**ECOLES NORMALES SUPERIEURES**

**CONCOURS D'ADMISSION 2022**

**JEUDI 28 AVRIL 2022**
**08h00 - 14h00**

**FILIERE MP - Epreuve n° 7**

# MATHEMATIQUES D (U)

***Durée : 6 heures***

***L'utilisation des calculatrices n'est pas autorisée pour cette épreuve***

*Le sujet comprend 13 pages, numérotées de 1 à 13.*

⋆ ⋆ ⋆

Début de l'épreuve

# Points rationnels de la quadrique

$$3x^2 + 3y^2 - z^2 = -1$$

*Le problème comporte 8 parties. La partie 1 n'est utilisée que dans la partie 8. Les parties 2 à 6 sont interdépendantes. La partie 7 est indépendante des précédentes. La partie 8 utilise les résultats de toutes les autres parties.*

## Notations et définitions

L'objet de ce problème est l'étude des solutions entières et rationnelles de l'équation

$$3x^2 + 3y^2 - z^2 = -1 \ . \tag{1}$$

- On note $V$ l'espace des vecteurs colonnes $M_{3,1}(\mathbb{R})$, canoniquement isomorphe à $\mathbb{R}^3$. Étant donné un vecteur $v$ de $V$, on note $x_v$, $y_v$ et $z_v$ ses coordonnées dans la base canonique, de sorte que
$$v = \begin{pmatrix} x_v \\ y_v \\ z_v \end{pmatrix}$$

- On munit $V$ de la forme bilinéaire symétrique
$$B : \left( \begin{pmatrix} x \\ y \\ z \end{pmatrix}, \begin{pmatrix} x' \\ y' \\ z' \end{pmatrix} \right) \mapsto 3xx' + 3yy' - zz'$$
Notons que $B$ n'est *pas* définie positive.
L'équation (1) se réécrit : $B\left( \begin{pmatrix} x \\ y \\ z \end{pmatrix}, \begin{pmatrix} x \\ y \\ z \end{pmatrix} \right) = -1.$

- On note $\mathcal{H}$ l'ensemble
$$\mathcal{H} = \{v \in V \mid B(v,v) = -1 \text{ et } z_v > 0\} \ .$$

- On note $v_0$ le vecteur $\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$. On remarquera que $v_0 \in \mathcal{H}$ et que pour tout $v \in V$, on a
$$B(v, v_0) = -z_v \ .$$

- On note $V_{\mathbb{Z}}$ l'ensemble des vecteurs de $V$ à coordonnées entières. Un vecteur entier est appelé *primitif* si ses coordonnées n'ont pas de diviseur commun autre que 1 et $-1$.
- On note $V_{\mathbb{Q}}$ l'ensemble des vecteurs de $V$ à coordonnées rationnelles. Étant donné un vecteur $v \in V_{\mathbb{Q}}$, on appelle *hauteur* de $v$, et on note $\mathrm{ht}(v)$, le plus petit dénominateur commun à $x_v$, $y_v$ et $z_v$, c'est-à-dire le plus petit entier $k \geq 1$ tel que $kv \in V_{\mathbb{Z}}$.
- Pour tout entier $k \geq 1$, on définit

$$P_k = \{v \in \mathcal{H} \cap V_{\mathbb{Q}} \text{ tels que } kv \in V_{\mathbb{Z}}\}$$

et pour tout $h \in \mathbb{R}_+^*$, on pose

$$P_{\leq h} = \bigcup_{k \leq h} P_k = \{v \in \mathcal{H} \cap V_{\mathbb{Q}} \text{ tels que } \mathrm{ht}(v) \leq h\} \ .$$

- Le cardinal d'un ensemble fini $A$ est noté $|A|$.
- Étant donné un nombre réel $x$, on note $\lfloor x \rfloor$ le plus grand entier inférieur ou égal à $x$ et $\lceil x \rceil$ le plus petit entier supérieur ou égal à $x$.

# Partie 1 : Un critère d'équidistribution

*Les résultats de cette partie ne seront utilisés que dans la partie 8.*

**1.1.** Soit $a$ un réel de l'intervalle ouvert $]0,1[$. Montrer qu'il existe $\lambda > 0$ tel que le polynôme

$$P(x) = x - \lambda x(x-a)(x-1)$$

vérifie les deux propriétés suivantes :

1. $P([0,1]) = [0,1]$,
2. $P$ est croissant sur $[0,1]$.

On fixe un tel choix de $\lambda$ et on note $P_a$ le polynôme $x - \lambda x(x-a)(x-1)$. Soit $(P_a^{\circ n})_{n \geq 0}$ la suite de polynômes définie par récurrence par

- $P_a^{\circ 0}(x) = x$,
- $P_a^{\circ n+1}(x) = P_a\left(P_a^{\circ n}(x)\right)$.

**1.2.** Montrer que $P_a^{\circ n}$ converge uniformément vers 1 sur tout compact de $]a,1]$ et uniformément vers 0 sur tout compact de $[0,a[$.

On note $\mathcal{C}([-1,1])$ l'espace vectoriel des fonctions continues de $[-1,1]$ dans $\mathbb{C}$ et $\mathcal{T}([-1,1])$ le sous-espace vectoriel complexe de $\mathcal{C}([-1,1])$ engendré par les fonctions

$$e_k : t \mapsto e^{i\pi kt} \ , \quad k \in \mathbb{Z} \ .$$

**1.3.** Montrer que $\mathcal{T}([0,1])$ est une sous-algèbre de $\mathcal{C}([-1,1])$ pour la loi de multiplication usuelle des fonctions.

**1.4.** Soit $b \in \mathbb{R}$ tel que $\cos(b) \in ]0,1[$. Montrer que la suite de fonctions $(f_{b,n})_{n\in\mathbb{N}}$ définie par

$$f_{b,n}(t) = P_{\cos(b)}^{\circ n}\left(\cos^2\left(\frac{\pi}{2}t\right)\right)$$

converge uniformément vers 1 sur tout compact de $]-\cos(b),\cos(b)[$ et converge uniformément vers 0 sur tout compact de $[-1,-\cos(b)[\cup]\cos(b),1]$.

On note $\mathcal{C}([-1,1]^2)$ l'espace des fonctions continues de $[-1,1]^2$ dans $\mathbb{C}$ et $\mathcal{T}([-1,1]^2)$ le sous-espace engendré par les fonctions

$$e_{u,v} : (s,t) \mapsto e^{i\pi us}e^{i\pi vt} \ , \quad (u,v) \in \mathbb{Z}^2 \ .$$

**1.5.** Soient $a,b,c,d \in [-1,1]$ tels que $a < b$ et $c < d$. Montrer que pour tout $\varepsilon < \min(\frac{b-a}{2}, \frac{d-c}{2})$, il existe $f_\varepsilon \in \mathcal{T}([-1,1]\times[-1,1])$ vérifiant les propriétés suivantes :

1. $f_\varepsilon(s,t) \in [0,1]$ pour tout $(s,t) \in [-1,1]^2$,
2. $f_\varepsilon(s,t) \leq \varepsilon$ pour $(s,t) \notin [a,b]\times[c,d]$,
3. $f_\varepsilon(s,t) \geq 1-\varepsilon$ pour $(s,t) \in [a+\varepsilon, b-\varepsilon]\times[c+\varepsilon,d-\varepsilon]$.

Soit $(E_n)_{n\in\mathbb{N}}$ une suite de parties finies de $[-1,1]^2$ telle que, pour tout $(u,v) \neq (0,0)$,

$$\frac{1}{|E_n|}\sum_{(s,t)\in E_n} e_{u,v}(s,t) \underset{n\to+\infty}{\longrightarrow} 0 \ .$$

**1.6.** Montrer que pour tout $f \in \mathcal{T}$,

$$\frac{1}{|E_n|}\sum_{(s,t)\in E_n} f(s,t) \underset{n\to+\infty}{\longrightarrow} \frac{1}{4}\int_{-1}^{1}\int_{-1}^{1} f(s,t)\,\mathrm{d}s\,\mathrm{d}t \ .$$

**1.7.** Montrer que pour tous $a,b,c,d \in [-1,1]$ tels que $a<b$ et $c<d$,

$$\frac{|E_n \cap ([a,b]\times[c,d])|}{|E_n|} \underset{n\to+\infty}{\longrightarrow} \frac{|b-a|\,|d-c|}{4} \ .$$

**On dit d'une telle suite $E_n$ qu'elle *s'équidistribue* dans $[-1,1]\times[-1,1]$.**

# Partie 2 : Pseudo-orthogonalité

Rappelons que la forme bilinéaire $B$ définie en préambule n'est *pas* définie positive. Étant donné un vecteur $v \in V$, on appelle *pseudo-orthogonal* de $v$ et on note $v^\perp$ l'ensemble des vecteurs $w$ tels que $B(v,w) = 0$.

**2.1.** Soit $v$ un vecteur non-nul de $V$. Montrer que $v^\perp$ est un sous-espace vectoriel de $V$ de codimension 1, et que $v^\perp$ est un supplémentaire de la droite engendrée par $v$ si et seulement si $B(v,v) \neq 0$.

**2.2.** Soient $v_1$ et $v_2$ deux vecteurs de $\mathcal{H}$. Montrer que

$$B(v_1, v_2) \leq -1 \ ,$$

avec égalité si et seulement si $v_1 = v_2$.

**2.3.** En déduire que si $v \in \mathcal{H}$, alors la restriction de $B$ à $v^\perp$ est un produit scalaire.

# Partie 3 : Symétries réelles

On identifie $M_3(\mathbb{R})$ avec les endomorphismes linéaires de $V$. Soit $G$ l'ensemble des endomorphismes $g$ tels que

$$B(gu, gv) = B(u,v)$$

pour tous $u, v \in V$.

**3.1.** Montrer que $G$ est un groupe pour la composition des applications linéaires.

**3.2.** Montrer que, pour tout $g \in G$, on a $g(\mathcal{H}) = \mathcal{H}$ ou $-g(\mathcal{H}) = \mathcal{H}$.

On notera $G_0$ le sous-groupe de $G$ formé des éléments $g$ tels que $g(\mathcal{H}) = \mathcal{H}$. Pour tout $w \in V$ tel que $B(w,w) > 0$, on définit l'application linéaire

$$s_w : v \mapsto v - 2\frac{B(v,w)}{B(w,w)} w \ .$$

**3.3.** Montrer que $s_w^2 = \mathrm{Id}_V$, et déterminer les valeurs propres et espaces propres de $s_w$.

**3.4.** Montrer que $s_w \in G_0$.

**3.5.** Montrer que pour tous $u, v \in \mathcal{H}$, il existe $w \in V$ tel que $B(w,w) > 0$ et $s_w(u) = v$.

# Partie 4 : Géométrie de $\mathcal{H}$

On note arcch : $[1, +\infty) \to \mathbb{R}_+$ la réciproque du cosinus hyperbolique, c'est-à-dire l'unique fonction telle que

$$\operatorname{arcch}(\operatorname{ch}(x)) = x$$

pour tout $x \in \mathbb{R}_+$. La fonction arcch est dérivable sur $]1, +\infty)$ et on a

$$\operatorname{arcch}'(x) = \frac{1}{\sqrt{x^2 - 1}} \ .$$

**4.1.** Soit $v \in \mathcal{H}$. Montrer que l'ensemble $T_v\mathcal{H}$ des vecteurs tangents à $\mathcal{H}$ au point $v$ est un sous-espace vectoriel de $V$ et déterminer ce sous-espace. En déduire que la restriction de $B$ à $T_v\mathcal{H}$ est un produit scalaire.

Soit $\gamma : [a, b] \to \mathcal{H}$ une courbe paramétrée continue et $\mathcal{C}^1$ par morceaux (vue comme fonction à valeurs dans $V$). On définit la *longueur hyperbolique* de $\gamma$ par

$$\ell(\gamma) = \int_a^b \sqrt{B(\gamma'(t), \gamma'(t))}\, \mathrm{d}t \ .$$

**4.2.** Montrer que si $h : [c, d] \to [a, b]$ est un difféomorphisme, alors $\ell(\gamma) = \ell(\gamma \circ h)$.

**4.3.** Posons $f(t) = -B(\gamma(a), \gamma(t))$ et $n(t) = \sqrt{B(\gamma'(t), \gamma'(t))}$. Montrer que

$$f'(t) \leq \sqrt{f(t)^2 - 1}\, n(t) \ .$$

**4.4.** En déduire que

$$-B(\gamma(a), \gamma(b)) \leq \operatorname{ch}(\ell(\gamma)) \ .$$

Soient $u$ et $v$ deux points de $\mathcal{H}$. On définit la *distance hyperbolique* entre $u$ et $v$ par

$$d(u, v) = \inf_{\gamma} \ell(\gamma) \ ,$$

où l'infimum est pris sur l'ensemble des chemins continus et $\mathcal{C}^1$ par morceaux $\gamma : [a, b] \to \mathcal{H}$ tels que $\gamma(a) = u$ et $\gamma(b) = v$.

**4.5.** Montrer que $d$ est une distance sur $\mathcal{H}$, c'est-à-dire que

- $d(u, v) = d(v, u)$,
- $d(u, w) \leq d(u, v) + d(v, w)$ et
- $d(u, v) = 0 \Leftrightarrow u = v$

pour tous $u, v, w \in \mathcal{H}$.

**4.6.** Montrer que $d(gu, gv) = d(u, v)$ pour tout $g \in G$.

Pour tout $(t,\theta) \in \mathbb{R}_+ \times [0,2\pi]$, on définit

$$F(t,\theta) = \begin{pmatrix} \frac{1}{\sqrt{3}}\mathrm{sh}(t)\cos(\theta) \\ \frac{1}{\sqrt{3}}\mathrm{sh}(t)\sin(\theta) \\ \mathrm{ch}(t) \end{pmatrix} .$$

**4.7.** Montrer que $F$ est à valeurs dans $\mathcal{H}$ et que $F : \mathbb{R}_+ \times [0,2\pi] \to \mathcal{H}$ est surjective.

**4.8.** Calculer, pour tout $\theta \in [0,2\pi]$, la longueur hyperbolique du chemin

$$\begin{array}{rccc} \gamma : & [0,b] & \to & \mathcal{H} \\ & t & \mapsto & F(t,\theta) . \end{array}$$

**4.9.** Montrer que pour tous $u, v \in \mathcal{H}$, on a

$$\mathrm{ch}(d(u,v)) = -B(u,v) .$$

# Partie 5 : Symétries entières

Rappelons que $G_0$ désigne le sous-groupe des endomorphismes de $V$ préservant $B$ et $\mathcal{H}$ (cf Question 3.2). On considère maintenant $\Gamma$ le sous-groupe de $G_0$ formé des éléments $g$ tels que $g(V_\mathbb{Z}) = V_\mathbb{Z}$.

**5.1.** Montrer que pour tout $v, w \in \mathcal{H}$ et tout $R \geq 0$, l'ensemble

$$\{g \in \Gamma \text{ tels que } d(gv,w) \leq R\}$$

est fini.

On considère les trois vecteurs

$$w_1 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} , \quad w_2 = \begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix} , \quad w_3 = \begin{pmatrix} -1 \\ 0 \\ -1 \end{pmatrix} .$$

**5.2.** Vérifier que $s_{w_1}, s_{w_2}$ et $s_{w_3}$ appartiennent à $\Gamma$ et calculer les matrices correspondantes.

On note $T$ l'ensemble des vecteurs $v \in \mathcal{H}$ tels que $B(v,w_i) \geq 0$ pour tout $i \in \{1,2,3\}$.

**5.3.** Montrer que $T$ est compact et contient $v_0$.

Soit $S_{1,2}$ le sous-groupe de $\Gamma$ engendré par $s_{w_1}$ et $s_{w_2}$. Soit $v \in \mathcal{H}$.

**5.4.** Montrer qu'il existe $g \in S_{1,2}$ tel que

$$B(gv,w_1) \geq 0 \quad \text{et} \quad B(gv,w_2) \geq 0 .$$

**5.5.** Montrer que si $B(v,w_3) < 0$, alors $d(v_0, s_{w_3}(v)) < d(v_0,v)$.

**5.6.** Montrer que pour tout $v \in \mathcal{H}$, il existe $g \in \Gamma$ tel que $gv \in T$.

# Partie 6 : Points rationnels de hauteur bornée

Dans cette section, on fixe un entier $k \geq 1$.

**6.1.** Montrer que l'ensemble $P_k$ défini en préambule est invariant par $\Gamma$.

Pour tout $s > 1$, on note $P_k(s)$ le sous-ensemble de $P_k$ formé des vecteurs $v$ tels que $z_v \leq s$.

**6.2.** Montrer que $P_k(s)$ est fini.

Le but de cette partie est d'estimer la croissance du cardinal de $P_k(s)$ lorsque $s$ tend vers $+\infty$.

**6.3.** Montrer qu'il existe une constante $C > 0$ telle que pour tout $v \in \mathcal{H}$,

$$|\{g \in \Gamma \text{ tels que } gv \in T\}| \leq C \ .$$

Pour tout $R \in \mathbb{R}$, on pose

$$\Gamma(R) = \{g \in \Gamma \text{ tels que } d(v_0, gv_0) \leq R\} \ .$$

Rappelons que $\Gamma(R)$ est un ensemble fini d'après la question 5.1. Enfin, posons $D = \sup_{v \in T} d(v_0, v)$.

**6.4.** Montrer que, pour tout $s \geq 0$,

$$\frac{1}{C}|\Gamma(\operatorname{arcch}(s) - D)| \cdot |P_k \cap T| \leq |P_k(s)| \leq |\Gamma(\operatorname{arcch}(s) + D)| \cdot |P_k \cap T| \ .$$

Soit $F : [0, 2\pi] \times \mathbb{R}_+ \to \mathcal{H}$ l'application définie à la question 4.6.

**6.5.** Pour tout $(\theta, \alpha) \in [0, 2\pi] \times \mathbb{R}_+$ montrer que

$$d(F(t, \theta), F(t, \theta + \alpha e^{-t})) \underset{t \to +\infty}{\longrightarrow} \operatorname{arcch}\left(1 + \frac{\alpha^2}{8}\right)$$

et que la convergence est uniforme sur tout compact de $[0, 2\pi] \times \mathbb{R}_+$.

Pour tout $n \in \mathbb{N}$, on définit

$$\Delta(n) = \left\{ F\left(k \ln(2), \frac{2\pi l}{2^k}\right), k \in \{0, \ldots, n\}, l \in \{1, \ldots, 2^k\} \right\} \ .$$

**6.6.** Montrer qu'il existe $r > 0$ vérifiant les deux propriétés suivantes :

1. pour tout $g \in \Gamma(n \ln(2))$, il existe $v \in \Delta(n)$ tel que $d(gv_0, v) \leq r$,
2. pour tout $v \in \Delta(n)$, il existe $g \in \Gamma(n \ln(2))$ tel que $d(gv_0, v) \leq r$.

Fixons un tel $r$.

**6.7.** Montrer qu'il existe une constante $A \geq 1$ vérifiant les deux propriétés suivantes :

1. pour tout $g \in \Gamma(n\ln(2))$,

$$|\{v \in \Delta(n) \text{ tels que } d(gv_0, v) \leq r\}| \leq A \ ,$$

2. pour tout $v \in \Delta(n)$,

$$|\{g \in \Gamma(n\ln(2)) \text{ tels que } d(gv_0, v) \leq r\}| \leq A \ .$$

**6.8.** Montrer l'existence de constantes $C_1 > C_2 > 0$ et $R_0 > 0$ telles que, pour tout $R \geq R_0$,

$$C_2 e^R \leq |\Gamma(R)| \leq C_1 e^R \ .$$

**6.9.** En déduire l'existence de constantes $C_1' > C_2' > 0$ et $s_0 > 1$ telles que, pour tout $k \in \mathbb{N}^*$ et tout $s \geq s_0$,

$$C_2' \, s \, |P_k \cap T| \leq |P_k(s)| \leq C_1' \, s \, |P_k \cap T| \ .$$

# Partie 7 : L'équation $a^2 + b^2 = 0 \mod d$

*Cette partie est indépendante des précédentes.*

Soit $d$ un entier non nul. On rappelle que, si $d = kd'$, $k, d' \in \mathbb{N}^*$, on a un morphisme injectif de groupes abéliens

$$\begin{array}{ccc} \mathbb{Z}/d'\mathbb{Z} & \to & \mathbb{Z}/d\mathbb{Z} \\ a & \mapsto & ka \end{array}$$

et un morphisme surjectif d'anneaux

$$\begin{array}{ccc} \mathbb{Z}/d\mathbb{Z} & \to & \mathbb{Z}/d'\mathbb{Z} \\ a & \mapsto & a \mod d' \end{array}$$

On note $S(d)$ l'ensemble des paires $(a, b) \in (\mathbb{Z}/d\mathbb{Z})^2$ qui satisfont

$$a^2 + b^2 = 0 \ .$$

On dira qu'une paire $(a, b) \in S(d)$ est *primitive* s'il n'existe pas de diviseur $k$ de $d$ et de paire $(a', b') \in S(\frac{d}{k})$ telle que $(a, b) = (ka', kb')$. On notera $S_{prim}(d) \subset S(d)$ le sous-ensemble des paires primitives. On fera attention au fait que la paire $(0, 0) \in S(d)$ n'est primitive pour aucun $d \geq 2$ puisqu'elle s'écrit $(d \cdot 0, d \cdot 0)$ avec $(0, 0) \in S(1)$.

Rappelons que l'application $n \mapsto e^{\frac{2i\pi}{d}n}$ définit un morphisme du groupe $\mathbb{Z}/d\mathbb{Z}$ vers le groupe des nombres complexes de module 1. Étant donnés deux entiers relatifs $u$ et $v$, on définit

$$L(u, v, d) = \sum_{(a,b) \in S(d)} e^{\frac{2i\pi}{d}ua} e^{\frac{2i\pi}{d}vb} \ ,$$

et

$$L_{prim}(u,v,d) = \sum_{(a,b)\in S_{prim}(d)} e^{\frac{2i\pi}{d}ua} e^{\frac{2i\pi}{d}vb} \ .$$

En particulier, on a $L(0,0,d) = |S(d)|$ et $L_{prim}(0,0,d) = |S_{prim}(d)|$.

**7.1.** Soit $u$ un entier. Montrer que la somme

$$\sum_{k\in\mathbb{Z}/d\mathbb{Z}} e^{\frac{2i\pi}{d}ku}$$

vaut $d$ si $u \equiv 0 \mod d$ et 0 sinon.

**7.2.** Soit $n$ un entier premier avec $d$. Montrer que l'application

$$(a,b) \mapsto (na, nb)$$

est une bijection de $S_{prim}(d)$ dans $S_{prim}(d)$.

Soient $d_1$ et $d_2$ deux entiers premiers entre eux et $m$ et $n$ deux entiers tels que $md_1 + nd_2 = 1$.

**7.3.** Montrer que l'application

$$\varphi : ((a_1,b_1),(a_2,b_2)) \mapsto (nd_2a_1 + md_1a_2\,, nd_2b_1 + md_1b_2)$$

est une bijection de $S_{prim}(d_1) \times S_{prim}(d_2)$ dans $S_{prim}(d_1d_2)$.

**7.4.** Montrer que pour tous $(u,v) \in \mathbb{Z}^2$,

$$L_{prim}(u,v,d_1d_2) = L_{prim}(u,v,d_1)\, L_{prim}(u,v,d_2) \ .$$

Soit $p$ un nombre premier et $\alpha \geq 1$ un entier.

**7.5.** Montrer que

$$L_{prim}(u,v,p^\alpha) = L(u,v,p^\alpha) - L(u,v,p^{\alpha-1}) \ .$$

**7.6.** Montrer qu'il existe $h \in \mathbb{Z}/p\mathbb{Z}$ tel que $h^2 = -1$ si et seulement si $p = 2$ ou $p \equiv 1 \mod 4$.

**On suppose que $p$ est congru à 1 modulo 4.**

**7.7.** Montrer que $(a,b) \in S(p)$ si et seulement si

$$b = ha \quad \text{ou} \quad b = -ha \ ,$$

où $h$ est une solution de $h^2 = -1 \mod p$.

**7.8.** Soit $\alpha \geq 1$. Montrer qu'il existe $j \in \mathbb{Z}/p^\alpha\mathbb{Z}$ tel que $j^2 = -1$.

On fixe un tel $j$.

**7.9.** Soit $a \in \mathbb{Z}/p^\alpha\mathbb{Z}$ tel que $p$ ne divise pas $a$. Montrer que $(a,b) \in S(p^\alpha)$ si et seulement si

$$b = ja \quad \text{ou} \quad b = -ja \ .$$

**7.10.** Soit $a \in \mathbb{Z}/p^\alpha\mathbb{Z}$ et $k \leq \alpha$ le plus grand entier tel que $p^k$ divise $a$. Montrer que si $k < \frac{\alpha}{2}$, alors $(a,b) \in S(p^\alpha)$ si et seulement si

$$b \equiv \pm ja \mod p^{\alpha-k}$$

et que si $k \geq \frac{\alpha}{2}$, alors $(a,b) \in S(p^\alpha)$ si et seulement si $p^{\lceil \frac{\alpha}{2} \rceil}$ divise $b$.

**7.11.** Montrer que pour tout $k \geq 1$, on a

$$|S_{prim}(p^{2k})| \geq \frac{1}{2} p^{2k} \ .$$

Soit $(u,v) \in \mathbb{Z}^2 \backslash (0,0)$.

**7.12.** Soit $\alpha \geq 2$. Montrer que $L(u,v,p^\alpha) = 0$ dès que $p^{\alpha-1}$ ne divise pas $u^2+v^2$. En déduire que si $\alpha \geq 3$, alors $L_{prim}(u,v,p^\alpha) = 0$ dès que $p^{\alpha-2}$ ne divise pas $u^2+v^2$.

**7.13.** Montrer que si $p$ ne divise pas $u^2+v^2$, alors

$$|L_{prim}(u,v,p)| \leq 2 \quad \text{et} \quad |L_{prim}(u,v,p^2)| \leq 1 \ .$$

**On admettra dans la suite que les résultats des questions 7.11, 7.12 et 7.13 sont valables aussi pour $p \equiv 3 \mod 4$, et que les résultats des questions 7.12 et 7.13 sont valables aussi pour $p = 2$.**

Pour tout entier $d \geq 2$, on note $\mathcal{P}(d)$ l'ensemble des nombres premiers divisant $d$.

**7.14.** Montrer l'inégalité

$$d \geq |\mathcal{P}(d)|!$$

En déduire que

$$|\mathcal{P}(d)| = \underset{d \to +\infty}{o}(\log(d)) \ .$$

**7.15.** Soit $d$ un entier impair. Montrer que

$$|S_{prim}(d^2)| \geq d^2 \, 2^{-|\mathcal{P}(d)|} \ .$$

En déduire que, pour tout $\varepsilon > 0$, on a

$$d^{2-\varepsilon} = \underset{d \to +\infty}{o}(S_{prim}(d^2)) \ .$$

**7.16.** Soit $(u,v) \neq (0,0)$. Montrer l'existence d'une constante $C$ (dépendant de $(u,v)$) telle que pour tout $d > 0$,

$$|L_{prim}(u,v,d)| \leq C \, 2^{|\mathcal{P}(d)|} \ .$$

En déduire que, pour tout $\varepsilon > 0$, on a

$$|L_{prim}(u,v,d)| = \underset{d \to +\infty}{o}(d^\varepsilon) \ .$$

# Partie 8 : Comportement asymptotique de $P_{\leq h}$

*Cette partie reprend les définitions, notations et résultats des parties précédentes. Le but est d'estimer le nombre de points de $\mathcal{H} \cap V_{\mathbb{Q}}$ de hauteur inférieure à $h$ contenus dans une boule hyperbolique donnée lorsque $h$ tend vers $+\infty$.*

On note $\mathbb{D}$ le disque ouvert de centre $(0,0)$ de rayon $\frac{1}{\sqrt{3}}$ dans le plan $\mathbb{R}^2$ muni de la norme euclidienne standard :

$$\|(s,t)\| = \sqrt{s^2+t^2}\ .$$

Considérons l'application $\varphi : \mathbb{D} \to V$ définie par

$$\Psi(s,t) = \begin{pmatrix} \dfrac{2s}{1-3s^2-3t^2} \\ \dfrac{2t}{1-3s^2-3t^2} \\ \dfrac{1+3s^2+3t^2}{1-3s^2-3t^2} \end{pmatrix}\ .$$

**8.1.** Montrer que $\Psi$ est un homéomorphisme de $\mathbb{D}$ dans $\mathcal{H}$ et déterminer l'homéomorphisme réciproque.

**8.2.** Montrer que $\Psi$ induit une bijection de $\mathbb{D} \cap \mathbb{Q}^2$ dans $\mathcal{H} \cap V_{\mathbb{Q}}$.

**8.3.** Montrer que l'image réciproque de $P_{\leq h}$ par $\Psi$ est l'ensemble des points $u \in \mathbb{D} \cap \mathbb{Q}^2$ qui s'écrivent

$$u = \left(\frac{a}{d}, \frac{b}{d}\right)$$

avec $a, b \in \mathbb{Z}$ et $d \in \mathbb{N}^*$ vérifiant les trois conditions suivantes :

1. $d$ divise $3a^2+3b^2$,
2. $d - 3a^2 - 3b^2$ est pair,
3. $d \leq h\,(z_{\Psi(u)}+1)$.

On note $Q_d$ l'ensemble des paires $(\frac{a}{d}, \frac{b}{d}) \in \mathbb{Q}^2 \cap ([-1,1[\times[-1,1[)$ vérifiant

1. $d$ divise $3a^2+3b^2$,
2. $d - 3a^2 - 3b^2$ est pair.

On note également $Q_d^{prim}$ le sous-ensemble de $Q_d$ formé des couples $(x,y)$ qui n'appartiennent pas à $Q_{d'}$ où $d' > 0$ est un diviseur de $d$ différent de $d$. Enfin, on note

$$Q_{\leq h} = \bigcup_{d \leq h} Q_d = \bigcup_{d \leq h} Q_d^{prim}\ .$$

**8.4.** Montrer que les ensembles $Q_d^{prim}$ sont deux à deux disjoints.

**8.5.** Supposons que 2 divise $d$ et que 3 ne divise pas $d$. Montrer que pour tout $(u,v) \in \mathbb{Z}^2$, on a

$$\sum_{(s,t)\in Q_d^{prim}} e_{u,v}(s,t) = 4L_{prim}(u,v,d) \ ,$$

où $e_{u,v}$ est la fonction définie à la question 1.4 et $L_{prim}$ est définie au début de la partie 7.

**On admettra les formules similaires suivantes :**

- si 6 divise $d$, alors

$$\sum_{(s,t)\in Q_d^{prim}} e_{u,v}(s,t) = 36\, L_{prim}\left(u,v,\frac{d}{3}\right) \ ,$$

- si ni 2 ni 3 ne divisent $d$, alors

$$\sum_{(s,t)\in Q_d^{prim}} e_{u,v}(s,t) = ((-1)^u + (-1)^v) L_{prim}(u,v,d) \ ,$$

- si 2 ne divise pas $d$ mais 3 divise $d$, alors

$$\sum_{(s,t)\in Q_d^{prim}} e_{u,v}(s,t) = 9((-1)^u + (-1)^v) L_{prim}\left(u,v,\frac{d}{3}\right) \ .$$

Pour tout $h \in \mathbb{R}_+$, on pose $A(h) = |Q_{\leq h}|$.

**8.6.** Montrer que

$$h^{\frac{3}{2}-\varepsilon} = \underset{h\to+\infty}{o}(A(h))$$

pour tout $\varepsilon > 0$.

**8.7.** En déduire que la suite $(Q_{\leq n})_{n\in\mathbb{N}^*}$ s'équidistribue dans $[-1,1]^2$ (au sens défini à la fin de la partie 1.)

Fixons $r \in \mathbb{R}_+^*$. Soit $v \in \mathcal{H}$. On note $b_r(v)$ la *boule hyperbolique ouverte* de centre $v$ de rayon $r$, c'est-à-dire

$$b_r(v) = \{v' \in \mathcal{H} \mid d(v,v') < r\} \ .$$

**8.8.** Montrer que l'image réciproque de $b_r(v)$ par $\Psi$ est la boule ouverte euclidienne de centre

$$\left(\frac{x_v}{z_v + \mathrm{ch}(r)}, \frac{y_v}{z_v + \mathrm{ch}(r)}\right)$$

et de rayon

$$\frac{\mathrm{sh}(r)}{\sqrt{3}\,(z_v + \mathrm{ch}(r))} \ .$$

**8.9.** Montrer qu'il existe deux constantes $C_2, C_1 > 0$ (dépendant de $r$) telles que, pour tout $v \in \mathcal{H}$ tel que $d(v,v_0) > r$, il existe $h_0 > 0$ tel que pour tout $h \geq h_0$,

$$C_1 \frac{A(h\,(1+\mathrm{ch}(d(v_0,v)-r)))}{\mathrm{ch}^2(d(v_0,v))} \leq |P_{\leq h} \cap B(v,r)| \leq C_2 \frac{A(h\,(1+\mathrm{ch}(d(v_0,v)+r)))}{\mathrm{ch}^2(d(v_0,v))} \ .$$

**8.10.** Soit $v \in \mathcal{H}$ tel que $d(v, v_0) > r$ et $g \in \Gamma$. Montrer qu'il existe $h_0 > 0$ tel que, pour tout $h \geq h_0$, on a

$$\frac{A(h\,(1+\mathrm{ch}(d(v_0,v)-r)))}{A(h\,(1+\mathrm{ch}(d(v_0,gv)+r)))} \leq \frac{C_2}{C_1}\left(\frac{\mathrm{ch}(d(v_0,v))}{\mathrm{ch}(d(v_0,gv))}\right)^2$$

et

$$\frac{A(h\,(1+\mathrm{ch}(d(v_0,v)+r)))}{A(h\,(1+\mathrm{ch}(d(v_0,gv)-r)))} \geq \frac{C_1}{C_2}\left(\frac{\mathrm{ch}(d(v_0,v))}{\mathrm{ch}(d(v_0,gv))}\right)^2 .$$

**8.11.** Montrer que pour tout $\varepsilon > 0$, on a

$$A(h) = \underset{h\to+\infty}{o}(h^{2+\varepsilon})$$

et

$$h^{2-\varepsilon} = \underset{h\to+\infty}{o}(A(h)) .$$

**8.12.** Conclure que pour tout $\varepsilon > 0$, tout point $v \in \mathcal{H}$ et tout $r > 0$, il existe $h_0 > 0$ tel que pour tout $h \geq h_0$,

$$h^{2-\varepsilon} \leq |P_{\leq h} \cap b(v, r)| \leq h^{2+\varepsilon} .$$

$\star\ \star\ \star$

Fin du sujet