Réseaux de $\mathbb{R}^n$ et applications

Vincent Pilaud

2007

Dans ce texte, on présente quelques thèmes en relation avec la théorie des réseaux d'un espace vectoriel réel de dimension finie. Dans un premier temps (§. 1), on donne les définitions et les propriétés de base des réseaux, et on présente rapidement l'exemple des groupes cristallographiques de l'espace euclidien. On s'intéresse ensuite (§. 2) au volume d'un réseau et en particulier au théorème de Minkowski, que l'on applique à la résolution de certaines équations diophantiennes telles que le théorème des deux carrés. On présente par ailleurs (§. 3) la preuve du théorème des deux carrés utilisant l'anneau des entiers de Gauss, ce qui nous permet de déterminer explicitement le nombre de décompositions d'un entier en somme de deux carrés. On s'intéresse ensuite (§. 4) aux propriétés de certaines figures géométriques relatives au réseau $\mathbb{Z}^2$: on montre par exemple que pour tout entier n, il existe un cercle qui passe par exactement n points de $\mathbb{Z}^2$. On étudie aussi (§. 5) les empilements de boules sur un réseau, l'inégalité d'Hermite et le problème du verger. Enfin (§. 6), on présente très rapidement le problème de la réduction de réseau et l'algorithme LLL, que l'on applique au cassage du cryptosystème par sac-à-dos.

1 Définitions et premiers exemples

1.1 Réseaux, sous-réseaux

Définition 1. *Soit $n \in \mathbb{N}^*$. Une partie Γ de $\mathbb{R}^n$ est appellée* sous-réseau *de $\mathbb{R}^n$ s'il existe une famille libre $e = (e_1, \dots, e_p)$ de $\mathbb{R}^n$ telle que*

$$\Gamma = \mathbb{Z}e_1 \oplus \mathbb{Z}e_2 \oplus \dots \oplus \mathbb{Z}e_p.$$

*On dit que e est une $\mathbb{Z}$-*base *du sous-réseau Γ et que $p = \mathrm{rg}(\Gamma)$ est son* rang. *Un* réseau *de $\mathbb{R}^n$ est un sous-réseau de rang n.*

Proposition 1. *Soit Γ un sous-réseau de $\mathbb{R}^n$ de rang p, e une $\mathbb{Z}$-base de Γ, v une base de* $\mathrm{vect}(\Gamma)$ *et P la matrice de passage de e à v. Alors les conditions suivantes sont équivalentes*

(i) v est une $\mathbb{Z}$-base du sous-réseau Γ,

(ii) $P \in GL_p(\mathbb{Z})$,

(iii) $P \in M_p(\mathbb{Z})$ et $|\det(P)| = 1$.

Théorème 1 (de la base adaptée)**.** *Soit Γ un sous-réseau de $\mathbb{R}^n$ et Λ un sous-groupe de Γ. Alors Λ est un sous-réseau de $\mathbb{R}^n$ de rang inférieur ou égal à celui de Γ. De plus, il existe une $\mathbb{Z}$-base $(e_1, \dots, e_{\mathrm{rg}(\Gamma)})$ de Γ et $\alpha_1, \dots, \alpha_{\mathrm{rg}(\Lambda)} \in \mathbb{Z}^*$ tels que*

(i) la famille $(\alpha_1 e_1, \dots, \alpha_{\mathrm{rg}(\Lambda)} e_{\mathrm{rg}(\Lambda)})$ est une $\mathbb{Z}$-base de Λ,

(ii) pour tout $1 \leq i \leq \mathrm{rg}(\Lambda) - 1$, α_i divise α_{i+1}.

Exemple.

1. $\mathbb{Z}^n$ est un réseau de $\mathbb{R}^n$. La base canonique est une $\mathbb{Z}$-base de $\mathbb{Z}^n$.
2. La matrice $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ transforme la $\mathbb{Z}$-base $e = \left(\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right)$ de $\mathbb{Z}^2$ en la $\mathbb{Z}$-base $e' = \left(\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right)$.
3. L'ensemble $\mathbb{Z} \begin{pmatrix} 1 \\ 0 \end{pmatrix} + 2\mathbb{Z} \begin{pmatrix} 1 \\ 1 \end{pmatrix}$ est un sous-réseau de $\mathbb{Z}^n$. La base adaptée est ici e'.

1.2 Sous-groupes discrets et réseaux

Définition 2. *Une partie X de $\mathbb{R}^n$ est* discrète *si pour tout $x \in X$, il existe $r > 0$ tel que $X \cap B(x, r) = \{x\}$.*
Un sous-groupe additif Γ de $\mathbb{R}^n$ est cocompact *si le quotient $\mathbb{R}^n/\Gamma$ est compact.*

Proposition 2. *1. Un sous-groupe Γ de $\mathbb{R}^n$ est un sous-réseau de $\mathbb{R}^n$ si et seulement si il est discret.*
2. Un sous-groupe Γ de $\mathbb{R}^n$ est un réseau de $\mathbb{R}^n$ si et seulement si il est discret et cocompact.

1.3 Exemple : les pavages de $\mathbb{R}^n$

Définition 3. *On dit qu'un sous-groupe de* $\mathrm{Is}(\mathbb{R}^2)$ *est un* groupe cristallographique *s'il est discret et cocompact.*

Remarque. Un sous-groupe de $\mathrm{Is}(\mathbb{R}^2)$ est un groupe cristallographique si et seulement s'il existe une partie P de $\mathbb{R}^2$ compacte, connexe, d'intérieur non vide telle que

$$(i)\ \mathbb{R}^2 = \bigcup_{g\in G} g(P), \qquad \text{et} \qquad (ii)\ \forall g,h\in G,\ g(\mathring{P})\cap h(\mathring{P})\neq\emptyset \Rightarrow g(P)=h(P).$$

Exemple. Si Γ est un réseau du plan, alors le groupe $G=\{t_u \mid u\in\Gamma\}$ est un groupe cristallographique.

Théorème 2 (Bieberbach)**.** *1. Le sous-groupe des translations d'un groupe cristallographique est un réseau.*

2. Il existe 17 *classes d'isomorphisme de groupes cristallographiques du plan.*

3. Deux sous-groupes cristallographiques isomorphes sont conjugués dans $GA(\mathbb{R}^2)$*.*

2 Volume d'un réseau et théorème de Minkowski

2.1 Volume d'un réseau

Définition 4. *Soit* Γ *un réseau de* $\mathbb{R}^n$ *et* $e=(e_1,\dots,e_n)$ *une* $\mathbb{Z}$*-base de* Γ*. On note* $P_e=\{t_1e_1+\ldots+t_ne_n \mid \forall i\in\{1,\dots,n\}, t_i\in[0,1]\}$ *le* parallèlogramme fondamental *du réseau* Γ *associé à la* $\mathbb{Z}$*-base* e*. On appelle* mesure *du réseau* Γ*, et on note* $\mu(\mathbb{R}^n/\Gamma)$*, le volume de* P_e *(pour la mesure de Lebesgue).*

Remarque. Si A_e est la matrice de $M_n(\mathbb{R})$ dont les vecteurs colonnes sont les vecteurs e_i (représentés dans la base canonique de $\mathbb{R}^n$), alors $\mu(P_e)=|\det(A_e)|$. Comme toute matrice de changement de $\mathbb{Z}$-base du réseau Γ a pour déterminant 1 ou -1, ce volume ne dépend pas de la $\mathbb{Z}$-base e choisie.

Proposition 3 (Inégalité d'Hadamard)**.** *Soit* Γ *un réseau de* $\mathbb{R}^n$ *et* $e=(e_1,\dots,e_n)$ *une* $\mathbb{Z}$*-base de* Γ*. Alors*

$$\mu(\mathbb{R}^n/\Gamma)\leq\prod_{i=1}^{n}\|e_i\|,$$

avec égalité si et seulement si $(e_1,\dots,e_n)$ *est une base orthogonale de* $\mathbb{R}^n$*.*

2.2 Théorème de Minkowski

Lemme 1. *Soit* Γ *un réseau de* $\mathbb{R}^n$ *et* $\psi:\mathbb{R}^n\to\mathbb{R}^n/\Gamma$ *la surjection canonique. Soit* A *une partie* μ*-mesurable de* $\mathbb{R}^n$ *telle que* $\mu(A)>\mu(\mathbb{R}^n/\Gamma)$*. Alors la restriction* $\psi_{|A}$ *de* ψ *à* A *n'est pas injective.*

Soient $e=(e_1,\dots,e_n)$ une $\mathbb{Z}$-base du réseau Γ et $D=\{t_1e_1+\ldots+t_ne_n \mid \forall i\in\{1,\dots,n\}, t_i\in[0,1[\}$. Puisque $\mathbb{R}^n=\bigsqcup_{\gamma\in\Gamma}D+\gamma$, on a

$$\mu(D)=\mu(\mathbb{R}^n/\Gamma)<\mu(A)=\sum_{\gamma\in\Gamma}\mu(A\cap(D+\gamma))=\sum_{\gamma\in\Gamma}\mu((A-\gamma)\cap D).$$

Par conséquent, les $A-\gamma$ ($\gamma\in\Gamma$) ne peuvent pas être deux-à-deux disjoints, ce qui prouve le lemme.

Théorème 3 (Minkowski)**.** *Soit* Γ *un réseau de* $\mathbb{R}^n$ *et* C *une partie de* $\mathbb{R}^n$ *convexe, symétrique par rapport à l'origine et* μ*-mesurable. Si* $\mu(C)>2^n\mu(\mathbb{R}^n/\Gamma)$*, alors* C *contient un élément non nul de* Γ*.*

Pour prouver ce théorème, on applique le lemme précédent à $A=B/2$. Par hypothèse, on a $\mu(A)>\mu(\mathbb{R}^n/\Gamma)$, donc il existe $x,y\in A$ tels que $x-y\in\Gamma\smallsetminus\{0\}$. On sait alors que $2x\in 2A=C$, $2y\in C$, et puisque C est symétrique par rapport à l'origine, $-2y\in C$. Par convexité, on obtient que $x-y=1/2(2x-2y)\in C\cap\Gamma\smallsetminus\{0\}$.

Remarque.

1. Soit $C=\{t_1e_1+\ldots+t_ne_n \mid \forall i\in\{1,\dots,n\}, t_i\in]-1,1[\}$. Alors C est convexe, symétrique par rapport à l'origine, μ-mesurable, avec $\mu(C)=2^n\mu(\mathbb{R}^n/\Gamma)$. Pourtant, $C\cap\Gamma=\{0\}$.
2. Si C est convexe, compact, symétrique par rapport à l'origine, μ-mesurable, avec $\mu(C)=2^n\mu(\mathbb{R}^n/\Gamma)$, alors alors C contient un élément non nul de Γ.

2.3 Application à certaines équations diophantiennes

Proposition 4. *Soient a, b, c, m quatre entiers tels que*

(i) $(x, y) \mapsto ax^2 + bxy + cy^2$ *est une forme quadratique définie positive,*

(ii) il existe $f \in \mathbb{Z}$ *tel que* $af^2 + bf + c \equiv 0\ [m]$,

(iii) $\sqrt{4ac - b^2} < \pi$.

Alors il existe $x, y \in \mathbb{Z}$ *tels que* $ax^2 + bxy + cy^2 = m$.

On considère d'une part l'ensemble $\Gamma = \{(x, y) \in \mathbb{Z}^2 \mid x \equiv fy\ [m]\}$. Il est clair que Γ est un réseau de $\mathbb{R}^2$ de volume m. On considère d'autre part l'ellipse

$$C = \{(x, y) \in \mathbb{R}^2 \mid ax^2 + bxy + cy^2 \leq \frac{2m\sqrt{4ac - b^2}}{\pi}\}.$$

La partie C est convexe, compacte, symétrique par rapport à l'origine, μ-mesurable et

$$\mu(C) = \frac{2\pi}{\sqrt{4ac - b^2}} \frac{2m\sqrt{4ac - b^2}}{\pi} = 4m = 4\mu(\mathbb{R}^2/\Gamma).$$

Le théorème de Minkowski assure donc qu'il existe un élément (x, y) non nul de Γ dans C. On a alors

(i) $ax^2 + bxy + cy^2 \equiv (af^2 + bf + c)y^2 \equiv 0\ [m]$,

(ii) $0 < ax^2 + bxy + cy^2 < \frac{2m\sqrt{4ac-b^2}}{\pi} < 2m$,

donc $ax^2 + bxy + cy^2 = m$.

3 Sommes de deux carrés

3.1 Le théorème des deux carrés

Pour tout $n \in \mathbb{N}$, on note $r(n) = \text{card}\{(x, y) \in \mathbb{Z}^2 \mid x^2 + y^2 = n\}$ le nombre de décompositions de n en somme de deux carrés. On note $\mathcal{S} = \{n \in \mathbb{N} \mid r(n) > 0\}$ l'ensemble des entiers qui admettent une telle décomposition. On commence par remarquer que :

Lemme 2. *L'ensemble $\mathcal{S}$ est stable par produit.*

En effet, pour tous $a, b, c, d \in \mathbb{N}$,

$$(a^2 + b^2)(c^2 + d^2) = a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2 = (ac + bd)^2 + (ad - bc)^2.$$

Pour comprendre l'ensemble $\mathcal{S}$, on peut donc se restreindre à étudier le cas des nombres premiers. La proposition suivante donne une caractérisation des nombres premiers qui sont dans $\mathcal{S}$:

Proposition 5. *Soit p un nombre premier. Alors $p \notin \mathcal{S}$ si et seulement si $p \equiv 3\ [4]$.*

Pour tout entier x, on sait que $x^2 \equiv 0$ ou $1\ [4]$ de sorte que pour tous $x, y \in \mathbb{N}$, $x^2 + y^2 \equiv 0, 1$ ou $2\ [4]$. Par conséquent, $p \equiv 3\ [4] \Rightarrow p \notin \mathcal{S}$. Réciproquement, si $p \equiv 1\ [4]$, alors il existe $u \in \mathbb{N}$ tel que $u^2 + 1 \equiv 0\ [p]$. Il suffit donc d'appliquer la proposition 4 aux entiers $1, 0, 1, p$. Enfin, $2 \in \mathbb{S}$.

On en déduit le théorème :

Théorème 4 (Sommes de deux carrés)**.**

$$\mathcal{S} = \{n \in \mathbb{N} \mid \forall p \in \mathbb{N}, p \text{ premier et } p \equiv 3\ [4] \Rightarrow \nu_p(n) \in 2\mathbb{Z}\},$$

où $\nu_p(n)$ désigne la plus grande puissance de p qui divise n

Dans ce qui suit, on rappelle une autre preuve de ce résultat utilisant l'anneau $\mathbb{Z}[i]$. Cette preuve nous permet de raffiner ce théorème pour donner explicitement le nombre de décompositions de n en sommes de deux carrés.

3.2 L'anneau des entiers de Gauss

On considère l'anneau $\mathbb{Z}[i] = \{a+ib \mid a, b \in \mathbb{Z}\}$. On définit la norme $N : \mathbb{Z}[i] \to \mathbb{N}$ par $N(a+ib) = |a+ib|^2 = a^2+b^2$. On a $\mathcal{S} = \{N(\alpha) \mid \alpha \in \mathbb{Z}[i]\}$.

Lemme 3. *La norme N est multiplicative. Les inversibles de $\mathbb{Z}[i]$ sont ± 1 et $\pm i$.*

Le module étant multiplicatif, la norme est clairement multiplicative. Soit $\alpha \in \mathbb{Z}[i]$ inversible et $\beta \in \mathbb{Z}[i]$ tel que $\alpha\beta = 1$. Alors $1 = N(\alpha\beta) = N(\alpha)N(\beta)$ donc $N(\alpha) = 1$. On en déduit que $\alpha \in \{\pm 1, \pm i\}$. Réciproquement, il est clair que ± 1 et $\pm i$ sont inversibles.

Notons que ce lemme donne en particulier une autre démonstration de la multiplicativité de $\mathcal{S}$.

Lemme 4. *L'anneau $\mathbb{Z}[i]$ est euclidien, de stathme N.*

Soient $\alpha, \beta \in \mathbb{Z}[i]$, avec $\beta \neq 0$. On considère dans $\mathbb{C}$ le quotient $\alpha/\beta = x + iy$ (où $x, y \in \mathbb{R}$). Soient $a, b \in \mathbb{Z}$ tels que $|x - a| \leq 1/2$ et $|y - b| \leq 1/2$. On a alors

$$\left|\frac{\alpha}{\beta} - (a + ib)\right|^2 = |(x - a) + i(y - b)|^2 \leq \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 < 1,$$

et par conséquent $N(\alpha - (a + ib)\beta) < N(\beta)$, ce qui prouve le lemme.

Proposition 6. *Soit p un entier premier. Il y a équivalence entre*

1. *p est irréductible dans $\mathbb{Z}[i]$,*
2. *$p \equiv 3$ [4],*
3. *p n'est pas somme de deux carrés.*

Supposons que p est irréductible dans $\mathbb{Z}[i]$ et que $p \equiv 1$ ou 2 [4]. Il existe alors $u \in \mathbb{Z}$ tel que $u^2 + 1 \equiv 0$ [p]. Par conséquent, p divise $(u + i)(u - i)$, et comme p est supposé irréductible et que $\mathbb{Z}[i]$ est euclidien, p divise $(u + i)$ ou $u - i$. Ceci est absurde puisqu'il est clair que ni $(u + i)/p$, ni $(u - i)/p$ ne sont dans $\mathbb{Z}[i]$.

Si $p \equiv 3$ [4], alors p ne peut pas être somme de deux carrés, puisque tout carré est congru à 0 ou 1 modulo 4.

Supposons enfin que p ne soit pas somme de deux carrés. Alors p ne peut pas être la norme d'un entier de Gauss. Or, si l'on écrit $p = \alpha\beta$, avec $\alpha, \beta \in \mathbb{Z}[i]$, on a $p^2 = N(p) = N(\alpha)N(\beta)$. Par conséquent, et comme p est premier, on a $N(\alpha) = 1$ ou $N(\beta) = 1$, ie. α ou β est inversible, donc p est irréductible.

On retrouve la proposition 5 et donc le théorème 4.

Proposition 7. *Les irréductibles de l'anneau $\mathbb{Z}[i]$ sont*

1. *les entiers de Gauss dont la norme est première,*
2. *les $\pm p$ et $\pm ip$ où p est un entier premier avec $p \equiv 3$ [4].*

La norme étant multiplicative, il est clair que tout entier de Gauss dont la norme est un nombre premier est irréductible. Par ailleurs, on vient de montrer que pour tout p premier congru à 3 modulo 4 est irréductible (donc $\pm p$ et $\pm ip$ le sont aussi).

Réciproquement, commençons par noter que si p est un nombre premier avec $p \equiv 3$ [4] et $\alpha = a + ib \in \mathbb{Z}[i]$ a pour norme p^2, alors $\alpha \in \{\pm p, \pm ip\}$. En effet, si l'on suppose que $b \notin \{0, p, -p\}$, alors b est inversible dans $\mathbb{Z}/p\mathbb{Z}$ et on a $a^2 + b^2 = N(\alpha) = p^2 \equiv 0$ [p], d'où $(ab^{-1})^2 = -1$ [p], ce qui est absurde.

Il ne reste donc plus qu'à prouver qu'un entier de Gauss α dont la norme n'est ni un nombre premier, ni le carré d'un nombre premier congru à 3 modulo 4, est réductible. Mais $N(\alpha)$ est alors le produit de deux sommes de deux carrés $e^2 + f^2$ et $g^2 + h^2$. On a donc

$$\alpha\bar{\alpha} = N(\alpha) = (e^2 + f^2)(g^2 + h^2) = ((e + if)(g + ih))\,((e - if)(g - ih)).$$

Si l'on suppose α irréductible, il doit diviser $(e + if)(g + ih)$ ou $(e - if)(g - ih)$. On peut écrire par exemple $\alpha\beta = (e + if)(g + ih)$, avec $\beta \in \mathbb{Z}[i]$. Mais $N(\alpha) = N((e + if)(g + ih))$, donc $N(\beta) = 1$ et β est inversible. On obtient $\alpha = \beta^-1(e + if)(g + ih)$, ce qui est absurde.

3.3 Nombre de décompositions d'un entier en somme de deux carrés

On rappelle que l'on note $r(n) = \text{card}\{(x,y) \in \mathbb{Z}^2 \mid x^2 + y^2 = n\}$ le nombre de décompositions de n en somme de deux carrés. Par ailleurs, pour $n \in \mathbb{N}$, on note $d_1(n)$ (resp. $d_3(n)$) le nombre de diviseurs de n congrus à 1 (resp. 3) modulo 4.

Théorème 5. *Pour tout $n \in \mathbb{N}$, $r(n) = 4(d_1(n) - d_3(n))$.*

On définit $d(n) = r(n)/4$. On veut montrer que d est multiplicative. Notons d'abord que $d(1) = r(1)/4 = 1$. Par ailleurs, on va montrer par une étude de cas que si $n \in \mathbb{N}$, si p est un nombre premier qui ne divise par n et si $\lambda \in \mathbb{N}$, alors $d(p^\lambda n) = d(p^\lambda)d(n)$.

Premier cas : $p = 2$

On sait que $1 - i$ est irréductible dans $\mathbb{Z}[i]$ (puisque $N(1-i) = 2$ est premier) et qu'il ne divise pas n (puisque si c'était le cas, $2 = (1+i)(1-i)$ diviserait n^2, et donc 2 diviserait n). Pour tout $\alpha \in \mathbb{Z}[i]$ tel que $N(\alpha) = 2^\lambda n$, on peut écrire $\alpha = (1-i)^\mu \beta$ avec μ entier, $\beta \in \mathbb{Z}[i]$ et $(1-i) \nmid \beta$. On a alors

$$(((1-i)(1+i))^\mu \beta\bar{\beta} = \alpha\bar{\alpha} = N(\alpha) = 2^\lambda n = (((1-i)(1+i))^\lambda n,$$

d'où $\lambda = \mu$ et $n = N(\beta)$. Réciproquement, si $\beta \in \mathbb{Z}[i]$ est tel que $n = N(\beta)$, alors $N((1-i)^\lambda \beta) = 2^\lambda n$. Par conséquent,

$$\{\alpha \in \mathbb{Z}[i] \mid N(\alpha) = 2^\lambda n\} = \{(1-i)^\lambda \beta \mid N(\beta) = n\},$$

et donc $r(2^\lambda n) = r(n)$. On obtient en particulier $r(2^\lambda) = r(1) = 4$. D'où

$$d(2^\lambda n) = \frac{r(2^\lambda n)}{4} = \frac{r(n)}{4} = d(n) = d(2^\lambda)d(n).$$

Deuxième cas : $p \equiv 1\ [4]$

Par le théorème précédent, p est somme de deux carrés. On écrit $p = a^2 + b^2 = (a+ib)(a-ib)$, avec $a, b \in \mathbb{Z}$. Les eux entiers de Gauss $a + ib$ et $a - ib$ sont irréductibles (car ler norme est un nombre premier) et non associés (sinon $|a| = |b|$ ou $a = 0$ ou $b = 0$, ce qui est impossible). Le même raisonnement que précédemment donne

$$\{\alpha \in \mathbb{Z}[i] \mid N(\alpha) = p^\lambda n\} = \{(a+ib)^x (a-ib)^{\lambda - x} \beta \mid 0 \leq x \leq \lambda \text{ et } N(\beta) = n\},$$

et donc $r(p^\lambda n) = (\lambda + 1)r(n)$. On obtient en particulier $r(p^\lambda) = 4(\lambda + 1)$. D'où

$$d(p^\lambda n) = \frac{r(p^\lambda n)}{4} = \frac{(\alpha+1)r(n)}{4} = d(p^\lambda)d(n).$$

Troisième cas : $p \equiv 3\ [4]$

Si λ est impair, le théorème des deux carrés affirme que $r(p^\lambda) = 0$ et $r(p^\lambda n) = 0$. On a donc bien $d(p^\lambda n) = 0 = d(p^\lambda)d(n)$.

Si λ est pair, p étant irréductible dans $\mathbb{Z}[i]$, on obtient comme précédemment

$$\{\alpha \in \mathbb{Z}[i] \mid N(\alpha) = p^\lambda n\} = \{p^{\lambda/2}\beta \mid N(\beta) = n\},$$

et donc $r(p^\lambda n) = r(n)$. On obtient en particulier $r(p^\lambda) = 4$. D'où

$$d(p^\lambda n) = \frac{r(p^\lambda n)}{4} = \frac{r(n)}{4} = d(n) = d(p^\lambda)d(n).$$

Définissons maintenant la fonction $\chi : \mathbb{N} \to \mathbb{N}$ par

$$\chi(n) = \begin{cases} 0 & \text{si } 2|n \\ 1 & \text{si } n \equiv 1\ [4] \\ -1 & \text{si } n \equiv 3\ [4] \end{cases}$$

Il est clair que χ est multiplicative. On en déduit que

$$n \mapsto d_1(n) - d_3(n) = \sum_{d|n} \chi(d)$$

et multiplicative. Pour montrer que $d(n) = d_1(n) - d_3(n)$ pour tout $n \in \mathbb{N}$, il suffit donc de montrer que pour tout nombre premier p et tout entier λ, $d(p^\lambda) = d_1(p^\lambda) - d_3(p^\lambda)$. Or

$$\sum_{d|p^\lambda} \chi(d) = \sum_{\mu=0}^{\lambda} \chi(p^\lambda) = \begin{cases} 1 & \text{si } p = 2 \\ \lambda + 1 & \text{si } p \equiv 1 \ [4] \\ 0 & \text{si } p \equiv 3 \ [3] \text{ et } \lambda \text{ est impair} \\ 1 & \text{si } p \equiv 3 \ [3] \text{ et } \lambda \text{ est pair} \end{cases}$$

Ceci termine la preuve du théorème 5.

4 Figures géométriques sur le réseau $\mathbb{Z}^2$

Dans cette partie, on trace des figures géométriques simples dans le plan, et on cherche le nombre de points du réseau $\mathbb{Z}^2$ qu'elles contiennent. On montre ainsi que pour tout $n \in \mathbb{N}$, il existe un disque (resp. un cercle, resp. un carré) qui contient exactement n points de $\mathbb{Z}^2$. On montre ensuite le théorème de Pick, qui permet de compter le nombre de points dans un polygone dont les sommets sont des points du réseau.

4.1 Cercles et disques

Proposition 8. *Pour tout entier n, il existe un cercle qui passe par exactement n points de $\mathbb{Z}^2$.*

Plus précisément, si $n \in \mathbb{N}$ alors

(i) si $n = 2k$, le cercle de centre $(\frac{1}{2}, 0)$ et de rayon $\frac{5^{\frac{k-1}{2}}}{2}$ passe par n points de $\mathbb{Z}^2$,

(ii) si $n = 2k+1$, le cercle de centre $(\frac{1}{3}, 0)$ et de rayon $\frac{5^k}{3}$ passe par n points de $\mathbb{Z}^2$.

Nous ne démontrons ici que le (i), le (ii) se prouvant de la même manière.

On considère les solutions de l'équation $x^2 + y^2 = 5^{k-1}$. Tout d'abord, le théorème 5 affirme qu'il y en a $4k$. Ensuite, il est clair que si (x, y) est une solution de cette équation, la parité de x et celle de y sont différentes. Par ailleurs, (y, x) est alors aussi une solution. On en déduit qu'il y a exactement $2k = n$ solutions (x, y) pour lesquelles x est impair et y est pair.

Or un point $(u, v) \in \mathbb{Z}^2$ est situé sur le cercle de centre $(\frac{1}{2}, 0)$ et de rayon $\frac{5^{\frac{k-1}{2}}}{2}$ si et seulement si

$$\left(u - \frac{1}{2}\right)^2 + v^2 = \frac{5^{k-1}}{4}, \quad \text{ie. si et seulement si} \quad (2u-1)^2 + (2v)^2 = 5^{k-1}.$$

Proposition 9. *Pour tout entier n, il existe un disque qui contient exactement n points de $\mathbb{Z}^2$.*

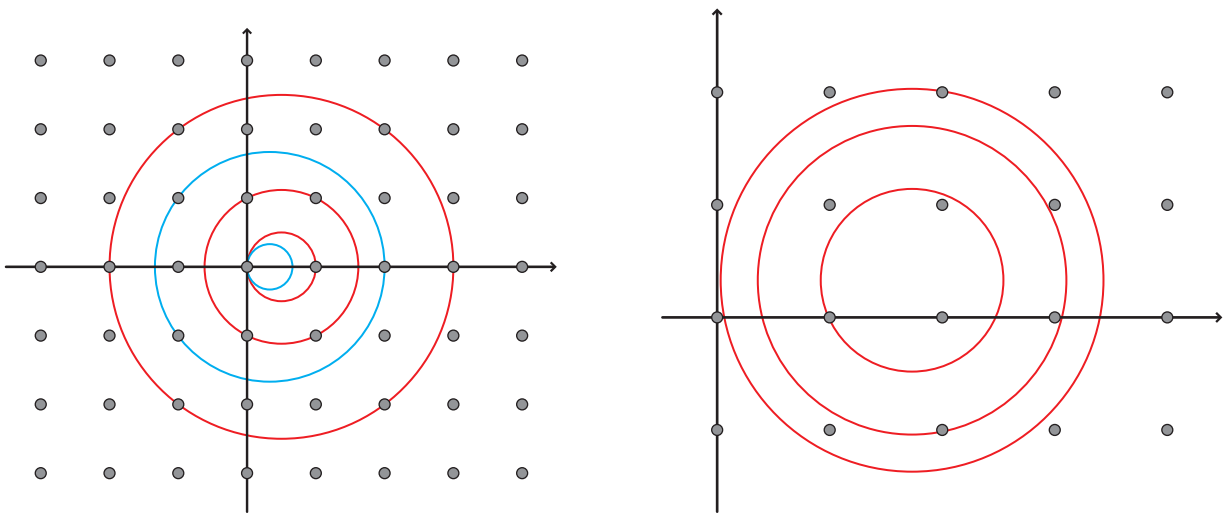

FIG. 1 – Cercles passant par $1, 2, 3, 4$ et 6 points de $\mathbb{Z}^2$ et disques contenant $3, 6$ et 9 points de $\mathbb{Z}^2$

Considérons le point $\Omega = (\sqrt{3}, 1/3)$ du plan. Montrons que l'application $f : \mathbb{Z}^2 \to \mathbb{R}$ définie par $f(x) = \|x - \Omega\|^2$ est injective : pour cela, considérons $a, b, c, d \in \mathbb{Z}$ tels que

$$(a - \sqrt{3})^2 + (b - 1/3)^2 = (c - \sqrt{3})^2 + (d - 1/3)^2.$$

En regroupant les parties rationnelles et irrationnelles, on obtient

$$a^2 + b^2 - 2b/3 - c^2 - d^2 + 2d/3 = 2(a - c)\sqrt{3},$$

ce qui impose $a = c$ et $b = d$, puisque $\sqrt{3}$ est irrationnel. Par conséquent, on peut définir $\theta : \mathbb{N} \to \mathbb{Z}^2$ de telle sorte que $\mathbb{Z}^2 = \theta(\mathbb{N})$ et que pour tout $i < j$, $f(\theta(i)) < f(\theta(j))$. Ainsi, le disque de centre Ω et passant par $\theta(n)$ contient exactement n points du réseau.

4.2 Carrés

Proposition 10. *Pour tout entier n, il existe un carré dont le bord passe par exactement n points de $\mathbb{Z}^2$.*

Soit $n \in \mathbb{N}$.

(i) Si n est pair, notons $U = [\frac{1}{2}, \frac{n+1}{2}] \times [0, \frac{n}{2}]$ et V la frontière de U. Alors $U \cap \Gamma = \{(i, 0) \mid i = 1, \dots, \frac{n}{2}\} \cup \{(i, \frac{n}{2}) \mid i = 1, \dots, \frac{n}{2}\}$ est de cardinal n.

(ii) Si n est impair, notons $U = [0, \frac{n}{2}]^2$ et V la frontière de U. Alors $U \cap \Gamma = \{(i, 0) \mid i = 0, \dots, \frac{n-1}{2}\} \cup \{(0, i) \mid i = 1, \dots, \frac{n-1}{2}\}$ est de cardinal n.

Proposition 11. *Pour tout entier n, il existe un carré contenant exactement n points de $\mathbb{Z}^2$.*

Considérons l'application

$$f : \left\{ \begin{array}{ccc} \mathbb{Z}^2 & \longrightarrow & \mathbb{R} \\ (x, y) & \longmapsto & |x + y\sqrt{3} - 1/3| + |x\sqrt{3} - y - 1/\sqrt{3}|. \end{array} \right.$$

La fonction f est injective. En effet, soient $a, b, c, d \in \mathbb{Z}$ tels que $f(a, b) = f(c, d)$. On note $\alpha, \beta, \gamma, \delta$ les signes respectifs de $a + b\sqrt{3} - 1/3$, $a\sqrt{3} - b - 1/\sqrt{3}$, $c + d\sqrt{3} - 1/3$ et $c\sqrt{3} - d - 1/\sqrt{3}$. On a

$$\alpha(a + b\sqrt{3} - 1/3) + \beta(a\sqrt{3} - b - 1/\sqrt{3}) = \gamma(c + d\sqrt{3} - 1/3) + \delta(c\sqrt{3} - d - 1/\sqrt{3}),$$

et en utilisant l'irrationalité de $\sqrt{3}$, on obtient

$$\text{ie.} \quad \alpha a - \beta b - \gamma c + \delta d - (\alpha - \gamma)/3 = 0 \quad \text{et} \quad -\alpha b - \beta a + \gamma d + \delta c + (\beta - \delta)/3 = 0.$$

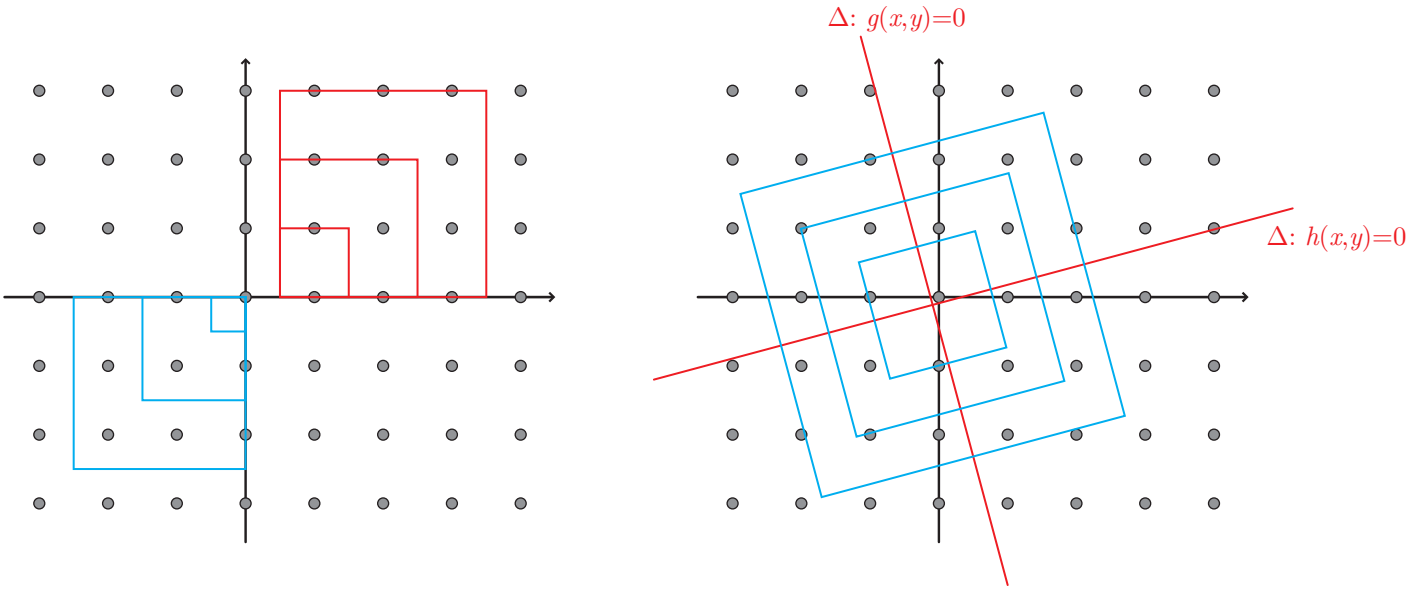

FIG. 2 – Carrés passant par $1, 2, \dots, 6$ points de $\mathbb{Z}^2$ et carrés contenant $3, 10$ et 20 points de $\mathbb{Z}^2$

Mais comme $\alpha, \gamma \in \{\pm 1\}$, on a $\alpha - \gamma \in \{0, \pm 1, \pm 2\}$. Pour que le terme de gauche soit entier, il faut donc que $\alpha = \gamma$. De même, $\beta = \delta$. En multipliant la première égalité par α et la seconde par β, on obtient donc

$$(a - c) + \alpha\beta(d - b) = 0 \quad \text{et} \quad \alpha\beta(d - b) - (a - c) = 0.$$

On en déduit que $a = c$ et $d = b$.

Soient $\iota : \mathbb{N} \to \mathbb{Z}^2$ et $\kappa : \mathbb{N} \to \mathbb{R}$ telles que $\mathbb{Z}^2 = \iota(\mathbb{N})$, et pour tout $i < j$, $f(\iota(i)) = \kappa(i) < \kappa(j) = f(\iota(j))$. Soient $g, h : \mathbb{R}^2 \to \mathbb{R}$ définies par

$$g(x, y) = x(1 + \sqrt{3}) + y(\sqrt{3} - 1) - 1/3 \quad \text{et} \quad h(x, y) = x(1 - \sqrt{3}) + y(\sqrt{3} + 1) - 1/3 + 1/\sqrt{3}.$$

On définit enfin pour tout $n \in \mathbb{N}$ l'ensemble

$$C_n = \{(x, y) \in \mathbb{R}^2 \mid |g(x, y)| \leq \kappa(n) \text{ et } |h(x, y)| \leq \kappa(n)\}.$$

On vérifie aisément que C_n est un carré. Par ailleurs, pour tout $(x, y) \in \mathbb{Z}^2$, on a

$$(x, y) \in C_n \Leftrightarrow |g(x, y)| \leq \kappa(n) \text{ et } |h(x, y)| \leq \kappa(n) \Leftrightarrow \left|\frac{g(x, y) + h(x, y)}{2}\right| + \left|\frac{g(x, y) - h(x, y)}{2}\right| \leq \kappa(n) \Leftrightarrow f(x, y) \leq \kappa(n).$$

Par conséquent, il y a bien n points de $\mathbb{Z}^2$ dans le carré C_n.

4.3 Théorème de Pick

Soit P un polygone de $\mathbb{R}^2$ (pas forcément convexe) dont les sommets sont des points du réseau $\mathbb{Z}^2$. On note $\iota(P)$ (resp. $\delta(P)$) le nombre de points de $\mathbb{Z}^2$ situés à l'intérieur de P (resp. sur la frontière de P).

Théorème 6 (Pick)**.** *Pour tout polygone P à sommets entiers, $\mu(P) = \iota(P) + \delta(P)/2 - 1$.*

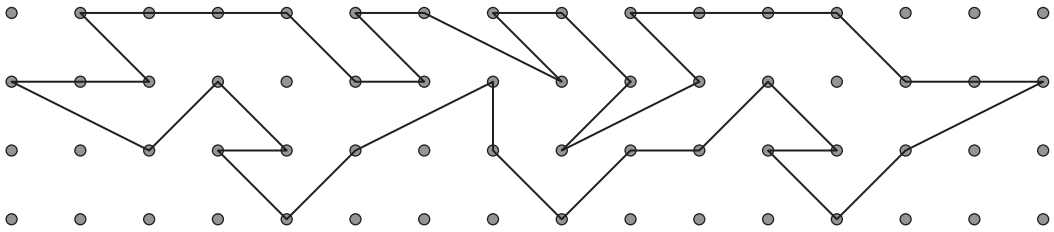

FIG. 3 – Un polygone P à sommets entiers avec $\iota(P) = 2, \delta(P) = 40$ et $\mu(P) = 21$

Pour prouver cette formule, on va utiliser son additivité. Soient P et Q deux polygones à sommets entiers, d'intérieurs disjoints, vérifiant la formule de Pick et partageant une arête. On note ℓ le nombre de points entiers situés sur cette arête et différents de ses extrémités. On a alors $\iota(P \cup Q) = \iota(P) + \iota(Q) + \ell$, $\delta(P \cup Q) = \delta(P) + \delta(Q) - 2\ell - 2$ et $\mu(P \cup Q) = \mu(P) + \mu(Q)$. Par conséquent,

$$\begin{aligned} \iota(P \cup Q) + \delta(P \cup Q)/2 - 1 &= \iota(P) + \iota(Q) + \ell + (\delta(P) + \delta(Q) - 2\ell - 2)/2 - 1 \\ &= \iota(P) + \delta(P)/2 - 1 + \iota(Q) + \delta(Q)/2 - 1 = \mu(P) + \mu(Q) = \mu(P \cup Q), \end{aligned}$$

et $P \cup Q$ vérifie aussi la formule de Pick.

Pour prouver la formule de Pick, il reste alors

(i) à trianguler le polygone P,

(ii) à montrer que tout triangle à sommets entiers s'obtient à partir d'un rectangle à sommets entiers dont les côtés sont parallèles aux axes en lui retirant au plus trois triangles rectangles à sommets entiers dont les côtés de l'angle droit sont parallèles aux axes,

(iii) à montrer que la formule de Pick est vérifiée pour les rectangles à sommets entiers dont les côtés sont parallèles aux axes et pour les triangles rectangles à sommets entiers dont les côtés de l'angle droit sont parallèles aux axes.

5 Empilements de boules sur un réseau, inégalité d'Hermite

5.1 Le problème de l'empilement de boules

Soit A une partie compacte de $\mathbb{R}^n$. Pour tout $x \in \mathbb{R}^n$, on note $A_x = A + x = \{a + x \mid a \in A\}$ la translation de A de vecteur x. Pour tout point $x \in \mathbb{R}^n$ et $R \in \mathbb{R}^{+*}$, on note $B(x, R)$ la boule de centre x et de rayon R. On note $B = B(0, 1)$ la boule unité centrée en 0. On a $B_x = B(x, 1)$.

Définition 5. *Soient P une partie discrète fermée de $\mathbb{R}^n$ et A une partie compacte de $\mathbb{R}^n$. On dit que P* empile *A si pour tout $\{x, y\} \subset P$, on a $\mathring{A}_x \cap \mathring{A}_y = \emptyset$. On note $E(P, A) = \bigcup_{x \in P} A_x$ l'*empilement *correspondant. On appelle* densité de l'empilement *$E(P, A)$ la limite*

$$\delta(E(P, A)) = \lim_{R \to \infty} \frac{\mu\left(B(0, R) \cap E(P, A)\right)}{\mu(B(0, R))},$$

lorsqu'elle existe.

Dans ce qui suit, on s'intéresse à l'empilement de boules dans $\mathbb{R}^n$. Le problème de déterminer s'il existe un empilement de boules qui maximise la densité est un problème difficile. Une idée naturelle consiste à restreindre cette recherche dans un premier temps aux réseaux de $\mathbb{R}^n$.

Lemme 5. *Soit Γ un réseau de $\mathbb{R}^n$ et $m = \min_{u \in \Gamma \setminus \{0\}} \|u\|$. Alors Γ empile B si et seulement si $m \geq 2$, et dans ce cas, la densité de l'empilement $E(\Gamma, B)$ existe et vaut $\delta_\Gamma = \mu(B)/\mu(\mathbb{R}^n/\Gamma)$.*

Le réseau Γ étant un sous-groupe de $\mathbb{R}^n$, pour tout $x, y \in \Gamma$, on a $x - y \in \Gamma$. Comme $m \geq 2$, pour tout $x, y \in \Gamma$, si $\|x - y\| < 2$, alors $x = y$. On en déduit que Γ empile B. La réciproque est évidente.

Soit $e = (e_1, \ldots, e_n)$ une $\mathbb{Z}$-base du réseau Γ et $D = \{t_1 e_1 + \ldots + t_n e_n \mid \forall i \in \{1, \ldots, n\}, t_i \in [0, 1[\}$. Notons d'abord que $\mu(D \cap E(\Gamma, B)) = \mu(B)$. Soit d le diamètre de D. Soit $R \in \mathbb{R}$ avec $R > d$. On note $U(R) = \{x \in \Gamma \mid D_x \subset B(0, R)\}$. Notons que si $y \in B(0, R - d)$ et $x \in \Gamma$ est tel que $y \in D_x$, alors $x \in U(R)$. On a donc

$$B(0, R) \supset \bigsqcup_{x \in U(R)} D_x \supset B(0, R - d).$$

On en déduit que

$$\begin{aligned}\mu(B(0, R) \cap E(\Gamma, B)) &\geq \mu\left(\bigsqcup_{x \in U(R)} D_x \cap E(\Gamma, B)\right) = \sum_{x \in U(R)} \mu(D_x \cap E(\Gamma, B)) = \frac{\mu(B)}{\mu(\mathbb{R}^n/\Gamma)} \sum_{x \in U(R)} \mu(D_x) \\ &= \frac{\mu(B)}{\mu(\mathbb{R}^n/\Gamma)}\, \mu\left(\bigsqcup_{x \in U(R)} D_x\right) \geq \frac{\mu(B)}{\mu(\mathbb{R}^n/\Gamma)}\, \mu(B(0, R - d)).\end{aligned}$$

On obtient ainsi

$$\frac{\mu(B(0, R) \cap E(\Gamma, B))}{B(0, R)} \geq \frac{\mu(B)}{\mu(\mathbb{R}^n/\Gamma)} \frac{\mu(B(0, R - d))}{B(0, R)} = \frac{\mu(B)}{\mu(\mathbb{R}^n/\Gamma)} \left(1 - \frac{d}{R}\right)^n.$$

Un raisonnement analogue assure que

$$\frac{\mu(B)}{\mu(\mathbb{R}^n/\Gamma)} \left(1 + \frac{d}{R}\right)^n \geq \frac{\mu(B(0, R) \cap E(\Gamma, B))}{B(0, R)},$$

et comme

$$\lim_{R \to \infty} \left(1 + \frac{d}{R}\right)^n = \lim_{R \to \infty} \left(1 - \frac{d}{R}\right)^n = 1,$$

on obtient le résultat.

Exemple. Soit Γ un réseau du plan qui empile le disque unité et (e_1, e_2) une $\mathbb{Z}$-base de Γ telle que $\|e_1\| = \min_{u \in \Gamma \setminus \{0\}} \|u\|$ et $\|e_2\| = \min_{u \in \Gamma \setminus \mathbb{Z}e_1} \|u\|$. On désigne par α l'angle entre e_1 et e_2. On peut supposer (quitte à changer e_2 en $-e_2$) que $\alpha \in [-\pi/2, \pi/2]$. Le théorème d'Al Kashi affirme alors que

$$\|e_1 - e_2\|^2 = \|e_1\|^2 + \|e_2\|^2 - 2\|e_1\|\|e_2\| \cos\alpha \leq (1 - 2\cos\alpha)\|e_1\|^2 + \|e_2\|^2.$$

Par conséquent, $\cos\alpha \leq 1/2$ donc $\sin\alpha \geq \sqrt{3}/2$. On obtient $\mu(\mathbb{R}^2/\Gamma) = \|e_1\|\|e_2\| \sin\alpha \geq 2\sqrt{3}$, et on en déduit que

$$\delta_\Gamma \leq \frac{\pi}{2\sqrt{3}}.$$

Il se trouve que le réseau $\mathbb{Z}\begin{pmatrix}2\\0\end{pmatrix} + \mathbb{Z}\begin{pmatrix}1\\\sqrt{3}\end{pmatrix}$ réalise ce minimum.

5.2 Inégalité d'Hermite

Lemme 6. *Soit Γ un réseau de $\mathbb{R}^n$ et $e_1 \in \Gamma$ tel que $\|e_1\| = \min_{u\in\Gamma\setminus\{0\}} \|u\|$. Soit p la projection orthogonale sur $H = e_1^\perp$ et $\Lambda = p(\Gamma)$. Alors*

1. *Λ est un réseau de H.*
2. *soit $(f_2, \dots, f_n)$ une $\mathbb{Z}$-base de Λ et $e_2, \dots, e_n \in \Gamma$ tels que pour tout $2 \le i \le n$, on a $p(e_i) = f_i$. Alors $(e_1, \dots, e_n)$ est une $\mathbb{Z}$-base de Γ.*
3. *pour tout $f \in \Lambda$, il existe $e \in \Gamma$ tel que $\|e\| \le \|f\|\sqrt{\frac{4}{3}}$.*

Si $(e_1, \dots, e_n)$ est une $\mathbb{Z}$-base de Γ, alors $(p(e_2), \dots, p(e_2))$ est une base de H. En effet, pour tout $2 \le i \le n$ on peut écrire $e_i = p(e_i) + \alpha_i e_1$ avec $\alpha_i \in \mathbb{R}$. Par conséquent, pour tout $\beta_2, \dots, \beta_n \in \mathbb{R}$, si $\sum_{i=2}^n \beta_i p(e_i) = 0$, alors $(\sum_{i=2}^n \alpha_i\beta_i)\, e_1 + \sum_{i=2}^n \beta_i e_i = 0$, ce qui impose $\beta_2 = \ldots = \beta_n = 0$. On en déduit que $\Lambda = \mathbb{Z}p(e_2) \oplus \ldots \oplus \mathbb{Z}p(e_n)$ est un réseau de H.

Soit $(f_2, \dots, f_n)$ une $\mathbb{Z}$-base de Λ et $e_2, \dots, e_n \in \Gamma$ tels que pour tout $2 \le i \le n$, on a $p(e_i) = f_i$. On a clairement $\sum_{i=1}^n \mathbb{Z}e_i \subset \Gamma$. Réciproquement, pour tout $x \in \Gamma$, il existe $\alpha_2, \dots, \alpha_n \in \mathbb{Z}$ tels que $p(x) = \sum_{i=2}^n \alpha_i f_i$. On a alors $x - \sum_{i=2}^n \alpha_i e_i \in (\mathbb{R}e_1 \cap \Gamma)$, donc il existe $\alpha_1 \in \mathbb{Z}$ tel que $x - \sum_{i=2}^n \alpha_i e_i = \alpha_1 e_1$. On en déduit que $x = \sum_{i=1}^n \alpha_i e_i \in \sum_{i=1}^n \mathbb{Z}e_i$. Par conséquent, $(e_1, \dots, e_n)$ est une $\mathbb{Z}$-base de Γ.

Enfin, pour tout $f \in \Lambda$, il existe $g \in \Gamma$ tel que $f = p(g)$. On a $g = f + \alpha e_1$, avec $\alpha \in \mathbb{R}$. Il existe $\beta \in \mathbb{Z}$ tel que $|\alpha - \beta| \le 1/2$. On pose alors $e = f + (\alpha - \beta)e_1$. Clairement, $e \in \Gamma$ et par le théorème de Pythagore, $\|f\|^2 = \|e\|^2 - |\alpha - \beta|^2\|e_1\|^2 \ge 3\|e\|^2/4$. On a donc $\|e\| \le \|f\|\sqrt{\frac{4}{3}}$, ce qui termine la preuve du lemme.

On en déduit par récurrence la preuve du théorème suivant :

Théorème 7 (Hermite)**.** *Tout réseau Γ de $\mathbb{R}^n$ admet une $\mathbb{Z}$-base $e = (e_1, \dots, e_n)$ telle que*

$$\prod_{i=1}^n \|e_i\| \le \left(\frac{4}{3}\right)^{\frac{n(n-1)}{4}} \mu(\mathbb{R}^n/\Gamma).$$

Corollaire 1. *Pour tout réseau Γ de $\mathbb{R}^n$ qui empile B, on a*

$$\delta_\Gamma \le \frac{\mu(B)}{2^n}\left(\frac{4}{3}\right)^{\frac{n(n-1)}{4}}.$$

En effet, comme Γ empile B, pour tout $x \in \Gamma$, on a $\|x\| \ge 2$. Donnons nous une $\mathbb{Z}$-base $(e = e_1, \dots, e_n)$ qui satisfait la condition du théorème d'Hermite. On a alors

$$\delta_\Gamma = \frac{\mu(B)}{\mu(\mathbb{R}^n/\Gamma)} \le \frac{\mu(B)}{\prod_{i=1}^n \|e_i\|}\left(\frac{4}{3}\right)^{\frac{n(n-1)}{4}} \le \frac{\mu(B)}{2^n}\left(\frac{4}{3}\right)^{\frac{n(n-1)}{4}}.$$

On retrouve le résultat de l'exemple précédent. On note que cette borne est atteinte pour $n = 1$ et $n = 2$.

5.3 Le problème du verger

On considère un verger circulaire, représenté par le cercle de rayon R centré à l'origine, dont les arbres sont représentés par des cylindres de rayon r, et sont plantés selon un réseau Γ du plan. On veut savoir si l'on peut voir l'extérieur du verger lorsque l'on supprime l'arbre situé à l'origine, et que l'on prend sa place. Autrement dit, on veut savoir s'il existe une droite Δ passant par l'origine qui ne rencontre pas la forêt

$$F(\Gamma, R, r) = \bigcup_{x\in\Gamma\cap B(0,R)\setminus\{0\}} B(x, r).$$

Proposition 12. *Soit Γ un réseau de $\mathbb{R}^n$. Alors*

1. *pour tout $r \in \mathbb{R}^{+*}$, il existe $R \in \mathbb{R}^{+*}$ tel que toute droite Δ passant par l'origine rencontre $F(\Gamma, R, r)$,*
2. *pour tout $R \in \mathbb{R}^{+*}$, il existe $r \in \mathbb{R}^{+*}$ tel qu'il existe une droite Δ passant par l'origine et ne rencontrant pas $F(\Gamma, R, r)$.*

Pour prouver le premier point, on va montrer que si $(r, R) \in (\mathbb{R}^+*)^2$ est tel que

$$\mu(B_{n-1})r^{n-1}\sqrt{R^2 - r^2} > 2^n\mu(\mathbb{R}^n/\Gamma),$$

(où B_{n-1} désigne la boule unité de $\mathbb{R}^{n-1}$), alors toute droite Δ passant par l'origine rencontre $F(\Gamma, R, r)$. En effet, si (r, R) est un tel couple, il existe $\varepsilon > 0$ tel que $\mu(B_{n-1})(r-\varepsilon)^{n-1}\sqrt{R^2 - (r-\varepsilon)^2} > 2^n\mu(\mathbb{R}^n/\Gamma)$. Soit Δ une passant par l'origine. Soit C le cylindre d'axe Δ, de rayon $r - \varepsilon$ et $\tilde{C} = C \cap B(0, R)$. Alors $\tilde{C}$ est une partie convexe, compacte, symétrique par rappport à l'origine, μ-mesurable et $\mu(\tilde{C}) \geq \mu(B_{n-1})(r-\varepsilon)^{n-1}\sqrt{R^2 - (r-\varepsilon)^2} > 2^n\mu(\mathbb{R}^n/\Gamma)$, donc le théorème de Minkowski affirme que $\tilde{C}$ contient un point x non nul de Γ. Mais alors $x \in \Gamma \cap B(0, R) \setminus \{0\}$ et Δ rencontre $B(x, r)$.

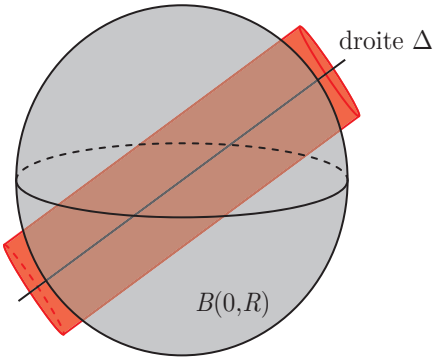

FIG. 4 – Cylindre autour d'une droite Δ

Pour prouver le second point, on commence par montrer que pour tout réseau Γ de $\mathbb{R}^n$, il existe une droite Δ telle que $\Delta \cap \Gamma = \{0\}$. Il suffit clairement de le montrer pour $\Gamma = \mathbb{Z}^2$. Or toute droite de $\mathbb{R}^2$ de pente irrationnelle et passant par l'origine convient. Ensuite, comme $\Gamma \cap B(0, R) \setminus \{0\}$ est compact, Δ est fermé, et $(\Gamma \cap B(0, R) \setminus \{0\}) \cap \Delta = \emptyset$, la distance d de Δ à $\Gamma \cap B(0, R) \setminus \{0\}$ est strictement positive, et tout rayon $r < d$ convient.

6 Réduction de réseaux : l'algorithme LLL

6.1 Vecteurs courts d'un réseau

Définition 6. *On appelle* minima successifs *d'un réseau Γ de $\mathbb{R}^n$ les réels $\lambda_1(\Gamma) \leq \ldots \leq \lambda_n(\Gamma)$, où $\lambda_i(\Gamma)$ est le plus petit réel t tel qu'il existe i vecteurs libres de norme inférieure où égale à t.*

On dit qu'une famille libre $e = (e_1, \ldots, e_n)$ de Γ est une famille de vecteurs courts *de Γ si pour tout $1 \leq i \leq n$, on a $\|e_i\| = \lambda_i(\Gamma)$. On dit que e est une $\mathbb{Z}$-*base de vecteurs courts *de Γ si c'est une $\mathbb{Z}$-base et une famille de vecteurs courts de Γ.*

Contrairement à ce que l'on pourrait penser, une famille de vecteurs courts d'un réseau Γ n'est pas forcément une $\mathbb{Z}$-base de Γ, dès que $n \geq 4$. Par exemple, considérons le réseau Γ de $\mathbb{R}^4$ donné par la $\mathbb{Z}$-base

$$e = \left(\begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} \right).$$

Notons que Γ est le sous-réseau de $\mathbb{Z}^4$ constitué des points dont la somme des coordonnées est paire. Par conséquent, les minima successifs de Γ sont $\sqrt{2}, \sqrt{2}, \sqrt{2}, \sqrt{2}$. La famille

$$f = \left(\begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \\ -1 \end{pmatrix} \right)$$

est donc une famille de vecteurs courts de Γ mais n'est pas une $\mathbb{Z}$-base de Γ (puisque $e_1 + e_3 \notin \bigoplus_{i=1}^4 \mathbb{Z}f_i$).

Plus étrangement encore, pour $n \geq 5$, il existe des réseaux qui n'admettent aucune base de vecteurs courts. Par exemple, considérons le réseau Λ de $\mathbb{R}^5$ donné par la $\mathbb{Z}$-base

$$e = \left(\begin{pmatrix} 2 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 2 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 2 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 2 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} \right).$$

On vérifie que les minima successifs de Λ sont $2, 2, 2, 2, 2$, et que la famille

$$f = \left(\begin{pmatrix} 2 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 2 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 2 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 2 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 2 \end{pmatrix} \right)$$

est la seule famille (à changement de signe près) de vecteurs courts, et n'est pas une $\mathbb{Z}$-base de Λ (puisque $e_5 \notin \bigoplus_{i=1}^{5} \mathbb{Z} f_i$).

Ainsi, il n'est pas possible de donner un sens à une notion de réduction optimale d'un réseau. On se contente de réductions approchées : on s'intéresse par exemple aux $\mathbb{Z}$-bases dont les vecteurs sont relativement courts (ie. leur norme est proche des minima successifs), ou dont les vecteurs sont quasi-orthogonaux. De telles notions ne sont pertinentes d'un point de vue algorithmique que si l'on peut déterminer de telles $\mathbb{Z}$-bases en temps raisonnable. Dans ce qui suit, on présente la réduction LLL : il s'agit de bases dont les vecteurs sont relativement courts, et que l'on peut trouver en temps polynomial par l'algorithme LLL.

6.2 Orthogonalisation de Gram-Schmidt et réduction faible

Définition 7. *Soit $b = (b_1, \ldots, b_n)$ une base de $\mathbb{R}^n$. On appelle* base orthogonalisée de Gram-Schmidt *associée à b la base $b^* = (b_1^*, \ldots, b_n^*)$, où pour tout $1 \leq i \leq n$, le vecteur b_i^* est la projection orthogonale de b_i sur le supplémentaire orthogonal de $\sum_{j=1}^{i-1} \mathbb{R} b_j$.*

En particulier, la base b^* est orthogonale et on a pour tout $1 \leq i \leq n$, $\sum_{j=1}^{i-1} \mathbb{R} b_j = \sum_{j=1}^{i-1} \mathbb{R} b_j^*$. Par ailleurs, on a la formule

$$b_i^* = b_i - \sum_{j=1}^{i-1} \frac{\langle b_i | b_j^* \rangle}{\|b_j^*\|^2} b_j^* = b_i - \sum_{j=1}^{i-1} \mu_{i,j} b_j^*.$$

La base orthogonalisée de Gram-Schmidt associée à une base d'un réseau permet de minorer ses minima successifs :

Lemme 7. *Soit $b = (b_1, \ldots, b_n)$ une $\mathbb{Z}$-base d'un réseau Γ. Alors pour tout $1 \leq i \leq n$, le i-ème minima de Γ est minoré par*

$$\lambda_i(\Gamma) \geq \min_{i \leq j \leq n} \|b_j^*\|.$$

En effet, soit $e = (e_1, \ldots, e_n)$ une famille libre de vecteurs courts de Γ. Pour tout $1 \leq i \leq n$, on note $(\alpha_{i,j})_{1 \leq j \leq n}$ (resp. $\beta_{i,j}$) les coordonnées de e_i sur la $\mathbb{Z}$-base b (resp. la base b^*) et $\ell_i = \max\{j \mid e_{i,j} \neq 0\}$ de sorte que l'on a

$$e_i = \sum_{j=1}^{\ell_i} \alpha_{i,j} b_j = \sum_{j=1}^{\ell_i} \beta_{i,j} b_j^*.$$

Puisque la famille est libre, il est clair qu'il existe $j \leq i$ tel que $\ell_j \geq i$. On a donc

$$\lambda_i(\Gamma) \geq \lambda_j(\Gamma) = \|e_j\| = \| \sum_{k=1}^{\ell_j} \beta_{j,k} b_j^* \| \geq |\beta_{j,\ell_j}| \|b_j^*\|.$$

Mais $\beta_{j,\ell_j} = \alpha_{j,\ell_j} \in \mathbb{Z}^*$, d'où le résultat.

Définition 8. *On dit qu'une $\mathbb{Z}$-base est* faiblement réduite *si pour tout $1 \leq j < i \leq n$, on a $|\mu_{i,j}| \leq 1/2$.*

L'algorithme suivant permet de réduire faiblement une $\mathbb{Z}$-base de Γ :

RÉDUCTION FAIBLE

$(\mu_{i,j})_{1\leq j<i\leq n} \leftarrow$ coefficients de Gram-Schmidt de b ;
for $i = 2$ to n **do**
  for $j = i-1$ to 1 **do**
    $b_i \leftarrow b_i - \lceil \mu_{i,j} \rfloor b_j$;
    for $k = 1$ to j **do**
      $\mu_{i,k} \leftarrow \mu_{i,k} - \lceil \mu_{i,j} \rfloor \mu_{j,k}$;
    end for
  end for
end for

6.3 Réduction LLL

Définition 9. *Soit b une $\mathbb{Z}$-base de Γ et $1/4 < \delta < 1$. On dit que b est LLL-réduite à un facteur δ si*

1. *elle est faiblement réduite,*
2. *pour tout $1 \leq i \leq n-1$, on a $\|b_{i+1}^* + \mu_{i+1,i} b_i^*\|^2 \geq \delta \|b_i^*\|^2$ (condition de Lovász).*

En général, si b est une base et β est la base obtenue à partir de b en intervertissant les deux vecteurs b_i et b_{i+1}, alors $\beta_i^* = b_{i+1}^* + \mu_{i+1,i} b_i^*$. Ainsi, la condition de Lovász permet d'assurer que l'on ne gagne pas trop en changeant l'ordre de la base.

Proposition 13. *Soit $1/4 < \delta < 1$ et $\alpha = \frac{1}{\delta - 1/4}$. Si b est une $\mathbb{Z}$-base LLL-réduite à u facteur δ du réseau Γ, alors pour tout $1 \leq i \leq n$,*

$$\|b_i\| \leq \alpha^{\frac{d-1}{2}} \lambda_i(\Gamma).$$

Pour prouver cette proposition, il faut essentiellement remarquer que la condition de Lovász, et la réduction faible donnent

$$\|b_{i+1}^*\|^2 \geq (\delta - \mu_{i+1,i}^2)\|b_i^*\|^2 \geq (\delta - 1/4)\|b_i^*\|^2.$$

On en déduit que pour tout $1 \leq i \leq j \leq n$, $\|b_j^*\|^2 \geq (\delta - 1/4)^{j-i}\|b_i^*\|^2$. D'où

$$\|b_i\|^2 = \left\| b_i^* + \sum_{k=1}^{i-1} \mu_{i,j} b_j^* \right\|^2 = \|b_i^*\|^2 + \sum_{k=1}^{i-1} |\mu_{i,j}|^2 \|b_j^*\|^2 \leq \left(\alpha^{j-i} + \frac{1}{4} \sum_{k=1}^{i-1} \alpha^{j-k} \right) \|b_j^*\| \leq \alpha^{j-1} \|b_j^*\|$$

Le lemme 7 permet donc de conclure.

Ainsi, si une base est LLL-réduite, elle est certainement proche des minima du réseau. Reste à savoir calculer efficacement une telle base. L'algorithme LLL (du nom de ses inventeurs Lenstra, Lenstra et Lovász) permet de le faire en temps polynomial :

RÉDUCTION LLL

Réduire faiblement b ;
S'il existe $1 \leq i \leq n-1$ tel que $\|b_{i+1}^* + \mu_{i+1,i} b_i^*\|^2 < \delta \|b_i^*\|^2$, échanger b_i et b_{i+1} et relancer l'algorithme.

6.4 Application au problème du sac-à-dos

Le problème du sac-à-dos est le suivant : étant donnés k objets de poids $a_1, \ldots, a_k \in \mathbb{N}^*$ et un sac-à-dos de capacité $C \in \mathbb{N}$, existe-t-il un choix d'objets $m_1, \ldots, m_k \in \{0, 1\}$ qui remplisse exactement le sac, c'est-à-dire tel que $\sum_{i=1}^k m_i a_i = C$. Ce problème est en général NP-complet. En revanche, lorsque pour tout $i \leq k$, on a $a_i > \sum_{j=1}^{i-1} a_j$, le problème se résout facilement par un algorithme glouton.

On peut donc définir un cryptosystème asymétrique de la manière suivante. Soient $a_1, \ldots, a_k \in \mathbb{N}^*$ tels que $a_i > \sum_{j=1}^{i-1} a_j$, pour tout $i \leq k$. Soit $M > \sum_{j=1}^k a_j$ et W un élément inversible de $\mathbb{Z}/M\mathbb{Z}$. Pour tout $1 \leq i \leq k$, soit $b_i = W a_i \mod M$. Le cryptosystème est alors défini par

(i) clé publique : $b_1, \ldots, b_k$,

(ii) clé privée : $a_1, \ldots, a_k, M, W$,

(iii) chiffrement : $m = (m_1, \ldots, m_k) \in \{0,1\}^k \longmapsto C = \sum_{i=1}^k m_i b_i$,

(iv) déchiffrement : $W^{-1}C = \sum_{i=1}^k m_i a_i \longmapsto m$ par l'algorithme glouton.

A priori, puisqu'il la résolution du problème est facile (glouton) avec les a_i, et difficile avec les b_i, ce cryptosystème a l'air viable. Mais en fait, il se trouve qu'il peut être attaqué par l'algorithme LLL. On considère le réseau engendré par les vecteurs lignes $(L_i)_{1\leq i\leq k+1}$ de la matrice

$$A = \begin{pmatrix} 1 & 0 & \ldots & \ldots & 0 & b_1 \\ 0 & 1 & 0 & \ldots & 0 & b_2 \\ \vdots & \ddots & \ddots & & & \vdots \\ \vdots & & \ddots & \ddots & & \vdots \\ 0 & \ldots & \ldots & 0 & 1 & b_k \\ 0 & \ldots & \ldots & \ldots & 0 & C \end{pmatrix}.$$

Si $m = (m_1, \ldots, m_k)$ est une solution au problème, alors le vecteur $\sum_{i=1}^k m_i L_i - L_{k+1} = (m_1, \ldots, m_k, 0)$ est de norme inférieure à $\sqrt{k}$, ce qui est particulièrement court. Ainsi, LLL pouvant trouver ce vecteur court, peut casser sac-à-dos.

7 Questions et remarques

7.1 Questions

On pourra traiter les problèmes suivants :

1. généralités :
   (a) donner une description des sous-groupes de $\mathbb{R}$. À quelle condition le sous-groupe $a\mathbb{Z} + b\mathbb{Z}$ est-il discret ? Montrer que la projection d'un réseau de $\mathbb{R}^2$ sur $\mathbb{R}$ n'est pas toujours un réseau de $\mathbb{R}$.
   (b) donner la preuve des propositions 1 et 3.
   (c) classifier les réseaux du plan en fonction de leur groupe d'isométries.
   (d) donner des contre-exemples au résultat de Minkowski lorsque C n'est pas convexe et symétrique par rapport à l'origine.
   (e) calculer le volume de la boule unité en dimension n.
2. sur les carrés dans $\mathbb{Z}/p\mathbb{Z}$:
   Pour tout entier premier p, on note $\mathbb{F}_p$ le corps fini à p éléments, $\mathbb{F}_p^2 = \{x \in \mathbb{F}_p \mid \exists y \in \mathbb{F}_p, y^2 = x\}$ l'ensemble des carrés de $\mathbb{F}_p$ et $\mathbb{F}_p^{*2} = \mathbb{F}_p^2 \setminus \{0\}$.
   (a) montrer que $\mathbb{F}_2^2 = \mathbb{F}_2$. On suppose par la suite $p \neq 2$.
   (b) montrer que $\mathbb{F}_p^{*2}$ est un sous-groupe de $\mathbb{F}_p^*$ d'indice 2 (on pourra considérer le morphisme de groupes $x \mapsto x^2$). En déduire que $\mathrm{card}(\mathbb{F}_p^2) = \frac{p+1}{2}$.
   (c) montrer que pour tous $(u, v, w) \in \mathbb{F}_p^* \times \mathbb{F}_p^* \times \mathbb{F}_p$, l'équation $ux^2 + vy^2 = w$ admet au moins une solution (x, y) dans $\mathbb{F}_p$.
   (d) montrer que pour tout $x \in \mathbb{F}_p^*$, on a $x \in \mathbb{F}_p^{*2} \Leftrightarrow x^{\frac{p-1}{2}} = 1$.
3. sur la loi de réciprocité quadratique :
   Pour tout $a \in \mathbb{Z}$, on note
   $$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{si } \bar{a} = 0 \\ 1 & \text{si } \bar{a} \in \mathbb{F}_p^{*2} \\ -1 & \text{sinon.} \end{cases}$$
   (a) montrer que
   $$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \ [p].$$
   En déduire que pour tous $a, b \in \mathbb{Z}$, $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{v}{p}\right)$.

(b) montrer que $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$. (On montrera que p^2-1 est divisible par 8. On en déduira l'existence d'une racine primitive huitième de l'unité ζ dans $\mathbb{F}_{p^2}$. On vérifiera que $\zeta + \zeta^{-1}$ est une racine carrée de 2 dans $\mathbb{F}_{p^2}$. On concluera en trouvant la condition nécessaire et suffisante pour que 2 soit un carré dans $\mathbb{F}_p$).

(c) soient p et q deux nombres premiers impairs, ω une racine primitive q-ème de l'unité dans une cloture algébrique de $\mathbb{F}_p$ et S la *somme de Gauss* définie par

$$S = \sum_{x \in \mathbb{F}_q} \left(\frac{x}{q}\right) \omega^x.$$

Montrer que $S^2 = (-1)^{\frac{q-1}{2}} q$, puis que $S^{p-1} = \left(\frac{p}{q}\right)$. En déduire la *loi de réciprocité quadratique*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

(d) en déduire que $\left(\frac{-3}{p}\right) \equiv p \ [3]$.

4. sur les applications à la théorie des nombres :

(a) pour tout $n \in \mathbb{N}$, on appelle n-ème nombre de Fermat le nombre $\mathbb{F}_n = 2^{2^n} + 1$. Montrer que si p est un nombre premier qui divise F_n, avec $n \geq 2$, alors $p \equiv 1 \ [2^{n+2}]$ (on utilisera l'ordre de 2 dans $\mathbb{F}_p^*$, puis le fait que si $8|p^2-1$, alors 2 est un carré de $\mathbb{F}_p$).

(b) appliquer la proposition 4 à la forme quadratique $(x,y) \mapsto x^2 + xy + y^2$. En remarquant que $x^2 + x + 1 = (x + \frac{1}{2})^2 - \frac{-3}{2^2}$, montrer que pour tout nombre premier p, il existe $f \in \mathbb{Z}$ tel que $f^2 + f + 1 \equiv 0 \ [p]$ si et seulement si -3 est un carré dans $\mathbb{F}_p$.

(c) montrer que tout entier est somme de quatres carrés (on montrera d'abord que l'ensemble $\mathcal{R}$ des nombres qui s'écrivent comme une somme de quatres carrés est stable par produit, puis pour un nombre premier p impair, on appliquera le théorème de Minkowski au réseau $\Lambda = \{(a,b,c,d) \in \mathbb{Z}^4 \mid xa + yb \equiv c \ [p] \text{ et } xb - ya \equiv d \ [p]\}$, où (x,y) est un couple d'entiers tel que $x^2 + y^2 + 1 \equiv 0 \ [p]$).

(d) montrer que si $f : \mathbb{N} \to \mathbb{N}$ est une fonction multiplicative, alors $g : \mathbb{N} \to \mathbb{N}$, définie par $g(x) = \sum_{y|x} f(y)$, est aussi multiplicative.

5. sur les figures géométriques sur un réseau :

(a) donner les détails du (ii) de la preuve de la proposition 8.

(b) montrer que pour tout $n, m \in \mathbb{N}$, il existe une boule de $\mathbb{R}^m$ qui contient (resp. qui passe par) exactement n points de $\mathbb{Z}^m$.

(c) montrer que pour tout réseau Γ de $\mathbb{R}^2$ et toute ellipse $\mathcal{E}$, il existe une translation τ et une homothétie h telles que $h \circ \tau(\mathcal{E})$ contient exactement n points du réseau Γ. Même question pour un ellipsoïde dans $\mathbb{R}^m$.

(d) montrer que pour tout entier n, il existe un triangle équilatéral qui contient (resp. qui passe par) exactement n points du réseau.

(e) terminer la preuve de la formule de Pick. Prouver une formule similaire lorsque le polygone présente t trous (qui seront eux-même des polygones à sommets entiers).

6. sur les empilements de boules :

(a) donner un exemple d'empilement qui n'admet pas de densité.

(b) pour chaque type de réseau du plan (les réseaux du plan sont classifiés en fonction de leur groupe d'isométrie), calculer la densité minimale.

(c) quel est le nombre maximal $f(x)$ de disques de diamètre 1 que l'on peut aligner dans une boite de taille x. Montrer que le nombre maximal $g(x)$ de disques de diamètre 1 que l'on peut ranger en quinconce dans une boite carrée de taille x (fig. 5) est donné par

$$g(x) = \left(1 + \left\lfloor \frac{2(x-1)}{\sqrt{3}} \right\rfloor - \left\lfloor \frac{1 + \left\lfloor \frac{2(x-1)}{\sqrt{3}} \right\rfloor}{2} \right\rfloor\right) . \lfloor x \rfloor + \left\lfloor \frac{1 + \left\lfloor \frac{2(x-1)}{\sqrt{3}} \right\rfloor}{2} \right\rfloor . \left\lfloor x - \frac{1}{2} \right\rfloor .$$

Comparer f et g.

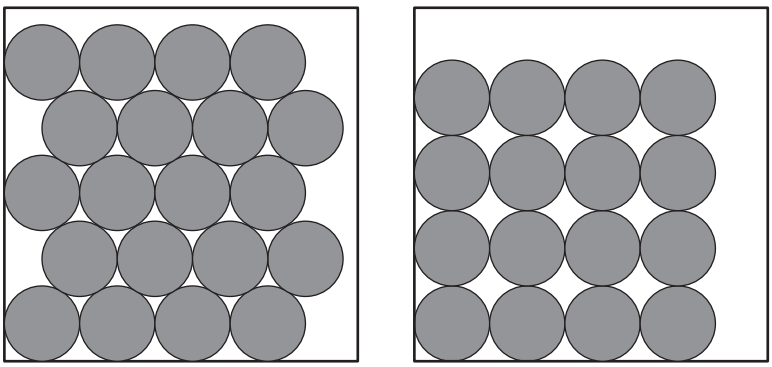

FIG. 5 – Empilement de disques alignés et de disques en quinconce dans un carré

(d) dans $\mathbb{R}^3$, on appelle configuration hexagonale compacte (resp. cubique faces centrées) l'empilement de boules obtenu de la manière suivante : on aligne des boules horizontalement en suivant un réseau hexagonal, puis on superpose les configurations obtenues en plaçant les boules de la seconde couche dans des trous de la première couche, puis les boules de la troisième couche au-dessus des boules de la première couche (resp. dans les trous de la seconde couche qui ne sont pas au-dessus des boules de la première couche), et ainsi de suite (fig. 6 et 7).

Quelle est la densité de la configuration hexagonale compacte (resp. cubique faces centrées) ?

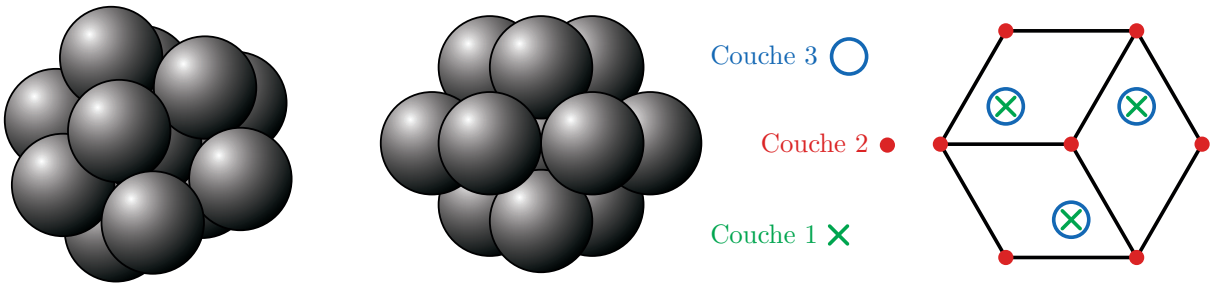

FIG. 6 – Configuration hexagonale compacte

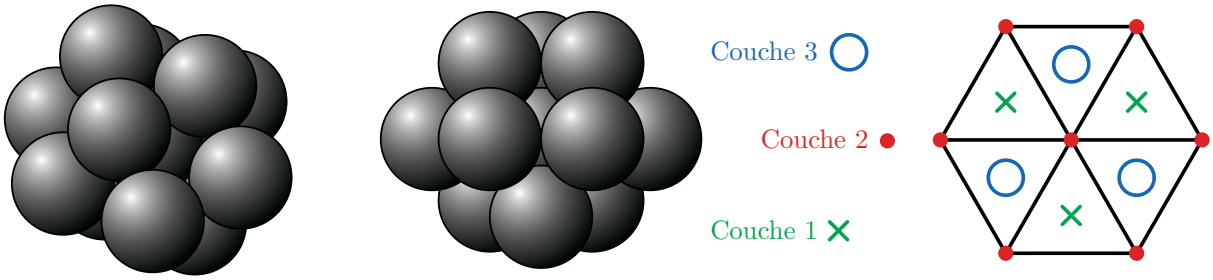

FIG. 7 – Configuration cubique faces centrées

(e) Soit $n \geq 2$. Dans le carré $[0,1]^n$, on place 2^n boules de rayon $1/4$ centrées aux points de l'ensemble $\{1/4, 2/4\}^n$. Au centre, il reste la place pour une petite boule de rayon optimal r_n (fig. 8). Montrer que cette boule béborde du carré lorsque la dimension devient grande.

(f) pour quelles valeurs de n l'inégalité d'Hermite donne-t-elle une information sur la densité du réseau.

7. sur la réduction de réseaux :

(a) vérifier les affimations dans les contre-exemples du paragraphe 6.1.

(b) montrer la correction de l'algorithme de réduction faible. Vérifier que la base de Gram-Schmidt reste inchangée au cours de l'algorithme.

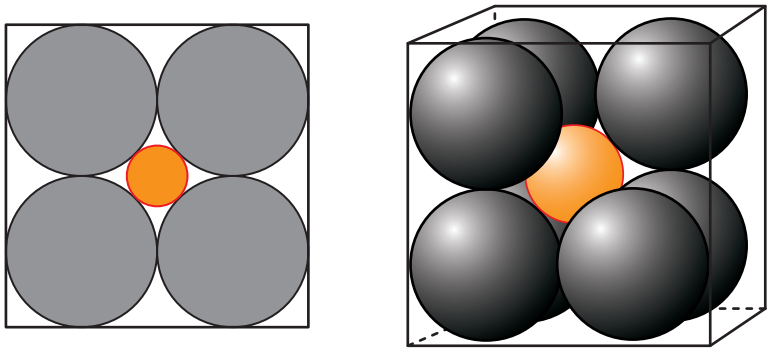

FIG. 8 – Placer un cochonet dans une boite de boules

(c) montrer que si b est une base LLL-réduite, alors

$$\prod_{i=1}^{n} \|b_i\|^2 \leq \alpha^{\binom{d}{2}} \mu(\mathbb{R}^n/\Gamma).$$

(d) compléter la preuve de la proposition 13 en montrant que pour tout $1 \leq i \leq n$,

$$\alpha^{1-i} + \frac{1}{4} \sum_{k=1}^{i-1} \alpha^{1-k} \leq 1.$$

(e) donner des procédures maple implémentant les algorithmes de réduction.

(f) implémenter le cryptosystème sac-à-dos et le casser par LLL.

7.2 Remarques et références

Les deux premières parties de ce texte sont présentées par exemple dans le chapitre sur les réseaux de *Mathématiques générales pour l'Agrégation* de P. TAUVEL. Pour les pavages, on renvoie aussi au tome 3 de *Géométrie* de M. BERGER. La troisième partie se trouve dans le *Cours d'algèbre* de D. PERRIN et dans le tome 1 d'algèbre des *Exercices de mathématiques pour l'agrégation* de S. FRANCINOU & H. GIANELLA. Pour la quatrième partie, on pourra consulter *Joyaux mathématiques* de R. HONSBERGER. On pourrait d'ailleurs parler aussi dans cette partie des polynômes d'Ehrhart.