À rendre pour le mardi 24 septembre

DM NORMAL

PROBLÈME 1

On note $G = \left\{ \begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix},\ \alpha, \beta \in \mathbb{C} \text{ tels que } |\alpha|^2 + |\beta|^2 = 1 \right\}$.
On pose $\mathbf{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $U = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$, $J = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$ et $K = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.
On note $H = \{xU + yJ + zK + t\mathbf{1},\ x, y, z, t \in \mathbb{R}\}$ et on admettra que c'est un espace vectoriel réel et que $(U, J, K, \mathbf{1})$ forme une base de celui-ci.
Pour $h = xU + yJ + zK + t\mathbf{1}$ dans H, on note $h^* = -h + 2t\mathbf{1}$.

Partie A

1. Montrer que G (muni du produit matriciel) est un groupe, et qu'il est infini ; G est-il commutatif ?

2. Vérifier que $h \mapsto h^*$ est un automorphisme de l'espace vectoriel réel H, et, pour h_1 et h_2 dans H, exprimer $(h_1 h_2)^*$ en fonction de h_1^* et h_2^*.

3. Vérifier que $(\mathrm{H}, +, \times)$ est un corps, non commutatif.

4. Pour $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{M}_2(\mathbb{C})$, on note $\overline{A} = \begin{pmatrix} \overline{a} & \overline{b} \\ \overline{c} & \overline{d} \end{pmatrix}$. Montrer que $[\overline{A}^T A = I_2 \text{ et } \det(A) = 1]$ si et seulement si A est dans G.

5. Montrer que :

$$G = \left\{ \begin{pmatrix} \mathrm{e}^{i\frac{\varphi}{2}} & 0 \\ 0 & \mathrm{e}^{-i\frac{\varphi}{2}} \end{pmatrix} \times \begin{pmatrix} \cos\dfrac{\theta}{2} & -\sin\dfrac{\theta}{2} \\ \sin\dfrac{\theta}{2} & \cos\dfrac{\theta}{2} \end{pmatrix} \times \begin{pmatrix} \mathrm{e}^{i\frac{\psi}{2}} & 0 \\ 0 & \mathrm{e}^{-i\frac{\psi}{2}} \end{pmatrix},\ (\varphi, \theta, \psi) \in \mathbb{R} \times [0, \pi] \times \mathbb{R} \right\}$$

Partie B

1. Pour $h = xU + yJ + zK + t\mathbf{1}$ dans H, exprimer $\det(h)$ en fonction de x, y, z, t.

2. En déduire que si $m = a_1^2 + b_1^2 + c_1^2 + d_1^2$ et $n = a_2^2 + b_2^2 + c_2^2 + d_2^2$, avec $a_1, a_2, b_1, b_2, c_2, c_2, d_1, d_2$ dans $\mathbb{Z}$, alors il existe a_3, b_3, c_3, d_3 dans $\mathbb{Z}$ tels que $mn = a_3^2 + b_3^2 + c_3^2 + d_3^2$.

3. ***a.*** Écrire en PYTHON une fonction `carres` qui pour $N \in \mathbb{N}^*$ renvoie le tableau associé aux entiers m dans $[\![0, N]\!]$ qui s'ecrivent sous la forme $m = a^2$, avec a dans $\mathbb{N}$ (on n'utilisera pas la fonction racine carrée).

b. Écrire en PYTHON une fonction `somme` qui à deux listes L_1 et L_2 d'entiers renvoie la liste L de toutes les sommes possibles d'un élément de L_1 et d'un élément de L_2.

c. Écrire une fonction PYTHON `quatrecarres` qui à un entier $N \in \mathbb{N}^*$, renvoie `True` si tous les entiers m de $[\![0, N]\!]$ peuvent s'écrire $m = a^2 + b^2 + c^2 + d^2$, avec a, b, c, d dans $\mathbb{N}$ et `false` sinon. On pourra s'aider des fonction `carres` et `somme`.

Partie C

Notons $\mathrm{H}_0 = \{h \in \mathrm{H} \mid h^* + h = 0\}$. Pour $v \in \mathrm{H}_0$ et $h \in \mathrm{G}$, on pose $T(h)(v) = hvh^{-1}$.

1. Montrer que H_0 est un hyperplan de H.

2. Soit $h \in G$. Montrer que : $T(h)(\mathrm{H}_0) \subset \mathrm{H}_0$.

3. Montrer que T est un morphisme de groupes de $(G, .)$ dans $(GL(\mathrm{H}_0), \circ)$.

4. Déterminer le noyau de T.

PROBLÈME 2

Notations et rappels

Étant donnés deux entiers relatifs a et b, le plus grand diviseur commun de a et b sera noté PGCD (a, b) ou $a \wedge b$. On rappelle que $a \wedge 0 = a$.
a est dit premier avec b si $a \wedge b = 1$.

On notera $(\mathbb{Z}/n\mathbb{Z})^*$ l'ensemble des éléments de $\mathbb{Z}/n\mathbb{Z}$ inversibles pour la multiplication et que $(\mathbb{Z}/n\mathbb{Z})^* = \{\overline{k},\ k \in \mathbb{Z} \text{ et } k \wedge n = 1\}$. On rappelle que $((\mathbb{Z}/n\mathbb{Z})^*, \times)$ est un groupe dont le cardinal est $\phi(n)$, avec ϕ l'indicatrice d'Euler. En particulier si k est dans $\mathbb{Z}$, avec $k \wedge n = 1$, alors dans $\mathbb{Z}/n\mathbb{Z}$, on a : $\overline{k}^{\phi(n)} = \overline{1}$.

Partie I : Nombres de Carmichaël

L'objet de cette partie est la caractérisation de certains nombres, appelés nombres de Carmichaël.
On rappelle que pour tout entier naturel premier p, et tout a entier premier avec p, $a^{p-1} \equiv 1 \bmod p$.
La réciproque n'est pas vraie ; un nombre n est appelé nombre de Carmichaël si :

a) n n'est pas premier
b) pour tout nombre a premier avec n, a^{n-1} est congru à 1 modulo n.

1. Montrer que si $n = p_1 \times p_2 \times \ldots \times p_k$ où p_1, p_2, …, p_k sont des nombres premiers deux à deux distincts tels que $(p_i - 1)$ divise $(n - 1)$ pour tout i de $\{1, 2, \ldots, k\}$, avec $k \geq 2$, alors n est un nombre de Carmichaël (on montrera d'abord que : $\forall i \in [\![1, k]\!],\ p_i | (a^{n-1} - 1)$).
Montrer en particulier que 561, 10585 sont des nombres de Carmichaël.

2. On suppose que n est une puissance de 2, $n = 2^\alpha$, où α est un entier supérieur ou égal à 2.
Quel est le cardinal de $(\mathbb{Z}/n\mathbb{Z})^*$?
Montrer que : $a^{2^{\alpha-1}} \equiv 1[n]$, pour tout entier a impair.
En déduire que pour tout entier a impair, on ne peut avoir $a^{2^{\alpha-1}} \equiv 1[n]$ sauf si $a \equiv 1[n]$; que peut-on conclure ?

3. Montrer qu'un nombre $n = p_1 p_2$ avec $p_1 > p_2$ des nombres premiers tels que $(p_1 - 1) | (n - 1)$ ne peut exister. Ainsi un nombre vérifiant la propriété de la question **1** a au moins trois facteurs premiers dans sa décomposition.

4. Résoudre l'équation $85p - 16k = 1$, où (k, p) appartient à $\mathbb{Z}^2$.
On admet que la réciproque de la question **1** est vraie. Déterminer le plus petit nombre de Carmichaël divisible par 5 et 17.

Partie II : Nombres pseudo-premiers forts

Dans toute cette partie, p désigne un entier impair supérieur ou égal à 3, et on notera $(p-1) = q \times 2^s$, où q est un entier naturel impair et s un entier naturel supérieur ou égal 1.

1. Dans cette question, on suppose p premier.

a. Soit a un entier premier avec p. Montrer que $\overline{a}^{\frac{p-1}{2}} = \overline{1}$ ou $\overline{a}^{\frac{p-1}{2}} = -\overline{1}$ dans $\mathbb{Z}/p\mathbb{Z}$. (on pourra penser au petit théorème de Fermat).

b. On dit qu'un entier naturel a vérifie la propriété $H_a(p)$ si :

$$(a^q \equiv 1[p]) \qquad \text{ou} \qquad (\text{il existe } r \in [\![0, s-1]\!] \text{ tel que } a^{q\times 2^r} \equiv -1[p]) \qquad H_a(p)$$

Montrer que tout entier naturel a premier avec p vérifie $H_a(p)$ (on supposera qu'il n'existe pas $r \in [\![0, s-1]\!]$ tel que $a^{q\times 2^r} \equiv -1[p]$ et on montrera que $a^q \equiv 1[p]$ en montrant par récurrence descendante sur r que $a^{q\times 2^r} \equiv 1[p]$).

2. On dit qu'un nombre p impair, non nécessairement premier, est pseudo-premier fort en base a si la propriété $H_a(p)$ est vérifiée ; on écrira en abrégé que p est a-ppf.

Par exemple, 25 est 7-ppf car $24 = 3 * 2^3$ et $7^{3\times 2} = 117649 \equiv 24 \equiv -1[25]$.

Montrer que si a est un entier tel que a et p ne soient pas premiers entre eux, alors p ne peut pas être a-ppf.

3. Construction d'un algorithme :

a. Un entier p impair et un entier a étant donnés, écrire une fonction en PYTHON permettant de tester si p est a-ppf.

b. Reportez le tableau suivant sur votre copie et complétez les cases vides pour "oui" ou "non" à l'aide du programme précédent.

p	49	91	111	121	135	1225
a	30	74	28	94	43	999
p est a-ppf						

DM DIFFICILE

EXERCICE

Soit $\mathbb{U}_n = \{z \in \mathbb{C},\ z^n = 1\} = \{\omega^k,\ k \in [\![0, n-1]\!]\}$, avec $\omega = e^{\frac{2i\pi}{n}}$.
On note $\mathcal{P}_n = \{\omega^k,\ k \in [\![0, n-1]\!] \text{ et } k \wedge n = 1\}$. Comme $\mathbb{U}_n$ s'identifie à $\mathbb{Z}/n\mathbb{Z}$, via l'isomorphisme de groupe $\begin{cases} \mathbb{Z}/n\mathbb{Z} & \to & \mathbb{U}_n \\ \overline{k} & \mapsto & \omega^k \end{cases}$, alors $\mathcal{P}_n$ est l'ensemble des générateurs du groupe $(\mathbb{U}_n, \times)$ et $card(\mathcal{P}_n) = \phi(n)$, avec ϕ la fonction indicatrice d'Euler.
Si $P = a_0 + ... + a_n X^n$ est dans $\mathbb{Z}[X]$, on définit son « contenu » noté c_P qui est $a_0 \wedge ... \wedge a_n$.

1. Soit $P, Q \in \mathbb{Z}[X]$.

- ***a.*** Si $c_P = c_Q = 1$, montrer que : $c_{PQ} = 1$ (on pourra raisonner par l'absurde et considérer p un diviseur premier de c_{PQ}).
- ***b.*** Montrer que $c_{PQ} = c_P c_Q$ dans tous les cas.

2. On dit qu'un polynôme P est irréductible dans $\mathbb{Z}[X]$, s'il n'existe pas de polynômes U, V dans $\mathbb{Z}[X]$ tels que $UV = P$ et $d^\circ(U) < d^\circ(P)$ et $d^\circ(V) < d^\circ(P)$. Déduire de la question précédente que si P est irréductible dans $\mathbb{Z}[X]$, alors il est irréductible dans $\mathbb{Q}[X]$ (on pourra se ramner au cas où $c_P = 1$).

3. **(Critère d'irréductibilité d'Eisenstein)** Soit $P = a_0 + ... + a_n X^n \in \mathbb{Z}[X]$. Montrer que s'il existe un nombre premier p tel que :

- $p \nmid a_n$;
- $\forall i \in [\![0, n-1]\!],\ p | a_i$;
- $p^2 \nmid a_0$,

alors P est irréductible dans $\mathbb{Z}[X]$ et donc dans $\mathbb{Q}[X]$ (grâce à la question précédente).

4. On pose $\Phi_n(X) = \prod_{\xi \in \mathcal{P}_n} (X - \xi) \in \mathbb{C}[X]$, le n-ème polynôme cyclotomique.
En particulier $d^\circ(\Phi_n) = \phi(n)$ et $\Phi_1(X) = X - 1$.

- ***a.*** Montrer que : $X^n - 1 = \prod_{d|n} \Phi_d(X)$.
- ***b.*** Montrer par récurrence que $\Phi_n \in \mathbb{Z}[X]$.
- ***c.*** Soit p un nombre premier.
  i. Déterminer Φ_p.
  ii. Montrer que Φ_p est irréductible dans $\mathbb{Q}[X]$ (on pourra considérer $\Phi_p(X+1)$).

PROBLÈME

Notations.
· *Dans tout le problème, n désignera un entier naturel non nul et* $\mathbf{L}$ *désignera le corps des nombres réels* $\mathbf{R}$ *ou le corps des nombres complexes* $\mathbf{C}$.
· *Si p désigne un entier naturel non nul et* $\mathbf{L}$ *un corps, on note $\mathcal{M}_p(\mathbf{L})$ l'ensemble des matrices carrées de taille $p \times p$ à coefficients dans* $\mathbf{L}$ *; on notera* $\mathrm{Tr}\,(M)$ *la trace d'une matrice carrée M.*
· *On appelle I_p la matrice identité de $\mathcal{M}_p(\mathbf{L})$, qui est la matrice diagonale constituée uniquement de* 1 *sur la diagonale.*
· *L'ensemble des matrices inversibles de $\mathcal{M}_p(\mathbf{L})$ est noté $GL_p(\mathbf{L})$ et l'ensemble des matrices de $GL_p(\mathbf{L})$ de déterminant* 1 *est noté $SL_p(\mathbf{L})$.*
· *Soit* $\mathbf{A}$ *un sous-anneau de* $\mathbf{L}$. *On note $\mathcal{M}_p(\mathbf{A})$ (respectivement $GL_p(\mathbf{A})$ et $SL_p(\mathbf{A})$) l'ensemble des matrices de $\mathcal{M}_p(\mathbf{L})$ (respectivement de $GL_p(\mathbf{L})$ et $SL_p(\mathbf{L})$) à coefficients dans* $\mathbf{A}$.
· *Pour $m, n \in \mathbb{Z}$, tel que $m \leq n$, on note $[\![m, n]\!]$ l'intervalle d'entiers relatifs constitué des éléments de l'ensemble $\{m, m+1, ..., n-1, n\}$.*
Dans le problème on pourra utiliser librement la relation suivante (que l'on peut montrer en travaillant sur les coefficients) :

$$\forall A \in \mathcal{M}_2(\mathbf{A}),\ A^2 - \mathrm{Tr}\,(A)A + \det(A) I_2 = 0 \quad (*).$$

I. Si $n \equiv 0[4]$, l'équation $X^n + Y^n = Z^n$ n'admet pas de solutions dans $SL_2(\mathbb{Z})$.

1. Montrer que $(SL_2(\mathbb{Z}), .)$ est un groupe.
2. Soit $M \in SL_2(\mathbb{Z})$. Démontrer que $\mathrm{Tr}\,(M^4) = \mathrm{Tr}\,(M)^4 - 4\,\mathrm{Tr}\,(M)^2 + 2$.
3. Démontrer que l'équation $X^4 + Y^4 = Z^4$ d'inconnues X, Y et Z n'admet pas de solutions dans $SL_2(\mathbb{Z})$.
4. En déduire que si 4 divise n, alors l'équation $X^n + Y^n = Z^n$ d'inconnues X, Y et Z n'admet pas de solutions dans $SL_2(\mathbb{Z})$.

II. Réseaux de $\mathbb{Q}^n$.

Dans cette partie, n et m désignent deux entiers naturels non nuls. Soient $v_1, ..., v_m$ des éléments non nuls de $\mathbb{Q}^n$, posons

$$\mathcal{R} = \mathbb{Z}v_1 + ... + \mathbb{Z}v_m = \left\{ \sum_{i=1}^{m} k_i v_i \;\middle|\; k_1, ..., k_m \in \mathbb{Z} \right\}.$$

Si $n \geq 2$, on note

$$\mathbb{Q}^{n-1} \times \{0\} = \Big\{ (x_1, ..., x_{n-1}, 0) \;\Big|\; x_1, ..., x_{n-1} \in \mathbb{Q} \Big\}.$$

5. Démontrer que $\mathcal{R}$ est un sous-groupe additif de $(\mathbb{Q}^n, +)$.
6. Si $n = 1$, montrer qu'il existe un élément r de $\mathbb{Q}$ tel que

$$\mathcal{R} = r\mathbb{Z} = \big\{ rk \;\big|\; k \in \mathbb{Z} \big\}.$$

Ce r est-il unique ?

7. On suppose $n \geq 2$, posons $\pi : \left\{ \begin{array}{ccc} \mathbb{Q}^n & \to & \mathbb{Q} \\ (x_1, ..., x_n) & \mapsto & x_n \end{array} \right.$. Montrer qu'il existe un élément w de $\mathcal{R}$ tel que

$$\pi(\mathcal{R}) = \pi(w)\mathbb{Z} = \{\pi(w)k \mid k \in \mathbb{Z}\}.$$

Dans la suite de cette partie, si $\pi(\mathcal{R}) = \{0\}$, on prendra $w = (0, ..., 0)$.

8. Soit x un élément de $\mathcal{R}$ et w un élément de $\mathcal{R}$ défini comme dans la question précédente.
   (a) Montrer qu'il existe un couple $(q, \widetilde{x})$ de $\mathbb{Z} \times \big(\mathcal{R} \cap (\mathbb{Q}^{n-1} \times \{0\})\big)$ tel que $x = qw + \widetilde{x}$.
   (b) Démontrer que $\widetilde{x}$ est unique. L'entier q est-il toujours unique ?
9. Démontrer que l'on a

$$\mathcal{R} \cap (\mathbb{Q}^{n-1} \times \{0\}) = \mathbb{Z}\widetilde{v_1} + ... + \mathbb{Z}\widetilde{v_m} = \left\{ \sum_{i=1}^{m} k_i \widetilde{v_i} \;\middle|\; k_1, ..., k_m \in \mathbb{Z} \right\}$$

où les éléments $\widetilde{v_1}, ..., \widetilde{v_m}$ de $\mathcal{R}$ sont définis comme dans la question précédente.

10. Montrer par récurrence sur la dimension de $\mathbb{Q}^n$, qu'il existe des éléments $u_1, ..., u_p$ de $\mathcal{R}$ tels que pour tout x de $\mathcal{R}$ il existe un unique p-uplet $(k_1, ..., k_p)$ de $\mathbb{Z}^p$ vérifiant $x = \sum_{i=1}^{p} k_i u_i$.

Une telle famille $(u_1, ..., u_p)$ de $\mathcal{R}$ est appelée $\mathbb{Z}$-base *de $\mathcal{R}$, on notera alors $\mathcal{R} = \bigoplus_{i=1}^{p} \mathbb{Z}u_i$.*

11. Supposons que $vect_{\mathbb{Q}}(v_1, ..., v_m) = \mathbb{Q}^n$. Si $(u_1, ..., u_p)$ est une $\mathbb{Z}$-base de $\mathcal{R}$ démontrer que $(u_1, ..., u_p)$ est une base de $\mathbb{Q}^n$ et que $p = n$.

III. Condition pour que certains sous-groupes de $SL_2(\mathbb{Q})$ soient semblables à un sous-groupe de $SL_2(\mathbb{Z})$

Soit p un entier strictement positif. Dans cette partie, on identifie $\mathcal{M}_{p,1}(\mathbb{Q})$ et $\mathbb{Q}^p$. On note $(e_1, ..., e_p)$ la base canonique de $\mathbb{Q}^p$ et on admet que $(SL_p(\mathbb{Q}), .)$ est un groupe.

12. Soit G un sous-groupe multiplicatif de $(SL_p(\mathbb{Q}), .)$ tel qu'il existe un entier strictement positif d vérifiant

$$\forall M \in G,\ dM \in \mathcal{M}_p(\mathbb{Z}).$$

Soit H le sous-groupe additif de $(\mathbb{Q}^p, +)$ engendré par les éléments Me_i, avec M une matrice de G et i un élément de $[\![1, p]\!]$; c'est le plus petit sous-groupe de $(\mathbb{Q}^p, +)$ contenant l'ensemble $\left\{Me_i \mid\ M \in G,\ i \in [\![1, p]\!]\right\}$ et il peut s'écrire sous la forme suivante

$$H = \left\{y_1 + y_2 + ... + y_q \mid q \in \mathbb{N}^*,\ y_1, y_2, ..., y_q \in \mathcal{M}\right\}$$

où

$$\mathcal{M} = \left\{Me_i \mid M \in G,\ i \in [\![1, p]\!]\right\} \cup \left\{-Me_i \mid M \in G,\ i \in [\![1, p]\!]\right\} \cup \{0\}.$$

(a) Démontrer que les vecteurs $e_1, ..., e_p$ appartiennent à H.

(b) Démontrer que H est stable par G, c'est-à-dire que l'on a

$$\forall M \in G, \forall h \in H,\ Mh \in H.$$

(c) Soient $M \in G$ et $j \in [\![1, p]\!]$. Montrer qu'il existe des éléments $r_1, ..., r_p$ de $[\![0, d-1]\!]$ et des éléments $q_1, ..., q_p$ de $\mathbb{Z}$ tels que

$$Me_j = \sum_{i=1}^{p} q_i e_i + \frac{1}{d} \sum_{i=1}^{p} r_i e_i.$$

(d) Montrer qu'il existe une famille génératrice $(v_1, ..., v_m)$ de $\mathbb{Q}^p$ telle que

$$H = \mathbb{Z}v_1 + ... + \mathbb{Z}v_m = \left\{\sum_{i=1}^{m} k_i v_i \mid k_1, ..., k_m \in \mathbb{Z}\right\}.$$

(e) En déduire qu'il existe une base $(u_1, ..., u_p)$ de $\mathbb{Q}^p$ telle que

$$\forall M \in G,\ Mu_i \in \mathbb{Z}u_1 + ... + \mathbb{Z}u_p = \left\{\sum_{i=1}^{p} k_i u_i \mid k_1, ..., k_p \in \mathbb{Z}\right\}.$$

(f) En déduire qu'il existe une matrice F de $GL_p(\mathbb{Q})$ telle que

$$\forall M \in G,\ F^{-1}MF \in SL_p(\mathbb{Z}).$$

Jusqu'à la fin du problème, on se place dans le cas particulier $p = 2$.

13. Soient A et B deux éléments de $SL_2(\mathbb{Q})$ et soit G le sous-groupe (multiplicatif) de $(SL_2(\mathbb{Q}), .)$ engendré par A et B. C'est le plus petit sous-groupe de $(SL_2(\mathbb{Q}), .)$ contenant A et B, il peut s'écrire

$$G = \left\{Q_1 Q_2 ... Q_p \mid p \in \mathbb{N}^*,\ Q_1, Q_2, ..., Q_p \in \{I_2, A, B, A^{-1}, B^{-1}\}\right\}.$$

On considère K le sous-groupe additif de $(\mathcal{M}_2(\mathbb{Q}), +)$ suivant

$$K = \mathbb{Z}I_2 + \mathbb{Z}A + \mathbb{Z}B + \mathbb{Z}AB + \mathbb{Z}BA + \mathbb{Z}ABA + \mathbb{Z}BAB$$

que l'on peut écrire

$$K = \left\{k_1 I_2 + k_2 A + k_3 B + k_4 AB + k_5 BA + k_6 ABA + k_7 BAB \mid k_1, ..., k_7 \in \mathbb{Z}\right\}.$$

On suppose de plus que $\mathrm{Tr}\,(A)$, $\mathrm{Tr}\,(B)$ et $\mathrm{Tr}\,(AB)$ appartiennent à $\mathbb{Z}$.

(a) Démontrer que A^{-1} et B^{-1} appartiennent à K.

(b) Démontrer que $G \subset K$.

(c) En déduire qu'il existe un entier strictement positif d tel que

$$\forall M \in G,\ dM \in \mathcal{M}_2(\mathbb{Z}).$$

14. Soient $A, B \in SL_2(\mathbb{Q})$.

(a) Montrer l'équivalence entre les deux propositions suivantes :

i) Il existe une matrice F de $GL_2(\mathbb{Q})$ telle que $F^{-1}AF$ et $F^{-1}BF$ appartiennent à $SL_2(\mathbb{Z})$.

ii) $\mathrm{Tr}\,(A), \mathrm{Tr}\,(B)$ et $\det(A+B)$ appartiennent à $\mathbb{Z}$.

(b) Soit n un entier strictement positif. Soient X, Y et Z des matrices de $SL_2(\mathbb{Q})$ telles que $\mathrm{Tr}\,(X)$ et $\mathrm{Tr}\,(Y)$ appartiennent à $\mathbb{Z}$ et qui satisfont la relation $X^n + Y^n = Z^n$.
Montrer qu'il existe une matrice F de $GL_2(\mathbb{Q})$ telle que $X_1 = F^{-1}XF$, $Y_1 = F^{-1}YF$ et $Z_1 = F^{-1}ZF$, avec X_1^n, Y_1^n et Z_1^n qui appartiennent à $SL_2(\mathbb{Z})$ et $X_1^n + Y_1^n = Z_1^n$.