbb{Z})$ sont dans $SL_2(\mathbb{Z})$. 1 pt.

III∼2) Montrez que pour M dans $C_2(\mathbb{Z})$, M^{-1} et M^T sont aussi dans $C_2(\mathbb{Z})$, et exprimez leur ordre à l'aide de celui de M. 3 pt.

III∼3) Montrez que si M est dans $C_2(\mathbb{Z})$, d'ordre 3 alors M^2 est dans $C_2(\mathbb{Z})$, et également d'ordre 3. 1 pt.

III∼4) Montrez que si M est dans $C_2(\mathbb{Z})$, d'ordre 6 alors M^2 est dans (quel est son ordre ?). 1 pt.

III∼5) Montrez que $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ est dans $C_2(\mathbb{Z})$. Montrez que $C_2(\mathbb{Z})$ n'est stable ni par addition, ni par multiplication. 1 pt.

IV∼0) Soit M dans $C_2(\mathbb{Z})$. On note λ_1 et λ_2 ses valeurs propres, éventuellement complexes. En étudiant $M^n.U$ où U est un vecteur propre de valeur propre λ_i, montrez que λ_1 et λ_2 ont pour module 1. 2 pt.

IV∼1) Déduisez que $Tr(M)$ vaut $-2, -1, 0, 1$ ou 2. 1 pt.

IV∼2) Déduisez que les matrices de $C_2(\mathbb{Z})$ n'ont pour polynômes caractéristiques que les polynômes ci dessous :
$X^2 + 2.X + 1$ $X^2 + X + 1$ $X^2 - X + 1$ $X^2 - 2.X + 1$ $X^2 + 1$ $X^2 - 1$ 2 pt.

Pourquoi n'a-t-on pas $X^2 - 2.X - 1$? 1 pt.

IV∼3) Donnez un exemple de matrice M de $C_2(\mathbb{Z})$ pour chacun de ces polynômes. 1 pt.

Rappel : polynôme caractéristique de M (matrice carrée de taille d) : $\det(M - X.I_2)$.

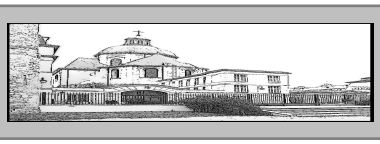
V∼0) *Dans ce qui suit, A est la matrice $\begin{pmatrix} 1 & 2 \\ 1 & 3 \end{pmatrix}$ et P est le plan contenant A et I_2, c'est à dire l'ensemble des matrices de la forme $\alpha.A + \beta.I_2$ avec α et β dans* $\mathbb{R}$. Montrez que ce plan est même un anneau pour l'addition et la multiplication usuelles. 2 pt.

V∼1) On pose alors $E_1 = \dfrac{I_2}{\sqrt{2}}$ et $E_2 = \dfrac{A - 2.I_2}{\sqrt{7}}$. Calculez $\varphi(I_2, I_2)$, $\varphi(I_2, A)$ et $\varphi(A, A)$ et enfin, calculez $\varphi(E_i,\ E_j)$ pour les quatre couples $(i,\ j)$. 3 pt.

V∼2) On se donne une matrice B dans $M_2(\mathbb{R})$. Montrez que $\varphi(B, E_1).E_1 + \varphi(B, E_2).E_2$ (notée H) est dans P. 1 pt.

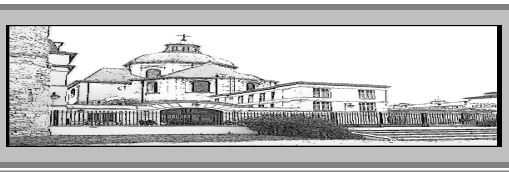
V∼3) Montrez pour toute matrice M de P : $\varphi(M - B,\ M - B)^2 = \varphi(M - H,\ M - H)^2 + \varphi(H - B,\ H - B)^2$. 2 pt.

V∼4) Déduisez : H est la matrice de P la plus proche de B (c'est à dire qui minimise la norme de $M - B$ quand M parcourt P). 2 pt.



2. un ensemble est borné si il existe K vérifiant $\forall M \in E,\ \sqrt{\varphi(M, M)} \leqslant K$
3. le plus petit de ces entiers non nuls k est appelé « ordre de M »

LYCEE CHARLEMAGNE
Vendredi 7 février
M.P.S.I.2



2024 2025
DS06
CORRECTION

DS06 Exerice sur les matrices symétriques.

Pour deviner ce qui ne passe pas : si on a $A^T = A$ et $B^T = B$, on n'a pas forcément $(A.B)^T = A.B$ puisqu'en fait $(A.B)^T = B^T.A^T = B.A$.

Mais ceci ne prouve rien. Il nous faut un contre-exemple, c'est tout.
On en propose un en taille 2 avec des matrices autres que I_2 et ses multiples, on s'en doute

$A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ est symétrique	$B = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ est symétrique	$A.B = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ n'est pas symétrique

Et ceci est mille fois mieux que $\begin{pmatrix} a & b \\ b & c \end{pmatrix} . \begin{pmatrix} \alpha & \beta \\ \beta & \gamma \end{pmatrix} = \begin{pmatrix} & a.\beta + b.\gamma \\ b.\alpha + c.\beta & \end{pmatrix}$ *car on apprend à réfléchir et pas juste à calculer.*

Mais attention, on a prouvé $\exists (A, B) \in (S_2)^2,\ A.B \notin S_2$.
Et pas $\forall (A, B) \in (S_2)^2,\ A.B \notin S_2$. On ne sait pas conclure pour $A = B$.
Et en fait, si A est symétrique, alors A^2 l'est aussi. En effet

$$(.A)^T = A^T.A^T = A.A$$

Et on n'a pas besoin de redescendre jusqu'aux coefficients.

DS06 Carré parfait $n^2 + 2025.n$.

On a des solutions, puisqu'avec $n = -2025$, la quantité $\sqrt{n^2 + 2025.n}$ est entière.
On l'a aussi avec $n = 0$.

$$\sqrt{(-2025)^2 + 2025.(-2025)} = 0 \text{ et } \sqrt{(0)^2 + 2025.0} = 0$$

Mais en a-t-on d'autres ?
On veut qu'il existe p dans $\mathbb{N}$ tel que $n^2 + 2025.n$ soit égal à p^2.
On reformule : $p^2 - n^2 = 2025.n$.
Et même $(p + n).(p - n) = 2025.n$.
Et en factorisant : $(p + n).(p - n) = 3^4.5^2.n$.

Peut on avoir par exemple $p + n = 2025$ et $p - n = n$? On trouve $p = 2.n$ et $3.n = 2025$ d'où $n = 675$ et $p = 1350$.
On vérifie :

$$\sqrt{675^2 + 675.2025} = \sqrt{675.(675 + 2025)} = \sqrt{3^3.5^2.3^3.10^2} = 1350$$

Peut on avoir $p + n = 675$ et $p - n = 3.n$? Oui, avec $n = 135$ et $p = 540$

$$\sqrt{135^2 + 135.2025} = \sqrt{135.(135 + 2025)} = \sqrt{(3^3.5).(2^4.3^3.5)} = 540$$

Encore des solutions : $p + n = 405$ et $p - n = 5.n$. Ah non pas là.

Si on a une approche informatique, on crée une fonction qui teste si un nombre est un carré parfait, puis on la met en boucle

```
L = [ ]
for n in range(10**4) : :
....if carreparfait(n*n+2025*n) :
........L.append(n)
```

Et pour la fonction de test de carré parfait dont certains sont des horreurs innommables de bas étage :

```
def carreparfait(n) :
....r = math.sqrt(n)
....if r == int(r) :
........return True
....else :
........return False
```

```
def carreparfait(n) :
....r = math.sqrt(n)
....return r == int(r)
```

```
def carreparfait(n) :
....r = math.sqrt(n)
....return n == int(r)**2
```

```
def carreparfait(n) :
....k = 0
....while k*k < n :
........k += 1
....return k*k == n
```

Et si on tenait compte de l'indication ?

$$(2.n + 2025)^2 - 2025^2 = 4.n^2 + 4.n.2025 = 4.(n^2 + n.2025)$$

4 étant le carré de 2, on voit que $(n^2 + n.2025)$ est un carré parfait si et seulement si $4.(n^2 + n.2025)$ est un carré parfait.

On va donc reprendre notre question : $(n^2 + n.2025)$ est un carré parfait si et seulement si il existe p vérifiant

$$(2.n + 2025)^2 - 2025^2 = p^2$$

L'équation devient

$$(2.n + 2025)^2 - p^2 = 2025^2$$

$$(2.n + 2025 + p).(2.n + 2025 - p) = 3^8.5^4$$

Et maintenant, on a des systèmes teles que $\begin{array}{lllllll} 2.n & +2025 & +p & = & 3^8 \\ 2.n & +2025 & -p & = & 5^4 \end{array}$, $\begin{array}{lllllll} 2.n & +2025 & +p & = & 3^7.5 \\ 2.n & +2025 & -p & = & 3.5^3 \end{array}$ et ainsi de suite.

On découpe 2025^2 en produit de deux facteurs $A.B$ (avec $A \geqslant B$) et on résout $\begin{array}{lllllll} 2.n & +2025 & +p & = & A \\ 2.n & +2025 & -p & = & B \end{array}$.

On a alors une solution.

Et de combien de façons peut on découper $3^8.5^4$ en $3^{8-a}.5^{4-b}$? Réponse 45.

On en garde la moitié à cause de la contrainte $A > B$. Et on a nos solutions.

[3, 135, 180, 576, 675, 784, 1620, 1815, 3267, 3600, 6615, 7220, 11664, 12675, 21780, 36963, 40000, 67335]

Je n'attendais pas que vous trouviez toutes le solutions.
Mais que vous donniez votre démarche pour en avoir.
Informatiquement.
Or arithmétiquement.

DS06 L'entier 294001.

Test en force brute pour savoir si un nombre est premier.
On fait défiler les entiers de `2` à `n` (`n` exclu) et on regarde si un d'entre eux divise `n`.

Si on en croise un, on sort tout de suite en disant « n n'es pas premier » (il a un diviseur propre).

Si on est arrivé au bout sans en croiser : « n est premier ».

```
def est_premier(n) :
....for d in range(2, n) :
........if n % d == 0 :
............return False
....return True
```

On peut dire aussi qu'il suffit de s'arrêter à $\sqrt{n}$ (si n admet un diviseur d plus grand que $\sqrt{n}$, alors $\frac{n}{d}$ est aussi un diviseur de n (puisque $\frac{n}{n/d} = d$), et lui il est plus petit que $\sqrt{n}$).

```
def est_premier(n) :
....for d in range(2, int(sqrt(n))+1) :
........if n % d == 0 :
............return False
....return True
```

Il faut bien sûr arrondit `sqrt(n)` en `int(sqrt(n))` pour le `range`. Et il faut ajouter `1` à cause du `range` (et même `2` par mesure de sécurité à cause d'éventuelles racines en `7.99999` qui vaudraient `8` mais seraient arrondies à `7`).

Et pour éviter de faire appel à la fonction `sqrt( )` qui nous fait quitter l'univers des entiers pour basculer dans le côté obscur des salles de TP, on crée un entier qui avance jusqu'à soit être un diviseur de `n`, soit avoir un carré trop grand (auquel cas on a atteint $\sqrt{n}$ effectivement). Il suffit de demander ensuite « on est sorti à cause d'un diviseur ou d'un nombre trop grand ? »).

```
def est_premier(n) :
....d = 2
....while (n%d != 0) and (d*d <= n) :
........d += 1
....return (n%qd) != 0
```

Chaque chiffre de l'entier peut être remplace par neuf autres chiffres.
Ensuite, ces neuf choix s'additionnent car on ne modifie qu'un chiffre à la fois.

Et pour des arbres multiplicatifs :
- quel chiffre modifie-t-on (unités, dizaines...) : six choix
- par quel autre chiffre le remplace-t-on : neuf choix

Total : 54 tests à effectuer.

> [94001, 194001, 394001, 494001, 594001, 694001, 794001, 894001, 994001, 204001, 214001, 224001, 234001, 244001, 254001, 264001, 274001, 284001, 290001, 291001, 292001, 293001, 295001, 296001, 297001, 298001, 299001, 294101, 294201, 294301, 294401, 294501, 294601, 294701, 294801, 294901, 294011, 294021, 294031, 294041, 294051, 294061, 294071, 294081, 294091, 294000, 294002, 294003, 294004, 294005, 294006, 294007, 294008, 294009]

Comment créer ces nombres ?
On part de l'entier `n` (ici `294001`), on en fait une liste de chiffres `list(str(n))`.

On va parcourir la liste de chiffres `for k in range(len(L))`.

A chaque fois, on parcourt les chiffres de `0` à `9`, sauf L[k] lui même

```
for c in range(10) :
....if c != int(L[k])
```

On crée une copie de la liste mais on remplace `L[k]` par `c`.
On l'ajoute la liste des solutions.

```
def variantes(n) :
....L = list(str(n))
....R = [ ] #les réponses
....for k in range(len(L)) :
........foc c in range(10) :
............if c != int(L[k]) :
................LL = L[ : ] # une copie
................LL[k] = str(c)
................R.append(LL[k])
....return R
```

Attention, ici la liste est faite de listes de caractères, comme
[['0', '9', '4', '0', '0', '1'], ['1', '9', '4', '0', '0', '1'], ['3', '9', '4', '0', '0', '1'], ['4', '9', '4', '0', '0', '1'], ['5', '9', '4', '0', '0', '1'], ['6', '9', '4', '0', '0', '1'], ['7', '9', '4', '0', '0', '1'], ...

Il faudra convertir en entiers, et tester ensuite.

```
def conv(LL) : #list of char -> int
....s = 0
....for c in LL :
........s = s*10 + int(c)
....return s
```

Et on peut alors lancer la batterie de tests de primalité.

Remarque de matheux :
on peut rester dans le brave univers des entiers sans passer par les chaines de caractères.
Comment transformer 294001 en 295001, 296001 et ainsi de suite ? En ajoutant 1000, 2000 et ainsi de suite.
Comment transformer 294001 en 293001, 292001 et ainsi de suite ? En soustrayant 1000, 2000 et ainsi de suite.

DS06 $SL_2(\mathbb{Z})$ est un groupe.

Les deux matrices $\begin{pmatrix} 1 & 2 \\ 1 & 3 \end{pmatrix}$ et $\begin{pmatrix} 5 & 2 \\ 8 & 3 \end{pmatrix}$ sont à coefficients dans $\mathbb{Z}$, inversibles, et ont pour inverses $\begin{pmatrix} 3 & -2 \\ -1 & 1 \end{pmatrix}$ et $\begin{pmatrix} -3 & 2 \\ 8 & -5 \end{pmatrix}$ elles aussi à coefficients dans $\mathbb{Z}$.
Ce sont donc des éléments de $SL_2(\mathbb{Z})$.
Et bien sûr, I_2 est dans $SL_2(\mathbb{Z})$.

Si A et B sont dans $SL_2(\mathbb{Z})$, leur produit est encore à coefficients entiers (stabilités de $\mathbb{Z}$ par addition et multiplication), et leur produit $A.B$ a pour inverse $B^{-1}.A^{-1}$ qui est encore dans $(M_2(\mathbb{Z}), +, \times)$.

Si une matrice A est dans $SL_2(\mathbb{Z})$, alors son inverse A^{-1} est à coefficients entiers, est inversible, d'inverse A, à coefficients entiers.

Enfin, le produit matriciel est associatif, c'est du cours.

> *Qui a passé sont temps à vérifier $(A.B).C = A.(B.C)$.*
> *Et qui a perdu du temps à écrire $(A.B).C = A.(B.C)$ en insistant en plus avec « coefficients entiers et inverse à coefficients entiers » ?*

Passons à non commutatif, avec un contre-exemple. Et pourquoi pas $\begin{pmatrix} 1 & 2 \\ 1 & 3 \end{pmatrix} \cdot \begin{pmatrix} 5 & 2 \\ 8 & 3 \end{pmatrix} \neq \begin{pmatrix} 5 & 2 \\ 8 & 3 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ 1 & 3 \end{pmatrix}$ (un coefficient suffit).

> *Pour perdre des points :*
> *je démontre « non commutatif », mais j'oublie « groupe »*
> *je parle de sous-groupe pour gagner du temps mais sans préciser de qui (ou pire « sous-groupe de $(M_2(\mathbb{R}), \times)$ », qui n'en est pas un)*

je dis « le produit matriciel n'est pas commutatif, donc c'est bon » alors qu'on a quand même des contraintes sur nos matrices qui pourraient les faire commuter deux à deux à cause de leurs histoires d'inverses à coefficients entiers

DS06 Sous-groupe engendré.

On se donne une matrice M dans $SL_2(\mathbb{Z})$. Par stabilité (et récurrence), toutes les puissances M^n avec n dans $\mathbb{N}$ sont dans $SL_2(\mathbb{Z})$.
De même, M^{-1} est dans $SL_2(\mathbb{Z})$ puis toutes les M^{-n} avec n entier naturel y sont aussi.
Bref, le sous-ensemble $< M >$ est inclus dans $SL_2(\mathbb{Z})$ (et hérite de l'associativité).

La matrice neutre I_2 s'écrit ici M^0.

Le produit de deux matrices de la forme M^net M^p est M^{n+p}. Il est encore dans $< M >$.

L'inverse d'un élément M^n de $< M >$ est l'élément M^{-n}, également dans $< M >$.

On a toutes les caractéristiques d'un sous-groupe.

On notera que $(SL_2(\mathbb{Z}),.)$ n'est pas commutatif, alors que $< M >$ l'est.
D'autre part, $< M >$ est le plus petit sous-groupe de $(SL_2(\mathbb{Z}),.)$ contenant M.

DS06 Critère sur le déterminant.

On prend une matrice à coefficients entiers dont le déterminant vaut 1 ou -1 : $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Son inverse est alors $\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$ ou $\begin{pmatrix} -d & b \\ c & -a \end{pmatrix}$, et il est à coefficients entiers. La matrice est donc dans $SL_2(\mathbb{Z})$.

Réciproquement, si la matrice $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ a son inverse $\frac{1}{a.d-b.c}.\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$ sont à coefficients entiers, en quoi pouvez vous déduire que $a.d - b.c$ vaut nécessairement -1 ou 1.
La condition est suffisante, mais de là à ce qu'elle soit nécessaire (hormis pour une personne qui fait des entorses à la logique, on n'en manque pas, même en Prépas hélàs).

Après tout, pourquoi n'aurait on pas $a.d - b.c$ égal à 3, mais tous les coefficients divisibles par 3 ?

La bonne idée, à connaître pour tout faire tomber en une ligne : on part de $A.A^{-1} = I_2$ et on passe au déterminant : $\det(A).\det(A^{-1}) = 1$.
Or, $\det(A)$ est entier (A est dans $M_2(\mathbb{Z})$), et $\det(A^{-1})$ aussi (A^{-1} est dans $M_2(\mathbb{Z})$).
Le produit de deux entiers vaut 1 ? C'est que les deux valent -1 ou 1 (raisonnement par l'absurde).

C'est bon, $|\det(A)|$ vaut forcément 1.

Aurait on eu intérêt à démontrer ce résultat avant pour pouvoir l'utiliser plusieurs fois plus tôt ?

Pour faire de $\begin{pmatrix} 5 & a \\ b & 1 \end{pmatrix}$ un élément de $SL_2(\mathbb{Z})$, il faut et il suffit que le produit $a.b$ soit égal à 4 (déterminant 1) ou 6 (déterminant -1). On trouve

$\begin{pmatrix} 5 & 4 \\ 1 & 1 \end{pmatrix}$	$\begin{pmatrix} 5 & -4 \\ -1 & 1 \end{pmatrix}$	$\begin{pmatrix} 5 & 2 \\ 2 & 1 \end{pmatrix}$	$\begin{pmatrix} 5 & -2 \\ -2 & 1 \end{pmatrix}$	$\begin{pmatrix} 5 & 6 \\ 1 & 1 \end{pmatrix}$	$\begin{pmatrix} 5 & -6 \\ -1 & 1 \end{pmatrix}$	$\begin{pmatrix} 5 & 3 \\ 2 & 1 \end{pmatrix}$	$\begin{pmatrix} 5 & -3 \\ -2 & 1 \end{pmatrix}$
$\begin{pmatrix} 5 & 1 \\ 4 & 1 \end{pmatrix}$	$\begin{pmatrix} 5 & -1 \\ -4 & 1 \end{pmatrix}$			$\begin{pmatrix} 5 & 1 \\ 6 & 1 \end{pmatrix}$	$\begin{pmatrix} 5 & -1 \\ -6 & 1 \end{pmatrix}$	$\begin{pmatrix} 5 & 2 \\ 3 & 1 \end{pmatrix}$	$\begin{pmatrix} 5 & -2 \\ -3 & 1 \end{pmatrix}$

DS06 Inclusion de $< M >$ dans le module $Module(I_2, M)$.

La relation (de Cayley-Hamilton) $M^2 = Tr(M).M - \det(M).I_2$ se démontre en prenant des coefficients

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}.\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a^2+b.c & a.b+d.b \\ a.c+d.c & b.c+d^2 \end{pmatrix} = (a+d).\begin{pmatrix} a & b \\ c & d \end{pmatrix} - (a.d-b.c).\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

On va montrer ensuite par récurrence sur n que chaque matrice M^n est de la forme $\alpha_n.M + \beta_n.I_2$ pour α_n et β_n bien choisis dans $\mathbb{Z}$.

On initialise pour n petit

$n=0$	$M^0 = I_2$	$= 0.M$	$+1.I_2$
$n=1$	$M^0 = M$	$= 1.M$	$+0.I_2$
$n=2$	M^2	$= Tr(M).M$	$-\det(M).I_2$

et les deux coefficients $Tr(M)$ et $-\det(M)$ sont entiers (et même, $\det(M)$ vaut 1 ou -1).

On se donne un entier n et on suppose que M^ns'écrit $\alpha_n.M + \beta_n.I_2$ pour α_n et β_n entiers bien choisis. On calcule alors

$$M^{n+1} = M^n.M = \alpha_n.M^2 + \beta_n.M = \alpha_n.(Tr(M).M - \det(M).I_2) + \beta_n.M$$

Il ne reste plus qu'à développer, regrouper

$$M^{n+1} = (\alpha_n.Tr(M) + \beta_n).M + (-\alpha_n.\det(M)).I_2$$

et pose $\alpha_{n+1} = \alpha_n.Tr(M) + \beta_n$ et $\beta_{n+1} = -\alpha_n.\det(M)$. Ce sont deux nouveaux entiers. Peu importe leur valeur, ce sont des entiers, ils existent, et la propriété se propage.

Une fois encore, la difficulté est de dire que la récurrence ne propage pas une formule mais l'existence de deux entiers.

Mais il nous manque les négatifs. On doit exprimer M^{-1} comme combinaison de I_2 et M.
On part de $M^2 = Tr(M).I_2 - \det(M).I_2$ et on multiplie par M^{-1} (qui existe) : $M = Tr(M).I_2 - \det(M).M^{-1}$ et on isole

$$M^{-1} = \frac{-M + Tr(M).I_2}{\det(M)}$$

Comme $\det(M)$ vaut 1 ou -1 (condition nécessaire et suffisante), on déduit

$$M^{-1} = -M + Tr(M).I_2 \text{ ou } M^{-1} = M - Tr(M).I_2$$

Première étape gagné, M^{-1} est combinaison à coefficients entiers de M et I_2.

On peut ensuite continuer par récurrence sur n.
On peut aussi élever à la puissance n avec formule du binôme (ici I_2 et M sont permutables).
La matrice $(M^{-1})^n$ est alors une combinaison de puissances de M a avec des coefficients entiers

$$(M^{-1})^n = \pm \sum_{k=0}^{n} \binom{n}{k}.(Tr(M))^{n-k}.(-1)^k.M^k$$

Comme chaque M^k est dans $Module(I_2, M)$, la combinaison à coefficients entiers y est aussi.

Et une fois encore, on ne cherche pas à exprimer M^{-n} explicitement comme combinaison.
C'est déjà une grande victoire que de dire qu'on n'a besoin que de I_2 et M.

DS06 Produit scalaire.

Une question de cours.

Forme.
Les formats sont compatibles, et $Tr(A^T.B)$ est un réel.

Symétrique.
On se donne A et B et on a aisément $Tr(A^T.B) = Tr(B^T.A)$ par la formule $Tr(M^T) = Tr(M)$.

Bilinéaire.
On se donne trois matrices et deux réels et on montre $Tr(A^T.(\lambda.B + \mu.C)) = \lambda.Tr(A^T.B) + \mu.Tr(A^T.C)$.

Positive. Défini positive.
On se donne A avec ses quatre coefficients et on constate $Tr(A^T.A) = a^2 + b^2 + c^2 + d^2$. En tant que somme de carrés de réels, ce nombre est positif.

Et il est même strictement positif, sauf si A est la matrice nulle.

Les deux matrices $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ et $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ sont dans $SL_2(\mathbb{Z})$. On calcule leur produit scalaire $Tr(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}) = 0$. Elles sont orthogonales entre elles.

On veut ensuite une matrice $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ de $SL_2(\mathbb{Z})$ (entiers avec $|a.d - b.c| = 1$), orthogonale à I_2 ($a + d = 0$) et à $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ ($b + c = 0$).

Bref, on veut une matrice de la forme $\begin{pmatrix} a & b \\ -b & -a \end{pmatrix}$ de déterminant -1 ou 1 : $-a^2 + b^2 = \pm 1$.

On n'a pas trop le choix : $(a - b).(a + b)$ est entier et vaut -1 ou 1.

$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$	$\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$

Ceci permet de créer quand même dans $SL_2(\mathbb{Z})$ des familles de quatre matrices deux à deux orthogonales

$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$

par exemple.

En revanche, pour cinq, ce sera impossible, car on ne peut pas trouver cinq matrices de $(M_2(\mathbb{R}), +, .)$ deux à deux orthogonales. C'est un problème de dimension.

DS06 Caractère non borné de $SL_2(\mathbb{Z})$.

On écrit la négation du caractère borné$\forall K \in \mathbb{R},\ \exists M \in SL_2(\mathbb{Z}),\ \sqrt{\phi(M,M)} > K$(toute valeur K peut être dépassée par au moins une matrice de $SL_2(\mathbb{Z})$).

On se donne K et on veut une matrice de $SL_2(\mathbb{Z})$ dont la norme (somme des carrés des coefficients) soit grande.
Pour chaque entier n, la matrice $\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$ est das $SL_2(\mathbb{Z})$ et a pour norme $\sqrt{2 + n^2}$, qui dépasse $|n|$.
Si on se donne un nombre K à dépasser, il suffit de prendre la matrice ci dessus avec $n = [K] + 1$ (car on veut un entier).

Avec un peu le même point de vue : la suite des matrices de la forme $\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$ voit ses normes croitre indéfiniment vers $+\infty$.

DS06 Ordre d'une matrice.

La matrice $\begin{pmatrix} 3 & -1 \\ 7 & -2 \end{pmatrix}$ est à coefficients entiers.
Si on doit montrer qu'elle est dans $C_2(\mathbb{Z})$, on va calculer ses puissances et espérer que son ordre ne soit pas trop élevé.

$$\begin{pmatrix} 3 & -1 \\ 7 & -2 \end{pmatrix}^2 = \begin{pmatrix} 2 & -1 \\ 7 & -3 \end{pmatrix},\ \begin{pmatrix} 3 & -1 \\ 7 & -2 \end{pmatrix}^3 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

Sans effort, on a alors $\begin{pmatrix} 3 & -1 \\ 7 & -2 \end{pmatrix}^6 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.
Son ordre vaut 6.

Il ne peut pas valoir moins, puisque on a $M^4 = -M$ et $M^5 = -M^2 \neq I_2$.

Un autre chemin moins risque ? On diagonalise pour calculer M^n.
Or, le spectre de M est formé des solutions de $x^2 - x + 1 = 0$ c'est à dire j et j^2.
En posant $D = \begin{pmatrix} j & 0 \\ 0 & j^2 \end{pmatrix}$ on a alors $D^6 = I_2$ puis $M^6 = I_2$.

Si la matrice M est dans $C_2(\mathbb{Z})$, d'ordre k alors elle est à coefficients entiers et vérifie $M^k = I_2$.
Mais alors en séparant $M^{k-1}.M = M.M^{k-1} = I_2$, on reconnaît que M est inversible, d'inverse M^{k-1}.

Et cet inverse est à coefficients entiers (stabilité de $(M_2(\mathbb{Z}), +, .)$).
On reconnaît le critère d'appartenance à $SL_2(\mathbb{Z})$.

On prend M dans $C_2(\mathbb{Z})$ d'ordre k. Son inverse M^{k-1} est encore à coefficients entiers.
Mais partant de $M^k = I_2$ on trouve $(M^{-1})^k = (M^k)^{-1} = I_2$. On caractérise une matrice de $C_2(\mathbb{Z})$.

De même, en répétant la formule $(A.B)^T = B^T.A^T$ on trouve $(M^T)^k = (M^k)^T = (I_2)^T = I_2$.
Et la matrice M^T est à coefficients entiers.
Bref, encore une dans $C_2(\mathbb{Z})$.

Mais pour l'ordre ?

> *Le fait d'avoir $(M^T)^k = I_2$ ne dit pas que M^T est d'ordre k .*
> *Son ordre est le plus petit entier vérifiant ceci. Peut être qu'un entier plus k vérifie aussi $(M^T)^i = I_2$.*
> *Au mieux, on peut dire que l'ordre de M^T est inférieur ou égal à k.*

Si une matrice M vérifie $M^6 = I_2$, on avait peut être déjà $M^2 = I_2$ ou $M^3 = I_2$. Et en tout cas, on aura $M^{12} = I_2$.

Mais regardons ce qu'on a prouvé en supposant M d'ordre k :

$$ordre(M^{-1}) \leqslant ordre(M) \text{ et } ordre(M^T) \leqslant ordre(M)$$

Mais alors, en appliquant ce résultat à M^{-1} et à M^T on a

$$ordre((M^{-1})^{-1}) \leqslant ordre(M^{-1}) \text{ et } ordre((M^T)^T) \leqslant ordre(M^T)$$

On déduit alors par antisymétrie $ordre(M^{-1}) = ordre(M)$ et $ordre(M^T) = ordre(M)$.

> *Un classique des idées géniales en maths : appliquer le résultat (qu'on a obtenu pour tout élément) à son symétrique pour avoir les deux sens de inégalité.*
> *Toute la beauté et l'efficacité des maths.*
> *Et toute la beauté est la rigueur des maths, c'est aussi de dire « tu es sûr qu'avec $(M^T) = I_2$ tu as obtenu $ordre(M^T) = ordre(M)$? n'as tu pas juste $ordre(M^T) \leqslant ordre(M)$? ».*

Cette fois, M est d'ordre 3 : $M \neq I_2$, $M^2 \neq I_2$ et $M^3 = I_2$.
On a déjà $M^2 \neq I_2$ et $(M^2)^3 = M^6 = (M^3)^2 = I_2$.

Il nous manque juste $(M^2)^2 \neq I_2$ pour que M^2 soit exactement d'ordre 3.

Mais si on avait $M^4 = I_2$ avec $M^3 = I_2$ on aboutirait à $M = I_2$ ce qui n'est pas le cas.

M^2 est bien dans $C_2(\mathbb{Z})$ et son ordre vaut bien 3.

Cette fois, M est d'ordre 6 : $M^6 = I_2$ et aucune des puissances précédentes ne donne I_2.

On a très vite $(M^2)^3 = I_3$. Bien partie pour être dans $C_2(\mathbb{Z})$ et être d'ordre 3.
En effet, on n'a pas $M^2 = I_2$ ni $(M^2)^2 = I_2$.

La matrice $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ est dans $C_2(\mathbb{Z})$, d'ordre 2.

Considérons alors $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ et $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Chacune est dans $\mathbb{C}2$. Leur somme est dans $M_2(\mathbb{Z})$ mais pas dans $\mathbb{C}2$, puisque déjà le déterminant ne vaut pas 1.

Ensuite, $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ et $\begin{pmatrix} 3 & -1 \\ 7 & -2 \end{pmatrix}$ (toutes deux dans $C_2(\mathbb{Z})$) ont pour produit $\begin{pmatrix} 7 & -2 \\ 3 & -1 \end{pmatrix}$.
Cette matrice n'a plus des puissances bien agréables : $\begin{pmatrix} 43 & -12 \\ 18 & -5 \end{pmatrix}$, $\begin{pmatrix} 265 & -74 \\ 111 & -31 \end{pmatrix}$. Mais ça ne prouve rien.

> *Mais si on la diagonalise avec courage, on a $\begin{pmatrix} 7 & -2 \\ 3 & -1 \end{pmatrix} = P.\begin{pmatrix} 3+\sqrt{10} & 0 \\ 0 & 3-\sqrt{10} \end{pmatrix}.P^{-1}$ avec P à préciser ($P = \begin{pmatrix} 4+\sqrt{10} & 4-\sqrt{10} \\ 3 & 3 \end{pmatrix}$ si on y tient). On a alors $M^k = P.D^k.P^{-1}$ puis $Tr(M^k) = (3+\sqrt{10})^k + (3-\sqrt{10})^k$ qui tend vers l'infini et ne retombera jamais sur 2.*

DS06 Polynôme caractéristique des matrices de $\mathbb{C}2$.

On a une matrice à coefficients entiers et un exposant k non nul vérifiant $M^k = I_2$.

On se donne une valeur propre λ et un vecteur propre qui va avec. C'est donc un vecteur U vérifiant $M.U = \lambda.U$.

Mais alors, naturellement

$$M^2.U = M.MU = M.(\lambda.U) = \lambda.M.U = \lambda.(\lambda.U) = \lambda^2.U$$

et par récurrence évidente $M^n.U = \lambda^n.U$ (d'une côté matrice fois vecteur, de l'autre complexe fois vecteur).

Mais en particulier pour l'exposant k : $M^k.U = \lambda^k.U$ puis $I_2.U = \lambda^k.U$.

Comme le vecteur U est non nul, au moins une de ses composants x_u ou $y_u$est non nulle : $\begin{pmatrix} x_u \\ y_u \end{pmatrix} = \lambda^k.\begin{pmatrix} x_u \\ y_u \end{pmatrix}$

et on a donc $\lambda^k = 1$.

> *Erreur à ne pas commettre : « je pars de $\lambda^k.U = U$ et je multiplie par U^{-1} pour arriver à $\lambda^k = 1$.*
> *Un vecteur n'a pas d'inverse. Seules les matrices carrées sont inversibles (et encore, on leur demandera d'avoir un déterminant non nul).*

Les seules valeurs propres possibles d'une matrice de $C_2(\mathbb{Z})$ sont des racines k^{ieme} de l'unité (où k est l'ordre de la matrice).

Attention, on est loin d'avoir toutes les racines k^{ieme}, puisqu'il n'y a que deux valeurs propres.

Mais les racines de l'unité ont pour module 1.

Et la trace est la somme des deux valeurs propres (formules de Viète).
La trace se majore donc en valeur absolue

$$|Tr(M)| = |\lambda_1 + \lambda_2| \leqslant |\lambda_{1|} + |\lambda_2| = 2$$

N'oublions pas que la matrice est à coefficients entiers. Sa trace l'est donc aussi.
Il n'y a que cinq entiers entre -2 et 2 : -2, -1, 0, 1 et 2.

Enfin, le déterminant est le produit des valeurs propres. Et de toutes façons, il vaut -1 ou 1 (questions du début).

En envisageant (à tort) tous les cas possibles, on a dix polynômes caractéristiques possibles

$X^2 - 2.X + 1$	$X^2 - X + 1$	$X^2 + 1$	$X^2 + X + 1$	$X^2 + 2.X + 1$
$X^2 - 2.X - 1$	$X^2 - X - 1$	$X^2 - 1$	$X^2 + X - 1$	$X^2 + 2.X - 1$

Mais la condition n'est que nécessaire. Il faut aussi revenir à « racines de module 1 ». On va donc en éliminer certains

$X^2 - 2.X + 1$	$X^2 - X + 1$	$X^2 + 1$	$X^2 + X + 1$	$X^2 + 2.X + 1$
1 double	$-j$ et $-j^2$	i et $-i$	j et j^2	-1 double
$X^2 - 2.X - 1$	$X^2 - X - 1$	$X^2 - 1$	$X^2 + X - 1$	$X^2 + 2.X - 1$
$1 - \sqrt{2}$ et $1 + \sqrt{2}$	$(1 - \sqrt{5})/2$ et $(1 + \sqrt{5})/2$	-1 et 1	$(-1 - \sqrt{5})/2$ et $(-1 + \sqrt{5})/2$	$-1 - \sqrt{2}$ et $-1 + \sqrt{2}$

Attention, éliminer ceux dont les racines ne sont pas de module 1 ne suffira peut être pas, il reste peut être encore des critères non exploités.

$X^2 - 2.X + 1$	$X^2 - X + 1$	$X^2 + 1$	$X^2 + X + 1$	$X^2 + 2.X + 1$
1 double	$-j$ et $-j^2$	i et $-i$	j et j^2	-1 double
		$X^2 - 1$		
		-1 et 1		

On va donc trouver des matrices qui obéissent au critère indiqué, pour s'assurer que ça existe
(par exemple, avec $X^2-2.X+1$, on a la matrice $\begin{pmatrix}1&1\\0&1\end{pmatrix}$ qui a la bonne trace et le bon déterminant mais n'est pas dans $C_2(\mathbb{Z})$.

$X^2-2.X+1$	X^2-X+1	X^2+1	X^2+X+1	$X^2+2.X+1$
1 double	$-j$ et $-j^2$	i et $-i$	j et j^2	-1 double
$\begin{pmatrix}1&0\\0&1\end{pmatrix}$ ordre 1	$\begin{pmatrix}1&1\\-1&0\end{pmatrix}$ ordre 6	$\begin{pmatrix}0&-1\\1&0\end{pmatrix}$ ordre 2	$\begin{pmatrix}-1&1\\-1&0\end{pmatrix}$ ordre 3	$\begin{pmatrix}-1&0\\0&-1\end{pmatrix}$ ordre 2
		X^2-1		
		-1 et 1	$\begin{pmatrix}-1&0\\0&1\end{pmatrix}$ ordre 2	

DS06 Plan P.

On a donc pose $P=\{\alpha.A+\beta.I_2 \mid (\alpha,\beta)\in\mathbb{R}^2\}$.
C'est une partie de $M_2(\mathbb{R})$ contenant la matrice nulle (pour $\alpha=\beta=0$).
L'addition et la multiplication sont associatives sur $M_2(\mathbb{R}),+,.)$, elles les restent sur P. De même pour la distributivité de la multiplication sur l'addition.

La stabilité additive est acquise en prenant quatre réels α, β, α' et β' et en écrivant

$$(\alpha.A+\beta.I_2)+(\alpha'.A+\beta'.I_2)=(\alpha+\alpha').A+(\beta+\beta').I_2$$

et même pour avoir les opposés

$$(\alpha.A+\beta.I_2)-(\alpha'.A+\beta'.I_2)=(\alpha-\alpha').A+(\beta-\beta').I_2$$

Pour la multiplication, c'est plus drôle

$$(\alpha.A+\beta.I_2).(\alpha'.A+\beta'.I_2)=(\alpha.\alpha').A^2+(\alpha.\beta'+\alpha'.\beta).A+(\beta.\beta').I_2$$

pour l'instant, ce n'est pas satisfaisant à cause de A^2. Mais on a $A^2=4.A-I_2$ et on peut tout regrouper.

$$(\alpha.A+\beta.I_2).(\alpha'.A+\beta'.I_2)=(\alpha.\beta'+\alpha'.\beta+4.\alpha.\alpha').A+(\beta.\beta'-\alpha.\alpha').I_2 Puisque$$

C'est demandé : $\varphi(I_2,I_2)=2$, $\varphi(I_2,A)=4$ et $\varphi(A,A)=15$.

Les deux matrices E_1 et E_2 sont des combinaisons de I_2 et A. Elles sont dans P.
On calcule ce qui se fait bien : $\varphi(E_1,E_1)=\varphi\Big(\frac{I_2}{\sqrt{2}},\frac{I_2}{\sqrt{2}}\Big)=\frac{1}{2}.\varphi(I_2,I_2)=\frac{1}{2}.2=1$.

On poursuit, toujours sans redescendre jusqu'aux coefficients car on est en maths (mais on peut aussi écrire $E_2=\begin{pmatrix}-1/\sqrt{7}&2/\sqrt{7}\\1/\sqrt{7}&1/\sqrt{7}\end{pmatrix}$)

$$\varphi(E_1,E_2)=\varphi\Big(\frac{I_2}{\sqrt{2}},\frac{A-2.I_2}{\sqrt{7}}\Big)=\frac{1}{\sqrt{14}}.\Big(\varphi(I_2,A)-2.\varphi(I_2,I_2)\Big)=0$$

et pour finir

$$\varphi(E_1,E_2)=\varphi\Big(\frac{A-2.I_2}{\sqrt{7}},\frac{A-2.I_2}{\sqrt{7}}\Big)=\frac{1}{7}.\Big(\varphi(A,A)-2.\varphi(A,I_2)-2.\varphi(I_2,A)+4.\varphi(I_2,I_2)\Big)=1$$

Avec un œil de matheux : deux matrices orthogonales entre elles, toutes deux de norme 1.
Avec un œil de géomètre : une base orthonormée de P.

DS06 Plus proche matrice.

Pour B donnée, les deux produits scalaires se calculent, puis $\varphi(B,E_1).E_1$ et $\varphi(B,E_2).E_2$ sont dans P , de même que leur somme.

Passons à la preuve de $\varphi(M-B,\ M-B)^2 = \varphi(M-H,\ M-H)^2 + \varphi(H-B,\ H-B)^2$.

Si on a une âme de PSI-chopathe, on prend quatre coefficients pour B ($B = \begin{pmatrix} x & y \\ z & t \end{pmatrix}$, on calcule les produits scalaires et on explicite la matrice H.
On prend une matrice M de P qu'on écrit $\begin{pmatrix} a+b & 2.a \\ a & 3.a+b \end{pmatrix}$ et on calcule tous ces produits scalaires.
Si on est plus matheux, on reste à l'étage des matrices.
Et on dit que M s'écrit non seulement $a.A + b.I_2$ mais aussi $\alpha.E_1 + \beta.E_2$.
Et on allège les notations en écrivant $H = \lambda_1.E_1 + \lambda_2.E_2$ avec $\lambda_k = \phi(B, E_k)$.

Il n'y a plus qu'à développer en utilisant $\varphi(E_1, E_1) = \varphi(E_2, E_2) = 1$ et $\varphi(E_1, E_2) = 0$.

Enfin, comme $\varphi(M-H,\ M-H)^2$ est positif (carré de réel), on a toujours

$$\varphi(M-B,\ M-B)^2 \geqslant \varphi(H-B,\ H-B)^2$$

quand M se promène dans P. La quantité $\varphi(M-B,\ M-B)$ ne pourra jamais être plus petite que $\varphi(H-B,\ H-B)$ quand M bougera dans P. Et elle attenidnra cette valeur pour $M = H$. C'est donc le minimum de ces distances.