*Journal de Théorie des Nombres*
*de Bordeaux* **6** *(1994), 135–159*

# Distribution de la constante d'Hermite et du plus court vecteur dans les réseaux de dimension deux

par Henri Laville et Brigitte Vallée

Résumé – En utilisant la géométrie du demi-plan de Poincaré et des familles de disques classiques – disques de Ford, disques de Farey – nous décrivons les domaines de niveau associés à la constante d'Hermite et au plus court vecteur d'un réseau. Nous en déduisons une évaluation très précise des fonctions de répartition correspondantes, en particulier au voisinage de l'origine.

## Introduction

Un réseau est l'ensemble des combinaisons linéaires entières de vecteurs linéairement indépendants. Plus précisément, si $b = (b_1, \ldots, b_n)$ désigne un système de $n$ vecteurs linéairement indépendants de $\mathbb{R}^p$, le réseau $R$ engendré par $b$ est défini par

$$R = \{\sum_{i=1}^{n} \lambda_i b_i \quad | \quad \lambda_i \in \mathbb{Z}\}.$$

Le système $b$ est appelé une base du réseau, et il y a, pour un réseau fixé, une multitude de bases possibles; la définition d'un réseau n'est donc pas intrinsèque. Cependant, il existe, dans un réseau, des objets intrinsèques, indépendants de la base particulière qui a servi à définir le réseau. Parmi eux, deux objets ont une importance particulière. Ce sont, d'une part, le premier minimum du réseau, et d'autre part le déterminant du réseau.

Le déterminant du réseau est le volume $n$-dimensionnel du parallélotope construit sur une base du réseau; il est indépendant de la base et noté $d(R)$. Cette quantité est aisément calculable en fonction de la matrice de Gram $M(b)$ associée à une base $b$ quelconque de $R$. Par définition, si $(.|.)$ désigne le produit scalaire euclidien de $\mathbb{R}^p$, et $|.|$ la norme associée, on a

$$M(b) = (b_i |\ b_j)_{1 \leq i,j \leq n} \text{ et } \ d(R)^2 = \det \ M(b).$$

Manuscrit reçu le 16 août 1993.

Le premier minimum $\lambda(R)$ du réseau $R$ est par définition la longueur d'un plus court vecteur non nul du réseau :

$$\lambda(R) = \min \{|v| \mid v \in R - \{0\}\}.$$

Il semble que le premier minimum du réseau soit très difficilement calculable : il est en général admis, bien que cela ne soit pas prouvé, que la détermination de $\lambda(R)$ est un problème NP-dur [VEB].

La constante d'Hermite $\gamma(R)$ du réseau $R$ relie ces deux quantités; par définition,

$$\gamma(R) = \frac{\lambda(R)^2}{d(R)^{2/n}}, \tag{1}$$

et le théorème de Minkowski montre l'existence d'une borne supérieure $\gamma_n$ pour toutes les constantes d'Hermite relatives à des réseaux $R$ de dimension $n$. On a ainsi

$$\lambda^2(R) \leq \gamma_n \ d(R)^{2/n}.$$

On montre que $\gamma_n$ est inférieur à $n$. Peu de résultats précis sont connus sur $\gamma_n$, et seules les huit premières valeurs de la suite $\gamma_n$ ont été déterminées. En particulier, la valeur $\gamma_2$ est égale à $2/\sqrt{3}$, et donc

$$\gamma(R) \leq \frac{2}{\sqrt{3}} \quad \text{pour tous les réseaux } R \text{ de rang 2.} \tag{2}$$

Ici nous nous intéressons à la distribution de ces deux grandeurs $\lambda(R)$ et $\gamma(R)$ pour des réseaux $R$ "aléatoires". En particulier, il est très important dans les applications à la cryptographie de pouvoir travailler sur des réseaux $R$ pour lesquels la constante d'Hermite $\gamma(R)$ n'est pas trop petite. Dans ce cas, il existe un parallélotope fondamental du réseau qui est suffisamment "régulier" pour être en première approximation assimilé à une boule euclidienne. Beaucoup de résultats de cryptanalyse, comme le cassage du générateur linéaire congruentiel [St], le cassage du "sac à dos" [F], [LO], [F], [JS], [CLOS], le cassage du système d'Okamoto [VGT], reposent sur le fait que des familles de réseaux cryptographiques sont formés de réseaux assez réguliers. Une première question importante est donc la suivante :

*y a-t-il, parmi les réseaux aléatoires, une grande proportion de réseaux suffisamment réguliers ?*

Par ailleurs, l'analyse de la complexité des algorithmes de réduction de réseaux fait intervenir de manière essentielle la longueur du plus court vecteur d'un réseau. En particulier, la distribution du premier minimum

$\lambda(R)$ semble jouer un rôle essentiel dans l'analyse en moyenne de l'algorithme LLL [LLL]. Daudé et Vallée [DV] ont obtenu un premier résultat dans ce sens, en travaillant dans un modèle naturel :

$$\Pr\,[\lambda(R) \le u] \ \le \sqrt{n}u. \tag{3}$$

D'autre part, il est clair que l'on a

$$\Pr\,[\lambda(R) \le u] \ \ge u^n. \tag{4}$$

La seconde question peut se formuler ainsi :

*quel est le comportement précis de la fonction de répartition du premier minimum, en particulier au voisinage de l'origine ?*

Ici, nous choisissons un point de vue algorithmique : un réseau est défini dans la pratique algorithmique par une base; nous travaillons donc sur les bases des réseaux et non sur les réseaux eux-mêmes, contrairement au modèle usuel étudié par exemple par Siegel [Si]. Les variables aléatoires que nous considérons ne dépendent pas seulement d'un réseau $R$ mais d'une base $b$ qui a servi à définir ce réseau $R$; nous désignerons ces variables par $\gamma(b)$ et $\lambda(b)$.

Par ailleurs, ces problèmes posés en dimension quelconque semblent très difficiles; nous nous limitons ici à la dimension 2, et nous travaillons dans un modèle probabiliste simple, déjà utilisé dans l'étude de la complexité moyenne de l'algorithme de Gauss [VF] : les bases possibles sont de la forme $(1, z)$ où $z$ est un point du plan complexe $\mathbb{C}$ choisi uniformément dans le demi-disque unité. Les variables aléatoires $\gamma$ et $\lambda$ relatives au réseau $R(z)$ engendré par $(1, z)$ sont alors des fonctions de la seule variable $z$, et seront désignées par $\gamma(z)$ et $\lambda(z)$.

Nous décrivons précisément les fonctions de répartition de ces deux variables aléatoires. En utilisant la géométrie classique du demi-plan de Poincaré, nous caractérisons les domaines $\gamma(z) \le r$ et $\lambda(z) \le t$ en fonction de deux familles de disques bien connus : les disques de Ford et les disques de Farey. Nous obtenons en particulier une évaluation précise des fonctions de répartition de $\gamma$ et $\lambda$ au voisinage de 0

$$\Pr\,[\gamma(z) \le r] = \frac{\zeta(3)}{\zeta(4)}\, r^2\, [1 + \alpha(r)] \qquad \text{avec} \ \ \alpha(r) \to 0 \text{ pour } r \to 0,$$

$$\Pr\,[\lambda(z) \le t] = \frac{2t^2|\log t|}{\zeta(2)}\, [1 + \beta(t)] \qquad \text{avec} \ \ \beta(t) \to 0 \text{ pour } t \to 0.$$

L'article est organisé comme suit. Après avoir défini dans le paragraphe 1 un modèle probabiliste complexe pour le problème, nous rappelons les propriétés de l'algorithme de Gauss, dont la configuration de sortie permet de calculer les deux variables étudiées dans le problème. Puis nous décrivons précisément le domaine de niveau associé à la constante d'Hermite. Cette description fait intervenir de manière naturelle les disques de Ford. Les disques de Farey, eux, interviennent dans le paragraphe 3, lors de la description du domaine de niveau du premier minimum. Le quatrième et dernier paragraphe permet alors d'obtenir les résultats annoncés sur les fonctions de répartition de chacune des deux variables considérées.

## 1. Le modèle complexe et l'algorithme de Gauss

### 1.1. Le modèle probabiliste complexe

En dimension 2, un réseau $R$ est déterminé par la donnée d'une base $b = (u, v)$ de $\mathbb{C} \times \mathbb{C}$. La longueur de la base $b$, qu'on désigne par $|b|$, est alors le maximum des normes $|u|$ et $|v|$. Rappelons que nous voulons étudier les probabilités
$$\Pr\,[\gamma(b) \leq r] \quad \text{et} \quad \Pr\,[\lambda(b) \leq t|b|] \tag{5}$$
lorsque la base $b$ est choisie uniformément parmi les bases possibles de longueur inférieure ou égale à un réel positif $M$.

D'abord, la base $b = (u, v)$ peut toujours être supposée directe et ordonnée de sorte que l'on ait $|v| \leq |u|$. Ensuite, les deux événements qui interviennent dans (5) sont invariants par similitude; pour une similitude $W$ de $\mathbb{C}$, de rapport $\rho$ positif, on a en effet :

$$\lambda(W\,b) = \rho\;\lambda(b), \quad |W\,b| = \rho\;|b| \quad \text{et} \quad \det\,(W\,b) = \rho^2\;\det\,(b).$$

On peut donc choisir le vecteur $u$, qui est le plus grand des deux vecteurs $u$ et $v$, fixe et égal à 1 et travailler ainsi dans le demi-disque

$$\mathcal{C} = \{z \in \mathbb{C} \;\;|\;\; |z| \leq 1 \quad \text{et} \quad \Im(z) > 0\}$$

défini par l'intersection du disque unité et du demi-plan de Poincaré, et muni de la probabilité uniforme. Si $F$ désigne l'application définie par l'égalité $F(u, v) = v/u$, alors $F$ induit sur

$$\mathcal{D} = \{(u, v) \in \mathbb{C} \times \mathbb{C} \;\;|\;\; |v| \leq |u| \leq M\}$$

la probabilité uniforme; ainsi, le modèle probabiliste complexe, clairement relié au premier modèle naturellement défini, sera choisi en raison de sa simplicité et de sa riche géométrie. En effet, les calculs sur le couple $(u, v)$ se transportent agréablement sur le complexe $z = v/u$; par exemple :

$$\Re(z) = \frac{(u|v)}{|u|^2} \quad \text{et} \quad \Im(z) = \det(1, z) = \frac{\det(u, v)}{|u|^2}. \tag{6}$$

### 1.2. La configuration de sortie de l'algorithme de Gauss

A partir d'une base $b = (u, v)$ engendrant un réseau $R$, l'algorithme de Gauss construit une base $b^\star = (u^\star, v^\star)$ satisfaisant les deux conditions

$$|u^\star| \leq |v^\star| \quad \text{et} \quad (v^\star|u^\star) \leq \frac{1}{2}|u^\star|^2. \tag{7}$$

La base $b^\star$ est alors minimale - elle contient deux vecteurs minimaux successifs du réseau - et, en particulier, le vecteur $u^\star$ est un plus court vecteur non nul de $R$; on a donc : $|u^\star| = \lambda(R)$.

C'est la formulation de cet algorithme adaptée au modèle choisi du demi-plan complexe qui sera utilisée ici. L'algorithme prend en entrée un nombre complexe $z = v/u$ du demi-disque $\mathcal{C}$ et construit le nombre complexe $z^\star = v^\star/u^\star$. La transcription donnée par (6), et les inégalités (7) satisfaites par la base de sortie $b^\star$ montrent alors que le nombre complexe $z^\star$ produit par l'algorithme de Gauss est un élément du domaine fondamental

$$\mathcal{F} = \{z \in \mathbb{C} \ \mid \Im(z) > 0,\ |\Re(z)| \leq \frac{1}{2} \quad \text{et} \quad |z| \geq 1\}. \tag{8}$$

Comme le déterminant est un invariant du réseau, il n'est pas modifié durant l'exécution de l'algorithme; grâce aux relations (1) et (6), les deux quantités à étudier $\gamma(z)$ et $\lambda(z)$ se calculent donc à partir du couple $(z, z^\star)$

$$\gamma(z) = \frac{1}{\Im(z^\star)} \quad \text{et} \quad \lambda^2(z) = \frac{\Im(z)}{\Im(z^\star)}. \tag{9}$$

### 1.3. Les transformations construites par l'algorithme de Gauss

La formulation complexe de l'algorithme de Gauss se décrit à l'aide de l'opérateur de décalage $U$ défini par la relation

$$U(z) := S(z) - [\Re S(z)].$$

Ici $S$ désigne l'inversion-symétrie définie par $S(z) = -1/z$ et $[x]$ désigne l'entier le plus proche du réel $x$.

**Algorithme de Gauss**

**Entrée :** $z \in \mathcal{C}$
**Sortie :** $z \in \mathcal{F}$
Tant que $z \notin \mathcal{F}$ faire $z := U(z)$.

Ainsi cette application $U$ est-elle la composée de deux transformations particulières : l'inversion-symétrie $S$ déjà mentionnée et la translation entière $T$ définie par $T(z) := z + 1$ qui, à elles deux, engendrent le groupe $\mathcal{H}$ des homographies unimodulaires

$$\mathcal{H} = \{h : \ z \ \mapsto \ \frac{az+b}{cz+d} \ \mid a, b, c, d \in \mathbb{Z} \ c \geq 0, d \geq 0, \quad \text{et} \quad ad - bc = 1\}.$$

Par conséquent, au cours de son exécution, l'algorithme de Gauss construit une homographie $h$ permettant de transformer $z$ en $z^\star$. Toutes les homographies de $\mathcal{H}$ ne sont pas construites par l'algorithme de Gauss. Nous nous intéresserons ici aux homographies de $\mathcal{H}$ effectivement utilisées par l'algorithme, décrit en sens “inverse” : ce sont donc les homographies de $\mathcal{H}$ qui envoient le domaine $\mathcal{F}$ défini en (8) dans le demi-disque unité $\mathcal{C}$; nous les appelons homographies de Gauss et nous désignons par $\mathcal{G}$ leur ensemble,

$$\mathcal{G} = \{h \in \mathcal{H} \ \mid \ h(\mathcal{F}) \subset \mathcal{C}\}. \tag{10}$$

Il est connu par ailleurs que le demi-disque unité $\mathcal{C}$ s'écrit comme une réunion quasi-disjointe[1] de transformés de $\mathcal{F}$ par le groupe $\mathcal{H}$. Par définition alors de l'ensemble $\mathcal{G}$ des transformations de Gauss donné en (10), on peut écrire

$$\mathcal{C} = \bigcup_{g \in \mathcal{G}} g(\mathcal{F}). \tag{11}$$

## 2. Domaines de niveau associé à la constante d'Hermite et disques de Ford

D'après les relations (9) et (10), l'ensemble $\Gamma(r)$ des nombres $z$ de $\mathcal{C}$ vérifiant $\gamma(z) \leq r$ s'exprime en fonction des transformés par $\mathcal{G}$ de l'ensemble

$$\mathcal{F}_r = \{z \in \mathcal{F} \ \mid \ \Im(z) \geq \frac{1}{r}\},$$

[1] on appelle quasi-disjointe une réunion d'ensembles dont les intersections deux à deux sont contenues dans les frontières.

sous la forme

$$\Gamma(r) = \bigcup_{g \in \mathcal{G}} g(\mathcal{F}_r).$$

Il est plus facile de considérer de manière globale $\mathcal{F}$ et ses translatés, et le domaine $\mathcal{L}_r$

$$\mathcal{L}_r = \{z \in \mathbb{C} \ \mid \ \Im(z) \geq \frac{1}{r}\} \tag{12}$$

s'introduit alors naturellement; puisque $\mathcal{F}_r$ est l'intersection de $\mathcal{F}$ avec $\mathcal{L}_r$, on obtient

$$\Gamma(r) = \bigcup_{g \in \mathcal{G}} g(\mathcal{L}_r \cap \mathcal{F}) = \mathcal{C} \cap \bigcup_{g \in \mathcal{G}} g(\mathcal{L}_r). \tag{13}$$

Or, les transformés de la bande $\mathcal{L}_r$ par les homographies sont des disques bien connus dans la géométrie du demi-plan de Poincaré : ce sont des disques de Ford.

### 2.1. Les disques de Ford

Le lemme géométrique suivant est essentiel pour la suite :

Lemme 1. *Le transformé de la bande $\mathcal{L}_r$ située au-dessus de la droite $\Im(z) = 1/r$*

$$\mathcal{L}_r = \{z \in \mathbb{C} \ \mid \ \Im(z) \geq \frac{1}{r}\}$$

*par une homographie $h$ de la forme $h(z) = (az + b)/(cz + d)$ est le disque $\mathcal{D}_r(a, c)$ de centre $(a/c) + ir/(2c^2)$ et de rayon $r/(2c^2)$ dont l'équation est*

$$\left(x - \frac{a}{c}\right)^2 + \left(y - \frac{r}{2c^2}\right)^2 \ \leq \ \left(\frac{r}{2c^2}\right)^2. \tag{14}$$

Ce disque $\mathcal{D}_r(a, c)$ est tangent à la droite réelle au point $a/c$. Pour $r = 1$ on retrouve le disque de Ford usuel; le disque $\mathcal{D}_r(a, c)$ est ainsi une généralisation du disque de Ford, on l'appelle $r$-disque de Ford d'indice $(a, c)$.

*Preuve.* Posant $s = 1/r$, on considère le transformé $z' = h(z)$ d'un point $z = x + is$ de la droite $\Im(z) = s$. On utilise l'égalité

$$\frac{-1}{cz + d} - \frac{i}{2sc} = \frac{-1}{c(x + is) + d} - \frac{i}{2sc} = \frac{-i}{2sc}\left[\frac{c(x - is) + d}{c(x + is) + d}\right].$$

En posant $h(z) = z'$, on remarque que

$$cz' - a = \frac{-1}{cz + d},$$

et on en déduit que

$$\left| cz' - a - \frac{i}{2sc} \right| = \frac{1}{2sc}$$

et donc

$$\left| z' - \left( \frac{a}{c} + i\frac{r}{2c^2} \right) \right| = \frac{r}{2c^2}.$$

On vérifie ensuite que les transformés des points de $\mathcal{L}_r$ sont intérieurs au disque. ∎

### 2.2. Propriétés des disques de Ford

Nous décrivons maintenant quelques propriétés de ces disques que nous utiliserons largement dans la suite. Nous avons rappelé en (2) qu'en dimension 2, la constante d'Hermite $\gamma(z)$ a une valeur maximale égale à $2/\sqrt{3}$. Par conséquent, seuls les $r$-disques de Ford, avec une valeur de $r$ inférieure à $2/\sqrt{3}$ interviendront ici.

Soient deux nombres $a$ et $c$ premiers entre eux et $r$ un réel positif inférieur ou égal à $2/\sqrt{3}$. Les $r$-disques de Ford vérifient les propriétés suivantes :

(Fo1) Pour $|a| > c$, ces disques sont extérieurs au demi-disque unité $\mathcal{C}$.

Dans toute la suite, on considère donc des couples $(a, c)$ d'entiers premiers entre eux et vérifiant $|a| \le c$. On désignera par $\mathcal{P}$ leur ensemble

$$\mathcal{P} = \{(a, c) \mid \text{pgcd } (a, c) = 1 \text{ et } |a| \le c\}. \tag{15}$$

(Fo2) Pour $0 < |a| < c$, les $r$ disques de Ford d'indice $(a, c)$ sont inclus dans le demi-disque unité $\mathcal{C}$.

(Fo3) Pour $a = 0$, le $r$-disque de Ford est inclus dans $\mathcal{C}$ si et seulement si $r$ est inférieur à 1. Pour $|a| = c = 1$, les $r$-disques de Ford coupent le demi-disque $\mathcal{C}$.

(Fo4) Pour $r < 1$, les $r$-disques de Ford sont disjoints deux à deux.

(Fo5) Pour $1 \le r < 2/\sqrt{3}$, deux $r$-disques de Ford $\mathcal{D}(a, c)$ et $\mathcal{D}(b, d)$ sont sécants si et seulement si on a $|ad - bc| = 1$.

La définition des disques de Ford et leurs principales propriétés permettent alors de décrire le domaine de niveau associé à la constante d'Hermite.

### 2.3. Description du domaine de niveau associé à la constante d'Hermite

PROPOSITION 1. *L'ensemble $\Gamma(r)$ des nombres $z$ de $\mathcal{C}$ vérifiant $\gamma(z) \le r$ est égal à la réunion des $r$-disques de Ford. Plus précisément,*

$$\Gamma(r) = \bigcup_{(a,c)\in\mathcal{P}} \mathcal{D}_r(a, c) \cap \mathcal{C}, \quad \textit{avec} \;\; \mathcal{P} = \{(a, c) \mid \textit{pgcd } (a, c) = 1 \textit{ et } |a| \le c\}.$$

*Preuve.* La relation (13), le lemme 1, et la propriété (Fo1) montrent les inclusions suivantes

$$\Gamma(r) \subset \bigcup_{g \in \mathcal{H}} g(\mathcal{L}_r) \cap \mathcal{C} \subset \bigcup_{(a,c) \in \mathcal{P}} \mathcal{D}_r(a,c) \cap \mathcal{C}.$$

Réciproquement, considérons un nombre complexe $z$ du demi-disque unité $\mathcal{C}$ appartenant à un $r$-disque de Ford d'indice $(a, c)$. Alors, puisque $z$ appartient à $\mathcal{C}$, il existe un élément $g$ de $\mathcal{G}$ pour lequel $g^{-1}(z)$ appartient à $\mathcal{F}$. Par ailleurs, puisque $z$ appartient à $\mathcal{D}_r(a, c)$, il existe une homographie $h$ de $\mathcal{H}$ pour laquelle $h^{-1}(z)$ appartient à la bande $\mathcal{L}_r$. En composant éventuellement avec une translation $T^i$, on en déduit l'existence d'une homographie $h$ de $\mathcal{H}$ pour laquelle $h^{-1}(z)$ appartient à la bande $\mathcal{B}_r$, partie de la bande fondamentale située au-dessus de la droite d'équation $\Im(z) = 1/r$. Deux cas peuvent alors se présenter :

- ou bien $h^{-1}(z)$ est élément de $\mathcal{F}_r$, alors $z$ est élément de $\Gamma(r)$; c'est d'ailleurs nécessairement le cas pour $r \leq 1$ puisque $\mathcal{B}_r$ et $\mathcal{F}_r$ sont égaux.

- ou bien $h^{-1}(z)$ n'est pas élément de $\mathcal{F}_r$; mais alors $r$ est nécessairement strictement plus grand que 1, et pour un tel $r$, on a, [voir Figure 1], l'inclusion

$$S(\mathcal{B}_r \backslash \mathcal{F}_r) \subset \mathcal{F}_r.$$

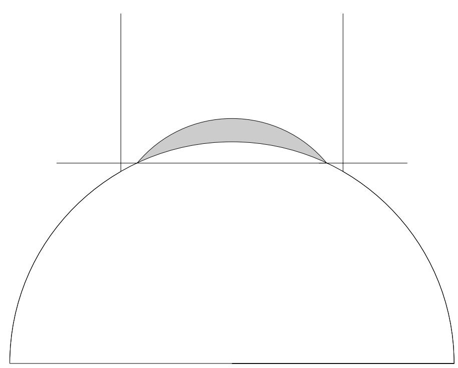

**Figure 1.** $S(\mathcal{B}_r \backslash \mathcal{F}_r) \subset \mathcal{F}_r$ pour $r \geq 1$.

On en déduit qu'alors $Sh^{-1}(z)$ est élément de $\mathcal{F}_r$.

Ainsi, dans tous les cas, il existe une transformation $h$ de $\mathcal{H}$ pour laquelle $h^{-1}(z)$ est élément de $\mathcal{F}_r$, et aussi une transformation $g$ de $\mathcal{G}$ pour laquelle

$g^{-1}(z)$ est élément de $\mathcal{F}$. On en déduit qu'il existe une transformation $g$ de $\mathcal{G}$ pour laquelle $g^{-1}(z)$ est élément de $\mathcal{F}_r$, et donc que $z$ appartient à $\Gamma(r)$.
∎

La figure 2 montre le domaine $\Gamma(r)$ pour trois valeurs du paramètre $r$, correspondant à $r = 1/2$, $r = 1$ et $r = (2/\sqrt{3})$.

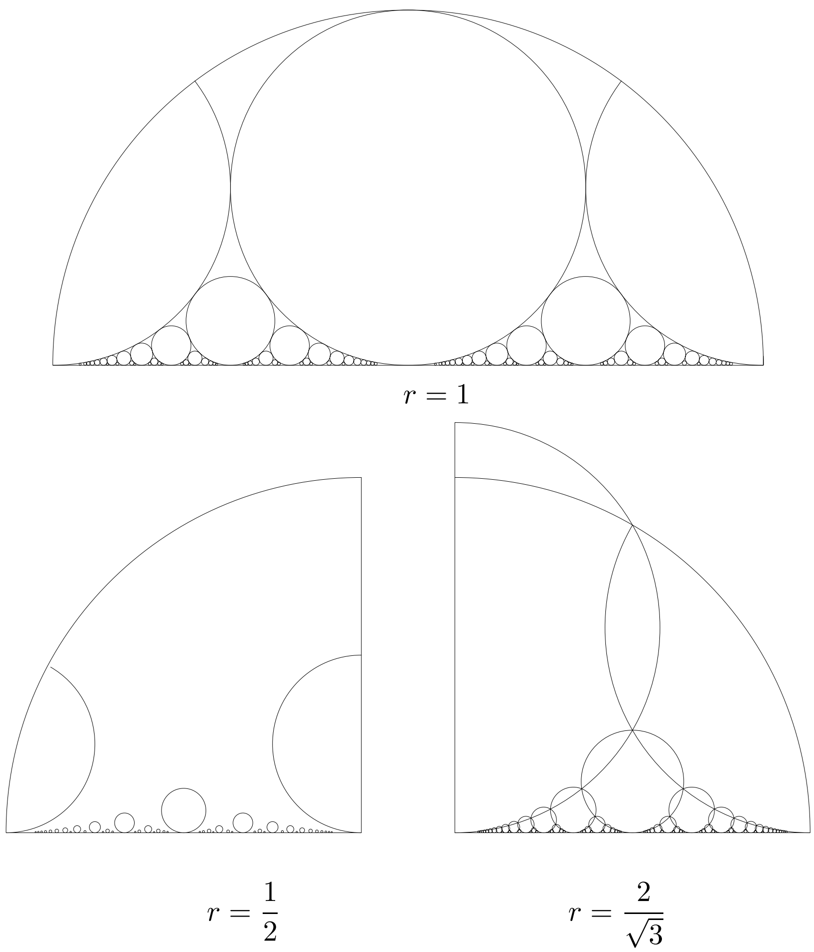


**Figure 2.** L'ensemble $\Gamma(r)$ pour $r = 1/2$, $r = 1$, $r = 2/\sqrt{3}$.

## 3. Demi-disques de Farey et domaines de niveau associés au premier minimum

La description des domaines de niveau associés au premier minimum se déduit de celle des domaines de niveau associés à la constante d'Hermite. Elle fait apparaître des demi-disques construits sur les intervalles de Farey.

Les intervalles de Farey d'ordre $t$ sont, par définition, les intervalles $\mathcal{I}_t(a,c)$ de centre $a/c$ et de rayon $t/c$ où $a$ et $c$ sont des entiers premiers entre eux vérifiant la condition $|a| \leq c$. On rappelle qu'en (15) on a désigné par $\mathcal{P}$ l'ensemble de tels couples.

On considère ici les demi-disques construits sur les intervalles $\mathcal{I}_t(a,c)$ lorque $(a,c)$ décrit $\mathcal{P}$; on les appelle des $t$-demi-disques de Farey et on les désigne par $\mathcal{D}'_t(a,c)$. Quand le couple $(a,c)$ décrit l'ensemble $\mathcal{P}$, on obtient une famille qui va intervenir dans la détermination des domaines de niveau associés à $\lambda(z) \leq t$.

### 3.1. Relation entre les demi-disques de Farey et le domaine de niveau associé au premier minimum

LEMME 2. *L'ensemble $\Lambda(t)$ des complexes $z$ vérifiant $\lambda(z) \leq t$ est égal à la réunion de $t$-demi-disques de Farey. Plus précisément :*

$$\Lambda(t) = \bigcup_{(a,c)\in\mathcal{P}} \mathcal{D}'_t(a,c) \cap \mathcal{C},$$

*où $\mathcal{P}$ est l'ensemble défini par*

$$\mathcal{P} = \{(a,c) \mid \text{pgcd } (a,c) = 1 \ \textit{et} \ \ |a| \leq c\}.$$

*Preuve.* Pour un nombre complexe $z$ de partie imaginaire $y = \Im(z)$ les deux conditions suivantes sont équivalentes en vertu de la relation (9) :

$z$ est élément de $\Lambda(t)$,

$z$ vérifie l'inégalité $\gamma(z) \leq t^2/\Im(z)$.

Or, le domaine de niveau $\gamma(z) \leq r$ est défini à partir des $r$-disques de Ford d'équation

$$\big(x - \frac{a}{c}\big)^2 + \big(y - \frac{r}{2c^2}\big)^2 \ \leq \ \big(\frac{r}{2c^2}\big)^2.$$

Le domaine de niveau $\lambda(z) \leq t$ est donc obtenu en remplaçant $r$ par $t^2/y$

$$\big(x - \frac{a}{c}\big)^2 + y^2 \ \leq \ \frac{t^2}{c^2}. \tag{16}$$

Lorsque $(a,c)$ décrit $\mathcal{P}$, on obtient ainsi les demi-disques de Farey de centre $a/c$ et de rayon $t/c$ dont on prend l'intersection avec $\mathcal{C}$. ∎

Lorsque $(a,c)$ décrit $\mathcal{P}$, la famille des demi-disques $\mathcal{D}'_t(a,c)$ de centre $a/c$ et de rayon $t/c$ forme une réunion "redondante". On cherche donc un ensemble $\mathcal{Q}(t)$ fini, le plus petit possible, pour lequel

$$\bigcup_{(a,c)\in\mathcal{P}} \mathcal{D}'_t(a,c) = \bigcup_{(a,c)\in\mathcal{Q}(t)} \mathcal{D}'_t(a,c). \tag{17}$$

On cherche aussi,afin d'obtenir une minoration simple de l'aire de la réunion (17), un sous-ensemble $\mathcal{Q}'(t)$ de $\mathcal{Q}(t)$, le plus grand possible, pour lequel la réunion

$$\bigcup_{(a,c)\in\mathcal{Q}'(t)} \mathcal{D}'_t(a,c) \tag{18}$$

soit une réunion disjointe ou au moins quasi-disjointe.
Un problème similaire se pose classiquement pour les intervalles de Farey, et nous rappelons maintenant la solution qui en est donnée dans ce cas et qui fournit des analogues $\mathcal{P}(t)$ et $\mathcal{P}'(t)$ aux ensembles définis en (17) et (18).

### 3.2. Les intervalles de Farey

On considère deux rationnels $a/c$ et $b/d$ vérifant $|ad-bc|=1$. Tous les rationnels de l'intervalle $](a/c),(b/d)[$ sont de la forme $(ma+nb)/(mc+nd)$ avec $m$ et $n$ strictement positifs et premiers entre eux. Pour $m=n=1$, on obtient le médian, qui est donc le rationnel de plus petit dénominateur de l'intervalle $](a/c),(b/d)[$.

On considère l'ensemble $\mathcal{P}(t)$ défini comme suit

$$\mathcal{P}(t) = \{(a,c) \mid \text{pgcd } (a,c)=1 \text{ et } \ |a|\le c\le \frac{1}{t}\}. \tag{19}$$

(Fa1) Deux rationnels $a/c$ et $b/d$ sont consécutifs dans $\mathcal{P}(t)$ si et seulement s'ils vérifient les deux conditions :

$$|ad-bc|=1 \text{ et } \ c+d>\frac{1}{t}.$$

(Fa2) Deux intervalles $\mathcal{I}_t(a,c)$ et $\mathcal{I}_t(b,d)$ associés à des éléments de $\mathcal{P}(t)$ sont sécants si et seulement s'ils sont consécutifs.
Deux intervalles $\mathcal{I}_t(a,c)$ et $\mathcal{I}_t(b,d)$ associés à des éléments de $\mathcal{P}(2t)$ sont toujours quasi-disjoints.

Parmi tous les rationnels $e/f$ compris entre deux rationnels consécutifs $a/c$ et $b/d$ de $\mathcal{P}(t)$, le médian joue un rôle particulier; en effet :

(Fa3) Si $e/f$ n'est pas le médian de $a/c$ et $b/d$, alors l'intervalle $\mathcal{I}_t(e,f)$ associé au rationnel $e/f$ est complètement inclus soit dans $\mathcal{I}_t(a,c)$ soit dans $\mathcal{I}_t(b,d)$.

(Fa4) L'intervalle $\mathcal{I}_t(e,f)$ associé au médian coupe chacun des deux intervalles $\mathcal{I}_t(a,c)$ et $\mathcal{I}_t(b,d)$; il est inclus dans la réunion $\mathcal{I}_t(a,c) \cup \mathcal{I}_t(b,d)$ et contient l'intersection $\mathcal{I}_t(a,c) \cap \mathcal{I}_t(b,d)$.

Tout ce qui précède montre que l'ensemble $\mathcal{P}(t)$ est solution minimale du problème posé :

$$\bigcup_{(a,c)\in\mathcal{P}} \mathcal{I}_t(a,c) = \bigcup_{(a,c)\in\mathcal{P}(t)} \mathcal{I}_t(a,c), \tag{20}$$

Par ailleurs, la propriété (Fa2) montre que $\mathcal{P}(2t)$ peut être choisi comme ensemble analogue à (18) puisque c'est un sous-ensemble de $\mathcal{P}(t)$ pour lequel la réunion

$$\bigcup_{(a,c)\in\mathcal{P}(2t)} \mathcal{I}_t(a,c) \quad \text{est disjointe.}$$

Notons l'existence d'un algorithme simple qui permet de construire l'ensemble $\mathcal{P}(t)$ à partir des trois couples $(-1,1),(0,1),(1,1)$ en rajoutant les médians d'éléments consécutifs :

**Algorithme construisant** $\mathcal{P}(t)$

(1) Au départ, $\mathcal{S} := \{(-1,1),(0,1),(1,1)\}$.

(2) Tant qu'il existe un médian de deux éléments consécutifs de $\mathcal{S}$ dont le dénominateur est inférieur à $1/t$, l'ajouter à $\mathcal{S}$.

(3) $\mathcal{P}(t) := \mathcal{S}$.

### 3.3. Les disques de Farey

On cherche maintenant à décrire les ensembles $\mathcal{Q}(t)$ et $\mathcal{Q}'(t)$ définis pour les demi-disques $\mathcal{D}'_t(a,c)$ en (17) et (18). L'ensemble $\mathcal{P}(2t)$ convient pour former une sous-réunion disjointe : on choisira dans toute la suite

$$\mathcal{Q}'(t) = \mathcal{P}(2t) = \{(a,c) \mid \text{pgcd } (a,c) = 1 \text{ et } \ |a| \le c \le \frac{1}{2t}\} \tag{21}$$

mais l'ensemble $\mathcal{P}(t)$ lui-même ne convient pas pour $\mathcal{Q}(t)$ car le demi-disque associé au médian de deux rationnels consécutifs de $\mathcal{P}(t)$ n'est plus en général inclus dans la réunion des deux demi-disques $\mathcal{D}'_t(a,c)$ et $\mathcal{D}'_t(b,d)$. Il est clair par ailleurs, d'après la propriété (Fa3) que l'ensemble obtenu en rajoutant à $\mathcal{P}(t)$ tous les médians des éléments successifs de $\mathcal{P}(t)$ convient, mais n'est sans doute pas minimal. Finalement, seuls des médians doivent être rajoutés, mais lesquels ? On a la caractérisation suivante, Lemme 3. *Pour deux rationnels consécutifs $a/c$ et $b/d$ de $\mathcal{P}(t)$, les deux conditions suivantes sont équivalentes*

$$(i)\ \mathcal{D}'_t(a+b, c+d) \subset \mathcal{D}'_t(a,c) \cup \mathcal{D}'_t(b,d),$$
$$(ii)\ c^2 + cd + d^2 \geq \frac{1}{t^2}.$$

*Preuve.* On suppose par exemple que $a/c$ est inférieur à $b/d$, et on désigne par $x_a$ [resp $x_b$] l'abscisse du point intersection du cercle frontière de $\mathcal{D}'_t(a,c)$ avec celui de $\mathcal{D}'_t(a+b, c+d)$ [resp. de $\mathcal{D}'_t(b,d)$ avec $\mathcal{D}'_t(a+b, c+d)$]. La condition (i) est alors équivalente à $x_a \geq x_b$, [voir Figure 3].

Or $x_a = \dfrac{(c+2d)(b-ct^2)+ad}{2d(c+d)}$ et $x_b = \dfrac{(2c+d)(a-dt^2)+bc}{2c(c+d)}$.

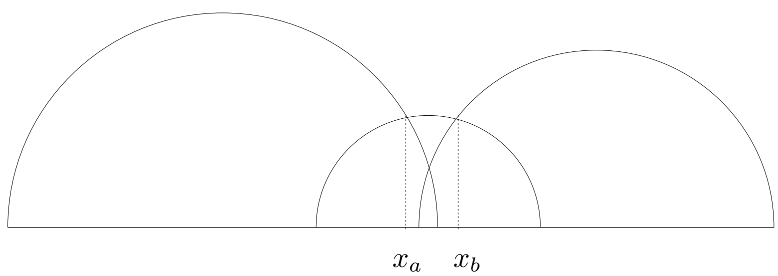


**Figure 3.** Deux disques de Farey et leur disque médian.

On en déduit l'équivalence cherchée. ∎

Pour obtenir un recouvrement de $\Lambda(t)$, il faut ainsi rajouter à l'ensemble $\mathcal{P}(t)$ les couples $(e,f)$ vérifiant

$(e,f) = (a+b, c+d)$ avec $\dfrac{a}{c}$ et $\dfrac{b}{d}$ consécutifs dans $\mathcal{P}(t)$ et $c^2+cd+d^2 < \dfrac{1}{t^2}$.

Mais, à part les trois couples exceptionnels $(-1,1)$, $(0,1)$, $(1,1)$, chaque couple $(a,c)$ de l'ensemble $\mathcal{P}(t)$ est lui-même un médian de deux éléments de $\mathcal{P}(t)$. L'ensemble cherché $\mathcal{Q}(t)$ est alors égal à la réunion de deux ensembles : un ensemble exceptionnel $\mathcal{Q}_e$ formé des trois couples $(-1,1)$, $(0,1)$, $(1,1)$ et un ensemble "ordinaire" $\mathcal{Q}_o(t)$

$$\mathcal{Q}_o(t) = \{(a+b, c+d),\ |ad-bc| = 1,\ |a| \leq c,\ |b| \leq d,\ c^2+cd+d^2 < \frac{1}{t^2}\}. \quad (22)$$

Il y a alors deux cas à considérer suivant que le dénominateur $e = c + d$ est celui d'un élément de $\mathcal{P}(t)$ ou non; remarquons que

$$c^2 + d^2 + dc = (c+d)^2 - cd = e^2 - c(e-c),$$

et donc :
(i) ou bien $e$ vérifie $e \leq 1/t$ et tous les couples $(a, c)$ et $(b, d)$ vérifiant

$$|ad - bc| = 1, \ |a| \leq c, \ |b| \leq d$$

sont par définition dans $\mathcal{P}(t)$ et donc dans $\mathcal{Q}(t)$.
(ii) ou bien $e > 1/t$; alors $c$ et $e$ vérifient les trois conditions suivantes

$$c(e-c) > e^2 - \frac{1}{t^2}, \quad 0 \leq c \leq e \quad \text{et} \quad \text{pgcd } (c, e) = 1.$$

Comme on a toujours $c(c-e) \leq e^2/4$ pour $0 \leq c \leq e$, on en déduit une borne supérieure pour les dénominateurs des rationnels de $\mathcal{Q}(t)$, et donc la double inclusion suivante

$$\mathcal{P}(t) \ \subset \ \mathcal{Q}(t) \ \subset \mathcal{P}(t\frac{\sqrt{3}}{2}). \tag{23}$$

Il existe aussi, comme c'était le cas précédemment pour $\mathcal{P}(t)$, une construction algorithmique pour $\mathcal{Q}(t)$, qui s'effectue par ajouts successifs de médians d'éléments consécutifs.

**Algorithme construisant** $\mathcal{Q}(t)$

(1) Au départ, $\mathcal{S} := \{(-1, 1), (0, 1), (1, 1)\}$.
(2) Tant qu'il existe un couple $(c, d)$ formé par les dénominateurs $c$ et $d$ de deux éléments consécutifs $(a/c)$ et $(b/d)$ qui vérifie

$$c^2 + d^2 + cd \leq \frac{1}{t^2},$$

ajouter le médian de $(a/c)$ et $(b/d)$ à $\mathcal{S}$.
(3) $\mathcal{Q}(t) := \mathcal{S}$.

Enonçons maintenant les propriétés décrivant l'intersection des demi-disques de la famille, analogues aux propriétés (Fa1) et (Fa2) des intervalles de Farey.

(Fa1') Deux rationnels $a/c$ et $b/d$ sont consécutifs dans $\mathcal{Q}(t)$ si et seulement s'ils vérifient les deux conditions :

$$|ad - bc| = 1 \text{ et } \; c^2 + d^2 + cd > \frac{1}{t^2}. \tag{24}$$

(Fa2') Deux demi-disques $\mathcal{D}'_t(a, c)$ et $\mathcal{D}'_t(b, d)$ associés à des éléments $(a, c)$ et $(b, d)$ de $\mathcal{Q}(t)$ peuvent être sécants dans les deux seuls cas suivants,

ou bien ces éléments sont deux éléments de $\mathcal{P}(t)$ consécutifs dans $\mathcal{Q}(t)$ : leur médian n'a donc pas été rajouté,

ou bien ils ne sont plus consécutifs dans $\mathcal{Q}(t)$, mais ils l'étaient dans $\mathcal{P}(t)$ : ils ont été séparés par l'arrivée de leur médian.

Dans ce dernier cas, il existe une intersection commune entre les trois demi-disques [voir Figure 3]; mais la propriété (Fa4) des intervalles de Farey montre que le demi-disque médian $\mathcal{D}'_t(a + b, c + d)$ contient dans ce cas l'intersection $\mathcal{D}'_t(a, c) \cap \mathcal{D}'_t(b, d)$. L'aire de la réunion des trois demi-disques s'exprime uniquement avec l'aire des trois demi-disques et l'aire des deux intersections de chacun des deux demi-disques d'indice $(a, c)$ et $(b, d)$ avec leur disque médian commun, [voir Figure 3].

Finalement, dans chacun des deux cas précédemment décrits, l'aire de la réunion s'exprimera en fonction de l'aire des demi-disques et de l'aire de l'intersection de disques consécutifs dont les indices $(a, c)$ et $(b, d)$ vérifient donc la relation (24).

### 3.4. Description du domaine de niveau associé au premier minimum

Tout ce qui précède permet de donner une description de l'ensemble $\mathcal{Q}(t)$ cherché, et d'en déduire une caractérisation minimale de l'ensemble $\Lambda(t)$.

Proposition 2. *L'ensemble $\Lambda(t)$ des nombres $z$ de $\mathcal{C}$ vérifiant $\lambda(z) \le t$ est égal à la réunion des $t$-demi-disques de Farey prise sur l'ensemble fini $\mathcal{Q}(t)$*

$$\Lambda(t) = \bigcup_{(a,c) \in \mathcal{Q}(t)} \mathcal{D}'_t(a, c) \cap \mathcal{C},$$

*avec $\mathcal{Q}(t) = \mathcal{Q}_o(t) \cup \mathcal{Q}_e$, où*

$$\mathcal{Q}_o(t) = \{(a + b, c + d), \; |ad - bc| = 1, \; |a| \le c, \; |b| \le d, \; c^2 + cd + d^2 < \frac{1}{t^2}\}$$

*et*

$$\mathcal{Q}_e = \{(-1, 1), (0, 1), (1, 1)\}.$$

La figure 4 montre le domaine $\Lambda(t)$ pour cinq valeurs du paramètre $t$, correspondant à $t = 1/\sqrt{3}$, $t = 1/2$, $t = 1/4$, $t = 5/22$, $t = 5/24$.

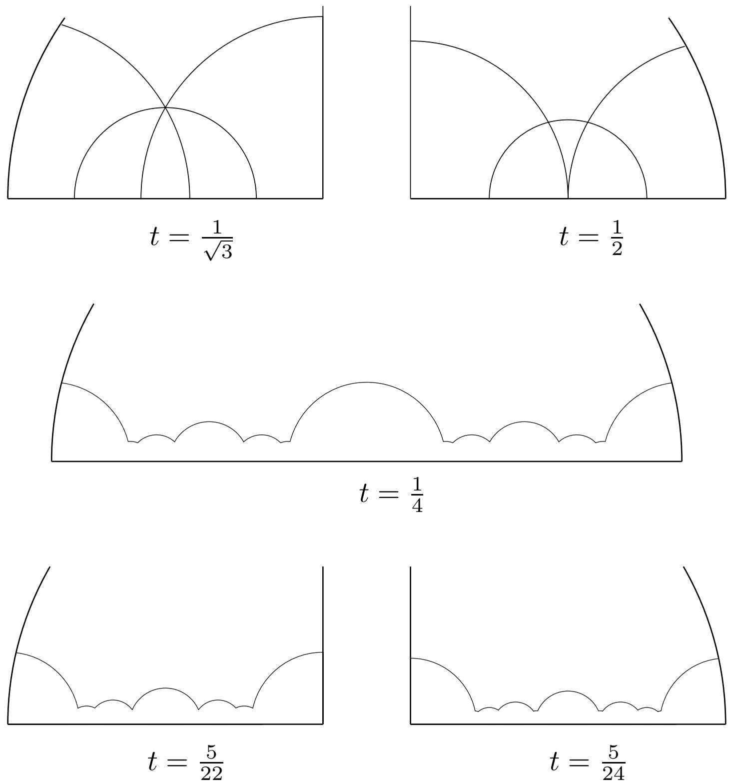


**Figure 4.** L'ensemble $\Lambda(t)$ pour $t = 1/\sqrt{3},\ \ 1/2,\ \ 1/4,\ \ 5/22,\ \ 5/24.$

## 4. Fonctions de répartition des variables étudiées

Les fonctions de répartition des deux variables étudiées se calculent à l'aide des aires des domaines $\Gamma(r)$ et $\Lambda(t)$. On désigne respectivement par $G(r)$ et $L(t)$ les aires de $\Gamma(r)$ et $\Lambda(t)$

$$\mathrm{Pr}\ [\gamma(z) \leq r] = \frac{2G(r)}{\pi} \text{ et } \mathrm{Pr}\ [\lambda(z) \leq t] = \frac{2L(t)}{\pi}.$$

Le principe adopté dans ces deux calculs est le même. D'après les propositions 1 et 2, les deux aires à calculer sont des aires de réunions non disjointes; on calcule donc à part l'aire des intersections, et on sépare l'aire restante en

deux, selon qu'il s'agit d'une aire “apportée” par les trois disques exceptionnels, d'indice $(-1, 1)$, $(0, 1)$, et $(1, 1)$ ou d'une aire “ordinaire”. Chacune des quantités $G(r)$ ou $L(t)$ s'exprimera comme la somme d'une aire ordinaire, indicée par $o$, à laquelle on retranchera l'aire exceptionnelle, indicée par $e$ et l'aire des intersections, indicée par $i$.
Au voisinage de l'origine, dans les deux cas, le terme principal proviendra de l'aire ordinaire.

### 4.1. Calcul des aires d'intersection

On a besoin, dans tout ce calcul, de l'aire de l'intersection de deux disques sécants; comme le montre la figure 5, une telle aire s'exprime comme la somme des aires de deux secteurs circulaires, à laquelle on retire l'aire d'un triangle.

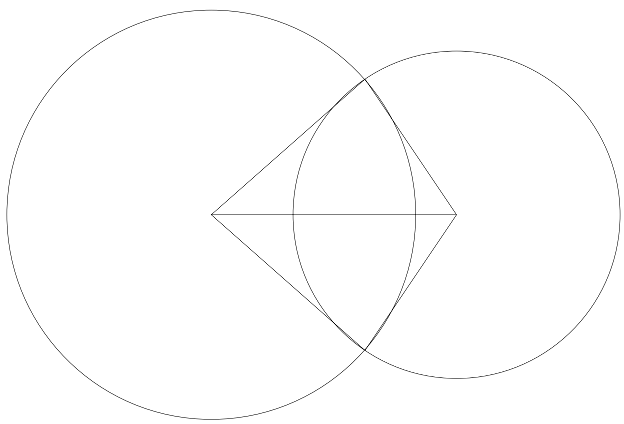

**Figure 5.** L'aire de l'intersection de deux disques.

L'aire $J$ de l'intersection de deux disques $\mathcal{D}_1$ et $\mathcal{D}_2$ sécants s'exprime uniquement en fonction des deux rayons $r_1$ et $r_2$ et de la distance des centres $\delta$ :

$$J = r_1^2 \arcsin \frac{r_2 \sin\theta}{\delta} + r_2^2 \arcsin \frac{r_1 \sin\theta}{\delta} - r_1 r_2 \sin\theta,$$

avec

$$\sin\,\theta = \frac{1}{2r_1r_2}[\delta^2 - (r_1 - r_2)^2]^{1/2}[(r_1 + r_2)^2 - \delta^2]^{1/2}. \qquad (25)$$

Dans le cas où ces disques sont orthogonaux, on obtient

$$J = (r_1^2 - r_2^2)\,\arctan \frac{r_2}{r_1} + \frac{\pi}{2} r_2^2 - r_1 r_2.$$

Dans chacun des cas où ce résultat (25) s'applique, pour l'intersection de deux demi-disques de Farey ou de deux disques de Ford d'indices $(a, c)$ et $(b, d)$, les couples $(a, c)$ et $(b, d)$ vérifient la relation

$$|ad - bc| = 1, \ |a| \leq c, \ |b| \leq d, \tag{26}$$

et les trois paramètres - les deux rayons, et la distance des centres - s'expriment uniquement en fonction des dénominateurs $c$ et $d$. On a ainsi, pour l'aire de l'intersection de deux $r$-disques de Ford

$$J(r, c, d) = \frac{r^2}{4c^4} \arcsin\left[c^2 \rho(r, c, d)\right] + \frac{r^2}{4d^4} \arcsin\left[d^2 \rho(r, c, d)\right] - \frac{1}{2c^2 d^2} \sqrt{r^2 - 1},$$

avec

$$\rho(r, c, d) = \left[\frac{4(r^2 - 1)}{4c^2 d^2 r^2 + r^4 (d^2 - c^2)^2}\right]^{1/2}. \tag{27}$$

De même, pour l'aire de l'intersection de deux $t$-demi-disques de Farey,

$$J'(t, c, d) = \frac{t^2}{2c^2} \arcsin \frac{\mu(t, c, d)}{2dt} + \frac{t^2}{2d^2} \arcsin \frac{\mu(t, c, d)}{2ct} - \frac{\mu(t, c, d)}{4c^2 d^2},$$

avec

$$\mu(t, c, d) = [1 - t^2 (c - d)^2]^{1/2} [t^2 (c + d)^2 - 1]^{1/2}. \tag{28}$$

Or, pour chaque couple non ordonné $(c, d)$ d'entiers positifs premiers entre eux, il existe exactement quatre couples $(a, b)$ vérifiant (26), et donc quatre intersections possibles; à chaque couple ordonné $(c, d)$, il correspond finalement deux intersections possibles.
Ainsi, la propriété (Fo5) des disques de Ford permet d'écrire

$$G_i(r) = 2 \sum_{\text{pgcd } (c,d)=1} J(r, c, d) \tag{29}$$

et, de même, la propriété (Fa2') des disques de Farey permet d'écrire

$$L_i(t) = 2 \sum_{(c,d) \in \mathcal{R}(t)} J'(t, c, d) \tag{30}$$

où $\mathcal{R}(t)$ est défini comme étant l'ensemble des couples ordonnés $(c, d)$ formés de deux dénominateurs de rationnels consécutifs de $\mathcal{Q}(t)$ et caractérisé par (24).
Comme, par ailleurs, les deux fonctions $\rho$ et $\mu$ sont des fonctions symétriques de $c$ et $d$, la sommation des deux premiers termes de chaque expression

$J(r,c,d)$ ou $J'(t,c,d)$ fait intervenir la même série, et on obtient finalement, d'après (27), (28), (29), (30) :

$$G_i(r) = r^2 \sum_{\text{pgcd }(c,d)=1} \frac{1}{d^4} \arcsin\left[d^2 \rho(r,c,d)\right] - \sqrt{r^2-1} \sum_{\text{pgcd }(c,d)=1} \frac{1}{c^2 d^2}, \qquad (31)$$

$$L_i(t) = 2t^2 \sum_{(c,d)\in\mathcal{R}(t)} \frac{1}{c^2} \arcsin \frac{\mu(t,c,d)}{2dt} - \frac{1}{2} \sum_{(c,d)\in\mathcal{R}(t)} \frac{\mu(t,c,d)}{c^2 d^2}. \qquad (32)$$

### 4.2. Calcul de l'aire ordinaire

Dans chacun des cas, la famille d'indices sur laquelle on somme les aires ordinaires fait intervenir, de manière directe ou indirecte, les couples$(a,c)$ d'entiers premiers entre eux et vérifiant $|a| \le c$. Dans cet ensemble, les trois couples $(-1,1),(0,1),(1,1)$ jouent un rôle exceptionnel puisqu'ils donnent lieu à des disques de Ford ou des demi-disques de Farey qui ne sont pas complètement inclus dans le demi-disque unité $\mathcal{C}$. On considèrera comme ordinaire l'aire apportée par le couple $(0,1)$ et la moitié de l'aire apportée par chacun des deux autres couples.

Ainsi, si $\varphi$ désigne la fonction d'Euler, il y a exactement, pour chaque valeur de l'entier $c$, y compris la valeur $c=1$, $2\varphi(c)$ tels couples. Comme, par ailleurs, le rayon ne dépend que du dénominateur $c$, on est amené aux séries de terme général $\varphi(n)/n^s$ pour les valeurs entières $s=4$ et $s=2$. On utilise alors les résultats classiques suivants (voir par exemple [HW]).

La série de terme général $\varphi(n)/n^s$ associée à la fonction d'Euler $\varphi$ a un comportement lié à la fonction $\zeta$ définie pour $s>1$ par

$$\zeta(s) = \sum_{n\ge 1} \frac{1}{n^s}.$$

Pour $s>2$, la série de terme général $\varphi(n)/n^s$ converge et sa somme est égale à $\zeta(s-1)/\zeta(s)$. En particulier, pour $s=4$, on obtient

$$\sum_{n\ge 1} \frac{\varphi(n)}{n^4} = \frac{\zeta(3)}{\zeta(4)}. \qquad (33)$$

Pour $s=2$, cette série diverge et la somme partielle $T(N)$ d'ordre $N$

$$T(N) = \sum_{n=1}^{N} \frac{\varphi(n)}{n^2}$$

admet, pour $N \geq 2$, l'encadrement suivant

$$|T(N) - \frac{1}{\zeta(2)}\,(\log N + \gamma_0 - \frac{\zeta'(2)}{\zeta(2)})\,| \leq \frac{5}{2}\frac{\log N}{N} \tag{34}$$

où $\gamma_0$ est la constante d'Euler.

**4.3. Fonction de répartition de la constante d'Hermite.**

On peut alors déterminer la valeur de l'aire $G(r)$ du domaine de niveau associé à la constante d'Hermite.

Théorème 1. *La surface $G(r)$ du domaine $\Gamma(r)$ s'exprime comme la somme de trois termes*

$$G(r) = G_o(r) - G_e(r) - G_i(r),$$

*avec*

$$G_o(r) = \frac{\pi r^2}{2}\frac{\zeta(3)}{\zeta(4)},$$

$$G_e(r) = \begin{cases} r - (2 - \frac{r^2}{2})\arctan\frac{r}{2} & \textit{si } r < 1, \\ r + \frac{1}{2}\sqrt{r^2-1} + (\frac{r^2}{2} - 2)\arctan\frac{r}{2} + (\frac{r^2}{2} - 1)\arccos\frac{1}{r} & \textit{si } 1 \leq r \leq \frac{2}{\sqrt{3}}, \end{cases}$$

$$G_i(r) = \begin{cases} 0 & \textit{si } r < 1, \\ -\frac{\zeta(2)^2}{\zeta(4)}\sqrt{r^2-1} + \frac{r^2}{\zeta(4)}S(r) & \textit{si } 1 \leq r \leq \frac{2}{\sqrt{3}}, \end{cases}$$

*où*

$$S(r) = \sum_{(c,d)} \frac{1}{d^4}\arcsin\,[\frac{4(r^2-1)\,d^4}{4c^2d^2r^2 + r^4(d^2-c^2)^2}]^{1/2}.$$

*Preuve.* L'expression de $G_o(r)$ se déduit clairement du paragraphe 4.2, plus particulièrement de l'égalité (33). On rappelle qu'on rajoute fictivement dans $G_o(r)$ le premier terme pour $c = 1$, quitte à le retirer dans $G_e(r)$.
L'expression de $G_e(r)$ est évaluée en remarquant que les deux disques $\mathcal{D}_r(-1,1)$, $\mathcal{D}_r(1,1)$ sont tous deux orthogonaux au demi-disque unité $\mathcal{C}$. Selon la valeur de $r$, le disque $\mathcal{D}_r(0,1)$ est inclus ou non dans $\mathcal{C}$.
L'expression de $G_i(r)$ est évaluée à l'aide de (31)

$$G_i(r) = \sum_{\text{pgcd }(c,d)=1} \frac{r^2}{d^4}\arcsin d^2\rho(r,c,d) - \sqrt{r^2-1}\sum_{\text{pgcd }(c,d)=1}\frac{1}{c^2d^2},$$

avec

$$\rho(r,c,d) = [\frac{4(r^2-1)}{4c^2d^2r^2 + r^4(d^2-c^2)^2}]^{1/2}.$$

Comme la fonction $\rho$ est une fonction du couple $(c,d)$ homogène de degré -2

$$\rho(r,mc,md) = \frac{1}{m^2}\rho(r,c,d),$$

la fonction sous l'arcsin est homogène de degré 0. Ainsi, chacune des deux séries a un terme général homogène de degré $-4$, et on peut transformer la sommation en une sommation sur tous les indices $(c,d)$, quitte à diviser par $\zeta(4)$. On déduit de ce qui précèdele résultat annoncé pour $G_i(r)$. ∎

Corollaire 1. *Au voisinage de l'origine, on a*

$$\Pr\,[\gamma(z) \le r] = \frac{\zeta(3)}{\zeta(4)}\ r^2\ [1+\alpha(r)] \qquad \textit{avec}\ \ \alpha(r)\to 0\ \textit{pour}\ r\to 0.$$

*Preuve.* En effet quand $r$ tend vers 0, le terme $G_e(r)$ est de l'ordre de $r^3$, car

$$(2-\frac{r^2}{2})\arctan\frac{r}{2} = r - \frac{r^3}{3} + r^3\epsilon(r) \text{ avec } \ \epsilon(r)\to 0 \text{ pour } r\to 0.$$

C'est donc $G_o(r)$ qui donne le terme principal au voisinage de l'origine. ∎

Corollaire 2. *La série $S = S(2/\sqrt{3})$, de la forme*

$$S = \sum_{(c,d)} \frac{1}{d^4}\arctan\frac{d^2}{c\sqrt{c^2+d^2}},$$

*peut s'exprimer en fonction de $\zeta(3)$ sous la forme suivante*

$$S = \frac{\pi}{2}\zeta(3) - \frac{\pi^5}{540}.$$

*Preuve.* Puisque la valeur $2/\sqrt{3}$ est la valeur maximale possible pour $\gamma(z)$, on déduit que

$$\Pr\,[\gamma(z) \le \frac{2}{\sqrt{3}}] = 1,$$

ce qui permet d'obtenir le résultat cherché. ∎

### 4.4. Fonction de répartition du premier minimum

On peut maintenant déterminer la valeur de l'aire $L(t)$ du domaine de niveau associé au premier minimum.

THÉORÈME 2. *La surface $L(t)$ du domaine $\Lambda(t)$ s'exprime comme la somme de trois termes*

$$L(t) = L_o(t) - L_e(t) - L_i(t),$$

*avec*

$$L_o(t) = \pi t^2 + \frac{\pi t^2}{2} \sum_{(a,c)\in\mathcal{Q}_o(t)} \frac{1}{c^2}$$

$$L_e(t) = t\sqrt{1-\frac{t^2}{4}} - (1-\frac{t^2}{2})(\pi - 2\arccos\frac{t}{2})$$

$$L_i(t) = 2t^2 \sum_{(c,d)\in\mathcal{R}(t)} \frac{1}{d^2}\arcsin\left[\frac{\mu(t,c,d)}{2ct}\right] - \frac{1}{2}\sum_{(c,d)\in\mathcal{R}(t)} \frac{\mu(t,c,d)}{c^2d^2}$$

*où $\mathcal{Q}_o(t)$ et $\mathcal{R}(t)$ sont les ensembles définis respectivement en (22) et (24), et où $\mu(t,c,d)$ est égal à*

$$\mu(t,c,d) = [1-t^2(c-d)^2]^{1/2}[t^2(c+d)^2-1]^{1/2}.$$

Cette expression exacte est peu maniable et on en cherche donc un encadrement.

LEMME 4. *Pour tout réel $t$ de l'intervalle $[0,1]$, l'aire $L(t)$ admet l'encadrement suivant*

$$\frac{2}{\pi}L(t) \le t^2\ T(\frac{2}{t\sqrt{3}}) \tag{35}$$

$$\frac{2}{\pi}L(t) \ge t^2\ [\ T(\frac{1}{2t}) - \frac{2}{\pi}\arcsin\frac{t}{2}] \tag{36}$$

*où la fonction $T(u)$ est égale par définition à*

$$T(u) = \sum_{1\le c\le u} \frac{\varphi(c)}{c^2}.$$

*Preuve.* L'encadrement de $\mathcal{Q}(t)$ obtenu en (23) permet d'obtenir la majoration (35). La minoration (36) est obtenue à partir de la caractérisation de $\mathcal{Q}'(t)$ obtenue en (21) et de la minoration suivante pour $L_e(t)$ :

$$L_e(t) \le t^2 \arcsin\frac{t}{2}.$$

∎

Corollaire 3. *Au voisinage de* 0*, la fonction de répartition du premier minimum admet l'équivalent suivant :*

$$\text{Pr }[\lambda(z) \leq t] = \frac{2t^2}{\zeta(2)}\ [|\log t| + \delta(t)],$$

*avec* $\delta(t)$ *restant bornée sur l'intervalle* $[0, 1]$*.*

*Preuve.* L'encadrement de la fonction $L$ obtenu dans le lemme 4 et celui de la fonction $T$ obtenu dans l'inégalité (34) permettent de conclure. ∎

**Conclusion.** Ainsi, nous avons étudié, dans un modèle probabiliste naturel, les fonctions de répartition de deux variables aléatoires fondamentales dans la théorie et la pratique algorithmique des réseaux. Les résultats très précis que nous avons obtenus sont rendus possibles par l'effectivité du problème en dimension 2 : le domaine fondamental, aussi bien que les transformations qui permettent d' y arriver sont totalement explicités dans ce cas. L'obtention de tels résultats est aussi grandement facilitée par la possibilité technique de travailler dans $\mathbb{C}$ plutôt que dans $\mathbb{C}^2$ et d'utiliser ainsi la géométrie du demi-plan de Poincaré.

Il est sans doute illusoire d'espérer obtenir des résultats aussi précis en dimension générale. Ce n'est peut-être pas exclu en dimension 3, puisqu'il existe encore une caractérisation du domaine fondamental [Ga], [Di], et un algorithme de réduction géométriquement naturel [Va]. En dimension générale, il n'existe plus de caractérisation explicite d'un domaine fondamental; sans doute est-il tout de même possible alors de préciser par exemple le comportement du premier minimum, en affinant l'encadrement obtenu en (3) et (4) $\cdots$

## Bibliographie

[CMOS] M. J. Coster, B. A. LaMacchia, A. M. Odlyzko, C. P. Schnorr, *An improved low-density subset sum algorithm*, Comptes-Rendus du congrès Eurocrypt'91, Lecture Notes in Computer Science **547** (1991), 54–67.

[Di] G. L. Dirichlet, *Über die Reduction der positiven quadratischen Formen mit drei unbestimmten ganzen Zahlen*, J. reine angew. Math. **40** (1850), 209–227.

[DV] H. Daudé, B. Vallée, *An upper bound on the average number of iterations of the LLL algorithm*, Theoret. Comput. Sci. **123** (1994), 95–115.

[FHFLS] A. M. Frieze, J. Hastad, R. Kannan, J. C. Lagarias, A. Shamir, *Reconstructing truncated integer variables satisfying linear congruences*, SIAM J. Comput. **17** (1988), 262–280.

[Ga] C. F. Gauss, *Recherches arithmétiques*, traduction française de Disquisitiones Arithmeticae, Blanchard, Paris, 1953.

[HW] G. H. Hardy, E. M. Wright, *An introduction to the theory of numbers*, Oxford Science Publications, 1989.

[JS] A. Joux, J. Stern, *Improving the critical density of the Lagarias-Odlyzko attack against subset sum problems*, Comptes-Rendus du congrès FCT'91, Lecture Notes in Computer Science **529** (1991), 258–264.

[LLL] A. K. Lenstra, H. W. Lenstra, L. Lovász, *Factoring polynomials with rationals coefficients*, Math. Ann. **261** (1982), 515–534.

[LO] J. C. Lagarias, A. M. Odlyzko, *Solving low-density sum problems*, J. Assoc. Comput. Mach. **32** (1985), 229–246.

[Si] C. L. Siegel, *Lectures on the geometry of numbers*, Springer-Verlag, 1989.

[St] J. Stern, *Secret linear congruential generators are not cryptographically secure*, Comptes-Rendus du 28e congrès IEEE-FOCS (1987), 421–426.

[Va] B. Vallée, *An affine algorithm for minima finding in integer lattices of three dimensions*, Rapport de Recherche A3L 1989-9, Département de mathématiques, Université de Caen, 1989.

[VEB] P. van Emde Boas, *Another NP-complete partition problem and the complexity of computing short vectors in a lattice*, Report 81-04, Department of Mathematics, University of Amsterdam, 1981.

[VF] B. Vallée, P. Flajolet, *The lattice reduction algorithm of Gauss: an average case analysis*, Comptes-Rendus du 31e congrès IEEE-FOCS (1990), 830–839.

[VGT] B. Vallée, M. Girault, P. Toffin, *How to guess $\ell$-th roots modulo n by reducing lattices bases*, Comptes-Rendus du congrès AAECC-88, Rome, juillet 1988, Lecture Notes in Computer Science **357** (1989), 427–442.

Henri LAVILLE
GRAL, Département de Mathématiques,
Université de Caen,
14032 Caen Cedex

Brigitte VALLÉE
LAIAC, Département d'Informatique,
Université de Caen et ISMRa,
14032 Caen Cedex