Correction feuille 4

1 Réseaux

Exercice 1. *Diverses propriétés des réseaux dans la suite K est l'un des corps $\mathbb{Q}$ ou $\mathbb{R}$ et V est un K-espace vectoriel de dimension finie $n > 0$. Une partie Γ de V est un sous-réseau s'il existe une famille libre $\mathbf{e} = (e_1, \cdots, e_r)$ de V telle que $\Gamma = \mathbb{Z}e_1 + \cdots + \mathbb{Z}e_r$. On dit que $\mathbf{e}$ est une $\mathbb{Z}$-base de Γ et r est son rang. On dit que Γ est un réseau si $r = n$.*

(i) $\mathbb{Z} + \sqrt{2}\mathbb{Z}$ est-il un sous-réseau de $\mathbb{R}$?

(ii) Soit Γ un réseau de V, $\mathbf{e}$ une $\mathbb{Z}$-base de Γ et $\mathbf{v}$ une base de V. Montrez que $\mathbf{v}$ est une $\mathbb{Z}$-base de Γ si et seulement si la matrice de passage de $\mathbf{e}$ à $\mathbf{v}$ appartient à $GL_n(\mathbb{Z})$.

(iii) Soient Γ un réseau de V et $\Lambda \subset \Gamma$ un sous-groupe. Montrez que Λ est un sous-réseau de V et qu'il existe une $\mathbb{Z}$-base $(e_1, \cdots, e_n)$ de Γ, $1 \leq s \leq n$ et $a_1, \cdots, a_s \in \mathbb{Z}^\times$ vérifiant:

- *$(a_1e_1, \cdots, a_se_s)$ est une $\mathbb{Z}$-base de Λ,*
- *pour $1 \leq i < s$, a_i divise a_{i+1}*

En déduire une CNS pour que Γ/Λ soit fini et calculez son cardinal en fonction des a_i.

(iv) On suppose ici $K = \mathbb{Q}$. Soient Γ, Λ des réseaux de V. Montrez que

- *il existe $d \in \mathbb{N}\backslash\{0\}$ tel que $d\Gamma \subset \Lambda$,*
- *$\Gamma + \Lambda$ et $\Gamma \cap \Lambda$ sont des réseaux de V.*

(v) On suppose ici $K = \mathbb{R}$ et on munit V de sa topologie canonique. Montrez que tout sous-groupe discret[1] Γ de V en est un sous-réseau.

Indication: soit $(e_1, \cdots, e_r)$ une famille libre maximale de Γ et $\mathcal{K} = \{\lambda_1e_1 + \cdots + \lambda_re_r; \lambda_i \in [0, 1]\}$. En utilisant le fait que $\mathcal{K} \cap \Gamma$ est fini et en considérant pour $j \in \mathbb{Z}$ et $x = \lambda_1e_1 + \cdots + \lambda_re_r \in \Gamma$, les $x_j = jx - ([j\lambda_1]e_1 + \cdots + [j\lambda_r]e_r)$[2], montrez que $\lambda_i \in \mathbb{Q}$ et conclure.

A quelles conditions est-ce un réseau?

Preuve : (i) $\sqrt{2}$ n'appartenant pas à $\mathbb{Q}$, $G = \mathbb{Z} + \sqrt{2}\mathbb{Z}$ est dense dans $\mathbb{R}$; si G était un réseau on aurait $G = \alpha\mathbb{Z}$ et serait discret, ce qui n'est pas.

(ii) Si $\mathbf{v}$ est une $\mathbb{Z}$-base de Γ, la matrice de passage de $\mathbf{e}$ à $\mathbf{v}$ et celle de $\mathbf{v}$ à $\mathbf{e}$ sont à coefficients dans $\mathbb{Z}$ et sont inverses l'une de l'autre, d'où le résultat. Réciproquement soit P (resp. P^{-1}) la matrice de passage de $\mathbf{e}$ à $\mathbf{v}$ (reps. de $\mathbf{v}$ à $\mathbf{e}$). Comme P est à coefficients dans $\mathbb{Z}$, le réseau engendré par $\mathbf{e}$ est inclus dans celui engendré par $\mathbf{v}$; l'inclusion inverse découle de même du fait que P^{-1} est à coefficients dans $\mathbb{Z}$.

(iii) C'est le théorème de la base adaptée, sur les modules de type fini sur un anneau principal. Le quotient Γ/Λ est fini si et seulement si les deux réseaux ont le même rang et alors le cardinal est égal à la valeur absolue du produit des a_i, $1 \leq i \leq n$.

(iv) - Soient $\mathbf{e}$ et $\mathbf{f}$ des $\mathbb{Z}$-bases de respectivement Γ et Λ. On note $P = (p_{i,j})_{1 \leq i,j \leq n} \in GL_n(\mathbb{Q})$ la matrice de passage de $\mathbf{f}$ à $\mathbf{e}$ et soit d le ppcm des dénominateurs des $p_{i,j}$, $1 \leq i, j \leq n$, écrits sous formes irréductibles. Il est alors clair que l'on a $d\Gamma \subset \Lambda$.

- Soit d comme ci-dessus. On a alors

$$d\Gamma \subset \Gamma \cap \Lambda \subset \Gamma$$

$$\Gamma \subset \Gamma + \Lambda \subset d^{-1}\Lambda$$

[1] i.e. tel que pour tout compact $\mathcal{K}$ de V, $\mathcal{K} \cap \Gamma$ est fini

[2] $[\lambda]$ désigne la partie entière de λ

L'inclusion $\Gamma \cap \Lambda \subset \Gamma$ (resp. $\Gamma + \Lambda \subset d^{-1}\Lambda$) prouve d'après (iii) que $\Gamma \cap \Lambda$ (resp. $\Gamma + \Lambda$) est un sous-réseau de Γ (resp. $d^{-1}\Lambda$). Les autres inclusions montrent que $\Gamma + \Lambda$ et $\Gamma \cap \Lambda$ sont de rang n.

(v) On procède comme suggéré dans l'indication; $\mathcal{K}$ étant compact, $\mathcal{K} \cap \Gamma$ est fini; on note $y_1, \cdots, y_s$ ses éléments. Soit $x = \sum_{i=1}^r \lambda_i e_i \in \Gamma$, $\lambda_i \in \mathbb{R}$. On considère pour $j \in \mathbb{Z}$, $x_j = jx - \sum_{i=1}^r [j\lambda_i] e_i$; $x_j \in \Gamma \cap \mathcal{K}$ de sorte qu'il existe $j \neq k$ tels que $x_j = x_k$, soit $(j-k)\lambda_i = [j\lambda_i] - [k\lambda_i]$ pour $1 \leq i \leq r$ et donc $\lambda_i \in \mathbb{Q}$. Pour $1 \leq i \leq s$, on écrit $y_i = \sum_{k=1}^r \lambda_k^i e_k$ avec $\lambda_k^i \in \mathbb{Q}$ et soit d le ppcm des dénominateurs des λ_k^i écrits sous forme irréductible. De l'égalité $x = x_1 + \sum_{i=1}^r [\lambda_i] e_i$, on en déduit $dx \in \mathbb{Z}e_1 + \cdots + \mathbb{Z}e_r$ soit $d\Gamma \subset \mathbb{Z}e_1 + \cdots + \mathbb{Z}e_r$, soit $\Gamma \subset \mathbb{Z}d^{-1}e_1 + \cdots + \mathbb{Z}d^{-1}e_r = \Lambda$ et ainsi Γ est un sous-groupe du sous-réseau Λ de V et donc Γ est un sous-réseau de V. En outre Γ est un réseau de V si et seulement si Γ est discret et V/Γ est compact.

Exercice 2. *On reprend les notations de l'exercice précédent avec $K = \mathbb{R}$. On note μ la mesure de Lebesgue de $\mathbb{R}^n$, $(\epsilon_1, \cdots, \epsilon_n)$ sa base canonique et $(.|.)$ le produit scalaire associé $(\epsilon_i|\epsilon_j) = \delta_{i,j}$. Pour Γ un réseau de $\mathbb{R}^n$ et $\mathbf{e} = (e_1, \cdots, e_n)$ une $\mathbb{Z}$-base de Γ, on pose*

- $P_{\mathbf{e},\Gamma} = \{\sum_{i=1}^n \lambda_i e_i;\ \lambda_1, \cdots, \lambda_n \in [0,1]\}$,
- $D_{\mathbf{e},\Gamma} = \{\sum_{i=1}^n \lambda_i e_i;\ \lambda_1, \cdots, \lambda_n \in [0,1[\}$,

On note $S_{\mathbf{e},\Gamma}$ (resp. $T_{\mathbf{e},\Gamma}$) la matrice de terme général $(e_i|e_j)$ (resp. $(\epsilon_i|e_j)$).

(a) Montrez que $S_{\mathbf{e},\Gamma} = {}^tT_{\mathbf{e},\Gamma}T_{\mathbf{e},\Gamma}$. En utilisant la formule du jacobien pour le changement de variables dans les intégrales multiples, en déduire l'égalité $\mu(P_{\mathbf{e},\Gamma}) = \sqrt{\det S_{\mathbf{e},\Gamma}}$. Montrez ensuite que $\mu(P_{\mathbf{e},\Gamma})$ ne dépend que de Γ et non de $\mathbf{e}$; on dit que c'est la mesure du réseau et on la note $\mu(\mathbb{R}^n/\Gamma)$.

(b) Une partie $\mathcal{D}$ de $\mathbb{R}^n$ est un domaine fondamental de Γ, si $\mathcal{D}$ est μ-mesurable et si ses translatés par les vecteurs de Γ forment une partition de $\mathbb{R}^n$. Montrez que $D_{\mathbf{e},\Gamma}$ est un domaine fondamental et que $\mu(\mathcal{D}) = \mu(\mathbb{R}^n/\Gamma)$ pour tout domaine fondamental $\mathcal{D}$ de Γ.

(c) En utilisant le théorème de la base adaptée, montrez que si $\Lambda \subset \Gamma$ sont des réseaux alors Γ/Λ est fini et

$$\mu(\mathbb{R}^n/\Lambda) = \mathrm{card}(\Gamma/\Lambda)\mu(\mathbb{R}^n/\Gamma)$$

(d) (i) Soit $\psi : \mathbb{R}^n \longrightarrow \mathbb{R}^n/\Gamma$ la surjection canonique associé au réseau Γ et soit F une partie de $\mathbb{R}^n$, μ-mesurable vérifiant $\mu(F) > \mu(\mathbb{R}^n/\Gamma)$. Montrez que la restriction de ψ à F n'est pas injective.

(ii) Déduire de (i), le théorème de Minkowski: soient Γ un réseau de $\mathbb{R}^n$ et A une partie μ-mesurable, convexe, symétrique par rapport à O et vérifiant $\mu(A) > 2^n\mu(\mathbb{R}^n/\Gamma)$, alors $A \cap \Gamma \neq \{O\}$.

(iii) Montrez que si C est un convexe compact de $\mathbb{R}^n$, symétrique par rapport à O tel que $\mu(C) \geq 2^n\mu(\mathbb{R}^n/\Gamma)$ alors $C \cap \Gamma \neq \{O\}$.

(iv) Soit v_n le volume de la boule unité fermée de $\mathbb{R}^n$. Montrez qu'il existe $\gamma \in \Gamma$ différent de O et de norme inférieure ou égale à deux fois la racine n-ième de $v_n^{-1}\mu(\mathbb{R}^n/\Gamma)$.

Preuve : (a) L'égalité $S_{\mathbf{e},\Gamma} = {}^tT_{\mathbf{e},\Gamma}T_{\mathbf{e},\Gamma}$ découle directement des formules classiques du cours d'algèbre bilinéaire en remarquant par exemple que $T_{\mathbf{e},\Gamma}$ est la matrice de passage de la base $\mathbf{e}$ à la base canonique; ainsi on a $\det S_{\mathbf{e},\Gamma} = (\det T_{\mathbf{e},\Gamma})^2 \geq 0$. En outre, par la formule du changement de variable dans une intégrale multiple via le jacobien, on a $\mu(P_{\mathbf{e},\Gamma} = \int_{P_{\mathbf{e},\Gamma}} d\mu = \int_0^1 \cdots \int_0^1 |\det T_{\mathbf{e},\Gamma}| dx_1 . \cdots . dx_n$, soit $\mu(P_{\mathbf{e},\Gamma}) = \sqrt{\det S_{\mathbf{e},\Gamma}}$.

Si $\mathbf{f}$ est une autre $\mathbb{Z}$-base de Γ, on ntoe Q la matrice de passage de $\mathbf{e}$ à $\mathbf{f}$; $Q \in GL_n(\mathbb{Z})$ et $S_{\mathbf{f},\Gamma} = {}^tQS_{\mathbf{e},\Gamma}Q$, soit $\det S_{\mathbf{f},\Gamma} = \det S_{\mathbf{e},\Gamma}(\det Q)^2$; or comme $Q \in GL_n(\mathbb{Z})$, on a $\det Q \in \mathbb{Z}^\times$, soit $\det Q = \pm 1$, d'où le résultat.

(b) $D_{\mathbf{e},\Gamma}$ est évidemment un domaine fondamental. Soient alors $\mathcal{D}_1$ et $\mathcal{D}_2$ des domaines fondamentaux quelconques. En considérant $\mathcal{D}_2$ comme un domaine fondamental, on écrit

$$\mathcal{D}_1 = \coprod_{v \in \Gamma} \mathcal{D}_1 \cap (v + \mathcal{D}_2),$$

Γ étant dénombrable et μ étant invariante par translation, on a

$$\begin{aligned} \mu(\mathcal{D}_1) &= \textstyle\sum_{v\in\Gamma} \mu(\mathcal{D}_1 \cap (v + \mathcal{D}_2)) \\ &= \textstyle\sum_{v\in\Gamma} \mu((-v + \mathcal{D}_1) \cap \mathcal{D}_2) \end{aligned}$$

Or comme $-\Gamma = \Gamma$, on en déduit $\mu(\mathcal{D}_1) = \sum_{v\in\Gamma} \mu(\mathcal{D}_2 \cap (v + \mathcal{D}_1)) = \mu(\mathcal{D}_2)$, la dernière égalité découlant du fait que $\mathcal{D}_1$ est un domaine fondamental.

(c) D'après le théorème de la base adaptée, il existe une $\mathbb{Z}$-base $\mathbf{v} = (v_1, \cdots, v_n)$ de Γ et des entiers $a_1|a_2|\cdots|a_n$ tels que $\mathbf{w} = (a_1v_1, \cdots, a_nv_n)$ est une $\mathbb{Z}$-base de Λ. Ainsi on obtient $\mathrm{card}(\Gamma/\Lambda) = \prod_{i=1}^n a_i$ et $S_{\mathbf{w},\Lambda} = {}^tDS_{\mathbf{v},\Gamma}D$ avec $D = \mathrm{diag}(a_1, \cdots, a_n)$, d'où le résultat.

(d) (i) Soit $\mathcal{D}$ un domaine fondamental:

$$\mu(F) = \sum_{\gamma\in\Gamma} \mu(F \cap (\gamma + \mathcal{D})) = \sum_{\gamma\in\Gamma} \mu((F - \gamma) \cap \mathcal{D}) > \mu(D)$$

d'où il en résulte que les $(F - \gamma) \cap \mathcal{D}$ pour $\gamma \in \Gamma$ ne sont pas deux à deux disjoints. Soient donc $x, y \in F$ et $\alpha \neq \beta \in \Gamma$ vérifiant $x - \alpha = y - \beta$ soit $x - y = \alpha - \beta \in \Gamma\backslash\{O\}$ et donc ψ non injective.

(ii) Soit $F = \frac{1}{2}A$; on a donc $\mu(F) > \mu(\mathbb{R}^n/\Gamma)$. D'après la question précédente, il existe donc $x, y \in F$ tels que $x - y \in \Gamma\backslash\{O\}$. En outre $2x$ et $-2y$ appartiennent à A d'après la propriété de symétrie de A par rapport à O, et donc $x - y = \frac{(2x-2y)}{2}$ appartient à A d'après la propriété de convexité de A, d'où le résultat.

(iii) Soit $C_r = (1 + 1/r)C$ pour $r \geq 1$; $C = \cap_{r\geq 1} C_r$ et $\mu(C_r) > 2^n\mu(\mathbb{R}^n/\Gamma)$. D'après la question précédente, soit $x_r \in C_r \cap (\Gamma\backslash\{O\}) \subset K := 2C \cap (\Gamma\backslash\{O\})$; K étant fini, on peut extraire de la suite $(x_r)_{r\geq 1}$ une sous-suite convergente, donc stationnaire, d'où le résultat.

(iv) Une boule $\bar{B}(O, r)$ vérifie $\bar{B}(O, r) \cap (\Gamma\backslash\{O\}) \neq$ dès que $v_n r^n \geq \mu(\mathbb{R}^n/\Gamma)$, d'où le résultat.

Exercice 3. *Quelques applications arithmétiques (utiliser le point (iii) ci-dessus)*

(a) Soient $\epsilon > 0$ et $(\alpha_1, \cdots, \alpha_n) \in \mathbb{R}^n\backslash\mathbb{Q}^n$; montrez qu'il existe $p_1, \cdots, p_n \in \mathbb{Z}$ et $q \in \mathbb{N}$ non nul tels que pour tout $1 \leq i \leq n$, on ait $|\alpha_i - \frac{p_i}{q}| < \frac{\epsilon}{q}$.

Indication: considérez le groupe Γ engendré par les vecteurs de la base canonique et le vecteur $(\alpha_1, \cdots, \alpha_n)$ et remarquez que Γ n'est pas un réseau et n'est donc pas discret.

(b) Montrez que si $p \equiv 1 \mod 4$, p premier, alors p est somme de deux carrés.

Indication: (-1) étant un carré modulo p, soit $u \in \mathbb{Z}$ tel que $u^2 + 1 \equiv 0 \mod p$ et soit $\Gamma = \{(a, b) \in \mathbb{Z}^2 \ / \ a \equiv ub \mod p\}$. Soit $\psi : \mathbb{Z}^2 \longrightarrow \mathbb{Z}/p\mathbb{Z}$ défini par $\psi(a, b) = \overline{a - ub}$. Montrez que Γ est un réseau de mesure p et utilisez le point (d) (iv) de l'exercice précédent.

(c) Montrez que tout nombre premier p est somme de quatre carrés.

Indication: montrez l'existence d'un couple $(u, v) \in \mathbb{Z}^2$ tel que $u^2 + v^2 + 1 \equiv 0 \mod p$. On fixe un tel couple et soit $\Gamma = \{(a, b, c, d) \in \mathbb{Z}^4 \ / \ ua + vb \equiv c \mod p$ et $ub - va \equiv d \mod p\}$. Soit $\psi : \mathbb{Z}^4 \longrightarrow (\mathbb{Z}/p\mathbb{Z})^2$ défini par $\psi(a, b, c, d) = (\overline{c - ua - vb}, \overline{d + va - ub})$. Montrez que Γ est un réseau de $\mathbb{R}^4$ de mesure p^2 et utilisez le point (d) (iv) de l'exercice précédent.

Preuve : (a) Soit Γ le groupe engendré par $(e_1, \cdots, e_n, e_0)$ où $e_1, \cdots, e_n$ sont les vecteurs de la base canonique de $\mathbb{R}^n$ et $e_0 = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}$. Si Γ était discret, il serait un réseau; soit $\mathbf{f}$ une $\mathbb{Z}$-base de Γ et P la matrice de passage de $(e_1, \cdots, e_n)$ à $\mathbf{f}$, $P \in M_n(\mathbb{Z})$ et $P^{-1} \in M_n(\mathbb{Q})$ de sorte que e_0 est une combinaison linéaire à coefficients dans $\mathbb{Q}$ des e_i, ce qui n'est pas. Ainsi Γ n'est pas discret et admet un point d'accumulation P. Soit alors $\epsilon > 0$ avec $\bar{B}(O, \epsilon) \cap \Lambda = \{O\}$, où Λ est le réseau $\mathbb{Z}e_1 + \cdots + \mathbb{Z}e_n$; il existe alors des entiers comme dans l'énoncé tels que $(qe_0 + p_1e_1 + \cdots + p_ne_n) - (q'e_0 + p'_1e_1 + \cdots + p'_ne_n)$ soit de norme inférieure à ϵ avec $q - q' \neq 0$, d'où le résultat.

(b) Soit x un générateur de $(\mathbb{Z}/p\mathbb{Z})^\times \simeq \mathbb{Z}/(p-1)\mathbb{Z}$; on a $x^{p-1} = 1$ et $u = x^{p-1/4}$ est d'ordre 4, soit u^2 d'ordre 2; or dans un corps commutatif de caractéristique différent de 2, il y a exactement un élément d'ordre 2, i.e. -1; en effet l'équation $X^2 - 1$ y a au plus deux solutions. Soit alors $\Gamma = \{(a, b) \in \mathbb{Z}^2 \ / \ a \equiv ub \mod p\}$ et $\psi : \mathbb{Z}^2 \longrightarrow \mathbb{Z}/p\mathbb{Z}$ défini par $\psi(a, b) = a - ub$; ψ est clairement surjective et son noyau est Γ de sorte que ψ induit un isomorphisme $\mathbb{Z}^2/\Gamma \simeq \mathbb{Z}/p\mathbb{Z}$. On en déduit donc que Γ est un réseau de mesure p car $\mu(\mathbb{R}^2/\mathbb{Z}^2) = 1$. D'après l'exercice précédent question (d) (iv), il existe donc $\gamma = ae_1 + be_2 \neq O \in \Gamma$ de module inférieur ou égal à $2\sqrt{\frac{p}{\pi}}$, soit $0 < a^2 + b^2 \leq 4p/\pi < 2p$; or comme $\gamma \in \Gamma$, on a $a^2 + b^2 \equiv b^2(u^2 + 1) \equiv 0 \mod p$, d'où $a^2 + b^2 = p$.

(c) Le cas $p = 2 = 1^2+1^2+0^2+0^2$ est vite traité, soit donc $p \geq 3$ premier. Soit $\phi : (\mathbb{Z}/p\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/p\mathbb{Z})^\times$ défini par $\phi(x) = x^2$; $\mathbb{Z}/p\mathbb{Z}$ étant un corps, $\mathrm{Ker}\,\phi = \{1, -1\}$ de sorte que $\Im\phi$ est de cardinal $(p-1)/2$. En remarquant que 0 est un carré, on en déduit que $\{u^2 \ / \ u \in \mathbb{Z}/p\mathbb{Z}\}$ est de cardinal $(p+1)/2$ et qu'il en est de même pour $\{1 - v^2 \ / \ v \in \mathbb{Z}/p\mathbb{Z}\}$; comme $2(p+1)/2 > p$ on en déduit que $\{u^2 \ / \ u \in \mathbb{Z}/p\mathbb{Z}\} \cap \{1 - v^2 \ / \ v \in \mathbb{Z}/p\mathbb{Z}\}$ est non vide, et on fixe u, v tels que $u^2 + v^2 + 1 \equiv 0 \mod p$. Avec les notations de l'énoncé, ψ est clairement surjective et son noyau est le groupe Γ; ψ induit donc un isomorphisme $\mathbb{Z}^4/\Gamma \simeq (\mathbb{Z}/p\mathbb{Z})^2$. On en déduit donc que Γ est un réseau de mesure p^2. D'après le point (d) (iv) de l'exercice précédent, soit $\gamma = (a, b, c, d) =\in \Gamma\backslash\{O\}$ de norme au carré inférieure ou égale à $4\sqrt{2}p/\pi < 2p$. Or comme $\gamma \in \Gamma$, on a $a^2 + b^2 + c^2 + d^2 \equiv (a^2 + b^2)(u^2 + v^2 + 1) \equiv 0 \mod p$, soit $p = a^2 + b^2 + c^2 + d^2$.

Remarque: En utilisant l'identité remarquable[3]

$$(a^2 + b^2 + c^2 + d^2)(\alpha^2 + \beta^2 + \gamma^2 + \delta^2) = (a\alpha - b\beta - c\gamma - d\delta)^2 + (a\beta + b\alpha + c\delta - d\gamma)^2 +$$
$$+(a\gamma + c\alpha + d\beta - b\delta)^2 + (a\delta + b\gamma + d\alpha - c\beta)^2$$

on en déduit que tout entier est somme de quatre carrés.

2 Codes correcteurs

Pour transmettre une information on utilise l'alphabet $\mathbb{F}_q$; on envoie des messages de n lettres. Le principe des codes correcteurs d'erreurs est de pouvoir corriger des erreurs de transmission (cf. les CD, les transmissions par satellite...). L'ensemble des mots $\mathbb{F}_q^n$ peut être muni de la distance de Hamming définie comme suit: pour $(x_1, \cdots, x_n)$ et $(x'_1, \cdots, x'_n)$ dans $\mathbb{F}_q^n$ alors

$$d(x, x') := \mathrm{card}\{i \in [1, n] \ / \ x_i \neq x'_i\}$$

On vérifie aisément qu'il s'agit bien d'une distance.

Un code est un sous-ensemble $\mathcal{C} \subset \mathbb{F}_q^n$ comportant au moins deux éléments de $\mathbb{F}_q^n$; on définit la distance d'un code comme

$$d(\mathcal{C}) := \min_{x \neq x' \in \mathcal{C}} d(x, x').$$

Le principe consiste, une fois choisi un code $\mathcal{C}$, à n'envoyer que des messages avec des mots appartenant à $\mathcal{C}$; on peut alors repérer jusqu'à $d(\mathcal{C}) - 1$ erreurs de transmission sur un mot en outre si le nombre d'erreurs commises t est tel que $2t + 1 \leq d(\mathcal{C})$, on voit qu'il existe un seul mot de $\mathcal{C}$ situé à une distance $\leq t$ du mot reçu. Le code permet donc de corriger $t := \lfloor \frac{d(\mathcal{C})-1}{t} \rfloor$ erreurs. On introduit le taux de corrections $\frac{t}{n}$ et le taux d'information $\log \mathrm{card}(\mathcal{C})/n \log q$. La théorie de l'information développée par Shannon, indique que si l'on accepte d'envoyer des messages de plus en plus long, il existe des codes aussi sûrs que l'on veut avec un taux d'information proche de 1: cependant le théorème de Shannon est un théorème d'existence, il ne dit pas comment construire les codes en question.

Exercice 1. *On considère des codes linéaires, i.e. $\mathcal{C} \subset \mathbb{F}_q^n$ est un sous-espace vectoriel. Pour tout $x \in \mathcal{C}$, on définit son poids $\omega(x)$ comme le nombre de composantes non nulles.*

(1) Montrer que $d(\mathcal{C}) = \min_{0 \neq x \in \mathcal{C}} \min \omega(x)$.

*(2) **exemple du bit de parité:** pour transmettre $(x_1, \cdots, x_{n-1}) \in \mathbb{F}_2^{n-1}$ on envoie $x = (x_1, \cdots, x_{n-1}, x_1 + \cdots + x_{n-1}) \in \mathbb{F}_2^n$. Montrer qu'il s'agit d'un code cyclique qui permet de repérer une erreur mais pas de la corriger.*

*(3) **Code de Hamming:** prenons l'ensemble des mots de sept chiffres binaires, $q = 2$, $n = 7$ et $\mathcal{C}$ le code ayant pour base*

$$e_0 = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \quad e_1 = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \quad e_2 = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \quad e_3 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \end{pmatrix},$$

[3] cf. le corps des quaternions

Pour transmettre un message $m = (m_0, m_1, m_2, m_3)$, on transmet $x = m_0e_0 + m_1e_1 + m_2e_2 + m_3e_3$. Expliquez le décodage dans le cas où une erreur au plus est commise.

(4) Une matrice génératrice A d'un code $\mathcal{C}$ est une matrice dont les lignes forment une base. Une matrice vérificatrice B d'un code $\mathcal{C}$ est une matrice dont les lignes forment une base des formes linéaires s'annulant sur $\mathcal{C}$. Montrer que $A^tB = 0$ et que la distance du code $\mathcal{C}$ est le plus petit nombre d tel qu'il existe d vecteurs colonnes de B distincts et liés.

(5) Supposons un code $\mathcal{C}$ donné avec une matrice vérificatrice B et supposons que le code est 1-correcteur. Soit alors un message x' reçu différant du message envoyé x en au plus une coordonée: on note $\epsilon = x' - x$ l'erreur commise. Montrer comment calculer ϵ à l'aide de B.

(6) Soit $\mathcal{C}$ un code de longueur n sur $\mathbb{F}_q$. Donnez la distance et des matrices génératrices et vérificatrices des codes suivants:

(i) ***Code raccourci****: soit $d(\mathcal{C}) \leq l \leq n$, on pose $\mathcal{C}^{(l)} := \{x \in \mathbb{F}_q^l \ / \ (x; 0, \cdots, 0) \in \mathcal{C}\}$.*

(ii) ***Code étendu****: $\bar{\mathcal{C}} := \{(x_1, \cdots, x_{n+1}) \in \mathbb{F}_q^{n+1} \ / \ (x_1, \cdots, x_n) \in \mathcal{C} \text{ et } x_1 + \cdots + x_{n+1} = 0\}$.*

(iii) ***Code dual****: $\mathcal{C}^* := \{x' \in \mathbb{F}_q^n \ / \ \forall x \in \mathcal{C}, \ < x, x' >= 0\}$ où $<,>$ est le produit scalaire canonique.*

(7) Soit $\mathcal{C}$ un code de dimension k et de longueur n sur $\mathbb{F}_q$, montrer que $d(\mathcal{C}) \leq n + 1 - k$ et que si $\mathcal{C}$ est t-correcteur alors

$$1 + C_n^1(q-1) + C_n^2(q-1)^2 + \cdots + C_n^t(q-1)^t \leq q^{n-k}$$

Un code tel que $d(\mathcal{C}) = n + 1 - k$ sera dit MDS maximal distance separable. Un code t-correcteur tel que $\mathcal{C} = \bigcup_{x \in \mathcal{C}} B(x, t)$ est dit t-correcteur parfait.

Montrer que le code de Hamming de longueur 7 est 1-correcteur parfait mais qu'il n'est pas MDS.

Preuve : (1) On a $d(x, x') = d(x - x', 0)$ avec $x - x' \in \mathcal{C}$ car $\mathcal{C}$ est un code linéaire.

(2) Pour savoir si le message reçu est correct on vérifie si $x_n = x_1 + \cdots + x_{n-1}$. On peut ainsi repérer une erreur mais on ne peut pas la corriger; sa distance est 2.

(3) Après avoir reçu le message $x = (x_0, \cdots, x_6)$, on vérifie si $f(x) = 0$ avec

$$f(x) = (x_0 + x_3 + x_5 + x_6, x_1 + x_3 + x_4 + x_6, x_2 + x_4 + x_5 + x_6)$$

Si $f(x) = 0$, le message est correct (on suppose qu'il y a au plus une erreur!). Si $f(x) = (1, 0, 0)$ (resp. $(0, 1, 0)$, resp. $(1, 0, 1)$, resp. $(1, 1, 1)$) il faut corriger x_0 (resp. x_1, resp. x_5, resp. x_6); on a alors $m = (x_0, x_1, x_5, x_6)$. Notons $T(x_1, \cdots, x_7) := (x_7, x_1, \cdots, x_6)$ le "décalage", de sorte que $t(e_0) = e_1$, $T(e_1) = e_2$, $T(e_2) = e_3$ et $T(e_3) = e_0 + e_1 + e_2$, ainsi $T(\mathcal{C}) = \mathcal{C}$, i.e. $\mathcal{C}$ est cyclique. On note que chaque vecteur non nul de $\mathcal{C}$ possède au moins trois coordonnées non nulles de sorte que $d(\mathcal{C}) = 3$. Ainsi ce code est 1-correcteur et repère deux erreurs.

(4) Se donner un matrice génératrice équivaut à se donner un base de l'espace vectoriel $\mathcal{C}$, tandis que la donnée d'une matrice vérificatrice reveint à se donner une base de l'espace dual, i.e. des équations linéaires définissant $\mathcal{C}$ en tant que sous-espace de $\mathbb{F}_q^n$. On obtient alors $A^tB = B^tA = 0$. La distance du code est aussi le plus petit nombre d tel qu'il existe d vecteurs colonnes de B distincts et liés.

(5) On a $B(x') = B(\epsilon)$. Si $B(x')$ est nul alors aucune erreur n'a été commise, sinon on calcule les $f_i = B(e_i)$ de sorte que si une seule erreur a été commise, il existe un unique i tel que $B(x')$ soit proportionnel à f_i soit $B(x') = a_i f_i$ et $\epsilon = a_i \epsilon_i$ et $x = x' - a_i e_i$.

(6) (i) Sa longueur est l et on voit aisément que $d(\mathcal{C}^{(l)}) \geq d(\mathcal{C})$.

(ii) On a $d(\mathcal{C}) \leq d(\bar{\mathcal{C}}) \leq d(\mathcal{C}) + 1$.

(iii) On a $\dim \mathcal{C}^* = n - \dim \mathcal{C}$.

(7) Les vecteurs de la forme $(x_1, \cdots, x_{n+1-k}, 0, \cdots, 0)$ forment un sous-espace vectoriel $\mathcal{D}$ de $\mathbb{F}_q^n$. Comme $\dim \mathcal{D} + \dim \mathcal{C} = n + 1$ on voit que $\mathcal{D} \cap \mathcal{C} \neq \{0\}$, d'où l'existence d'un vecteur non nul de $\mathcal{D}$ de poids inférieur ou égal à $n + 1 - k$.

Pour le point suivant, on a $\mathrm{card}B(x,t) = 1+C_n^1(q-1)+C_n^2(q-1)^2+\cdots+C_n^t(q-1)^t$. Si le code est t-correcteur, les boules $B(x,t)$ de centre $x \in \mathcal{C}$ sont disjointes et donc

$$\mathrm{card}\big(\bigcup_{x\in\mathcal{C}} B(x,t)\big) = q^k \mathrm{card}B(0,t) \leq q^n$$

Pour le code de Hamming, on a $\mathrm{card}B(x,1) = 1+7 = 8$ et $8\mathrm{card}\mathcal{C} = 2^7$. Ce code n'est pas MDS car $d(\mathcal{C}) = 3 < 4 = n-k+1$.

3 Quelques équations diophantiennes

Exercice 1. *On considère l'équation $y^2 = x^3 + 7$:*

(i) Montrez qu'il n'y a pas de solutions avec x pair;

(ii) En écrivant l'équation sous la forme $y^2+1 = x^3+8 = (x+2)(x^2-2x+4)$ et en utilisant l'exercice 1 b, déduisez en qu'il n'existe pas de solutions entières.

Preuve : (i) Si x est pair, on a $y^2 \equiv -1 \mod 8$. En écrivant y impair sous la forme $2k+1$, on obtient $y^2 = 1+4k(k+1) \equiv 1 \mod 8$ contradiction.

(ii) On a $x^3+8 = (x+2)(x^2-2x+4)$ avec x impair de la forme $2k+1$; $(x^2-2x+4) = 4k^2+3$. On en déduit donc qu'il existe un p premier divisant x^2-2x+4 avec $p \equiv 3 \mod 4$. Or si p premier divise y^2+1 alors $p \equiv 1 \mod 4$, d'où la contradiction.

Exercice 2. *Soit $A = \mathbb{Z}[i\sqrt{2}] = \{a+ib\sqrt{2} \ / \ (a,b) \in \mathbb{Z}^2\}$. On définit pour $z = a+ib\sqrt{2} \in A$, $N(z) = a^2+2b^2$.*

(a) Montrez que B est euclidien et donc factoriel.

(b) Soient $(x,y) \in \mathbb{Z}^2$, vérifiant l'équation $y^2+2 = x^3$. Montrez que x est impair puis que dans B, $y+i\sqrt{2}$ et $y-i\sqrt{2}$ sont premiers entre eux. En déduire qu'il existe $(a,b) \in \mathbb{Z}^2$ tels que $x = a^2+2b^2$ et $y+i\sqrt{2} = (a+ib\sqrt{2})^3$, puis décrire les solutions de l'équation précédente.

(c) Étudiez comme dans l'exercice précédent l'ensemble $S = \{n \in \mathbb{N} \ / \ \exists (x,y) \in \mathbb{Z}^2, \ n = x^2+2y^2\}$.
Indication: on utilisera que -2 est un carré dans $\mathbb{Z}/p\mathbb{Z}$ si et seulement si $p \equiv 1,3 \mod 8$.

(d) Étudiez de même l'ensemble $\{n \in \mathbb{Z} \ / \ \exists (x,y) \in \mathbb{Z}^2, \ n = x^2-2y^2\}$.

Preuve : (a) On raisonne comme dans l'exercice précédent; soit $N(a+ib\sqrt{2}) = a^2+2b^2$ la norme qui est une fonction multiplicative, et soit $z \in A^\times$; on a $zz' = 1$ soit $N(z)N(z') = 1$ et donc $N(z) = 1$, soit $z = \pm 1$.
Pour montrer que A est euclidien, on remarque à nouveau que z_1/z_2 peut s'écrire sous la forme $q+e$ avec $q \in A$ et $e \in \mathbb{C}$ de norme strictement plus petite que 1. Ainsi on a $z_1 = qz_2+r$, avec $r = z_1 - qz_2 \in A$ et $N(r) < N(z_2)$.

(b) Si x est pair, on a $y^2 \equiv -2 \mod 8$, ce qui ne se peut pas, car les carrés dans $\mathbb{Z}/8\mathbb{Z}$, sont $0,1,4$. On factorise ensuite dans A: $x^3 = (y+i\sqrt{2})(y-i\sqrt{2})$ et soit δ un pgcd de $y+i\sqrt{2}$ et $y-i\sqrt{2}$; on a $\delta = (y+i\sqrt{2}, (i\sqrt{2})^3)$, or $i\sqrt{2}$ est irréductible car de norme 2, et la seule factorisation de 2 est 1×2, de sorte que $i\sqrt{2} = zz'$ implique que $N(z) = 1$ soit z inversible (ou z'). Or $i\sqrt{2}$ ne divise pas y car sinon y^2 serait pair et donc y pair soit x pair, ce qui n'est pas; ainsi $\delta = 1$. On en déduit donc que $(y \pm i\sqrt{2})$ sont des cubes parfaits: $(y \pm i\sqrt{2}) = (a \pm i\sqrt{2})^3$ et $x = a^2+2b^2$. En séparant partie réelle et imaginaire, on trouve alors $y = a^3-6ab^2$ et $1 = b(3a^2-2b^2)$ soit $b = \epsilon = \pm 1 = 3a^2-2$, ce qui donne $b = 1$ et $a = \pm 1$ soit $y = \pm 5$ et $x = 3$ qui est bien une solution de l'équation.

(c) On a à nouveau $n \in S$ si et seulement si il existe $z \in A$ tel que $n = N(z)$. On étudie à nouveau les irréductibles de B; p est irréductible si et seulement si $A/(p)$ est intègre, i.e. X^2+2 n'a pas de racine dans $\mathbb{Z}/p\mathbb{Z}$, i.e. si et seulement si -2 n'est pas un carré dans $\mathbb{Z}/p\mathbb{Z}$, i.e. si et seulement si $p \equiv 5,7 \mod 8$. En raisonnant comme dans l'exercice précédent, on trouve que les irréductibles de A, outre les premiers $p \equiv 5,7 \mod 8$, sont les $z \in A$ tels que $N(z)$ est premier. Toujours en suivant la même démarche, on trouve alors que $n \in S$ si et seulement si $v_p(n)$ est pair pour $p \equiv 5,7 \mod 8$.

(d) De la même façon, la détermination de S se fait via l'étude de $A = \mathbb{Z}[\sqrt{2}]$, dont la norme est a^2-2b^2, avec le morphisme de corps $c(a+b\sqrt{2}) = a-\sqrt{2}b$ de sorte que N est multiplicative. Soit $z \in A^\times$, on a alors $N(z) = \pm 1$.

A nouveau A est euclidien pour le stathme $|N|$. On remarque que -1 est une norme $-1 = 1^2 - 2\times 1^2 = N(1+\sqrt{2})$. Si n est un diviseur de $x^2 - 2y^2$ avec x, y premiers entre eux, alors au signe près n est de la forme $u^2 - 2v^2$. En effet soit $x + \sqrt{2}y = \pi_1 \cdots \pi_r$ une décomposition en produit d'irréductibles; aucun des π_i n'appartient à $\mathbb{Z}$ car x et y sont premiers entre eux, de sorte que comme précédemment les $N(\pi_i)$ sont des premiers de $\mathbb{Z}$; on a alors $x^2 - 2y^2 = N(\pi_1)\cdots N(\pi_r)$ et n au signe près, est un produit de certains de ces $N(\pi_i)$ et donc n est de la forme $N(z) = u^2 - 2v^2$.
L'égalité $-(u^2 - 2v^2) = N((1+\sqrt{2})(u + v\sqrt{2})) = (u+2v)^2 - 2(u+v)^2$ permet de négliger le signe $\pm$. Ainsi un premier impair p est de la forme $x^2 - 2y^2$ si et seulement si 2 est un carré modulo p ce qui est équivalent à $p \equiv \pm$ mod 8.

Exercice 3. *Étude de l'équation de Pell-Fermat: $x^2 - Ny^2 = 1$.*

(i) Traitez le cas $N \leq 0$.

(ii) Montrez que dans le cas où N est un carré parfait, les solutions triviales $x = \pm 1, y = 0$ sont les seules.

(iii) On suppose donc $N > 1$ et N n'est pas un carré parfait. En utilisant l'anneau $\mathbb{Z}[\sqrt{N}]$, montrez l'égalité:

$$(x_1^2 - Ny_1^2)(x_2^2 - Ny_2^2) = (x_1x_2 + Ny_1y_2)^2 - N(x_1y_2 + x_2y_1)^2$$

En déduire que s'il existe un solution non triviale (x_0, y_0) à l'équation de Pell-Fermat, alors il en existe une infinité (x_n, y_n) définie par récurrence:

$$\begin{cases} x_{n+1} = x_0x_n + Ny_0y_n \\ y_{n+1} = x_0y_n + x_ny_0 \end{cases}$$

Calculez par exemple pour $N = 2$, les 3 premiers termes de cette suite en remarquant que $(3, 2)$ est solution.

(iv) Montrez que pour (x_1, y_1) et (x_2, y_2) des solutions positives de l'équation, les équivalences

$$x_1 < x_2 \Leftrightarrow y_1 < y_2 \Leftrightarrow (x_1 + y_1\sqrt{N}) < (x_2 + y_2\sqrt{N})$$

En déduire que s'il existe des solutions non triviales alors il existe une solution minimale (x_0, y_0) pour une relation d'ordre que l'on définira. Montrez ensuite que l'ensemble des solutions sont les (x_n, y_n) définis ci-dessus.

(v) On veut montrer l'existence d'une solution non triviale. Montrez qu'il existe une infinité de rationnels p/q tels que $|\sqrt{N} - p/q| < 1/q^2$.

Indication: commencez par remarquer que p ou $p-1$ est la partie entière de $q\sqrt{N}$, puis appliquez le principe des chaussettes et des tiroirs ($n+1$ chaussettes rangées dans n tiroir, implique qu'un tiroir contient au moins deux chaussettes), où les chaussettes sont les $n\sqrt{N} - [n\sqrt{N}]$ pour $0 \leq n \leq q$ et les tiroirs sont les intervalles $[k/q, (k+1) : q]$ pour $0 \leq k < q$.

En déduire qu'il existe une infinité de couples $(p, q) \in \mathbb{N}^2$ premiers entre eux tels que $-1 - 2\sqrt{N} < p^2 - Nq^2 < 1 + 2\sqrt{N}$. En utilisant à nouveau le principe des tiroirs, montrez qu'il existe un entier $l < 1 + 2\sqrt{N}$, $p_1 \equiv p_2$ mod l, $q_1 \equiv q_2$ mod l tels que $p_1^2 - Nq_1^2 = p_2^2 - Nq_2^2 = \pm l$, et en déduire l'existence d'une solution non triviale.

Preuve : Evidemment, on se limite à chercher les solutions $x, y \geq 0$.

(i) Pour $N \leq -2$, les seules solutions sont clairement $x = 1$ et $y = 0$; pour $N = -1$, on obtient $(x, y) = (1, 0)$ ou $(0, 1)$.

(ii) Soit $N = d^2$; $x^2 - d^2y^2 = (x - dy)(x + dy) = 1$, soit $x + dy = 1 = x - dy$, d'où $x = 1$ et $y = 0$.

(iii) Soit $A = \mathbb{Z}[\sqrt{N}]$ et $N(a + b\sqrt{N}) = a^2 - Nb^2 = (a + b\sqrt{N})(a - b\sqrt{N})$. L'application N est multiplicative, d'où $N((a + b\sqrt{N})(c + d\sqrt{N})) = N(a + b\sqrt{N})N(c + d\sqrt{N})$ ce qui donne l'identité remarquable de l'énoncé.

Avec ces notations (x, y) est solution si et seulement si $N(x + y\sqrt{N}) = 1$, ainsi si (x_0, y_0) est solution alors (x_n, y_n) tel que $x_n + y_n\sqrt{N} = (x_0 + y_0\sqrt{N})^n$, est solution, ce qui donne la relation de récurrence de l'énoncé. On

remarque simplement que la suite (x_n, y_n) prend une infinité de valeur car la solution (x_0, y_0) étant non triviale, $x_0 \geq 2$ et $y_0 \geq 1$ ce qui implique $x_{n+1} > x_n$ et $y_{n+1} > y_n$.

Avec $N = 2$ et $(x_0, y_0) = (3, 2)$, on obtient les premiers termes de la suite (x_n, y_n): $(17, 12)$, $(99, 70)$, $(577, 408)$.

(iv) Soient (x_1, y_1) et (x_2, y_2) des solutions positives; on a alors les équivalences:

$$x_1 < x_2 \Leftrightarrow x_1^2 < x_2^2 \Leftrightarrow 1 + Ny_1^2 < 1 + Ny_2^2 \Leftrightarrow y_1 < y_2 \Leftrightarrow x_1 + y_1\sqrt{N} < x_2 + y_2\sqrt{N}$$

On choisit alors la relation d'ordre suivante sur les solutions positives: $(x_1, y_1) \leq (x_2, y_2)$ si et seulement si $x_1 \leq x_2$. Parmi les solutions positives non triviales, soit donc (x_0, y_0) la solution minimale dont l'existence découle du fait que $\mathbb{N}$ est discret.

Soit alors (x, y) une solution (positive) et $n \geq 0$ tel que $x_n \leq x < x_{n+1}$; on a alors $y_n \leq y < y_{n+1}$ et donc $1 \leq \frac{x+y\sqrt{N}}{x_n+y_n\sqrt{N}} < x_0 + y_0\sqrt{N}$. Or $\frac{x+y\sqrt{N}}{x_n+y_n\sqrt{N}}$ est égal à $X + Y\sqrt{N}$ avec $X = xx_n - Nyy_n$ et $Y = yx_n - xy_n$ avec $X^2 - NY^2 = 1$. En outre, on a $X \geq 0$ car $x \geq y \geq 0$ et $x_n \geq y_n \geq 0$; de même $Y \geq 0$ car sinon $X + Y\sqrt{N} = \frac{1}{X+\sqrt{X^2+1}} < 1$ ce qui n'est pas. Ainsi (X, Y) est une solution positive et $X + Y\sqrt{N} < x_0 + y_0\sqrt{N}$ ce qui contredit la minimalité de (x_0, y_0).

(v) Commençons par montrer l'existence d'une infinité de rationnels p/q tels que $|\sqrt{N} - p/q| < 1/q^2$, soit $-1/q < q\sqrt{N} - p < 1/q$ et donc soit $p = [q\sqrt{N}]$ soit $p = [q\sqrt{N}] + 1$. On raisonne par l'absurde, en supposant la finitude de l'ensemble E de ces rationnels. Soit alors $\epsilon = \min_{p/q \in E} |\sqrt{N} - p/q|$. Comme $\sqrt{N} \notin \mathbb{Q}$, on a $\epsilon > 0$. Soit donc $q_0 > 0$ tel que $1/q_0 < \epsilon$, on va montrer qu'il existe $q \leq q_0$ et p tel que $|\sqrt{N} - p/q| < 1/qq_0 \leq 1/q^2$ ce qui est en contradiction avec le fait que l'on devrait avoir $|\sqrt{N} - p/q| \geq \epsilon$. Considérons donc les q_0-tiroirs $[k/q_0, (k+1)/q_0]$ pour $k = 0, \cdots, q_0 - 1$, et les chaussettes $|q\sqrt{N} - [q\sqrt{N}]|$ pour $n = 1, \cdots, q_0$. Si une chaussette est dans le premier tiroir, c'est gagné. Plaçons-nous dans la situation contraire et soient $q_1 \neq q_2$ deux chaussettes dans le même tiroir, soit $|(q_1 - q_2)\sqrt{N} - [q_1\sqrt{N}] + [q_2\sqrt{N}]| < 1/q_0$. Ainsi en posant $q = |q_1 - q_2|$ et $p = [q_1\sqrt{N}] - [q_2\sqrt{N}]$, on a bien $|a\sqrt{N} - p| < 1/q_0$, d'où le résultat.

Des inégalités $-1/q^2 < \sqrt{N} - p/q < 1/q^2$ avec $p, q > 0$, on obtient $-1/q < q\sqrt{N} - p < 1/q$, soit $0 < p + q\sqrt{N} < 1 : q + 2q\sqrt{N}$ soit $-1 - 2\sqrt{N} < p^2 - Nq^2 < 1 + 2\sqrt{N}$. On obtient de la sorte une infinité de couples (p, q) avec p et q premiers entre eux, et $p^2 - Nq^2$ appartenant à l'intervalle $[-1 - 2\sqrt{N}, 1 + 2\sqrt{N}]$ dans lequel il y a un nombre fini d'entiers (de tiroirs). Selon le principe des tiroirs, il existe un entier l de l'intervalle précédent tel qu'il existe une infinité de couples (p, q) (les chaussettes) avec p et q premiers entre eux, tels que $p^2 - Nq^2 = l$. Comme ${}^s qrtN \notin \mathbb{Q}$, l n'est pas nul; si $l = \pm 1$ c'est gagné, sinon les nouveaux tiroirs sont les éléments de $\mathbb{Z}/l\mathbb{Z}$ et on place la chaussette (p, q) dans le tiroir $\bar{p}$. On en déduit donc l'existence d'une infinité de couples (p, q) comme ci-dessus, tels que tous les p ont la même congruence modulo l. En envoyant ces chaussettes (p, q) dans le tiroir $\bar{q}$, on obtient finalement l'existence d'un infinité de couples (p_i, q_i) tels que p_i et q_i sont premiers entre eux, $p_i^2 - Nq_i^2 = l$, tous les p_i ont la même congruence modulo l; de même que tous les q_i.

Soient alors (p_1, q_1) et (p_2, q_2) des éléments distincts de cet ensemble; on a $p_1^2 - Nq_1^2 = p_2^2 - Nq_2^2 = l$ et $p_1 \equiv p_2 \mod l$ et $q_1 \equiv q_2 \mod l$. Ainsi $p_1q_2 - p_2q_1$ est divisible par l. De l'égalité $(p_1p_2 - Nq_1q_2)^2 - N(p_1q_2 - p_2q_1)^2 = l^2$, on en déduit que l divise $p_1p_2 - Nq_1q_2$ et $(\frac{p_1p_2 - Nq_1q_2}{l}, \frac{p_1q_2 - p_2q_2}{l})$ est alors une solution non triviale de l'équation.