Les calculatrices, téléphones, tablettes, ordinateurs, montres connectées et tous appareils électroniques de communication ou de stockage, ainsi que les documents sont interdits.

La qualité de la rédaction est un facteur important d'appréciation des copies. Les candidats sont donc invités à produire des raisonnements clairs, complets et concis.

Les candidats peuvent utiliser les résultats énoncés dans les questions ou parties précédentes, en veillant dans ce cas à préciser la référence du résultat utilisé.

Notations et rappels.

— Si $\mathscr{E}$ est un ensemble fini, on note $\#\mathscr{E}$ son cardinal.

— Si x est un nombre réel, on note $E(x)$ sa partie entière.

— Si $\mathbf{K}$ désigne le corps des nombres réels $\mathbf{R}$ ou le corps des nombres complexes $\mathbf{C}$, pour tous entiers naturels non nuls d, e, on note $\mathcal{M}_{d,e}(\mathbf{K})$ le $\mathbf{K}$-espace vectoriel des matrices à d lignes et e colonnes à coefficients dans $\mathbf{K}$; lorsque $d = e$, on note aussi $\mathcal{M}_d(\mathbf{K})$ la $\mathbf{K}$-algèbre des matrices à d lignes et d colonnes à coefficients dans $\mathbf{K}$, $GL_d(\mathbf{K})$ le groupe des matrices inversibles, et I_d la matrice identité dans $\mathcal{M}_d(\mathbf{K})$.

— Si $M = (m_{ij})_{i,j\in\{1,\dots,d\}} \in \mathcal{M}_d(\mathbf{K})$, on note ${}^tM = (m_{ji})_{i,j\in\{1,\dots,d\}} \in \mathcal{M}_d(\mathbf{K})$ sa transposée.

— Une matrice M de $\mathcal{M}_d(\mathbf{K})$ définit un endomorphisme sur $\mathbf{K}^d$, endomorphisme qui envoie un vecteur V de $\mathbf{K}^d$ sur le vecteur MV. Cet endomorphisme est aussi noté M.

— Si $v = (v_1, ..., v_d) \in \mathbf{K}^d$, on note $\|v\|_2 = \left(\sum_{i=1}^d |v_i|^2\right)^{1/2}$ et $\|v\|_\infty = \max_{i\in\{1,\dots,d\}} |v_i|$. Pour tout entier $k \geq 0$, si $g = \sum_{i=0}^k g_i t^i \in \mathbf{K}[t]$ est un polynôme de degré au plus k, on note $\|g\|_2 = \left(\sum_{i=0}^k |g_i|^2\right)^{1/2}$ et $\|g\|_\infty = \max_{i\in\{0,\dots,k\}} |g_i|$.

— Si p est un nombre premier, on note π_p la projection canonique sur $\mathbf{Z}/p\mathbf{Z}$, c'est-à-dire le morphisme d'anneaux qui envoie un entier sur sa classe modulo p. Cette projection canonique s'étend en une application, notée elle aussi π_p, sur l'algèbre des polynômes $\mathbf{Z}[t]$, ainsi définie : si $P = \sum_{i=0}^d a_i t^i \in \mathbf{Z}[t]$ est un polynôme, on note $\pi_p(P)$ le polynôme $\sum_{i=0}^d \pi_p(a_i) t^i \in \mathbf{Z}/p\mathbf{Z}[t]$.

— On rappelle que l'anneau $\mathbf{Z}[t]$ est un anneau factoriel. On pourra utiliser sans démonstration le fait que deux polynômes f et g à coefficients entiers dont l'un est unitaire ont un unique pgcd unitaire qu'on notera $\mathrm{pgcd}(f, g)$. Ce pgcd est aussi l'unique pgcd unitaire de f et g considérés dans $\mathbf{Q}[t]$.

— Soit $f = t^d + \sum_{i=0}^{d-1} f_i t^i \in \mathbf{C}[t]$ un polynôme unitaire de degré $d \geq 1$. On lui associe la

matrice

$$A_f = \begin{pmatrix} 0 & 0 & 0 & \dots & 0 & 0 & -f_0 \\ 1 & 0 & 0 & \dots & 0 & 0 & -f_1 \\ 0 & 1 & 0 & \dots & 0 & 0 & -f_2 \\ \vdots & & \ddots & \ddots & & \vdots & \vdots \\ \vdots & & & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & 0 & -f_{d-2} \\ 0 & 0 & 0 & \dots & 0 & 1 & -f_{d-1} \end{pmatrix} \in \mathcal{M}_d(\mathbf{C}). \quad (1)$$

On rappelle que le polynôme caractéristique de A_f est f.

Les questions préliminaires des différentes parties ont été rassemblées, sous forme d'exercices, au début du sujet ; il est vivement conseillé de les traiter en priorité.

Exercice 1

On considère la matrice

$$A = \begin{pmatrix} 1/2 & 1/2 & 0 & 0 \\ 1/4 & 1/4 & 1/2 & 0 \\ 1/8 & 1/8 & 1/4 & 1/2 \\ 1/8 & 1/8 & 1/4 & 1/2 \end{pmatrix} \in \mathcal{M}_4(\mathbf{R}).$$

1. Déterminer la dimension du noyau de la matrice A.
2. Quel est le déterminant de A ? Préciser le rang de A.
3. Déterminer les valeurs propres de la matrice A.

   Indication : on pourra calculer $A \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}$ *et* $A \begin{pmatrix} 2 \\ 0 \\ -1 \\ -1 \end{pmatrix}$.

   La matrice A est-elle diagonalisable ?

Exercice 2

Soit $f = t^d + \sum_{i=0}^{d-1} f_i t^i \in \mathbf{R}[t]$ un polynôme unitaire de degré $d \geq 1$ à coefficients réels.

1. Soit $A = (a_{ij})_{i,j \in \{1,\dots,d\}} \in \mathcal{M}_d(\mathbf{C})$ une matrice. Montrer que si $\lambda \in \mathbf{C}$ est tel que, pour tout i, $|a_{ii} - \lambda| > \sum_{j \neq i} |a_{ij}|$, alors $A - \lambda I_d$ est inversible.
2. Soit λ une racine de f : montrer que la matrice $A_f - \lambda I_d$, avec la définition (1), n'est pas inversible.
3. Soit μ dans $\mathbf{C}$ tel que $|\mu| > 1 + \max_{i \in \{0,\dots,d-1\}} |f_i|$; montrer que la matrice $A_f - \mu I_d$ est inversible. En déduire que toutes les racines ρ de f vérifient $|\rho| \leq 1 + \|f\|_\infty$.
4. Soit $g = t^k + \sum_{j=0}^{k-1} g_j t^j \in \mathbf{C}[t]$ un polynôme unitaire divisant f, où $k \geq 1$. Montrer que

$$\|g\|_\infty \leq (2 + 2\|f\|_\infty)^k.$$

Exercice 3

Pour u et v deux vecteurs de $\mathbf{R}^n$, on note $(u|v) = \sum_{i=1}^n u_i v_i$ leur produit scalaire usuel. Soit $(b_1, \ldots, b_d)$ une famille de d vecteurs linéairement indépendants de $\mathbf{R}^n$.

1. On se propose de démontrer qu'il existe une famille de d vecteurs $(b_1^*, \ldots, b_d^*)$ vérifiant les propriétés :

   [P1] $b_1^* = b_1$.

   [P2] pour $i \in \{2, ..., d\}$, $b_i^* = b_i - \sum_{j<i} \mu_{ij} b_j^*$, avec pour tout j dans $\{1, .., i-1\}$, $\mu_{ij} = \frac{(b_i|b_j^*)}{(b_j^*|b_j^*)}$.

   [P3] $(b_i^*|b_j^*) = 0$ pour tous i, j dans $\{1, ..., d\}$ tels que $i \neq j$.

   (a) Soient $(b_1^\sharp, \ldots, b_d^\sharp)$ des vecteurs de $\mathbf{R}^n$ tels que $b_1^\sharp = b_1$ et, pour tout i dans $\{2, ..., d\}$, il existe des nombres réels $(\alpha_{ij})_{1 \leq j \leq i}$ tels que $b_i^\sharp = b_i - \sum_{j<i} \alpha_{ij} b_j^\sharp$. Démontrer que, pour tout i dans $\{1, ..., d\}$, $\mathrm{Vect}(b_1, ..., b_i) = \mathrm{Vect}(b_1^\sharp, \ldots, b_i^\sharp)$ et en déduire que $b_i^\sharp$ est non nul.

   (b) Construire par récurrence une famille de d vecteurs $(b_1^*, \ldots, b_d^*)$ vérifiant les propriétés **[P1]** et **[P2]**.

   (c) Démontrer que la famille de vecteurs ainsi construite vérifie la propriété **[P3]**.

On note B la matrice de $\mathcal{M}_{n,d}(\mathbf{R})$ dont les colonnes sont les vecteurs $b_1, ..., b_d$ dans cet ordre.

2. Montrer que $\prod_{i=1}^d \|b_i^*\|_2 = (\det {}^t BB)^{1/2}$.
3. En déduire que, si $d = n$, $|\det B| \leq \prod_{i=1}^d \|b_i\|_2$.

Exercice 4

Soit p un nombre premier. Si n est un entier naturel, on définit $P_n \in \mathbf{Z}[t]$ par $P_n = t^{p^n} - t$.

1. Soient r et n deux entiers naturels, avec $r > 0$; on note $n = qr + k$, $0 \leq k < r$, la division euclidienne de n par r. Montrer qu'il existe un polynôme $Q \in \mathbf{Z}[t]$ tel que $P_n = QP_r + P_k$.
2. En déduire que $\mathrm{pgcd}\,(P_n, P_r) = P_{\mathrm{pgcd}(n,r)}$.
3. Soit $f \in \mathbf{Z}/p\mathbf{Z}[t]$ un polynôme irréductible de degré r ; on note (f) l'idéal $f\mathbf{Z}/p\mathbf{Z}[t]$. Montrer que l'anneau $F = \mathbf{Z}/p\mathbf{Z}[t]/(f)$ est un corps fini de cardinal p^r. En déduire que f divise $\pi_p(P_r)$.

Soit $\mathcal{I}_n$ l'ensemble des polynômes irréductibles unitaires de degré divisant n dans $\mathbf{Z}/p\mathbf{Z}[t]$. On considère le polynôme :

$$Q = \prod_{\varphi \in \mathcal{I}_n} \varphi.$$

4. Démontrer que Q divise $\pi_p(P_n)$.

Dans la suite du problème, on admettra l'égalité $Q = \pi_p(P_n)$.

Préambule au problème

L'objet de ce problème est de développer un ensemble d'outils permettant de calculer la décomposition en produit de puissances de polynômes irréductibles d'un polynôme unitaire de $\mathbf{Z}[t]$, en la déduisant d'un procédé analogue dans $\mathbf{Z}/p\mathbf{Z}[t]$.
La stratégie est de construire, étant donné un nombre premier p assez grand, un polynôme $g \in \mathbf{Z}[t]$, $\deg g < \deg f$, ayant de "petits" coefficients et tel que $\operatorname{pgcd}(\pi_p(f), \pi_p(g)) \neq 1$.
Le problème s'organise de la manière suivante :

- La première partie étudie une suite matricielle de type arithmético-géométrique ; elle établit des résultats qui seront utiles dans la dernière partie.
- La deuxième partie établit que la stratégie est fondée, c'est-à-dire que si g est comme ci-dessus, alors $\operatorname{pgcd}(f, g) \notin \{1, f\}$ dans $\mathbf{Z}[t]$.
- La troisième partie propose une méthode de factorisation dans $\mathbf{Z}/p\mathbf{Z}[t]$.
- Les deux dernières parties décrivent un procédé qui peut être utilisé pour construire le polynôme g, ou *a contrario* prouver l'irréductibilité de f.

Partie 1

Dans cette partie, d est un entier naturel ≥ 2. On note

- H l'hyperplan de $\mathbf{R}^d$ défini par $H = \{(x_1, ..., x_d) \text{ tel que } \sum_{i=1}^{d} x_i = 0\}$,
- $\mathcal{E}$ le vecteur de $\mathbf{R}^d$ dont toutes les coordonnées sont égales à 1.

Pour $k \in \{1, ..., d-1\}$, on introduit les matrices $M_k \in \mathcal{M}_d(\mathbf{R})$ définies par

$$\forall i, j \in \{1, ..., d\}, \qquad (M_k)_{ij} = \begin{cases} \delta_{ij} & \text{si } i \notin \{k, k+1\}, \\ 1/2 & \text{si } (i,j) \in \{k, k+1\}^2, \\ 0 & \text{sinon,} \end{cases} \tag{2}$$

où $\delta_{ij} = 1$ si $i = j$ et $\delta_{ij} = 0$ sinon.

1. Soit k dans $\{1, ..., d-1\}$.
   (a) Démontrer que $\mathbf{R}^d = \operatorname{Vect}(\mathcal{E}) \oplus H$, que $\mathcal{E}$ est un vecteur propre de M_k associé à la valeur propre 1, et que H est stable par l'endomorphisme associé à M_k dans la base canonique de $\mathbf{R}^d$.
   (b) Montrer que pour tout $x \in \mathbf{R}^d$, $\|M_k x\|_2 \leq \|x\|_2$. Etudier le cas d'égalité.

On pose $A = M_{d-1} \cdot M_{d-2} \cdot \cdots \cdot M_2 \cdot M_1$.

2. Démontrer que $\mathcal{E}$ est un vecteur propre de A associé à la valeur propre 1, et que H est stable par l'endomorphisme associé à A dans la base canonique de $\mathbf{R}^d$.
3. Montrer que si $x \notin \operatorname{Vect}(\mathcal{E})$, alors $\|Ax\|_2 < \|x\|_2$. En déduire que le sous-espace propre associé à la valeur propre 1 est $\operatorname{Vect}(\mathcal{E})$.
4. Soit A_H l'endomorphisme induit par A sur H. Justifier que la limite de la suite $(A_H^k)_{k \in \mathbf{N}}$ est l'endomorphisme nul.

On note Π la projection sur $\operatorname{Vect}(\mathcal{E})$ parallèlement à H.

5. Démontrer que la suite $(A^k)_{k \in \mathbf{N}}$ converge vers Π.

Soit G un vecteur dans H.

6. Démontrer que l'équation $X = AX + G$ admet une unique solution dans H, qui sera notée Z. En déduire l'ensemble des solutions de l'équation $X = AX + G$ d'inconnue $X \in \mathbf{R}^d$.
7. Soit $X_0 \in \mathbf{R}^d$ un vecteur et $(X_\ell)_{\ell\in\mathbf{N}}$ la suite d'éléments de $\mathbf{R}^d$ définie par récurrence par

$$X_{\ell+1} = AX_\ell + G, \quad \ell \in \mathbf{N}.$$

Démontrer que la suite $(X_\ell)_{\ell\in\mathbf{N}}$ converge vers le vecteur

$$\lim_{\ell\to\infty} X_\ell = \Pi(X_0) + Z,$$

Partie 2

Soit $f = t^{\deg f} + \sum_{j=0}^{\deg f-1} f_j t^j$ un polynôme unitaire de $\mathbf{Z}[t]$ non constant.

1. Soit $g = \sum_{j=0}^{\deg g} g_j t^j$ un polynôme de $\mathbf{Z}[t]$, qu'on suppose premier avec f.
   (a) Justifier l'existence de $u = \sum_{j=0}^{\deg g-1} u_j t^j$ et $v = \sum_{j=0}^{\deg f-1} v_j t^j$ dans $\mathbf{Q}[t]$ tels que

$$uf + vg = 1.$$

Pour $i \in \{0, ..., \deg g-1\}$ et $j \in \{0, ..., \deg f-1\}$, on introduit les vecteurs w_i et z_j de $\mathbf{R}^{\deg f+\deg g}$ définis par

$$w_i = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ f_0 \\ f_1 \\ \vdots \\ f_{\deg f} \\ 0 \\ \vdots \\ 0 \end{pmatrix} \begin{matrix} \left.\begin{matrix} \\ \\ \\ \end{matrix}\right\} i \\ \\ \\ \\ \\ \left.\begin{matrix} \\ \\ \\ \end{matrix}\right\} \deg g - 1 - i \end{matrix} \qquad z_j = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ g_0 \\ g_1 \\ \vdots \\ g_{\deg g} \\ 0 \\ \vdots \\ 0 \end{pmatrix} \begin{matrix} \left.\begin{matrix} \\ \\ \\ \end{matrix}\right\} j \\ \\ \\ \\ \\ \left.\begin{matrix} \\ \\ \\ \end{matrix}\right\} \deg f - 1 - j \end{matrix}$$

et la matrice $M(f, g)$ dont les colonnes sont $w_0, \ldots, w_{\deg g-1}, z_0, \ldots, z_{\deg f-1}$, de sorte que l'identité

$$uf + vg = 1, \quad u = \sum_{i=0}^{\deg g-1} u_i t^i, \quad v = \sum_{i=0}^{\deg f-1} v_i t^i$$

se réécrit sous la forme du système linéaire suivant :

$$M(f, g) \begin{pmatrix} u_0 \\ u_1 \\ \vdots \\ u_{\deg g-1} \\ v_0 \\ v_1 \\ \vdots \\ v_{\deg f-1} \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

(b) Montrer que $|\det M(f,g)|$ est un entier naturel inférieur ou égal à $\|f\|_2^{\deg g}\|g\|_2^{\deg f}$. **On admet que** $0 \neq \det M(f,g)$**.**

(c) Soit $r = |\det M(f,g)|$. Démontrer que les polynômes $\tilde{u}$ et $\tilde{v}$ définis par $\tilde{u} = ur$ et $\tilde{v} = vr$ sont dans $\mathbf{Z}[t]$ et vérifient $\tilde{u}f + \tilde{v}g = r$.

(d) Soit p un nombre premier tel que $\pi_p(f)$ et $\pi_p(g)$ ne sont pas premiers entre eux dans $\mathbf{Z}/p\mathbf{Z}[t]$.

i. Montrer que p divise $\det M(f,g)$.

ii. En déduire que $p \leq \|f\|_2^{\deg g}\|g\|_2^{\deg f}$.

2. On suppose que le polynôme f est sans facteur carré c'est-à-dire que la décomposition en produit de facteurs irréductibles de f s'écrit sous la forme $f = \prod_{i=1}^{t} f_i$, où les f_i sont irréductibles et deux-à-deux distincts. Soit p un nombre premier tel que

$$p > (\deg f)^{\deg f/2}\, \|f\|_2^{\deg f - 1}\, (2 + 2\|f\|_\infty)^{\deg f(\deg f - 1)}.$$

Soit $h \in \mathbf{Z}[t]$ unitaire, $h \neq 1$, $h \neq f$, et tel que $\pi_p(h)$ est un diviseur irréductible de $\pi_p(f)$ dans $\mathbf{Z}/p\mathbf{Z}[t]$. On note

$$\mathcal{L}_p(h) = \{h \cdot h_1 + ph_2, h_1, h_2 \in \mathbf{Z}[t], \deg(hh_1) \leq \deg f - 1, \deg h_2 \leq \deg f - 1\}.$$

(a) Montrer qu'il existe un polynôme irréductible $g \in \mathbf{Z}[t]$ tel que $\pi_p(h)$ divise $\pi_p(g)$ et g divise f.

(b) Montrer que f n'est pas irréductible dans $\mathbf{Z}[t]$ si et seulement s'il existe $u \in \mathcal{L}_p(h)$ non nul avec

$$\|u\|_\infty \leq (2 + 2\|f\|_\infty)^{\deg f - 1}$$

et que dans ce cas $\operatorname{pgcd}(u, f)$ est un diviseur non trivial de f (c'est-à-dire que $\operatorname{pgcd}(u, f) \notin \{1, f\}$).
Indication : on pourra remarquer que si f n'est pas irréductible dans $\mathbf{Z}[t]$, alors $g \in \mathcal{L}_p(h)$, et exploiter les rappels faits en préambule sur $\mathbf{Z}[t]$.

Partie 3

Dans toute cette partie, p est un nombre premier différent de 2, f est un polynôme unitaire, non constant, de $\mathbf{Z}/p\mathbf{Z}[t]$ de degré n sans facteur carré, et on note $f = f_1 \dots f_r$ la décomposition de f en produit de facteurs irréductibles unitaires dans $\mathbf{Z}/p\mathbf{Z}[t]$.
On définit deux suites de polynômes $\left(u_i\right)_{i \in \mathbf{N}\setminus\{0\}}$ et $\left(g_i\right)_{i \in \mathbf{N}\setminus\{0\}}$ de $\mathbf{Z}/p\mathbf{Z}[t]$ par

$$u_1 = \operatorname{pgcd}(f, t^p - t),\ g_1 = f/u_1 \text{ et, pour tout } i \geq 2,\ u_i = \operatorname{pgcd}(g_{i-1}, t^{p^i} - t),\ g_i = g_{i-1}/u_i.$$

Les pgcd utilisés pour cette définition sont tous choisis unitaires.

1. (a) Montrer que $\prod_{i=1}^{n} u_i = f$.

(b) Montrer que tous les facteurs irréductibles de u_i sont de degré i.

(c) Montrer que f est irréductible sur $\mathbf{Z}/p\mathbf{Z}[t]$ si et seulement si $f = g_{E(n/2)+1}$.

On fait maintenant l'hypothèse que $f = f_1 \dots f_r$, avec $r \geq 2$, les f_i irréductibles, deux à deux distincts et de même degré d. Soit C l'application

$$\begin{aligned} C \ : \mathbf{Z}/p\mathbf{Z}[t] &\longrightarrow \mathbf{Z}/p\mathbf{Z}[t] \\ h(t) &\longmapsto h(t)^{(p^d-1)/2}. \end{aligned}$$

En notant ω la projection canonique de $\mathbf{Z}/p\mathbf{Z}[t]$ sur $\mathbf{Z}/p\mathbf{Z}[t]/(f)$, l'application C définit par factorisation une application $\overline{C}$ (on ne demande pas de vérifier cela) :

$$\begin{aligned} \overline{C} \ : \mathbf{Z}/p\mathbf{Z}[t]/(f) &\longrightarrow \mathbf{Z}/p\mathbf{Z}[t]/(f) \\ \omega(h) &\longmapsto \omega(h)^{(p^d-1)/2}. \end{aligned}$$

2. Soit h dans $\mathbf{Z}/p\mathbf{Z}[t]$ premier avec f. Montrer que $\overline{C}(\omega(h))^2 = 1$.
3. Montrer que $\#\overline{C}^{-1}(\{1\}) = \#\overline{C}^{-1}(\{-1\}) = \left(\frac{p^d-1}{2}\right)^r$.
4. On note $\mathbf{Z}/p\mathbf{Z}[t]_{rd}$ le sous-espace vectoriel de $\mathbf{Z}/p\mathbf{Z}[t]$ de dimension rd constitué des éléments dont le degré est **strictement** inférieur à rd.
   (a) Soit U une variable aléatoire de loi uniforme à valeurs dans $\mathbf{Z}/p\mathbf{Z}[t]_{rd}$. On note A l'événement $\{\text{pgcd}\,(U, f) \notin \{1, f\}\}$ et B l'événement $\{\text{pgcd}\,(C(U) - 1, f) \notin \{1, f\}\}$. Montrer que, pour $r \geq 2$, $p \geq 3$ et tout d,

$$\Pr(A \cup B) = 1 - \frac{1}{p^{rd}} - 2\left(\frac{p^d - 1}{2p^d}\right)^r \geq \frac{1}{2}.$$

   (b) Soit $(U_i)_{i\in\mathbf{N}}$ une suite de variables aléatoires indépendantes de loi uniforme à valeurs dans $\mathbf{Z}/p\mathbf{Z}[t]_{rd}$, et S la variable aléatoire à valeurs dans $\mathbf{N} \cup \{+\infty\}$ définie par

$$S = \min\{i \in \mathbf{N} \text{ tel que } \text{pgcd}\,(U_i, f) \notin \{1, f\} \text{ ou } \text{pgcd}\,(C(U_i) - 1, f) \notin \{1, f\}\}$$

   avec la convention que le minimum de l'ensemble vide est $+\infty$. On note $\mathbf{E}(S)$ son espérance. Montrer que $\mathbf{E}(S) \leq 2$.

Partie 4

Pour tout nombre réel α, on note $[\alpha]$ la partie entière de α si $\alpha - \frac{1}{2}$ est un entier, et l'entier le plus proche de α sinon.
Pour tous vecteurs $u, v \in \mathbf{Q}^d$ avec v non nul, on pose

$$Q(u, v) = \left[\frac{(u|v)}{\|v\|_2^2}\right].$$

On note $\mathcal{M}(u, v) \in \mathcal{M}_{d,2}(\mathbf{R})$ la matrice dont la première colonne est u et la seconde colonne est v.

1. Montrer que $\|u - qv\|_2 \geq \|u - Q(u, v)v\|_2$, pour tout entier q.
2. Montrer que $|(u - Q(u, v)v|v)| \leq \|v\|_2^2/2$.

À partir de maintenant, on suppose donnés deux vecteurs $u, v \in \mathbf{Q}^d$ linéairement indépendants dans $\mathbf{R}^d$, et on pose $L(u,v) = \{au + bv, (a,b) \in \mathbf{Z}^2\}$.
On construit deux suites $\big(u_n\big)_{n\in\mathbf{N}}$, $\big(v_n\big)_{n\in\mathbf{N}}$ de vecteurs de $\mathbf{Q}^d$ par :

$$u_0 = u, \qquad v_0 = v, \qquad (u_{n+1}, v_{n+1}) = \begin{cases} (u_n, v_n) \text{ si } \|v_n\|_2 \geq \frac{\|u_n\|_2}{\sqrt{2}} \text{ et } n > 0, \\ (v_n, u_n - q_n v_n) \text{ avec } q_n = Q(u_n, v_n) \text{ sinon.} \end{cases}$$

3. Montrer que, pour tout n, il existe $\Gamma_n(u,v) \in \mathcal{M}_2(\mathbf{Z})$, avec $|\det \Gamma_n(u,v)| = 1$, tel que $\mathcal{M}(u_n, v_n) = \mathcal{M}(u,v)\Gamma_n(u,v)$.
4. Montrer que, pour tout n, $L(u_n, v_n) = L(u,v)$.
5. Montrer qu'il existe $\lambda \in \mathbf{N} \setminus \{0\}$ tel que, pour tout $x \in L(u,v)$, $\lambda x \in \mathbf{Z}^d$.
6. Montrer qu'il existe k tel que $(u_{k+1}, v_{k+1}) = (u_k, v_k)$.
7. Pour cet entier k on note w le projeté de v_k orthogonalement à $\mathrm{Vect}(u_k)$. Montrer que $\|w\|_2 \geq \|u_k\|_2/2$.

On désigne par $\tilde{\Gamma}$ l'application qui à (u,v) associe la matrice $\Gamma_k(u,v) = \tilde{\Gamma}(u,v)$, où k est l'entier exhibé à la question 6.

Partie 5

On suppose dans cette partie que $(b_1, \ldots, b_d)$ sont des vecteurs de $\mathbf{Z}^n$ linéairement indépendants. On leur associe la famille $(b_1^*, \ldots, b_d^*)$ définie dans l'Exercice 3 (ce sont alors des vecteurs de $\mathbf{Q}^n$). Pour $i \in \{2, ..., d\}$, on note ω_i la projection orthogonale sur $\mathrm{Vect}(b_i^*, \ldots, b_d^*)$. Enfin, on pose

$$L(b_1, \ldots, b_d) = \left\{ \sum_{i=1}^{d} x_i b_i, \ (x_1, ..., x_d) \in \mathbf{Z}^d \right\}.$$

1. Montrer que $\inf_{x \in L(b_1,...,b_d)\setminus\{0\}} \|x\|_2 = \min_{x \in L(b_1,...,b_d)\setminus\{0\}} \|x\|_2$.
2. Montrer que $\min_{x \in L(b_1,...,b_d)\setminus\{0\}} \|x\|_2 \geq \min_{i\in\{1,...,d\}} \|b_i^*\|_2$.
3. Soit $k \in \{2, ..., d-1\}$. Étant donnés $(b_1, \ldots, b_d)$ d vecteurs de $\mathbf{Z}^n$, on pose

$$T_k(b_1, \ldots, b_d) = (b_1, \ldots, b_{k-1}, b'_k, b'_{k+1}, b_{k+2}, \ldots, b_d),$$

où

$$\mathcal{M}(b'_k, b'_{k+1}) = \mathcal{M}(b_k, b_{k+1})\tilde{\Gamma}(\omega_k(b_k), \omega_k(b_{k+1})).$$

Montrer que $L(T_k(b_1, \ldots, b_d)) = L(b_1, \ldots, b_d)$.

Si $(u_1, \ldots, u_d)$ est une famille de vecteurs linéairement indépendants de $\mathbf{R}^n$ et $(u_1^*, \ldots, u_d^*)$ la famille orthogonale associée définie dans l'Exercice 3, on introduit le vecteur $V(u_1, \ldots, u_d) \in \mathbf{R}^d$ dont les coordonnées sont données par

$$\Big(\log \|u_i^*\|_2 - \frac{1}{d} \sum_{k=1}^{d} \log \|u_k^*\|_2 \Big), \quad i \in \{1, ..., d\}.$$

On définit les vecteurs $C_1, ..., C_{d-1}$ de $\mathbf{R}^d$ suivants : C_k est le vecteur dont les coordonnées sont

$$(C_k)_i = \begin{cases} 0 & \text{si } i \notin \{k, k+1\}, \\ 1 & \text{si } i = k, \\ -1 & \text{si } i = k+1. \end{cases}$$

On pose $\gamma = \log(2)/2$. Enfin, on introduit les vecteurs définis par les relations

$$g_1 = \gamma C_1, \quad g_{k+1} = M_{k+1} g_k + \gamma C_{k+1} \text{ pour } k \in \{1, ..., d-2\}, \quad G = g_{d-1},$$

où les matrices M_k sont définies par (2) dans la Partie 1. On va aussi utiliser la matrice $A = M_{d-1}...M_1$.
On définit un ordre partiel sur $\mathbf{R}^d$: avec $u = (u_1, ..., u_d)$ et $v = (v_1, ..., v_d)$ dans $\mathbf{R}^d$, on a $u \preceq v$ si et seulement si $u_i \leq v_i$ pour tout $i \in \{1, ..., d\}$.

4. Soit $M \in \mathcal{M}_d(\mathbf{R})$ une matrice dont tous les coefficients sont positifs ou nuls. Montrer que pour tous u, v dans $\mathbf{R}^d$ tels que $u \preceq v$, on a $Mu \preceq Mv$.

On définit la matrice $P \in \mathcal{M}_d(\mathbf{R})$ dont les coefficients sont

$$P_{ij} = 1 \text{ si } i \geq j, \; P_{ij} = 0 \text{ sinon, pour } i, j \in \{1, ..., d\}.$$

On admet que les résultats de la Partie 4 se réécrivent sous la forme

$$PV(T_k(b_1, ..., b_d)) \preceq P\big(M_k V(b_1, ..., b_d) + \gamma C_k\big),$$

pour tout $k \in \{1, \ldots, d-1\}$ et pour toute famille $(b_1, \ldots, b_d)$ de vecteurs linéairement indépendants de $\mathbf{Z}^n$.

5. En déduire qu'en définissant $T(b_1, \ldots, b_d) = T_{d-1}(T_{d-2}(\ldots(T_1(b_1, \ldots, b_d))))$, on a

$$PV(T(b_1, \ldots, b_d)) \preceq P\big(AV(b_1, \ldots, b_d) + G\big).$$

Indication : on pourra remarquer que P est inversible et PAP^{-1} est une matrice à coefficients positifs ou nuls.

6. On pose $Z = \gamma \begin{pmatrix} d-1 \\ d-3 \\ \vdots \\ 3-d \\ 1-d \end{pmatrix} \in \mathbf{R}^d$ (la $k^{\text{ème}}$ coordonnée est donc $d-(2k-1)$). Montrer que $M_k Z = Z - \gamma C_k$. En déduire que $Z = AZ + G$ et que $Z \in H$, l'hyperplan défini en Partie 1.

7. (a) On considère la suite de vecteurs définie par

$$X_0 = V(b_1, \ldots, b_d), \qquad X_{\ell+1} = AX_\ell + G.$$

En exploitant les résultats de la Partie 1, analyser le comportement de X_ℓ quand $\ell \to \infty$.

(b) Établir que, pour tout $\ell \in \mathbf{N}$, on a $PV(T^\ell(b_1, \ldots, b_d)) \preceq PX_\ell$.

(c) Soit $\varepsilon > 0$ fixé. Montrer qu'il existe un entier $N_0(\varepsilon)$ tel que si $N \geq N_0(\varepsilon)$ et $(c_1, \ldots, c_d) = T^N(b_1, \ldots, b_d)$ alors on a

$$\|c_1\|_2 \leq 2^{(d-1)/2} \ \exp(\varepsilon) \left(\prod_{i=1}^{d} \|b_i^*\|_2 \right)^{1/d} \leq 2^{d-1} \exp(d\varepsilon) \|c_d^*\|_2.$$

On note $c_i^{(0)} = c_i$ pour $i \in \{1, ..., d\}$. En reproduisant la même manipulation que précédemment sur $(c_1, \ldots, c_{d-1})$, on obtient $(c_1^{(1)}, \ldots, c_{d-1}^{(1)})$; puis de nouveau sur $(c_1^{(1)}, \ldots, c_{d-2}^{(1)})$ on obtient $(c_1^{(2)}, \ldots, c_{d-2}^{(2)})$, etc. jusqu'à obtenir $c_1^{(d-1)}$. On pose $\beta_i = c_i^{(d-i)}$ pour $i \in \{1, ..., d\}$.

8. Montrer que $L(\beta_1, \ldots, \beta_d) = L(b_1, \ldots, b_d)$, et que

$$\min_{i \in \{1,\ldots,d\}} \|c_1^{(i)}\|_2 \leq 2^{d-1} \ \exp(d\varepsilon) \ \min_{x \in L(b_1,\ldots,b_d) \setminus \{0\}} \|x\|_2.$$

Les techniques de cette partie permettent donc de trouver un élément « presque minimal » de $\mathcal{L}_p(h)$ au sens de la norme euclidienne. En les combinant avec les techniques de la Partie 2, on peut construire un algorithme de factorisation de polynômes unitaires de $\mathbf{Z}[t]$.