Université de Montréal

Dénombrement dans les empilements apolloniens généralisés et distribution angulaire dans les extensions quadratiques imaginaires

par

Dias Dimitri

Département de mathématiques et de statistique
Faculté des arts et des sciences

Thèse présentée à la Faculté des études supérieures
en vue de l'obtention du grade de
Philosophiæ Doctor (Ph.D.)
en mathématiques
orientation mathématiques fondamentales

Juillet 2015

Université de Montréal

Faculté des études supérieures

Cette thèse intitulée

Dénombrement dans les empilements apolloniens généralisés et distribution angulaire dans les extensions quadratiques imaginaires

présentée par

Dias Dimitri

a été évaluée par un jury composé des personnes suivantes :

Lalín Matilde

(président-rapporteur)

Granville Andrew

(directeur de recherche)

Koukoulopoulos Dimitris

(membre du jury)

Kontorovich Alex

(examinateur externe)

Lalín Matilde

(représentant du doyen de la FAS)

Thèse acceptée le

25 Novembre 2015

RÉSUMÉ

Cette thèse traite de deux thèmes principaux.

Le premier concerne l'étude des empilements apolloniens généralisés de cercles et de sphères. Généralisations des classiques empilements apolloniens, dont l'étude remonte à la Grèce antique, ces objets s'imposent comme particulièrement attractifs en théorie des nombres. Dans cette thèse sera étudié l'ensemble des courbures (les inverses des rayons) des cercles ou sphères de tels empilements. Sous de bonnes conditions, ces courbures s'avèrent être toutes entières. Nous montrerons qu'elles vérifient un principe local-global partiel, nous compterons le nombre de cercles de courbures plus petites qu'une quantité donnée et nous nous intéresserons également à l'étude des courbures premières.

Le second thème a trait à la distribution angulaire des idéaux (ou plutôt ici des nombres idéaux) des corps de nombres quadratiques imaginaires (que l'on peut voir comme la distribution des points à coordonnées entières sur des ellipses). Nous montrerons que la discrépance de l'ensemble des angles des nombres idéaux entiers de norme donnée est « faible » et nous nous intéresserons également au problème des écarts bornés entre les premiers d'extensions quadratiques imaginaires dans des secteurs.

Mots-clefs : empilements apolloniens, principe local-global, distribution angulaire, écarts bornés, formes quadratiques.

SUMMARY

This thesis consists of two main parts.

In the first one, we study generalized Apollonian circles and spheres packings. Apollonian packings date back to ancient Greece and, from a number theoretical point of view, are very attractive objects. In this thesis, we will study the set of curvatures (the inverses of the radii) of a generalization of such packings. Under the right conditions, these curvatures are integers. We will show that they satisfy a partial local-global principle, we will count the number of circles of curvatures bounded by some parameter T and we will study the set of prime curvatures.

The second part is related to the angular distribution of ideals (or ideal numbers in our case) in imaginary quadratic number fields (which can be seen as the distribution of lattice points on ellipses). We will show that the discrepancy of the set of angles of integral ideal numbers of a given norm is "small" and we will look at the problem of bounded gaps between prime elements of imaginary quadratic extensions in sectors.

Keywords: apollonian packings, local-global principle, angular distribution, bounded gaps, quadratic forms.

TABLE DES MATIÈRES

TABLE DES FIGURES

REMERCIEMENTS

Je remercie tout d'abord mon directeur de recherche, Andrew Granville, de m'avoir offert l'opportunité d'accomplir mon doctorat. De par notamment son soutien financier et mathématique, il a rendu possible la réalisation de cette thèse.

Je tiens également à exprimer toute ma gratitude envers Guillaume Ricotta, sans qui rien ne serait arrivé. Je lui serai à jamais reconnaissant de m'avoir permis de venir étudier à Montréal et d'avoir ainsi changé ma vie.

Je remercie Alex Kontorovich et Elena Fuchs d'avoir bien voulu offrir des réponses inspirantes à mes multiples questions.

Merci également à l'ensemble du personnel du Département de Mathématiques et de Statistique de l'Université de Montréal, et particulièrement à Anne-Marie Dupuis, pour avoir fait de mon séjour en leurs murs une expérience des plus agréables.

Je remercie mes amis pour leur soutien indéfectible tout au long de ma thèse. Aziz Raymond Elmahdaoui, une infinie reconnaissance pour avoir supporté le maudit Français que je suis durant ce long périple et avoir fait de moi un Québécois de cœur. Sans ordre particulier, Marc Munsch, Maria Myronova, Lenka Motlochová, Golnaz Shaverdi, Yasmine Boulahia, Clarence Simard, Lenka Háková, Sara Zafar Jafar-Zadeh, Crystel Bujold, Cíntia Soares, Daniel Barrera Salazar, Nicolas Delfosse, Eric Naslund, Sara Golyari, Roberto Persechino, Zofia Grabowiecka, Mohammad Bardestani, Kevin Henriot, Daniel Fiorilli, Oleksiy Klurman, Marzieh Mehdizadeh, Farzad Aryan, merci d'avoir été à mes côtés. À ceux que j'ai laissés loin et qui me manquent tant, Julien Husser, Mathias Salmon, Sophie Marques, Maÿlis Limouzineau, Aurélien Bajolet, merci d'être venu me rendre visite ou de m'avoir accueilli.

Je remercie enfin ma famille, qui a toujours été là pour moi. Maman, Papa, Iris, je vous aime.

AVANT-PROPOS

Cette thèse s'intéresse principalement à deux thèmes, plus ou moins directement liés aux formes quadratiques.

Le premier concerne l'étude des empilements apolloniens généralisés de cercles et de sphères. La construction d'un empilement apollonien généralisé de cercles se base sur la propriété suivante : dans une configuration de trois cercles mutuellement tangents, il existe une unique façon d'inscrire, dans chaque espace vide, trois nouveaux cercles mutuellement tangents, de sorte que chaque cercle inscrit soit tangent à exactement deux des cercles d'origine. En itérant ce procédé, on obtient un empilement apollonien généralisé de cercles.

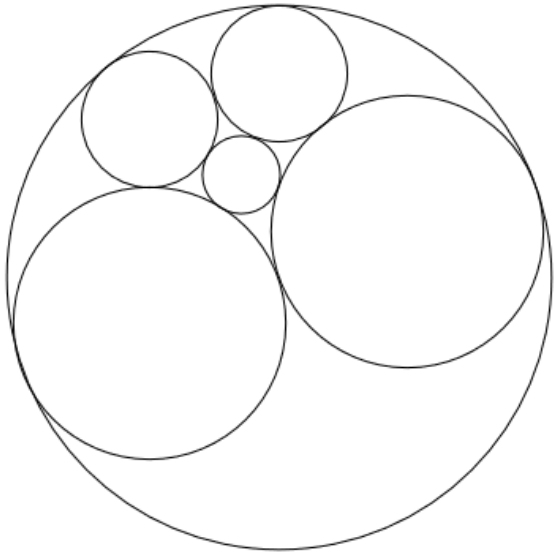

FIGURE 1. Un exemple de configuration généralisée de cercles

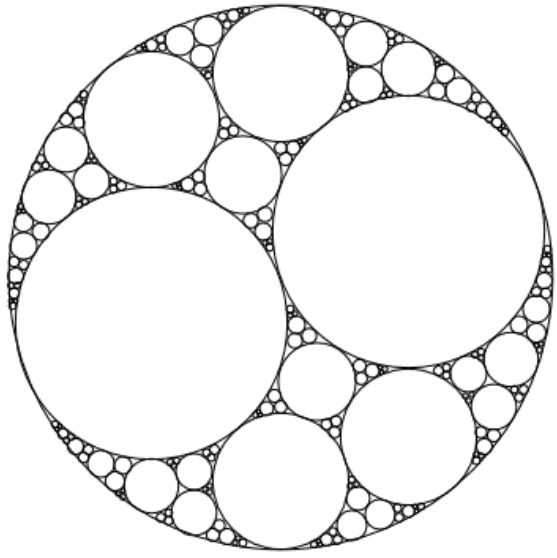

FIGURE 2. Un exemple d'empilement apollonien généralisé de cercles

Ce problème est un analogue au classique cas des empilements apolloniens de cercles, dont l'étude remonte à la Grèce antique et qui a été récemment l'objet d'une recherche approfondie avec, par exemple, les travaux de Bourgain, Kontorovich, Oh, Fuchs, et al.

Une des propriétés remarquables de ce type d'empilements, qui les rend particulièrement attractifs en théorie des nombres, est que, sous de bonnes conditions, l'ensemble des courbures (les inverses des rayons) des cercles seront entières. Une telle construction peut être généralisée à la dimension 3, tout comme la propriété d'intégralité des courbures, et sera étudiée dans cette thèse.

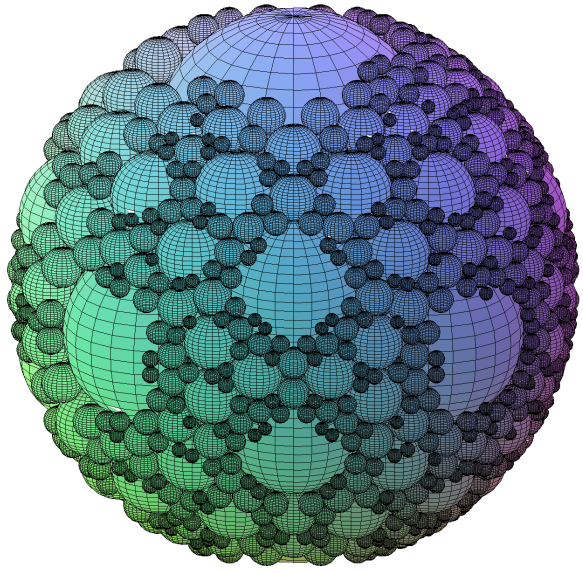

FIGURE 3. Un exemple d'empilement apollonien généralisé de sphères

Plus particulièrement, nous nous attacherons à montrer un principe local-global partiel pour ce type d'empilements, à savoir :

Théorème 1. *Pour tout empilement généralisé de sphères, il existe une classe de congruence modulo* 4 *et un entier* $n \geq 1$ *(tous deux dépendants de l'empilement) tels qu'un entier* m *suffisamment grand avec* $\mathrm{pgcd}(m, n) = 1$ *est courbure d'une sphère de l'empilement si et seulement si* m *est dans cette classe de congruence.*

L'autre aspect des empilements apolloniens abordé dans cette thèse traite du décompte avec multiplicité des courbures dans un empilement généralisé de cercles. Plus précisément, il sera montré les deux résultats suivants :

Théorème 2. *Soit* $N_{\mathcal{P}}(T)$ *le nombre de cercles de courbures plus petites que* T *dans un empilement généralisé de cercles* $\mathcal{P}$*. Alors, il existe des constantes* $c(\mathcal{P}) \neq 0$ *(ne dépendant que de* $\mathcal{P}$*) et* δ *et* s_0 *(indépendantes de* $\mathcal{P}$*) telles que :*

$$N_{\mathcal{P}}(T) = c(\mathcal{P})T^{\delta} + O(T^{\delta - \frac{2s_0}{63}}) .$$

Remarque : $\delta > 1$ et s_0 correspondent respectivement à la dimension de Hausdorff de l'espace résiduel de l'empilement et au trou spectral du groupe d'Apollonius généralisé.

Théorème 3. *Soit $\pi_{\mathcal{P}}(T)$ le nombre de cercles de l'empilement de courbures premières et plus petites que T. Alors,*

$$\pi_{\mathcal{P}}(T) \ll \frac{T^{\delta}}{\log T}\,.$$

La seconde partie de cette thèse traite de la distribution angulaire des idéaux (ou plutôt, dans le cas présent, des nombres idéaux) d'un corps de nombres quadratique imaginaire. Il est aisé de voir que les entiers de Gauss de norme donnée ne sont pas uniformément distribués sur le cercle. Cette absence d'équidistribution peut être quantifiée et Erdős et Hall ont ainsi montré que la discrépance de cette suite est relativement faible.

Nous étendrons ici leur résultat à n'importe quelle extension quadratique imaginaire, en se demandant ce que cela signifie quant à la distribution des points entiers sur les ellipses. Plus précisément, si Φ_n dénote l'ensemble des arguments des nombres idéaux entiers de norme n, on définit la discrépance $\Delta(n)$ de l'ensemble Φ_n comme

$$\Delta(n) = \max\left\{ |\operatorname{card}^*\{\phi \in \Phi_n, \phi \in [\theta_1, \theta_2] \bmod 2\pi\} - \frac{(\theta_2 - \theta_1)}{2\pi} r(n)|, 0 \leq \theta_1 < \theta_2 \leq 2\pi \right\}$$

où l'astérisque dénote que si l'angle est θ_1 ou θ_2, alors il compte pour $\frac{1}{2}$. Alors, nous montrerons que, dans toute extension quadratique imaginaire $\mathbb{K}$, le théorème suivant est vérifié :

Théorème 4. *Soit $\varepsilon > 0$. Alors, pour tous les entiers plus petits que x norme d'un idéal de $\mathcal{O}_{\mathbb{K}}$, avec au plus $o\left(\frac{x}{\sqrt{\log x}}\right)$ exceptions,*

$$\Delta(n) \leq \frac{r(n)}{(\log x)^{\frac{1}{2}\log\left(\frac{\pi}{2}\right)-\varepsilon}}\,.$$

où $r(n)$ est le nombre d'idéaux de $\mathcal{O}_{\mathbb{K}}$ de norme n.

Nous généraliserons par la suite le théorème de Maynard sur les écarts bornés entre les premiers afin de chercher des écarts bornés entre les premiers dans des secteurs dans un corps de nombres quadratique imaginaire. Plus précisément, après avoir défini la notion d'admissibilité d'un k-uplet, nous montrerons, en l'essence, un résultat semblable au théorème suivant :

Théorème 5. *Soient S un secteur d'angle Ψ et $\mathcal{C}$ une classe de nombres idéaux. Soit $m \geq 2$. Alors, il existe une constante $k_0 = k_0(m, \mathbb{K}, \Psi)$ telle que, pour tout k-uplet admissible $\mathcal{H} = (h_1, \ldots, h_k)$ avec $k \geq k_0$, il existe une infinité d'entiers n tels qu'au moins m éléments parmi $n + h_1, \ldots, n + h_k$ soient la norme d'un nombre idéal premier dans la classe $\mathcal{C}$ dont l'argument est dans S.*

De ce résultat nous pourrons par exemple déduire que :

Corollaire 1. *Dans toute extension quadratique imaginaire, pour tout secteur angulaire S de taille Ψ, il existe une constante $c(\mathbb{K}, \Psi)$ et une infinité de couples de nombres premiers π_1, π_2 de $\mathcal{O}_\mathbb{K}$ tels que $\arg(\pi_j) \in S$, $j = 1, 2$ et $|N(\pi_1) - N(\pi_2)| \leq c(\mathbb{K}, \Psi)$.*

CONVENTIONS ET NOTATIONS

On note de façon usuelle les ensembles de nombres $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.

On écrit $f(x) = O(g(x))$, ou $f \ll g$, lorsqu'il existe des constantes N et C telles que $f(x) \leq Cg(x)$ pour tout $x > N$. Le cas échéant, la dépendance de la constante C sera notée sous le symbole O ou $\ll$.

On écrit $f(x) = o\,(g(x))$ lorsque, pour tout $C > 0$, il existe une constante N telle que $f(x) \leq Cg(x)$ pour tout $x > N$.

On écrit $f(x) \sim g(x)$ lorsque $f(x) - g(x) = o\,(g(x))$.

Le cardinal d'un ensemble fini A sera noté $|A|$.

On utilisera la définition usuelle des fonctions arithmétiques $\omega(n)$, $\mu(n)$, $\phi(n)$.

Le plus grand commun diviseur de deux nombres entiers a et b sera noté $\mathrm{pgcd}(a, b)$ ou (a, b).

Toute autre notation nécessaire sera rappelée au fil du texte.

Première partie

Empilements de cercles et de sphères

Chapitre 1

EMPILEMENTS APOLLONIENS

1.1. Empilements apolloniens de cercles

L'histoire des empilements apolloniens remonte à la Grèce antique. Au géomètre et astronome Apollonius de Perge (III^{e} siècle av. J.-C.) est généralement attribué le théorème suivant :

Théorème 1.1.1 (Théorème d'Apollonius)**.** *Étant donnés trois cercles mutuellement tangents, il existe exactement deux cercles tangents à ces trois.*

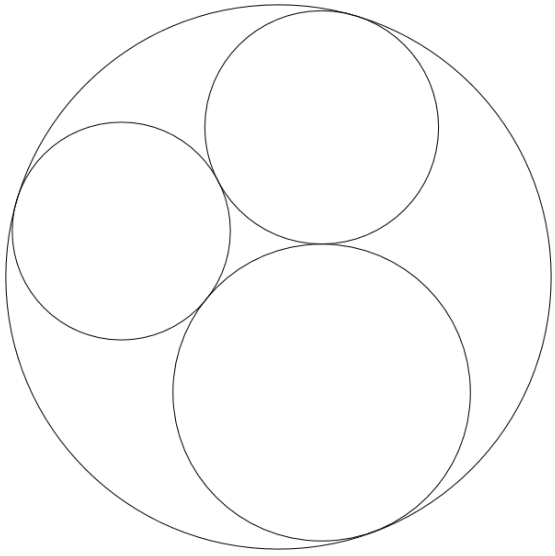

Figure 4. Un exemple de configuration d'Apollonius

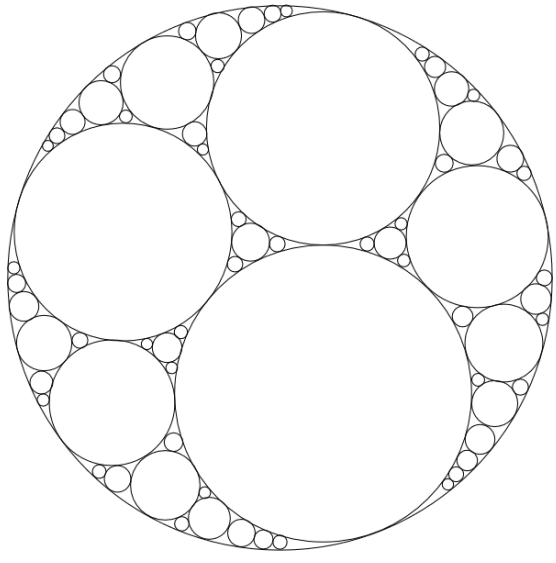

Figure 5. Un exemple d'empilement apollonien de cercles

On appelle configuration d'Apollonius tout ensemble de quatre cercles mutuellement tangents. En se donnant trois cercles mutuellement tangents, il est possible de construire deux nouveaux cercles, tangents à ces trois, donnant naissance à deux configurations

d'Apollonius. Maintenant, en choisissant un nouvel ensemble de trois cercles parmi les cinq déjà construits, il est encore possible de construire deux cercles (dont l'un a en fait déjà été construit précédemment). Une itération de ce procédé permet d'obtenir un objet géométrique appelé empilement apollonien de cercles (ou baderne d'Apollonius).

Cette construction, avant tout géométrique, fait toutefois intervenir certaines remarquables propriétés algébriques. Ainsi, il est légitime de se demander s'il existe une relation entre les rayons des cercles formant une configuration d'Apollonius. Dans l'étude des empilements apolloniens, il est coutume de considérer les inverses des rayons, appelés courbures, plutôt que les rayons eux-mêmes et le théorème suivant, dû à Descartes, exhibe la relation algébrique souhaitée :

Théorème 1.1.2 (Théorème de Descartes)**.** *Soient quatre cercles mutuellement tangents, de courbures a_1, a_2, a_3 et a_4 (l'inverse de leurs rayons). Alors, $Q(a_1, a_2, a_3, a_4) = 0$, où Q est la forme quadratique :*

$$Q(x, y, z, t) = 2(x^2 + y^2 + z^2 + t^2) - (x + y + z + t)^2 .$$

Une remarquable conséquence de ce théorème, amenant à la définition du groupe d'Apollonius comme introduit par Hirst [**Hir67**], est la description suivante de l'ensemble des courbures dans l'empilement :

Proposition 1.1.1. *Si $v = (a_1, a_2, a_3, a_4)$ est un quadruplé de courbures de quatre cercles mutuellement tangents dans l'empilement, alors l'ensemble des courbures apparaissant dans l'empilement est exactement l'ensemble des coordonnées des vecteurs de l'orbite $A \cdot v^t$, où $A = \langle S_1, S_2, S_3, S_4 \rangle$ est appelé groupe d'Apollonius, avec*

$$S_1 = \begin{pmatrix} -1 & 2 & 2 & 2 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad , \quad S_2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 2 & -1 & 2 & 2 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} ,$$

$$S_3 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 2 & 2 & -1 & 2 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad , \quad S_4 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 2 & 2 & 2 & -1 \end{pmatrix} .$$

Cette proposition a plusieurs remarquables conséquences, la plus importante ici étant sans doute que si quatre cercles mutuellement tangents dans un empilement ont des courbures entières, alors tout cercle de l'empilement aura une courbure entière. Un tel empilement sera appelé empilement entier. Ce type d'empilements, et son ensemble infini de courbures entières, s'offre ainsi comme objet d'intérêt en théorie des nombres.

Les questions gravitant autour de telles constructions sont multiples et depuis longtemps présentes en théorie des nombres. Dans [GLM+03], nombre d'entre elles sont formellement posées et partiellement résolues : quelle est la densité des entiers apparaissant comme courbures dans un empilement, combien sont des nombres premiers, peut-on compter les courbures avec multiplicité, etc...

Une des questions d'un intérêt principal dans cette thèse sera de déterminer la densité des entiers apparaissant dans un empilement dit généralisé. Dans le cas des empilements apolloniens de cercles, Sarnak dans [Sar08] fut le premier à offrir une réponse satisfaisante, mais toutefois encore très éloignée de la réalité. Sa méthode sert toutefois de base à la preuve du théorème principal du chapitre 2 et, dans le cas des empilements apolloniens de cercles, a été utilisée par Bourgain et Fuchs [BF11] puis Bourgain et Kontorovich [BK14] afin de prouver le résultat suivant, pour lequel la condition d'admissibilité est détaillée dans Fuchs [Fuc11] et est une condition sur les classes modulo 24 :

Théorème 1.1.3. *Considérons un empilement entier. Alors, presque tout nombre admissible est courbure d'un cercle de l'empilement. Plus précisément, le nombre d'exceptions plus petites que N est au plus $O(N^{1-\eta})$, où η est une constante effectivement calculable.*

Ce résultat est proche du théorème local-global espéré, à savoir que tout nombre admissible suffisamment grand est une courbure de l'empilement. Ce dernier reste toutefois aujourd'hui toujours à l'état de conjecture.

Une autre question naturelle se posant est d'estimer le nombre de cercles de courbures plus petites qu'une borne donnée dans un empilement. Cette quantité est clairement bornée, mais existe-t-il une formule asymptotique ? Une première réponse fut donnée par Boyd qui, dans [Boy82], démontre à l'aide de méthodes élémentaires le résultat suivant :

Théorème 1.1.4. *Soit $N_{\mathcal{P}}(X)$ le nombre de cercles de courbures inférieures ou égales à un entier X. Alors,*

$$\frac{\log N_{\mathcal{P}}(X)}{\log X} \underset{X\to+\infty}{\longrightarrow} \alpha$$

où α est l'exposant de l'empilement, c'est-à-dire

$$\alpha = \sup\left\{e \text{ tel que } \sum_{C\in\mathcal{P}} r(C)^e = \infty\right\} = \inf\left\{e \text{ tel que } \sum_{C\in\mathcal{P}} r(C)^e < \infty\right\},$$

où la somme porte sur l'ensemble des cercles de l'empilement et $r(C)$ est le rayon du cercle C.

Il est à noter que α est également la dimension de Hausdorff de l'espace résiduel de l'empilement, dont la valeur exacte n'est pas connue mais qui est estimée être environ $1,3057$ [McM98].

Le résultat suivant, plus précis, est quant à lui prouvé par Kontorovich et Oh dans [**BK14**] :

Théorème 1.1.5. *Pour un empilement apollonien de cercles $\mathcal{P}$, il existe une constante $c(\mathcal{P})$ telle que, quand $X \to \infty$,*

$$N_{\mathcal{P}}(X) \sim c(\mathcal{P}) X^{\alpha}\,.$$

Plusieurs articles vont par la suite traiter du même résultat, et notamment le travail de Lee et Oh [**LO13**] qui propose une version avec terme d'erreur effectif de ce résultat, que nous généralisons dans le chapitre 3 au cas des empilements apolloniens généralisés de cercles.

Le résultat précédent, et les améliorations subséquentes, sont en fait plus précis que la formulation donnée ci-dessus. Ils permettent en effet un certain contrôle sur les entrées des vecteurs de l'orbite sous l'action du groupe d'Apollonius modulo un entier d. Ainsi, de tels résultats permettent d'appliquer, par exemple, le crible de Selberg pour obtenir une estimation sur le nombre de courbures entières dans un empilement entier (voir par exemple [**BK14**]).

1.2. Empilements d'hypersphères

Le cas des empilements apolloniens de cercles est bidimensionnel. Mais il est également possible de considérer des empilements aux règles de construction semblables en dimension supérieure. Ainsi, on peut étendre la définition de configuration de Descartes à la dimension n, comme étant une configuration de $n+2$ hypersphères mutuellement tangentes.

En 1936, Sir Soddy publie dans Nature [**Sod36**] son poème « The Kiss Precise », décrivant le théorème de Descartes (qui lui est ainsi parfois attribué de manière erronée). Par la suite, il enrichit sa prose d'une verset supplémentaire, abordant le cas des configurations de sphères et décrivant un théorème de Descartes tridimensionnel.

La même année, Gosset fait parvenir à Coxeter, à l'occasion du mariage de ce dernier, une copie de son poème traitant du même problème en dimension quelconque, qui sera publié dans Nature en 1937 [**Gos37**].

Les trois poèmes sus-mentionnés sont disponibles en annexe A.

Théorème 1.2.1 (Théorème de Soddy-Gosset)**.** *Pour une configuration de Descartes en dimension n, dont les courbures sont $a_1, \ldots, a_{n+2}$, on a*

$$\sum_{i=1}^{n+2} a_i^2 = \frac{1}{n}\left(\sum_{i=1}^{n+2} a_i\right)^2 .$$

Comme précédemment, en itérant le procédé qui consiste à inscrire une nouvelle hypersphère dans chaque espace vide, on obtient un empilement apollonien d'hypersphères, dont un exemple est présenté ci-dessous dans le cas de la dimension 3.

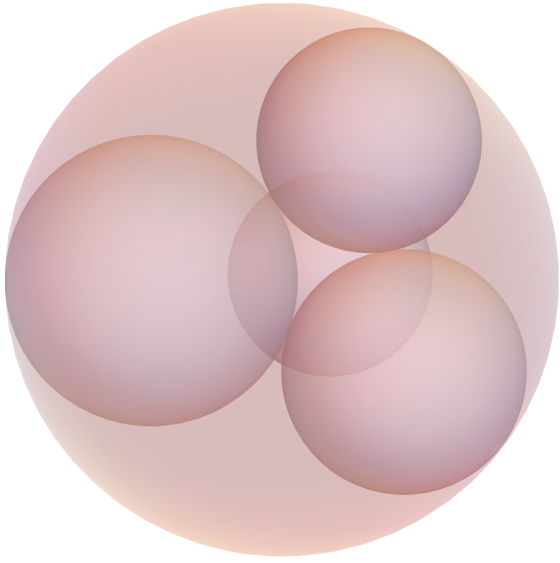

FIGURE 6. Un exemple de configuration de Descartes en dimension 3

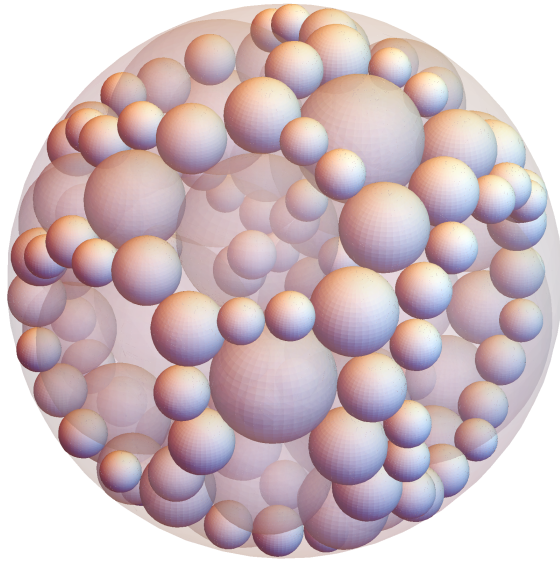

FIGURE 7. Un exemple d'empilement apollonien de sphères

Remarquons que le théorème 1.2.1 implique que si l'on se donne $n+2$ hypersphères de courbures $a_1, \ldots, a_{n+2}$, alors l'unique autre hypersphère tangente aux hypersphères de courbures $a_2, \ldots, a_{n+2}$ a pour courbure

$$a_1^{'} = \frac{2}{n-1} \sum_{i=2}^{n+2} a_i - a_1 \, .$$

Ainsi, en dimension strictement plus grande que 3, le fait que les hypersphères d'origine aient des courbures entières n'implique pas nécessairement que ce soit le cas pour toutes les hypersphères de l'empilement. Ceci rend ce type d'empilements moins intéressant pour la théorie des nombres, c'est pourquoi ces constructions ne seront pas abordées dans la suite de cette thèse.

Le cas de la dimension 3 a quant à lui fait l'objet de plusieurs travaux, dont ceux de Kontorovich [**Kon12**], qui prouve le principe local-global pour les empilements apolloniens de sphères.

1.3. Empilements généralisés

Plutôt que d'explorer les dimensions supérieures, Guettler et Mallows dans [**GM10**] proposent une autre règle d'empilement. Plus de détails seront donnés sur ces empilements dans le chapitre 3.

En partant d'une configuration de trois cercles mutuellement tangents, au lieu d'inscrire un unique cercle dans chaque espace vide, Guettler et Mallows décrivent une procédure pour en inscrire trois mutuellement tangents.

Pour ce type de construction, un analogue au théorème d'Apollonius existe : il y a une unique manière d'inscrire trois cercles mutuellement tangents telle que chaque cercle inscrit soit tangent à exactement deux des cercles d'origine. En itérant le procédé, on obtient ce que Guettler et Mallows appellent un empilement généralisé (ou encore empilement 3-apollonien d'après Xin Zhang [**Zha13**]).

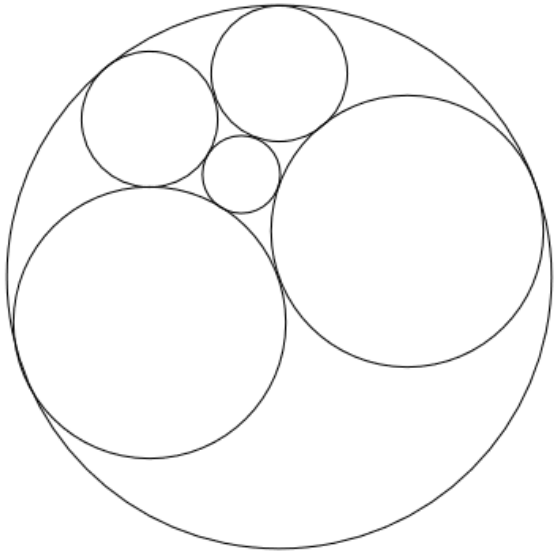

Figure 8. Un exemple de configuration généralisée de cercles

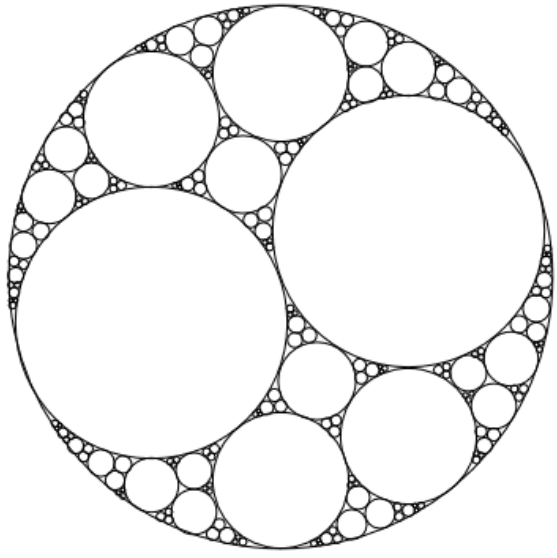

Figure 9. Un exemple d'empilement apollonien généralisé de cercles

Ce type d'empilements présente nombre de similarités avec le cas classique. Ainsi, les méthodes d'étude des empilements apolloniens de cercles peuvent être appliquées ici, menant à de multiples résultats. L'un d'entre eux, concernant le comptage des courbures et des courbures premières avec multiplicité, est l'objet du chapitre 3.

Il est également possible de considérer ce type de constructions en dimension supérieure. Ainsi, le chapitre 2 décrit la construction de tels empilements en dimension 3 et présente la preuve d'un principe local-global partiel similaire à celui prouvé dans [**Kon12**].

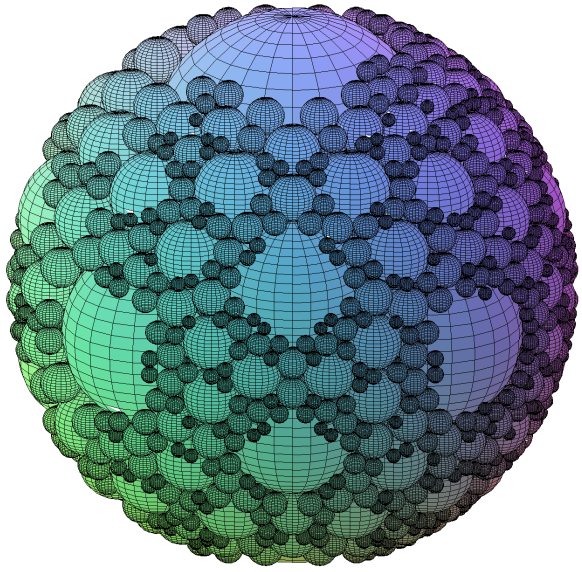

FIGURE 10. Un exemple d'empilement apollonien généralisé de sphères

Il est à noter que, comme dans le cas des empilements classiques, en dimension strictement plus grande que 3, l'intégralité de l'empilement ne peut être garantie par la simple intégralité de la configuration initiale. Ainsi, ce type d'empilements ne sera pas abordé dans la suite de cette thèse.

Les figures de la présente partie ont été réalisées, dans le cas des empilements bidimensionnels et des empilements de sphères classiques, à l'aide des programmes mis à disposition par Alex Kontorovich sur son site internet, et à l'aide d'un programme de l'auteur de cette thèse dans le cas des empilements généralisés de sphères.

Chapitre 2

EMPILEMENTS GÉNÉRALISÉS DE SPHÈRES ET PRINCIPE LOCAL-GLOBAL PARTIEL

2.1. Généralités

Le présente section concerne certaines généralités, dont nous aurons besoin par la suite, sur les empilements apolloniens généralisés de sphères. Elles seront dans un premier temps d'ordre géométrique, puis algébrique, et généralisent en grande partie à la dimension 3 le travail de [GM10].

La construction des empilements apolloniens de cercles vue précédemment se basait sur des applications successives du théorème d'Apollonius (théorème 1.1.1). Le théorème suivant se présente comme un analogue nous permettant, une fois encore par des applications successives, de construire un empilement apollonien généralisé de sphères.

Théorème 2.1.1. *Quatre sphères mutuellement tangentes forment deux espaces vides. Dans chacun de ces espaces, on peut inscrire, de manière unique, quatre sphères mutuellement tangentes de telle sorte qu'à chacune de ces sphères il y ait exactement une des sphères d'origine qui ne soit pas tangente (et la sphère non tangente est différente pour chacune des quatre sphères inscrites).*

L'exemple 1 peut être considéré comme un exemple « canonique ». De par sa simplicité, il rend certaines des propriétés de cette section aisées à prouver. Ainsi, plusieurs preuves à venir consisteront à se rapporter à ce cas particulier.

> **Exemple 1 :** Considérons les deux sphères de rayon infini (donc les plans) $z = 1$ et $z = -1$ ainsi que les deux sphères de rayon 1 et de centres $(-1, -1, 0)$ et $(-1, 1, 0)$. Nous avons ainsi quatre sphères mutuellement tangentes qui définissent deux espaces vides (dans les régions $x \geq -1$ et $x \leq -1$ entre les deux plans) dans chacun desquels il est possible d'inscrire quatre nouvelles sphères en suivant la procédure du théorème 2.1.1.

Dans l'un de ces espaces vides, les deux sphères de rayon 1 et centres $(1, 1, 0)$ et $(1, -1, 0)$, et les deux sphères de rayon $\frac{1}{2}$ et centres $(0, 0, \frac{1}{2})$ et $(0, 0, -\frac{1}{2})$ peuvent être inscrites.

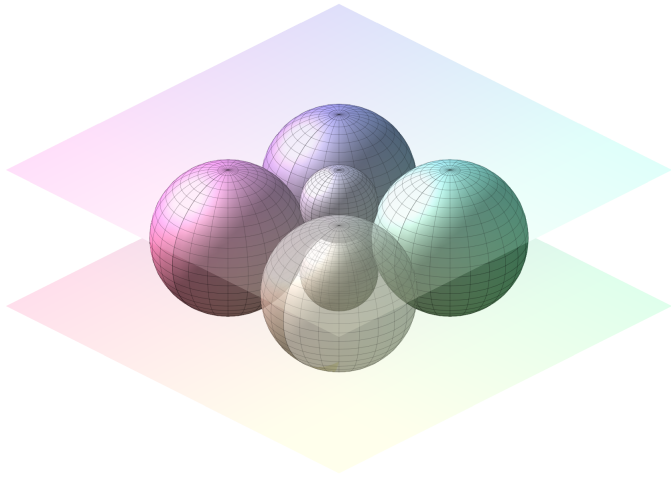

FIGURE 11. Un exemple de configuration de sphères

Exemple 2 : Cet exemple présente une autre configuration de sphères, moins simple que la première. Une sphère extérieure de rayon 1 englobe deux sphères de rayon $\frac{1}{2}$, deux de rayon $\frac{1}{3}$, deux de rayon $\frac{1}{4}$ et une de rayon $\frac{1}{7}$.

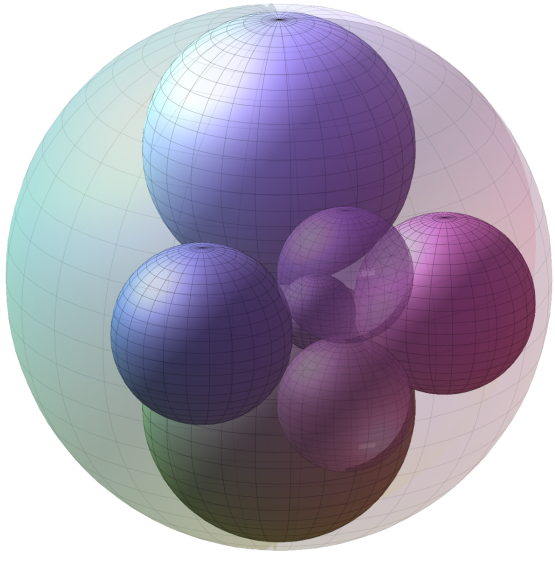

FIGURE 12. Un autre exemple de configuration de sphères

Preuve du théorème 2.1.1. À l'aide d'une transformation de Möbius, d'une rotation, d'une translation et d'une homothétie, n'importe quelle configuration de quatre sphères mutuellement tangentes peut être transformée en la configuration de l'exemple 1 (voir par exemple le théorème 3 de [**Wil81**]). La preuve pour cette configuration ne nécessite alors que de la géométrie élémentaire. □

Ainsi, dans chacun des deux espaces vides formés par quatre sphères mutuellement tangentes, il est possible d'inscrire quatre nouvelles sphères. Les quatre sphères d'origine et les quatre nouvelles forment alors un octuplet de sphères. Dans un tel octuplet, les sphères peuvent être groupées en quatre paires, en associant chaque sphère avec l'unique sphère de l'octuplet qui ne lui est pas tangente. Les sphères de chaque paire ne sont pas tangentes entre elles, mais sont tangentes aux six autres sphères.

Prenons maintenant quatre sphères mutuellement tangentes parmi celles formant un octuplet. Comme précédemment, elles forment deux espaces vides, dans chacun desquels il est possible, d'après le théorème 2.1.1, d'inscrire quatre nouvelles sphères. En répétant l'opération, on construit ce que l'on appellera dans la suite de cette thèse un empilement apollonien généralisé de sphères (ou empilement apollonien orthoplicial de sphères dans [**Nak14**]).

Exemple 3 : L'exemple suivant montre les 3000 premières sphères de l'empilement construit à partir de la configuration de l'exemple 2.

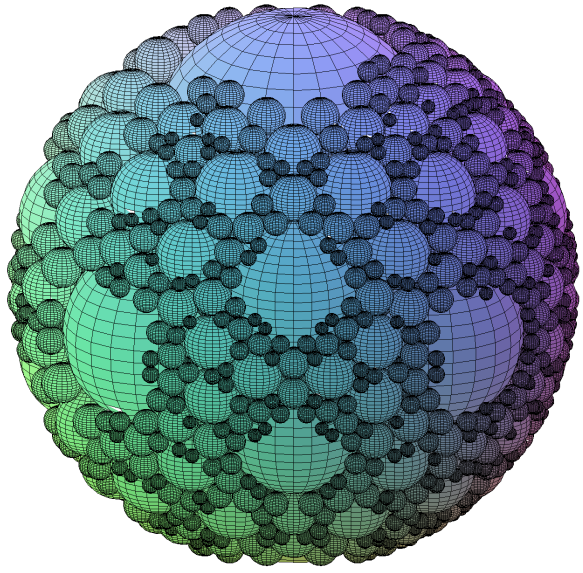

Figure 13. Un exemple d'empilement apollonien généralisé de sphères

Définition 2.1.1. *Pour une sphère $\mathcal{S}$ de courbure $b \neq 0$ et de centre (x, y, z) on définit ses coordonnées abbc (« augmented bend, bend*center »), notées $\boldsymbol{a}(\mathcal{S})$, comme*

$$\boldsymbol{a}(\mathcal{S}) = (\overline{b}, b, bx, by, bz) \;\; \text{où} \;\; \overline{b} = b(x^2 + y^2 + z^2) - \frac{1}{b}\,.$$

Pour un plan (donc une sphère de courbure 0) d'équation $p_1x + p_2y + p_3z = h$, avec (p_1, p_2, p_3) un vecteur unitaire, les coordonnées abbc sont $(2h, 0, p_1, p_2, p_3)$.

Remarque 1 : Une sphère est totalement décrite par ses coordonnées *abbc* et à chaque ensemble de coordonnées *abbc* correspond une unique sphère.

Remarque 2 : $\overline{b}$ correspond à la courbure de la sphère image de $\mathcal{S}$ par l'opération d'inversion par rapport à la sphère unité. On rappelle que deux points P et P' sont dits inverses par rapport à la sphère de centre C et de rayon r si $P' \in [CP)$ et $CP.CP' = r^2$.

2.1.1. Octuplets de sphères

Dans ce qui suit, un octuplet dénotera toujours une configuration de huit sphères obtenue par la procédure du théorème 2.1.1. Comme expliqué précédemment, un octuplet peut être vu comme un ensemble de quatre paires de sphères, chaque paire consistant en une sphère et l'unique sphère de l'octuplet qui ne lui est pas tangente. Les sphères d'une paire seront généralement dénotées $\mathcal{S}$ et $\mathcal{S}'$.

Remarque 3 : Dans le cas où la configuration consiste en une sphère incluant les sept autres, la courbure de la sphère extérieure sera définie comme négative. Dans un octuplet (et dans un empilement), seule une sphère peut avoir une courbure négative.

Soit

$$\mathbf{W} = \begin{pmatrix} 0 & -\frac{1}{2} & 0 & 0 & 0 \\ -\frac{1}{2} & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Lemme 2.1.1. *Soient $\mathcal{S}_1$ et $\mathcal{S}_2$ deux sphères. Alors*

$$\boldsymbol{a}(\mathcal{S}_1)\,\boldsymbol{W}\boldsymbol{a}(\mathcal{S}_2)^t = \begin{cases} 1 \text{ si } \mathcal{S}_1 = \mathcal{S}_2\,, \\ -1 \text{ si } \mathcal{S}_1 \text{ et } \mathcal{S}_2 \text{ sont extérieurement tangentes}\,. \end{cases}$$

Démonstration. Considérons deux sphères dont les coordonnées *abbc* sont données par $\mathbf{a}(\mathcal{S}_1) = (\overline{b}_1, b_1, b_1x_1, b_1y_1, b_1z_1)$ et $\mathbf{a}(\mathcal{S}_2) = (\overline{b}_2, b_2, b_2x_2, b_2y_2, b_2z_2)$. Alors,

$$\mathbf{a}(\mathcal{S}_1)\mathbf{W}\mathbf{a}(\mathcal{S}_2)^t = -\frac{b_1b_2}{2}\left((x_1 - x_2)^2 + (y_1 - y_2)^2 + (z_1 - z_2)^2\right) + \frac{b_1}{2b_2} + \frac{b_2}{2b_1}\,.$$

Ceci suffit à conclure au résultat. □

Lemme 2.1.2. *Soient $\mathcal{S}$ et $\mathcal{S}'$ deux sphères non tangentes dans un octuplet. Alors,*

$$\boldsymbol{a}(\mathcal{S})\,\boldsymbol{W}\boldsymbol{a}(\mathcal{S}')^t = -3\,.$$

DÉMONSTRATION. La preuve peut être facilement faite dans le cas de l'octuplet introduit dans l'exemple 1. Tout octuplet étant image par une transformation de Möbius de cette configuration (voir par exemple le théorème 3 de [**Wil81**]), il reste seulement à étudier l'effet des rotations, translations, homothéties et inversions de sphère d'inversion la sphère unité sur les coordonnées *abbc* d'une sphère $\mathcal{S}$.

- Une homothétie de rapport λ consiste à remplacer $\mathbf{a}(\mathcal{S})$ par $\mathbf{a}(\mathcal{S})\mathbf{m}$, où

$$\mathbf{m} = \begin{pmatrix} \lambda & 0 & 0 & 0 & 0 \\ 0 & \frac{1}{\lambda} & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}\,.$$

- Une rotation consiste à remplacer $\mathbf{a}(\mathcal{S})$ par $\mathbf{a}(\mathcal{S})\mathbf{m}$, où

$$\mathbf{m} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & \cos\theta & -\sin\theta \\ 0 & 0 & 0 & \sin\theta & \cos\theta \end{pmatrix} \text{ ou } \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & \cos\theta & 0 & -\sin\theta \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & \sin\theta & 0 & \cos\theta \end{pmatrix} \text{ ou } \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & \cos\theta & -\sin\theta & 0 \\ 0 & 0 & \sin\theta & \cos\theta & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}\,.$$

- Une translation de vecteur (u, v, w) consiste à remplacer $\mathbf{a}(\mathcal{S})$ par $\mathbf{a}(\mathcal{S})\mathbf{m}$, où

$$\mathbf{m} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ u^2+v^2+w^2 & 1 & u & v & w \\ 2u & 0 & 1 & 0 & 0 \\ 2v & 0 & 0 & 1 & 0 \\ 2w & 0 & 0 & 0 & 1 \end{pmatrix}\,.$$

- L'inversion de sphère d'inversion la sphère unité consiste à remplacer $\mathbf{a}(\mathcal{S})$ par $\mathbf{a}(\mathcal{S})\mathbf{m}$, où

$$\mathbf{m} = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}\,.$$

Il est aisé de vérifier que, pour chacune des matrices précédentes, $\mathbf{m}\mathbf{W}\mathbf{m}^t = \mathbf{W}$. □

Lemme 2.1.3. *Dans un octuplet contenant les couples de sphères $\mathcal{S}_1$ et $\mathcal{S}'_1$, $\mathcal{S}_2$ et $\mathcal{S}'_2$, $\mathcal{S}_3$ et $\mathcal{S}'_3$, $\mathcal{S}_4$ et $\mathcal{S}'_4$, nous avons*

$$\boldsymbol{a}(\mathcal{S}_1) + \boldsymbol{a}(\mathcal{S}'_1) = \boldsymbol{a}(\mathcal{S}_2) + \boldsymbol{a}(\mathcal{S}'_2) = \boldsymbol{a}(\mathcal{S}_3) + \boldsymbol{a}(\mathcal{S}'_3) = \boldsymbol{a}(\mathcal{S}_4) + \boldsymbol{a}(\mathcal{S}'_4)\,.$$

DÉMONSTRATION. Pour $1 \leq j \leq 4$, soit

$$\mathbf{w}_j = \frac{\mathbf{a}(\mathcal{S}_j) + \mathbf{a}(\mathcal{S}'_j)}{2}\,.$$

Des lemmes 2.1.1 et 2.1.2, on obtient $\mathbf{w}_i \mathbf{W} \mathbf{w}_j^t = -1$ pour tout $1 \leq i, j \leq 4$. Ainsi, si $\mathbf{F}_j$ désigne la matrice 5×5 ayant pour lignes $\mathbf{a}(\mathcal{S}_1), \mathbf{a}(\mathcal{S}_2), \mathbf{a}(\mathcal{S}_3), \mathbf{a}(\mathcal{S}_4)$ et $\mathbf{w}_j$, alors,

$$\mathbf{F}_i \mathbf{W} \mathbf{F}_j^t = \mathbf{K} = \mathbf{F}_j \mathbf{W} \mathbf{F}_j^t \tag{2.1.1}$$

avec

$$\mathbf{K} = \begin{pmatrix} 1 & -1 & -1 & -1 & -1 \\ -1 & 1 & -1 & -1 & -1 \\ -1 & -1 & 1 & -1 & -1 \\ -1 & -1 & -1 & 1 & -1 \\ -1 & -1 & -1 & -1 & -1 \end{pmatrix}\,.$$

Comme $\mathbf{K}$ est inversible, on a de l'équation (2.1.1) que $\mathbf{F}_i$ et $\mathbf{F}_j$ sont inversibles. Ainsi, on en déduit que $\mathbf{F}_i = \mathbf{F}_j$ et donc $\mathbf{w}_i = \mathbf{w}_j$, pour tout $1 \leq i, j \leq 4$. □

À l'aide de ce résultat, on peut donc définir une façon commode de représenter un octuplet, comme expliqué ci-dessous.

Définition 2.1.2. *Pour un octuplet de sphères $\mathcal{S}_1$ et $\mathcal{S}'_1$, $\mathcal{S}_2$ et $\mathcal{S}'_2$, $\mathcal{S}_3$ et $\mathcal{S}'_3$, $\mathcal{S}_4$ et $\mathcal{S}'_4$, on définit une matrice $\boldsymbol{F}$ associée à l'octuplet comme une matrice dont les quatre premières lignes sont les coordonnées abbc de quatre des sphères (une de chaque paire) et la cinquième ligne est la moyenne des coordonnées abbc des sphères de chaque paire.*

Remarque 4 : Il n'existe pas une unique matrice associée à un octuplet. Étant donné qu'il est possible de choisir les paires dans différents ordres et qu'il existe deux choix d'un représentant pour chaque paire, il y a (au plus) 384 matrices $\mathbf{F}$ différentes associées au même octuplet.

Théorème 2.1.2. *Soient $\mathcal{S}_1$, $\mathcal{S}_2$, $\mathcal{S}_3$ et $\mathcal{S}_4$ quatre sphères mutuellement tangentes, de courbures respectives b_1, b_2, b_3, b_4, formant deux espaces vides. Alors, les courbures des deux ensembles de quatre sphères qui peuvent être inscrits dans chaque espace vide sont données par $(2\omega - b_1, 2\omega - b_2, 2\omega - b_3, 2\omega - b_4)$ et $(2\omega' - b_1, 2\omega' - b_2, 2\omega' - b_3, 2\omega' - b_4)$, où ω et ω' sont les racines de*

$$2\omega^2 - 2\omega(b_1 + b_2 + b_3 + b_4) + b_1^2 + b_2^2 + b_3^2 + b_4^2 = 0\,. \tag{2.1.2}$$

DÉMONSTRATION. D'après l'équation (2.1.1), $\mathbf{FWF}^t = \mathbf{K}$ et donc $\mathbf{F}^t\mathbf{K}^{-1}\mathbf{F} = \mathbf{W}^{-1}$. L'élément en position $(2,2)$ dans cette équation nous donne l'équation (2.1.2). □

Remarque 5 : De manière analogue, un résultat semblable est vérifié pour l'ensemble des courbures $*$ centres.

2.1.2. Empilements généralisés de sphères

Étant données quatre sphères mutuellement tangentes, formant deux espaces vides, il existe une unique manière d'inscrire quatre sphères mutuellement tangentes dans chacun de ces espaces vides en suivant la procédure du théorème 2.1.1. Les quatre sphères d'origine appartiennent à exactement deux octuplets distincts et l'équation (2.1.2) du théorème 2.1.2 nous permet de passer d'un octuplet à l'autre, puisqu'elle implique :

$$\omega + \omega' = b_1 + b_2 + b_3 + b_4 \,.$$

Plus précisément, du résultat analogue au théorème 2.1.2 pour l'ensemble des éléments courbures$*$centres, on obtient que, si $\mathbf{F}$ est la matrice associée à l'un de ces octuplets, avec comme quatre premières lignes les coordonnées *abbc* des quatre sphères d'origine, alors l'autre octuplet peut être décrit par la matrice $\mathbf{A}_5\mathbf{F}$, où

$$\mathbf{A}_5 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & -1 \end{pmatrix} .$$

Tout octuplet peut être décrit à l'aide d'une matrice $\mathbf{F}$, qui donne explicitement les coordonnées *abbc* de quatre des sphères de l'octuplet. À l'aide de la dernière ligne de $\mathbf{F}$ (qui correspond à la moyenne commune des coordonnées *abbc* des paires de l'octuplet), les coordonnées *abbc* des quatre autres sphères de l'octuplet peuvent être calculées. Ainsi, on a par exemple :

$$\begin{pmatrix} \mathbf{a}(\mathcal{S}_1') \\ \mathbf{a}(\mathcal{S}_2) \\ \mathbf{a}(\mathcal{S}_3) \\ \mathbf{a}(\mathcal{S}_4) \\ \mathbf{w} \end{pmatrix} = \begin{pmatrix} 2\mathbf{w} - \mathbf{a}(\mathcal{S}_1) \\ \mathbf{a}(\mathcal{S}_2) \\ \mathbf{a}(\mathcal{S}_3) \\ \mathbf{a}(\mathcal{S}_4) \\ \mathbf{w} \end{pmatrix} = \begin{pmatrix} -1 & 0 & 0 & 0 & 2 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} \mathbf{a}(\mathcal{S}_1) \\ \mathbf{a}(\mathcal{S}_2) \\ \mathbf{a}(\mathcal{S}_3) \\ \mathbf{a}(\mathcal{S}_4) \\ \mathbf{w} \end{pmatrix} .$$

Par conséquent, il nous suffit de regarder les produits $\mathbf{A}_i\mathbf{F}$, $1 \leq i \leq 4$, où

$$\mathbf{A}_1 = \begin{pmatrix} -1 & 0 & 0 & 0 & 2 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}, \quad \mathbf{A}_2 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 2 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix},$$

$$\mathbf{A}_3 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 2 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}, \quad \mathbf{A}_4 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -1 & 2 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

En répétant le processus, on obtient un empilement apollonien généralisé de sphères. L'ensemble des coordonnées *abbc* des sphères dans l'empilement est alors exactement l'ensemble des quatre premières lignes des matrices de l'orbite $\mathcal{A} \cdot \mathbf{F}$, où $\mathcal{A}$ est le groupe

$$\mathcal{A} = \langle \mathbf{A}_1, \mathbf{A}_2, \mathbf{A}_3, \mathbf{A}_4, \mathbf{A}_5 \rangle .$$

Remarque 6 : L'empilement peut être construit à partir de n'importe quel octuplet qu'il contient. Ainsi, il sera possible de choisir un octuplet particulier qui « représente » l'empilement, comme expliqué plus tard dans la définition 2.1.3.

Lemme 2.1.4. *S'il existe un octuplet de sphères d'un empilement apollonien généralisé de sphères dont toutes les courbures sont entières (ou, de manière équivalente, dont la seconde colonne de la matrice $\boldsymbol{F}$ associée a des entrées entières), alors toutes les sphères de l'empilement auront des courbures entières. Un tel empilement sera appelé un empilement apollonien généralisé entier de sphères.*

S'il existe un octuplet de sphères d'un empilement apollonien généralisé entier de sphères dont les courbures sont copremières (ou, de manière équivalente, dont la seconde colonne de la matrice $\boldsymbol{F}$ associée a des entrées copremières), alors il en sera de même pour tout octuplet de l'empilement. Un tel empilement sera appelé un empilement apollonien généralisé primitif de sphères.

Démonstration. Soient $(b_1, b_2, b_3, b_4, b'_1, b'_2, b'_3, b'_4)$ les courbures d'un octuplet entier dans l'empilement et ω la moyenne des courbures de chaque paire. Alors, $2\omega \in \mathbb{Z}$. D'après l'équation (2.1.2), nous avons également $2\omega^2 \in \mathbb{Z}$ et donc $\omega \in \mathbb{Z}$. Réciproquement, si $\omega \in \mathbb{Z}$ et b_1, b_2, b_3, b_4 sont entiers, il en est de même pour les courbures des huit sphères de l'octuplet. Ainsi, l'intégralité d'un octuplet est équivalente à celle de la seconde colonne de la matrice associée à cet octuplet.

Le groupe $\mathcal{A}$ est engendré par des matrices à coefficients entiers. Ainsi, si la seconde colonne d'une matrice $\mathbf{F}$ associée à un octuplet de l'empilement a des coordonnées entières, il en sera de même pour la seconde colonne de n'importe quelle matrice associée à n'importe quel octuplet de l'empilement, étant donné que de telles matrices forment l'orbite $\mathcal{A} \cdot \mathbf{F}$.

Supposons que l'octuplet $(b_1, b_2, b_3, b_4, b'_1, b'_2, b'_3, b'_4)$ est tel que

$$\text{pgcd}(b_1, b_2, b_3, b_4, b'_1, b'_2, b'_3, b'_4) = 1\,.$$

Alors, on en déduit que

$$\text{pgcd}(b_1, b_2, b_3, b_4, b'_1, b'_2, b'_3, b'_4) = \text{pgcd}(b_1, b_2, b_3, b_4, 2\omega) = 1\,.$$

Ainsi, on a $\text{pgcd}(b_1, b_2, b_3, b_4, \omega) = 1$. Réciproquement,

$$\text{pgcd}(b_1, b_2, b_3, b_4, \omega) = 1 \Longrightarrow \text{pgcd}(b_1, b_2, b_3, b_4, 2\omega) = 1 \text{ ou } 2\,.$$

Mais ce pgcd ne peut valoir 2. En effet, d'après l'équation (2.1.2), on aurait $2|\omega$ et donc $\text{pgcd}(b_1, b_2, b_3, b_4, \omega) = 2$. Ainsi,

$$\text{pgcd}(b_1, b_2, b_3, b_4, b'_1, b'_2, b'_3, b'_4) = \text{pgcd}(b_1, b_2, b_3, b_4, 2\omega) = 1\,.$$

Il est également aisé de voir que la multiplication par une matrice de $\mathcal{A}$ ne change pas le pgcd de $(b_1, b_2, b_3, b_4, \omega)$. □

Lemme 2.1.5. *Soient b_1, b_2, b_3, b_4 les courbures de quatre sphères mutuellement tangentes dans un empilement primitif. Alors, parmi b_1, b_2, b_3, b_4, il y a deux nombres pairs et deux nombres impairs. De plus, les deux nombres impairs sont dans la même classe de congruence modulo 4.*

Démonstration. Tout d'abord, considérons l'équation (2.1.2) mod 2. Nous obtenons

$$b_1 + b_2 + b_3 + b_4 = 0 \bmod 2\,.$$

Il y a donc trois possibilités pour les parités de b_1, b_2, b_3, b_4 :

- b_1, b_2, b_3, b_4 sont tous pairs,
- b_1, b_2, b_3, b_4 sont tous impairs,
- il y a deux éléments pairs et deux éléments impairs parmi b_1, b_2, b_3, b_4.

Par primitivité, b_1, b_2, b_3, b_4 ne peuvent pas être tous pairs, sinon $\text{pgcd}(b_1, b_2, b_3, b_4, 2\omega) = 2$, ce qui est impossible.

Supposons que b_1, b_2, b_3, b_4 soient tous impairs. Alors, l'équation (2.1.2) mod 4 donne $2\omega^2 \equiv 0 \bmod 4$ et donc ω est pair. La même équation donne $b_1^2 + b_2^2 + b_3^2 + b_4^2 \equiv 0 \bmod 8$ mais, comme b_1, b_2, b_3, b_4 sont tous impairs, $b_1^2 + b_2^2 + b_3^2 + b_4^2 \equiv 4 \bmod 8$.

Ainsi, il y a deux éléments pairs et deux éléments impairs parmi b_1, b_2, b_3, b_4. En réduisant mod 4 l'équation (2.1.2), on déduit que ω est impair. Supposons, sans perte de généralité, que b_1 et b_2 soient les deux éléments impairs et qu'il ne soient pas dans la même classe modulo 4. L'équation (2.1.2) mod8 donne

$$-2\omega(b_3 + b_4) + (b_3 + b_4)^2 \equiv 4 \bmod 8 \Rightarrow (b_3 + b_4)(b_3 + b_4 - 2\omega) \equiv 4 \bmod 8\,.$$

Mais, comme ω est impair, $b_3 + b_4 - 2\omega \equiv b_3 + b_4 - 2 \bmod 4$. Ainsi, il est impossible que $(b_3 + b_4)(b_3 + b_4 - 2\omega)$ soit 4 mod 8. □

Lemme 2.1.6. *Dans tout empilement primitif, les courbures impaires sont dans la même classe de congruence modulo* 4.

Démonstration. D'après le lemme précédent, les deux courbures impaires de l'octuplet de départ sont égales modulo 4. Comme ω est impair, il est aisé de voir qu'aucune des matrices de $\mathcal{A}$ ne change la classe modulo 4 d'un entier impair. □

De manière analogue au cas des empilements apolloniens de cercles ou de sphères classiques, il est possible de définir la notion d'octuplet racine comme étant l'octuplet « minimal » de l'empilement, dans le sens où il décrit l'octuplet avec le plus petit ω (contenant les quatre plus grandes sphères).

Définition 2.1.3. *Un octuplet d'un empilement primitif dont la seconde colonne de la matrice* $\boldsymbol{F}$ *associée est* $(a, b, c, d, \omega)^t$ *est appelé octuplet racine si*

$$a \leq 0 \leq b \leq c \leq d \leq \omega \text{ et } \omega \leq \frac{a + b + c + d}{2}\,.$$

Remarque 7 : De manière analogue au cas classique, l'octuplet racine est unique et il existe un algorithme de réduction qui permet, à partir de n'importe quel octuplet de l'empilement, de calculer l'octuplet racine. Toutefois, il peut exister dans l'empilement plusieurs configurations ayant comme octuplet cet octuplet racine.

Entrée: Un octuplet $(a, b, c, d, \omega)^t$ d'un empilement.
Sortie: L'octuplet racine de l'empilement correspondant.
1 En multipliant par les matrices $\mathbf{A}_1, \ldots, \mathbf{A}_4$, obtenir un vecteur avec $a, b, c, d \leq \omega$.
2 Si $\omega \leq \frac{a+b+c+d}{2}$, ordonner a, b, c, d et terminer. Sinon, multiplier par $\mathbf{A}_5$ et retourner en 1.

Cet algorithme se termine toujours dans le cas d'un octuplet entier, car chaque étape diminue strictement la valeur de ω, qui doit être positive.

La condition $a \leq 0$ dans la définition d'un octuplet racine n'apparait pas dans l'algorithme puisqu'elle est automatiquement vérifiée si $\omega \leq \frac{a+b+c+d}{2}$, car alors :

$$0 = 2\omega^2 - 2\omega(a+b+c+d) + a^2 + b^2 + c^2 + d^2 \leq -\omega(a+b+c+d) + a^2 + b^2 + c^2 + d^2 \,.$$

2.2. Un principe local-global partiel

Dans cette section, nous allons utiliser une méthode semblable à celle utilisée dans [Sar08] pour prouver un principe local-global partiel pour les empilements apolloniens généralisés primitifs de sphères. Comme seules les courbures sont concernées par notre étude, nous n'avons pas besoin de considérer les matrices $\mathbf{F}$ dans leur intégralité. Nous allons seulement nous intéresser à la seconde colonne de telles matrices, pour laquelle les quatre premières entrées sont les courbures de quatre sphères (une par paire) d'un octuplet et la cinquième coordonnée est la moyenne des courbures de chaque paire.

Dans ce qui suit, $\mathcal{P}$ dénotera toujours un empilement apollonien généralisé primitif de sphères. Soit $v^t_{\mathcal{P}} = (a_0, b_0, c_0, d_0, \omega_0)^t$ l'octuplet racine de $\mathcal{P}$. D'après le lemme 2.1.5, deux éléments parmi a_0, b_0, c_0, d_0 sont pairs et deux sont impairs. Quitte à permuter a_0, b_0, c_0 et d_0, on peut supposer que a_0 est pair et b_0 est impair. Si $a_0 = 0$, on peut remplacer a_0 par $2\omega - a_0$ pour le rendre non nul. Remarquons que $a_0 + b_0$ sera impair et positif, car, si $a_0 < 0$, alors $b_0 > |a_0|$ (car, dans ce cas, la sphère de courbure a_0 est extérieure et contient la sphère de courbure b_0. Ainsi, $0 < |a_0| < b_0$). Ce vecteur sera toujours dénoté $v^t_{\mathcal{P}}$. Remarquons qu'un tel $v^t_{\mathcal{P}}$ n'est plus nécessairement un octuplet racine.

Théorème 2.2.1. *Soit $v^t_{\mathcal{P}} = (a_0, b_0, c_0, d_0, \omega_0)^t$ comme ci-dessus. Alors, l'ensemble des courbures des sphères de $\mathcal{P}$ contient l'ensemble des entiers impairs de la forme*

$$f_{a_0}(\alpha_1, \alpha_2, \beta_1, \beta_2) - a_0 \quad \textit{avec} \quad \operatorname{pgcd}_{\mathbb{Z}[i]}(\alpha_1 + i\alpha_2, \beta_1 + i\beta_2) = 1$$

où f_{a_0} est la forme quadratique quaternaire entière définie positive suivante :

$$f_{a_0}(x, y, z, t) = A_0x^2 + A_0y^2 + 4D_0z^2 + 4D_0t^2 + 4xtB_0 - 4yzB_0 + 4xzC_0 + 4ytC_0$$

avec

$$A_0 = a_0 + b_0, \quad B_0 = -\frac{a_0 + b_0 + c_0 + d_0 - 2\omega_0}{2},$$
$$C_0 = -\frac{a_0 + b_0 + c_0 - d_0}{2}, \quad D_0 = a_0 + c_0 \,.$$

Remarque 8 :

$$\mathrm{disc}(f_{a_0}) = 16\left(A_0D_0 - (B_0^2 + C_0^2)\right)^2 = 16a_0^4$$

et il est aisé de vérifier que f_{a_0} est définie positive (car A_0 et tous les mineurs principaux sont positifs).

DÉMONSTRATION. Comme expliqué dans ce qui précède, l'ensemble des courbures des sphères de l'empilement est exactement l'ensemble des quatre premières coordonnées des vecteurs dans l'orbite $\mathcal{A} \cdot v_{\mathcal{P}}^t$.

Nous allons étudier l'orbite, plus petite, $\mathcal{A}_1 \cdot v_{\mathcal{P}}^t$, où

$$\mathcal{A}_1 = \langle \mathbf{A}_2, \mathbf{A}_3, \mathbf{A}_4, \mathbf{A}_5 \rangle .$$

Ce sous-groupe de $\mathcal{A}$ laisse la première coordonnée de chaque vecteur invariante. D'après le théorème 2.1.2, pour tout vecteur (a_0, b, c, d, ω) dans cette orbite,

$$2\omega^2 - 2\omega(a_0 + b + c + d) + a_0^2 + b^2 + c^2 + d^2 = 0 .$$

Le changement de variables $(x_2, x_3, x_4, x_5) = (b + a_0, c + a_0, d + a_0, \omega + a_0)$ nous permet de réécrire l'équation sous la forme

$$Q(x_2, x_3, x_4, x_5) = 2x_5^2 - 2x_5(x_2 + x_3 + x_4) + x_2^2 + x_3^2 + x_4^2 = -2a_0^2 . \tag{2.2.1}$$

En terme d'orbite, cela revient à considérer l'action sous $\mathcal{A}_1' = U^{-1}\mathcal{A}_1 U$, où

$$U = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 & 0 \\ -1 & 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 1 & 0 \\ -1 & 0 & 0 & 0 & 1 \end{pmatrix} .$$

$\mathcal{A}_1'$ est isomorphe à $\Gamma = \langle \mathbf{M}_2, \mathbf{M}_3, \mathbf{M}_4, \mathbf{M}_5 \rangle$, où

$$\mathbf{M}_2 = \begin{pmatrix} -1 & 0 & 0 & 2 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} , \quad \mathbf{M}_3 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 2 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} ,$$

$$\mathbf{M}_4 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 2 \\ 0 & 0 & 0 & 1 \end{pmatrix} , \quad \mathbf{M}_5 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & -1 \end{pmatrix} .$$

Alors, l'étude de l'action de $\mathcal{A}_1$ sur $v_{\mathcal{P}}^t$ peut être ramenée à celle de l'action de Γ sur $u_0^t = (x_2^0, x_3^0, x_4^0, x_5^0)^t = (b_0 + a_0, c_0 + a_0, d_0 + a_0, \omega_0 + a_0)^t$. De plus $\Gamma \leq O_Q(\mathbb{Z})$.

Soit $(x_2, x_3, x_4, x_5) = (A, D, A + 2C + D, A + B + C + D)$. À l'aide de ce changement de variables, l'équation peut être réécrite comme

$$\Delta(A, B, C, D) = B^2 + C^2 - AD = -a_0^2 \,.$$

En terme d'orbite, cela revient à considérer l'action sous $G = V^{-1}\Gamma V$, où

$$V = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 2 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix} .$$

Alors, $G = \langle \mathbf{g}_2, \mathbf{g}_3, \mathbf{g}_4, \mathbf{g}_5 \rangle$ avec

$$\mathbf{g}_2 = \begin{pmatrix} 1 & 2 & 2 & 2 \\ 0 & 0 & -1 & -1 \\ 0 & -1 & 0 & -1 \\ 0 & 0 & 0 & 1 \end{pmatrix} , \quad \mathbf{g}_3 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ -1 & 0 & -1 & 0 \\ -1 & -1 & 0 & 0 \\ 2 & 2 & 2 & 1 \end{pmatrix} ,$$

$$\mathbf{g}_4 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} , \quad \mathbf{g}_5 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

et $G \leq O_\Delta(\mathbb{Z})$. Soit $G' = G \cap SO_\Delta(\mathbb{Z}) = \langle \mathbf{g}_2\mathbf{g}_3, \mathbf{g}_2\mathbf{g}_4, \mathbf{g}_2\mathbf{g}_5, \mathbf{g}_3\mathbf{g}_4, \mathbf{g}_3\mathbf{g}_5, \mathbf{g}_4\mathbf{g}_5 \rangle$. En procédant comme dans le chapitre 13.9 de [**Cas78**], on obtient l' isomorphisme

$$\begin{array}{ccc} \rho : \mathrm{PSL}_2(\mathbb{C}) & \longrightarrow & \mathrm{SO}_\Delta(\mathbb{R}) \\ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} & \longmapsto & \begin{pmatrix} |\alpha|^2 & 2\Im(\beta\overline{\alpha}) & 2\Re(\beta\overline{\alpha}) & |\beta|^2 \\ \Im(\alpha\overline{\gamma}) & \Re(\overline{\alpha}\delta - \overline{\beta}\gamma) & \Im(\alpha\overline{\delta} + \beta\overline{\gamma}) & \Im(\beta\overline{\delta}) \\ \Re(\alpha\overline{\gamma}) & \Im(\overline{\alpha}\delta - \overline{\beta}\gamma) & \Re(\alpha\overline{\delta} + \beta\overline{\gamma}) & \Re(\beta\overline{\delta}) \\ |\gamma|^2 & 2\Im(\delta\overline{\gamma}) & 2\Re(\delta\overline{\gamma}) & |\delta|^2 \end{pmatrix} \end{array} . \tag{2.2.2}$$

Soient

$$\mathbf{M}_1 = \begin{pmatrix} 1 & 1+i \\ -1+i & -1 \end{pmatrix} , \quad \mathbf{M}_2 = \begin{pmatrix} i & -1+i \\ 0 & -i \end{pmatrix} ,$$

$$\mathbf{M}_3 = \begin{pmatrix} (-1+i)\frac{\sqrt{2}}{2} & i\sqrt{2} \\ 0 & (-1-i)\frac{\sqrt{2}}{2} \end{pmatrix} , \quad \mathbf{M}_4 = \begin{pmatrix} i & 0 \\ -1-i & -i \end{pmatrix} ,$$

$$\mathbf{M}_5 = \begin{pmatrix} (-1+i)\frac{\sqrt{2}}{2} & 0 \\ -i\sqrt{2} & (-1-i)\frac{\sqrt{2}}{2} \end{pmatrix}, \quad \mathbf{M}_6 = \begin{pmatrix} (1+i)\frac{\sqrt{2}}{2} & 0 \\ 0 & (1-i)\frac{\sqrt{2}}{2} \end{pmatrix}.$$

Alors,

$$\rho(\mathbf{M}_1) = \mathbf{g}_2\mathbf{g}_3\,, \quad \rho(\mathbf{M}_2) = \mathbf{g}_2\mathbf{g}_4\,,$$
$$\rho(\mathbf{M}_3) = \mathbf{g}_2\mathbf{g}_5\,, \quad \rho(\mathbf{M}_4) = \mathbf{g}_3\mathbf{g}_4\,,$$
$$\rho(\mathbf{M}_5) = \mathbf{g}_3\mathbf{g}_5\,, \quad \rho(\mathbf{M}_6) = \mathbf{g}_4\mathbf{g}_5\,.$$

Soit $\mathcal{M} = \langle \mathbf{M}_1, \mathbf{M}_2, \mathbf{M}_3, \mathbf{M}_4, \mathbf{M}_5, \mathbf{M}_6 \rangle$. Une recherche à l'ordinateur donne :

$$\mathbf{M}_6^{-2}\mathbf{M}_3^{-2} = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \quad \mathbf{M}_6^2\mathbf{M}_5^2 = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix},$$
$$\mathbf{M}_4^{-1}\mathbf{M}_6^{-1}\mathbf{M}_5 = \begin{pmatrix} 1 & 0 \\ 2i & 1 \end{pmatrix}, \quad \mathbf{M}_3^{-1}\mathbf{M}_6\mathbf{M}_2 = \begin{pmatrix} 1 & 2i \\ 0 & 1 \end{pmatrix},$$
$$\mathbf{M}_6^2 = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad \mathbf{M}_5^{-2}\mathbf{M}_3^{-1}\mathbf{M}_1\mathbf{M}_3^{-1}\mathbf{M}_5^{-1}\mathbf{M}_6^{-1}\mathbf{M}_2^{-1} = \begin{pmatrix} 1+2i & 2i \\ -2i & 1-2i \end{pmatrix},$$
$$\mathbf{M}_6^2\mathbf{M}_1^{-1}\mathbf{M}_5^{-1}\mathbf{M}_2^{-1}\mathbf{M}_6^{-1} = \begin{pmatrix} 1-2i & 2i \\ -2i & 1+2i \end{pmatrix}, \quad \mathbf{M}_6^2\mathbf{M}_2\mathbf{M}_5\mathbf{M}_1^{-1}\mathbf{M}_6 = \begin{pmatrix} 1+2i & 2 \\ 2 & 1-2i \end{pmatrix}.$$

Cet ensemble de matrices engendre le sous-groupe Ξ du groupe de Picard $PSL_2(\mathbb{Z}[i])$:

$$\Xi = \Gamma(2) \cup \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \Gamma(2)$$

où

$$\Gamma(2) = \left\{ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in PSL_2(\mathbb{Z}[i]) \text{ tel que } \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod (2) \right\}.$$

En effet, il est prouvé dans [**FN87**] que $\Gamma(2)$ est la clôture normale dans $PSL_2(\mathbb{Z}[i])$ du sous-groupe engendré par :

$$\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \text{ et } \begin{pmatrix} 1 & 2i \\ 0 & 1 \end{pmatrix}.$$

Un ensemble de générateurs de $PSL_2(\mathbb{Z}[i])$ est, par exemple (voir [**Bru92**]) :

$$\begin{pmatrix} 1 & 0 \\ -i & 1 \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} i & i \\ i & 0 \end{pmatrix}.$$

Alors, en calculant tous les conjugués possibles des huit matrices données précédemment par les deux générateurs de $PSL_2(\mathbb{Z}[i])$, on peut voir que ces matrices engendrent un sous-groupe normal de $PSL_2(\mathbb{Z}[i])$, qui, par conséquent, contient $\Gamma(2)$.

Ainsi,

$$V\rho(\Xi)V^{-1} \subset \Gamma \Rightarrow V\rho(\Xi)V^{-1} \cdot u_0^t \subset \Gamma \cdot u_0^t\,.$$

Soit

$$\begin{pmatrix} A_0 \\ B_0 \\ C_0 \\ D_0 \end{pmatrix} = V^{-1}u_0^t = \begin{pmatrix} a_0 + b_0 \\ -\frac{a_0+b_0+c_0+d_0-2\omega_0}{2} \\ -\frac{a_0+b_0+c_0-d_0}{2} \\ a_0 + c_0 \end{pmatrix}.$$

D'après le lemme 2.1.5, ce vecteur a des composantes entières. Par définition de ρ, nous obtenons que l'ensemble des vecteurs de la forme

$$V \begin{pmatrix} |\alpha|^2 & 2\Im(\beta\overline{\alpha}) & 2\Re(\beta\overline{\alpha}) & |\beta|^2 \\ \Im(\alpha\overline{\gamma}) & \Re(\overline{\alpha}\delta - \overline{\beta}\gamma) & \Im(\alpha\overline{\delta} + \beta\overline{\gamma}) & \Im(\beta\overline{\delta}) \\ \Re(\alpha\overline{\gamma}) & \Im(\overline{\alpha}\delta - \overline{\beta}\gamma) & \Re(\alpha\overline{\delta} + \beta\overline{\gamma}) & \Re(\beta\overline{\delta}) \\ |\gamma|^2 & 2\Im(\delta\overline{\gamma}) & 2\Re(\delta\overline{\gamma}) & |\delta|^2 \end{pmatrix} \begin{pmatrix} A_0 \\ B_0 \\ C_0 \\ D_0 \end{pmatrix} \tag{2.2.3}$$

avec

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \Xi$$

est un sous-ensemble de l'orbite $\Gamma \cdot u_0^t$.

Étant donnés nos changements de variables précédents, les entiers de la forme $x_2 - a_0$, $x_3 - a_0$, $x_4 - a_0$ et $x_5 - a_0$, où $(x_2, x_3, x_4, x_5)^t$ parcourt l'orbite $\Gamma \cdot u_0^t$, apparaissent en deuxième, troisième, quatrième et cinquième coordonnées des vecteurs de l'orbite $\mathcal{A}_1 \cdot v_{\mathcal{P}}^t$.

En particulier, par (2.2.3), les entiers de la forme

$$|\alpha|^2 A_0 + 2\Im(\beta\overline{\alpha})B_0 + 2\Re(\beta\overline{\alpha})C_0 + |\beta|^2 D_0 - a_0$$

avec

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \Xi$$

apparaissent en deuxième coordonnée des vecteurs de l'orbite $\mathcal{A}_1 \cdot v_{\mathcal{P}}^t$. Ainsi, l'ensemble des entiers de la forme

$$A_0\alpha_1^2 + A_0\alpha_2^2 + D_0\beta_1^2 + D_0\beta_2^2 + 2\alpha_1\beta_2 B_0 - 2\alpha_2\beta_1 B_0 + 2\alpha_1\beta_1 C_0 + 2\alpha_2\beta_2 C_0 - a_0$$

avec

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \Xi \quad \text{et} \quad \alpha = \alpha_1 + i\alpha_2 \quad \text{et} \quad \beta = \beta_1 + i\beta_2$$

est un sous-ensemble de l'ensemble des entiers apparaissant en deuxième coordonnée des vecteurs de l'orbite $\mathcal{A}_1.v_{\mathcal{P}}^t$. Par définition de Ξ, cela signifie que l'ensemble des entiers de la forme

$$f_{a_0}(x,y,z,t) - a_0$$

avec $x+iy$ et $z+it$ copremiers dans $\mathbb{Z}[i]$, $x+iy \equiv 1$ ou $i \bmod (2)$ et

$$f_{a_0}(x,y,z,t) = A_0x^2 + A_0y^2 + 4D_0z^2 + 4D_0t^2 + 4xtB_0 - 4yzB_0 + 4xzC_0 + 4ytC_0$$

est un sous-ensemble de l'ensemble des courbures de l'empilement. De notre choix de $v_{\mathcal{P}}^t$, nous avons $A_0 = a_0 + b_0$ impair. Ainsi, si m est un entier impair qui peut être écrit comme $m = f_{a_0}(x,y,z,t)$ avec $x+iy$ et $z+it$ copremiers dans $\mathbb{Z}[i]$, automatiquement x et y sont de parités différentes, c'est-à-dire, $x+iy \equiv 1$ ou $i \bmod 2$. □

Remarque 9 : Soit $z = z_1 + iz_2 \in \mathbb{Z}[i]$. Alors,

$$\begin{aligned}|z_1+iz_2|^2 f_{a_0}(x_1,x_2,x_3,x_4) &= f_{a_0}(z_1x_1 - z_2x_2, z_2x_1 + z_1x_2, z_1x_3 - z_2x_4, z_2x_3 + z_1x_4)\\ &= f_{a_0}\left(\Re(z(x_1+ix_2)), \Im(z(x_1+ix_2)), \Re(z(x_3+ix_4)), \Im(z(x_3+ix_4))\right) .\end{aligned}$$

2.2.1. Représentations $\mathbb{Z}[i]$-primitives par f_{a_0}

Nous allons étudier les entiers copremiers à $disc(f_{a_0})$ pouvant être écrits comme $m = f_{a_0}(x,y,z,t) = f_{a_0}(x+iy, z+it)$ avec $x+iy$ et $z+it$ copremiers dans $\mathbb{Z}[i]$. Une telle représentation sera dite $\mathbb{Z}[i]$-primitive. Nous allons utiliser dans notre étude des résultats classiques sur la représentation des entiers par les formes quadratiques quaternaires définies positives.

Afin de contrôler la condition de coprimalité dans $\mathbb{Z}[i]$, nous avons besoin de la fonction de Möbius généralisée aux entiers de Gauss. On rappelle que tout idéal I de $\mathbb{Z}[i]$ peut être factorisé sous la forme

$$I = \mathfrak{p}_1^{\alpha_1} \dots \mathfrak{p}_k^{\alpha_k}$$

où les $\mathfrak{p}_i$ sont des idéaux premiers de $\mathbb{Z}[i]$. Cette factorisation est unique, à permutation des facteurs près. Alors, pour I un idéal de $\mathbb{Z}[i]$, on définit la fonction μ par

$$\mu(I) = \begin{cases} 0 & \text{s'il existe } i \text{ tel que } \alpha_i \geq 2, \\ (-1)^k & \text{sinon .} \end{cases}$$

De manière analogue au cas des entiers, μ est multiplicative et

$$\sum_{\substack{J \text{ ideaux de } \mathbb{Z}[i] \\ J \supset I}} \mu(J) = \begin{cases} 1 & \text{si } I = (1), \\ 0 & \text{sinon.} \end{cases} \tag{2.2.4}$$

Dans la suite, m désignera toujours un entier copremier avec $disc(f_{a_0})$.

Soit $\mathcal{N}(m)$ le nombre de représentations de m par f_{a_0} et $\mathcal{N}_P(m)$ le nombre de celles étant $\mathbb{Z}[i]$-primitives. À l'aide de la remarque 9, nous pouvons associer les représentations de $f_{a_0}(x,y,z,t) = m$ telles que $\mathrm{pgcd}_{\mathbb{Z}[i]}(x+iy, z+it) = \pi \in \mathbb{Z}[i]$ et les représentations $\mathbb{Z}[i]$-primitives de $\frac{m}{|\pi|^2}$ par f_{a_0}, et

$$\mathcal{N}(m) = \sum_{\substack{\pi\in\mathbb{Z}[i]\\ |\pi|^2|m}} \mathcal{N}_P\left(\frac{m}{|\pi|^2}\right) = 4 \sum_{\substack{I \text{ idéal de } \mathbb{Z}[i]\\ N(I)|m}} \mathcal{N}_P\left(\frac{m}{N(I)}\right).$$

À l'aide de (2.2.4), on peut inverser cette relation

$$\mathcal{N}_P(m) = \frac{1}{4} \sum_{\substack{I \text{ idéal de } \mathbb{Z}[i]\\ N(I)|m}} \mu(I)\mathcal{N}\left(\frac{m}{N(I)}\right). \tag{2.2.5}$$

Or, la formule asymptotique pour $\mathcal{N}(m)$ est connue (voir, par exemple, le corollaire 1 de [**HB96**] ou le théorème 20.9 de [**IK04**]) et rappelée ci-dessous.

Théorème 2.2.2.

$$\mathcal{N}(m) = \frac{\pi^2}{2a_0^2} m\mathfrak{S}(m) + O(m^{\frac{3}{4}+\varepsilon})$$

pour tout $\varepsilon > 0$, où

$$\mathfrak{S}(m) = \prod_p \delta_p(m)$$

avec

$$\delta_p(m) = \lim_{k\to\infty} p^{-3k} |x \in \left(\mathbb{Z}/p^k\mathbb{Z}\right)^4 \text{ tel que } f_{a_0}(x) \equiv m \bmod p^k|.$$

La constante impliquée ne dépend que de ε.

De ceci et de (2.2.5), on obtient :

$$\mathcal{N}_P(m) = \frac{\pi^2}{8a_0^2} m \sum_{\substack{I \text{ idéal de } \mathbb{Z}[i]\\ N(I)|m}} \frac{\mu(I)}{N(I)} \mathfrak{S}\left(\frac{m}{N(I)}\right) + O\left(m^{\frac{3}{4}+\varepsilon} \sum_{\substack{I \text{ idéal de } \mathbb{Z}[i]\\ N(I)|m}} \frac{1}{N(I)^{\frac{3}{4}+\varepsilon}}\right). \tag{2.2.6}$$

2.2.1.1. *Le terme d'erreur*

Lemme 2.2.1. *Le terme d'erreur dans (2.2.6) est $O(m^{\frac{3}{4}+\varepsilon})$ pour tout $\varepsilon > 0$ (et la constante impliquée ne dépend que de ε).*

DÉMONSTRATION. Soit $r_2(d)$ le nombre de représentations de d comme somme de deux carrés. Comme $r_2(d) \ll \tau(d)$,

$$\sum_{\substack{I \text{ idéal de } \mathbb{Z}[i] \\ N(I)|m}} \frac{1}{N(I)^{\frac{3}{4}+\varepsilon}} = \frac{1}{4}\sum_{d|m} \frac{r_2(d)}{d^{\frac{3}{4}+\varepsilon}} \ll \sum_{d|m} \frac{\tau(d)}{d^{\frac{3}{4}+\varepsilon}}$$

$$\ll \tau(m) \sum_{d|m} \frac{1}{d^{\frac{3}{4}+\varepsilon}} \ll \tau(m)^2 .$$

Ainsi, le terme d'erreur est $O(m^{\frac{3}{4}+\varepsilon})$ pour tout $\varepsilon > 0$. □

2.2.1.2. *Le terme principal*

Pour obtenir une version plus explicite du terme principal, il nous faut une compréhension plus approfondie des densités locales $\delta_p(\frac{m}{N(I)})$. Pour cela, nous utilisons le lemme suivant, que l'on peut par exemple trouver comme lemme 16 dans [**Sie35**]) :

Lemme 2.2.2. *Soit $p \not| disc(f_{a_0})$, alors*

$$\delta_p(m) = \left(1 - \frac{1}{p^2}\right)\left(1 + \frac{1}{p} \cdots + \frac{1}{p^{v_p(m)}}\right)$$

où $v_p(m)$ est tel que $p^{v_p(m)}||m$.

DÉMONSTRATION. On remarque tout d'abord que :

$$|x \in \left(\mathbb{Z}/p^k\mathbb{Z}\right)^4 \text{ tel que } f_{a_0}(x) \equiv m \bmod p^k| = \frac{1}{p^k} \sum_{n \bmod p^k} \sum_{x \in \left(\mathbb{Z}/p^k\mathbb{Z}\right)^4} \mathrm{e}^{2i\pi \frac{(f_{a_0}(x)-m)n}{p^k}} .$$

Or, $disc(f_{a_0}) = 16a_0^4$ (donc un carré) et $p \not| disc(f_{a_0})$. Ainsi, f_{a_0} peut être diagonalisée mod p^k et est équivalente à la forme quadratique $x_1^2 + x_2^2 + x_3^2 + x_4^2$. Alors,

$$|x \in \left(\mathbb{Z}/p^k\mathbb{Z}\right)^4 \text{ tel que } f_{a_0}(x) \equiv m \bmod p^k| = \frac{1}{p^k} \sum_{n \bmod p^k} \mathrm{e}^{-2i\pi \frac{mn}{p^k}} \left(\sum_{x \bmod p^k} \mathrm{e}^{2i\pi \frac{nx^2}{p^k}}\right)^4$$

$$= \frac{1}{p^k} \sum_{j=0}^{k} p^{4(k-j)} \sum_{\substack{n=1 \\ (n,p)=1}}^{p^j} \mathrm{e}^{-2i\pi \frac{mn}{p^j}} \left(\sum_{x \bmod p^j} \mathrm{e}^{2i\pi \frac{nx^2}{p^j}}\right)^4 .$$

La somme intérieure est une somme de Gauss quadratique, dont la valeur est, classiquement :

$$\sum_{x \bmod p^j} \mathrm{e}^{2i\pi \frac{nx^2}{p^j}} = \varepsilon_{p^j} \left(\frac{n}{p^j}\right) \sqrt{p^j} \quad \text{avec} \quad \varepsilon_a = \begin{cases} 1 \text{ si } a \equiv 1 \bmod 4 , \\ i \text{ si } a \equiv 3 \bmod 4 . \end{cases}$$

Ainsi,

$$|x \in \left(\mathbb{Z}/p^k\mathbb{Z}\right)^4 \text{ tel que } f_{a_0}(x) \equiv m \bmod p^k| = p^{3k} \sum_{j=0}^{k} p^{-2j} \sum_{\substack{n=1 \\ (n,p)=1}}^{p^j} \mathrm{e}^{-2i\pi\frac{mn}{p^j}}$$

$$= p^{3k} \sum_{j=0}^{k} p^{-2j} \sum_{n|(p^j,m)} \mu\left(\frac{p^j}{n}\right) n\,.$$

Alors, pour $k \geq v_p(m)+1$, on obtient :

$$|x \in \left(\mathbb{Z}/p^k\mathbb{Z}\right)^4 \text{ tel que } f_{a_0}(x) \equiv m \bmod p^k| = p^{3k} \sum_{j=0}^{v_p(m)+1} p^{-2j} \sum_{n|(p^j,m)} \mu\left(\frac{p^j}{n}\right) n$$

$$= p^{3k} \sum_{j=1}^{v_p(m)} p^{-2j}\left(p^j - p^{j-1}\right) + p^{3k}\left(1 - p^{-v_p(m)-2}\right)\,,$$

ce qui donne le résultat souhaité. □

Lemme 2.2.3. *Soit $(p,m)=1$. Alors, $\delta_p(\frac{m}{N(I)}) = \delta_p(m)$ pour tout idéal I de $\mathbb{Z}[i]$ avec $N(I)|m$.*

Démonstration.

$$\delta_p\left(\frac{m}{N(I)}\right) = \lim_{k\to\infty} p^{-3k} A_{p^k}\left(\frac{m}{N(I)}\right)$$

avec

$$A_{p^k}\left(\frac{m}{N(I)}\right) = |x \in \left(\mathbb{Z}/p^k\mathbb{Z}\right)^4 \text{ tel que } f_{a_0}(x) = \frac{m}{N(I)} \bmod p^k|$$

$$= \frac{1}{p^k} \sum_{x\in\left(\mathbb{Z}/p^k\mathbb{Z}\right)^4} \sum_{h\in\mathbb{Z}/p^k\mathbb{Z}} \mathrm{e}\left(\frac{(f_{a_0}(x) - \frac{m}{N(I)})h}{p^k}\right)\,.$$

En utilisant le changement de variables $h \longrightarrow N(I)h$ (qui est un isomorphisme de $\mathbb{Z}/p^k\mathbb{Z}$, car $N(I)|m$ et $(p,m)=1$)

$$A_{p^k}\left(\frac{m}{N(I)}\right) = \frac{1}{p^k} \sum_{x\in\left(\mathbb{Z}/p^k\mathbb{Z}\right)^4} \sum_{h\in\mathbb{Z}/p^k\mathbb{Z}} \mathrm{e}\left(\frac{(N(I)f_{a_0}(x) - m)h}{p^k}\right)\,.$$

$I = (z_1 + iz_2)$ pour un certain $z_1 + iz_2 \in \mathbb{Z}[i]$ (car $\mathbb{Z}[i]$ est un anneau principal), et donc, en utilisant la remarque 9,

$$N(I) f_{a_0}(x) = f_{a_0}(xA)$$

avec

$$A = \begin{pmatrix} z_1 & z_2 & 0 & 0 \\ -z_2 & z_1 & 0 & 0 \\ 0 & 0 & z_1 & z_2 \\ 0 & 0 & -z_2 & z_1 \end{pmatrix}$$

et l'application $x \longrightarrow xA$ est un isomorphisme de $\left(\mathbb{Z}/p^k\mathbb{Z}\right)^4$ (car $p \not| N(I) = det(A)$). Ainsi,

$$A_{p^k}\left(\frac{m}{N(I)}\right) = \frac{1}{p^k} \sum_{x \in \left(\mathbb{Z}/p^k\mathbb{Z}\right)^4} \sum_{h \in \mathbb{Z}/p^k\mathbb{Z}} \mathrm{e}\left(\frac{(f_{a_0}(x) - m)h}{p^k}\right) = A_{p^k}(m)\,.$$

□

Lemme 2.2.4. *Le terme principal dans (2.2.6) est*

$$\frac{\pi^2}{8a_0^2} m\mathfrak{S}(m) \prod_{\substack{p \| m \\ p \equiv 1 \bmod 4}} \left(1 - \frac{2}{p+1}\right) \prod_{\substack{p^2 | m \\ p \equiv 1 \bmod 4}} \left(1 - \frac{1}{p}\right)^2 \left(1 - \frac{1}{p^{v_p(m)+1}}\right)^{-1} \times \prod_{\substack{p^2 | m \\ p \equiv 3 \bmod 4}} \left(1 - \frac{1}{p^2}\right) \left(1 - \frac{1}{p^{v_p(m)+1}}\right)^{-1}.$$

Démonstration. D'après les lemmes 2.2.2 et 2.2.3,

$$\begin{aligned} \mathfrak{S}\left(\frac{m}{N(I)}\right) &= \prod_{(p,m)=1} \delta_p\left(\frac{m}{N(I)}\right) \prod_{p|m} \delta_p\left(\frac{m}{N(I)}\right) \\ &= \prod_{(p,m)=1} \delta_p(m) \prod_{p|m} \left(1 - \frac{1}{p^2}\right)\left(1 + \frac{1}{p} \cdots + \frac{1}{p^{v_p\left(\frac{m}{N(I)}\right)}}\right) \\ &= \mathfrak{S}(m) \prod_{p|N(I)} \left(\frac{1 + \frac{1}{p} \cdots + \frac{1}{p^{v_p\left(\frac{m}{N(I)}\right)}}}{1 + \frac{1}{p} \cdots + \frac{1}{p^{v_p(m)}}}\right). \end{aligned}$$

Ainsi, le terme principal est donné par

$$\frac{\pi^2}{8a_0^2} m\mathfrak{S}(m) \sum_{\substack{I \text{ idéal de } \mathbb{Z}[i] \\ N(I)|m}} g(I)$$

avec

$$g(I) = \frac{\mu(I)}{N(I)} \prod_{p|N(I)} \left(\frac{1 + \frac{1}{p} \cdots + \frac{1}{p^{v_p\left(\frac{m}{N(I)}\right)}}}{1 + \frac{1}{p} \cdots + \frac{1}{p^{v_p(m)}}}\right).$$

Or, en écrivant $m = m_1 m_3$ où $m_1 = \prod_{p\equiv 1 \bmod 4} p^{v_p(m)}$ et $m_3 = \prod_{p\equiv 3 \bmod 4} p^{v_p(m)}$, on a

$$\sum_{\substack{I \text{ idéal de } \mathbb{Z}[i] \\ N(I)|m}} g(I) = \sum_{\substack{I \text{ idéal de } \mathbb{Z}[i] \\ N(I)|m_1}} g(I) \sum_{\substack{I \text{ idéal de } \mathbb{Z}[i] \\ N(I)|m_3}} g(I)\,.$$

Remarquons que g est multiplicative sur l'ensemble des idéaux dont la norme est composée uniquement de facteurs premiers $\equiv 3 \bmod 4$. De plus, les idéaux premiers dont la norme est composée uniquement de facteurs premiers $\equiv 3 \bmod 4$ sont exactement les idéaux de la forme $\mathfrak{p} = (p)$ avec $p \equiv 3 \bmod 4$ et alors $N(\mathfrak{p}) = p^2$. Ainsi,

$$\begin{aligned}\sum_{\substack{I \text{ idéal de } \mathbb{Z}[i] \\ N(I)|m_3}} g(I) = \prod_{N(\mathfrak{p})|m_3} (1+g(\mathfrak{p})) &= \prod_{\substack{p^2|m \\ p\equiv 3 \bmod 4}} \left(1 - \frac{1+\frac{1}{p}\cdots+\frac{1}{p^{v_p(m)-2}}}{p^2(1+\frac{1}{p}\cdots+\frac{1}{p^{v_p(m)}})}\right) \\ &= \prod_{\substack{p^2|m \\ p\equiv 3 \bmod 4}} \left(1-\frac{1}{p^2}\right)\left(1-\frac{1}{p^{v_p(m)+1}}\right)^{-1}.\end{aligned}$$

Notons maintenant $f(k) = \sum_{\substack{I \text{ idéal de } \mathbb{Z}[i] \\ N(I)=k}} g(I)$. On obtient $\sum_{\substack{I \text{ idéal de } \mathbb{Z}[i] \\ N(I)|m_1}} g(I) = \sum_{k|m_1} f(k)$.

Soit $k|m_1$, $k = p_1^{\alpha_1}\dots p_r^{\alpha_r}$. Si $\mathfrak{p}_i$ et $\overline{\mathfrak{p}}_i$ sont les deux idéaux de norme p_i de $\mathbb{Z}[i]$, tout idéal I de norme k est de la forme

$$I = \mathfrak{p}_1^{\beta_1}\overline{\mathfrak{p}}_1^{\alpha_1-\beta_1}\dots\mathfrak{p}_r^{\beta_r}\overline{\mathfrak{p}}_r^{\alpha_r-\beta_r} \text{ avec } 0 \le \beta_i \le \alpha_i\,.$$

Remarquons si k a un facteur cubique, I a nécessairement un facteur carré et alors $g(I) = 0$. De plus, si k est sans facteur cubique, en parcourant toutes les écritures possibles de I,

$$f(k) = \frac{(-1)^{\Omega(k)}2^{2\omega(k)-\Omega(k)}}{k}\prod_{p|k}\left(\frac{1+\frac{1}{p}\cdots+\frac{1}{p^{v_p(m/k)}}}{1+\frac{1}{p}\cdots+\frac{1}{p^{v_p(m)}}}\right).$$

Mais cette fonction est multiplicative en k et donc

$$\begin{aligned}\sum_{\substack{I \text{ idéal de } \mathbb{Z}[i] \\ N(I)|m_1}} g(I) &= \prod_{\substack{p\|m \\ p\equiv 1 \bmod 4}} (1+f(p)) \prod_{\substack{p^2|m \\ p\equiv 1 \bmod 4}} \left(1+f(p)+f(p^2)\right) \\ &= \prod_{\substack{p\|m \\ p\equiv 1 \bmod 4}} \left(1-\frac{2}{p+1}\right) \prod_{\substack{p^2|m \\ p\equiv 1 \bmod 4}} \left(1-\frac{1}{p}\right)^2\left(1-\frac{1}{p^{v_p(m)+1}}\right)^{-1}.\end{aligned}$$

□

Lemme 2.2.5.

$$\mathcal{N}_P(m) = \frac{\pi^2}{8a_0^2} m\mathfrak{S}(m) \prod_{\substack{p\|m \\ p\equiv 1 \bmod 4}} \left(1-\frac{2}{p+1}\right) \prod_{\substack{p^2|m \\ p\equiv 1 \bmod 4}} \left(1-\frac{1}{p}\right)^2 \left(1-\frac{1}{p^{v_p(m)+1}}\right)^{-1} \times \prod_{\substack{p^2|m \\ p\equiv 3 \bmod 4}} \left(1-\frac{1}{p^2}\right)\left(1-\frac{1}{p^{v_p(m)+1}}\right)^{-1} + O(m^{\frac{3}{4}+\varepsilon}).$$

DÉMONSTRATION. C'est une conséquence directe des lemmes 2.2.1 et 2.2.4. □

2.2.2. Un principle local-global partiel

Théorème 2.2.3. *Soit m un entier copremier avec $disc(f_{a_0})$. Supposons que l'équation $f_{a_0}(x) \equiv m \bmod p$ admette une solution pour tout $p|disc(f_{a_0})$, $p \neq 2$ et que l'équation $f_{a_0}(x) \equiv m \bmod 8$ ait une solution. Alors, pour un tel m, avec m suffisamment grand, m est représenté $\mathbb{Z}[i]$-primitivement par f_{a_0}.*

Afin de prouver ce théorème, nous aurons besoin du lemme suivant, que l'on peut trouver par exemple comme lemme 13 de [**Sie35**] :

Lemme 2.2.6. *Pour tout $k > 2v_p(2m)$, $p^{-3k}A_{p^k}$ ne dépend pas de k.*

PREUVE DU THÉORÈME 2.2.3. On utilise le lemme 2.2.5. On a

$$\prod_{\substack{p\|m \\ p\equiv 1 \bmod 4}} \left(1-\frac{2}{p+1}\right) \prod_{\substack{p^2|m \\ p\equiv 1 \bmod 4}} \left(1-\frac{1}{p}\right)^2 \geq \prod_{p\leq m} \left(1-\frac{1}{p}\right)^2$$

et par la formule de Mertens,

$$\prod_{p\leq m} \left(1-\frac{1}{p}\right) \sim \frac{e^{-\gamma}}{\log m}.$$

De plus,

$$\prod_{\substack{p\equiv 3 \bmod 4 \\ p^2|m}} \left(1-\frac{1}{p^2}\right) \geq \prod_{p} \left(1-\frac{1}{p^2}\right) = \frac{1}{\zeta(2)}$$

et

$$\prod_{\substack{p\equiv 1 \bmod 4 \\ p^2|m}} \left(1-\frac{1}{p^{v_p(m)+1}}\right)^{-1} \prod_{\substack{p\equiv 3 \bmod 4 \\ p^2|m}} \left(1-\frac{1}{p^{v_p(m)+1}}\right)^{-1} \geq 1.$$

Il faut maintenant montrer que $\mathfrak{S}(m)$ est suffisamment éloigné de zéro. Par le lemme 2.2.2,

$$\prod_{p\nmid disc(f_{a_0})} \delta_p(m) \gg 1.$$

Il reste à prouver que $\delta_p(m)$ est suffisamment éloigné de zéro pour l'ensemble fini des premiers $p|disc(f_{a_0})$.

Par le lemme 2.2.6, pour $p \neq 2$,

$$\delta_p(m) = p^{-3}|x \in (\mathbb{Z}/p\mathbb{Z})^4 \text{ tel que } f_{a_0}(x) \equiv m \bmod p|\,.$$

Mais, par hypothèse, il existe une solution de $f_{a_0}(x) \equiv m \bmod p$ et donc $\delta_p(m) > 0$.

Enfin, encore une fois par le lemme 2.2.6, pour $p = 2$, on obtient que

$$\delta_2(m) = \frac{1}{512}|x \in (\mathbb{Z}/8\mathbb{Z})^4 \text{ tel que } f_{a_0}(x) \equiv m \bmod 8|\,.$$

Comme précédemment, ceci est positif. Ainsi, par le lemme 2.2.5,

$$\mathcal{N}_P(m) \gg \frac{m}{\log^2 m} + O(m^{\frac{3}{4}+\varepsilon})$$

et donc $\mathcal{N}_P(m) > 0$ pour m assez grand. □

Théorème 2.2.4 (Un principe local-global partiel)**.** *Soit*

$$\mathcal{S} = \{n \in \mathbb{Z}, n > 0 \text{ tel que } n \equiv b_0 \bmod 4\}\ .$$

Alors, un entier m suffisamment grand avec $\gcd(m, a_0) = 1$ *est courbure d'une sphère dans l'empilement si et seulement si $m \in \mathcal{S}$.*

Démonstration. On regarde les entiers m satisfaisant les conditions suivantes :

- $m + a_0$ est impair,
- $\gcd(m + a_0, disc(f_{a_0})) = 1$,
- $m + a_0$ est représenté par f_{a_0} modulo 8 et modulo tout premier impair divisant le discriminant.

De par notre choix de $v^t_{\mathcal{P}}$, $a_0 + b_0$ est impair. On se restreint à $m + a_0$ impair pour pouvoir ensuite appliquer le théorème 2.2.1 qui traite des représentations $\mathbb{Z}[i]$-primitives des entiers impairs par f_{a_0}.

On veut également que $\gcd(m + a_0, disc(f_{a_0})) = \gcd(m + a_0, 16a_0^4) = 1$ afin de pouvoir appliquer le théorème 2.2.3. Mais, comme $m + a_0$ est impair, cela signifie simplement que $\gcd(m, a_0) = 1$.

On veut que $m + a_0$ soit représenté par f_{a_0} modulo 8. Mais, comme A_0 est impair, il est facile de voir que f_{a_0} représente exactement deux classes impaires modulo 8, à savoir A_0 et $5A_0$ mod 8. Ainsi, on veut simplement $m + a_0$ dans la classe A_0 mod 4, c'est-à-dire

$m \equiv b_0 \bmod 4$. Remarquons que cette condition inclut la condition $m + a_0$ impair.

On veut que $m + a_0$ soit représenté par f_{a_0} modulo tout premier divisant le discriminant. Remarquons que, comme A_0 est impair,

$$\begin{aligned}\operatorname{pgcd}(A_0, B_0, C_0, D_0) &= \operatorname{pgcd}(a_0 + b_0, a_0 + b_0 + c_0 + d_0 - 2\omega_0, a_0 + b_0 + c_0 - d_0, a_0 + c_0) \\ &= \operatorname{pgcd}(a_0 + b_0, a_0 + c_0, a_0 + d_0, a_0 + \omega_0)\,.\end{aligned}$$

Mais, par l'équation (2.2.1),

$$\begin{aligned}p \neq 2 \text{ et } p|\operatorname{pgcd}(a_0 + b_0, a_0 + c_0, a_0 + d_0, a_0 + \omega_0) &\Rightarrow p|a_0 \\ &\Rightarrow p|\operatorname{pgcd}(a_0, b_0, c_0, d_0, \omega_0)\end{aligned}$$

ce qui contredit la primitivité. Il est facile de vérifier que cela signifie que f_{a_0} peut prendre toutes les valeurs possibles modulo p. Ainsi, cela n'impose aucune restriction sur $m + a_0$, excepté $\operatorname{pgcd}(m, a_0) = 1$.

Par le théorème 2.2.1, nous savons que l'ensemble des entiers impairs de la forme

$$f_{a_0}(x, y, z, t) - a_0 \quad \operatorname{pgcd}_{\mathbb{Z}[i]}(x + iy, z + it) = 1$$

est un sous-ensemble de l'ensemble des courbures de $\mathcal{P}$. Par le théorème 2.2.3 et les observations précédentes, on déduit que tous les entiers m suffisamment grands avec $\operatorname{pgcd}(m, a_0) = 1$ et $m \equiv b_0 \bmod 4$ sont représentés $\mathbb{Z}[i]$-primitivement par $f_{a_0}(x, y, z, t) - a_0$, et sont donc des courbures de l'empilement.

Réciproquement, d'après le lemme 2.1.6, toute courbure m de l'empilement vérifiant $\operatorname{pgcd}(m, a_0) = 1$ sera telle que $m \equiv b_0 \bmod 4$. □

Remarque 10 : Ce résultat implique que l'ensemble des courbures dans un empilement apollonien généralisé primitif de sphères a une densité positive. Plus précisément , la densité est au moins

$$\frac{1}{4} \prod_{\substack{p|a_0 \\ p \neq 2}} \left(1 - \frac{1}{p}\right)\,.$$

Chapitre 3

COMPTAGE AVEC MULTIPLICITÉ POUR LES EMPILEMENTS GÉNÉRALISÉS DE CERCLES

3.1. Généralités sur les empilements apolloniens généralisés de cercles

Guettler et Mallows proposent, dans [**GM10**], de construire un empilement de cercles à l'aide d'une règle d'empilement différente de celle des empilements apolloniens classiques. Plus précisément, en partant d'une configuration de trois cercles mutuellement tangents, au lieu d'inscrire un unique cercle dans chaque espace vide, ils décrivent une procédure pour en inscrire trois mutuellement tangents. Comme dans le cas classique, un théorème d'Apollonius est vérifié : il y a une unique manière d'inscrire trois cercles mutuellement tangents telle que chaque cercle inscrit soit tangent à exactement deux des cercles d'origine.

En itérant le procédé, on obtient ce que Guettler et Mallows appellent un empilement généralisé (ou encore empilement 3-apollonien d'après Zhang [**Zha13**]).

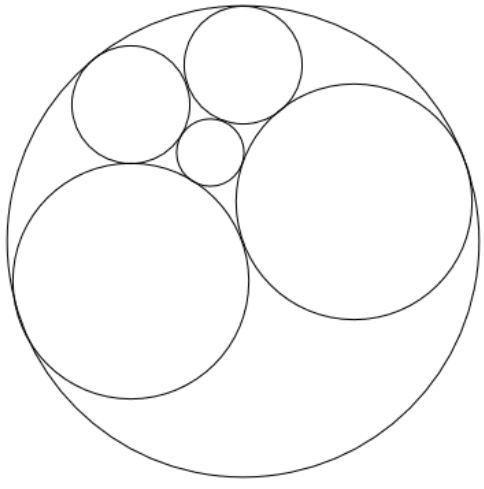

Figure 14. Un exemple de configuration généralisée

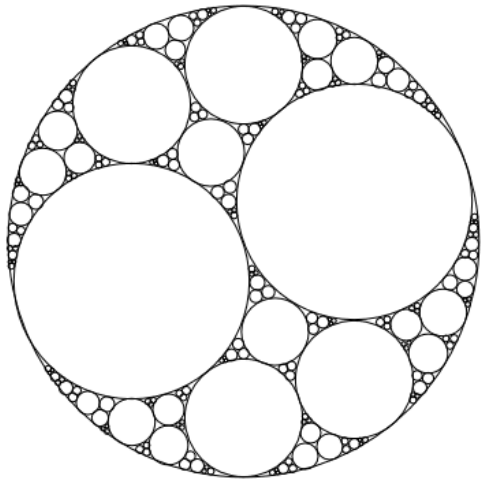

Figure 15. Un exemple d'empilement apollonien généralisé de cercles

Une fois encore, il est intéressant de se demander comment se comportent les courbures des cercles dans de tels empilements, si elles peuvent être entières et si, le cas échéant, on peut étudier les propriétés de ces entiers. L'existence d'un équivalent au théorème de Descartes, donné ci-dessous et prouvé dans [**GM10**], est une importante similarité avec le cas classique et s'avère être un outil fondamental dans l'étude des courbures.

Théorème 3.1.1. *Soient $\mathcal{C}_1$, $\mathcal{C}_2$ et $\mathcal{C}_3$ trois cercles mutuellement tangents, de courbures respectives b_1, b_2, b_3, formant deux espaces vides. Alors, les courbures des deux ensembles de trois cercles qui peuvent être inscrits dans chaque espace vide sont données par $(2\omega - b_1, 2\omega - b_2, 2\omega - b_3)$ et $(2\omega' - b_1, 2\omega' - b_2, 2\omega' - b_3)$, où ω et ω' sont les racines de*

$$Q(b_1, b_2, b_3, \omega) = \omega^2 - 2\omega(b_1 + b_2 + b_3) + b_1^2 + b_2^2 + b_3^2 = 0\,. \tag{3.1.1}$$

Considérons une configuration généralisée de six cercles, de courbures $b_1, b_2, b_3, b_1', b_2', b_3'$. Le théorème précédent indique que les courbures viennent par paires

$$b_1 + b_1' = b_2 + b_2' = b_3 + b_3' = \omega$$

et nous incite à représenter un tel sextuplé de cercles comme un vecteur $(b_1, b_2, b_3, \omega)^t$ constitué des courbures d'un cercle de chaque paire et de la moyenne (commune) des courbures de chaque paire. Ainsi, on appellera sextuplé un vecteur $(b_1, b_2, b_3, \omega)^t$ associé à une configuration généralisée de six cercles.

Remarque 11 : Il n'existe pas un unique sextuplé associé à une configuration généralisée. D'autres tels sextuplés peuvent être donnés en permutant l'ordre des cercles ou en changeant le choix du cercle sélectionné dans chaque paire. Ainsi, à une configuration de cercles correspondent au plus 48 sextuplés.

De manière analogue au cas des empilements apolloniens classiques, ou comme dans le chapitre 2, l'équation de Descartes nous permet de définir le groupe d'Apollonius généralisé $\mathcal{A} = \langle S_{123}, S_{1'23}, S_{12'3}, S_{123'}, S_{1'2'3}, S_{1'23'}, S_{12'3'}, S_{1'2'3'} \rangle$ où

$$S_{123} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 2 & 2 & 2 & -1 \end{pmatrix}, \; S_{1'23} = \begin{pmatrix} -3 & 4 & 4 & 4 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ -2 & 2 & 2 & 3 \end{pmatrix}, \; S_{12'3} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 4 & -3 & 4 & 4 \\ 0 & 0 & 1 & 0 \\ 2 & -2 & 2 & 3 \end{pmatrix},$$

$$S_{123'} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 4 & 4 & -3 & 4 \\ 2 & 2 & -2 & 3 \end{pmatrix}, \; S_{1'2'3} = \begin{pmatrix} -3 & -4 & 4 & 12 \\ -4 & -3 & 4 & 12 \\ 0 & 0 & 1 & 0 \\ -2 & -2 & 2 & 7 \end{pmatrix}, \; S_{1'23'} = \begin{pmatrix} -3 & 4 & -4 & 12 \\ 0 & 1 & 0 & 0 \\ -4 & 4 & -3 & 12 \\ -2 & 2 & -2 & 7 \end{pmatrix},$$

$$S_{12'3'} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 4 & -3 & -4 & 12 \\ 4 & -4 & -3 & 12 \\ 2 & -2 & -2 & 7 \end{pmatrix}, S_{1'2'3'} = \begin{pmatrix} -3 & -4 & -4 & 20 \\ -4 & -3 & -4 & 20 \\ -4 & -4 & -3 & 20 \\ -2 & -2 & -2 & 11 \end{pmatrix}.$$

Alors, pour tout sextuplé v^t dans l'empilement, l'orbite $\mathcal{A}.v^t$ décrit l'ensemble des courbures des sextuplés de cercles de l'empilement. De ce fait, on déduit que, si le sextuplé original de cercles dans l'empilement est à courbures entières, il en sera de même pour tout cercle de l'empilement. Un tel empilement sera appelé empilement entier et s'impose comme un objet attractif pour la théorie des nombres.

Zhang, dans [**Zha13**], prouve, par une méthode analogue à Kontorovich et Bourgain [**BK14**], un théorème semblable au théorème 1.1.3 sur la densité des courbures apparaissant dans un empilement entier. La question du comptage des courbures avec multiplicité, offrant un analogue à un résultat de Oh et Lee dans [**LO13**], succédant au travail de Kontorovich et Oh [**KO11**], est abordée dans la suite de ce chapitre.

Pour un empilement apollonien généralisé borné entier (sans cercle de courbure nulle) de cercles $\mathcal{P}$, on peut définir son sextuplé racine comme étant le sextuplé « minimal », dans le sens où il représente le sextuplé des trois plus grands cercles de l'empilement et du plus petit ω. Plus précisément, $v^t = (a, b, c, d, \omega)^t$ dans l'empilement est appelé un sextuplé racine si $a \leq 0 \leq b \leq c \leq \omega$ et $\omega \leq a + b + c$.

Remarque 12 : Le sextuplé racine d'un empilement est unique. Toutefois, il peut exister plusieurs configurations dans l'empilement correspondant à ce sextuplé.

On appelle empilement primitif tout empilement entier dont le sextuplé racine $v^t_{\mathcal{P}} = (a_0, b_0, c_0, \omega_0)^t$ vérifie $\text{pgcd}(a_0, b_0, c_0) = 1$. À la manière de la propriété d'intégralité de l'empilement, la primitivité du sextuplé racine entraîne la primitivité de tout sextuplé de l'empilement.

Dans tout ce qui suit, les empilements considérés seront des empilements primitifs bornés.

On déduit de [**Zha13**] que, de manière analogue aux empilements apolloniens de cercles classiques, on dispose d'une manière élégante de décrire l'ensemble des courbures de l'empilement, à l'aide du groupe d'Apollonius généralisé et du sextuplé racine, manière résumée dans la proposition 3.1.1 ci-dessous.

Définition 3.1.1. *Pour un vecteur $v = (v_1, v_2, v_3, v_4) \in \mathbb{R}^4$, on définit*

$$\tilde{v} = (|v_1|, |v_2|, |v_3|, |2v_4 - v_1|, |2v_4 - v_2|, |2v_4 - v_3|)\,.$$

Proposition 3.1.1. *Soit $\mathcal{P}$ un empilement apollonien généralisé borné de cercles, de sextuplé racine $v_{\mathcal{P}}^t$. Alors, l'ensemble des courbures des cercles de l'empilement $\mathcal{P}$ (avec multiplicité) est exactement l'ensemble consistant en les trois entrées maximales de $\tilde{v}$ où v^t parcourt l'orbite $\mathcal{A}.v_{\mathcal{P}}^t$ et en les entrées a_0, b_0, c_0 du sextuplé racine.*

Soit $\tilde{\mathcal{A}} = \mathcal{A} \cap \mathrm{SO}_Q(\mathbb{Z})$ le sous-groupe engendré par :

$$S_{123}S_{1'23}, S_{123}S_{12'3}, S_{123}S_{123'}, S_{123}S_{1'2'3}, S_{123}S_{1'23'}, S_{123}S_{12'3'}, S_{123}S_{1'2'3'}\,.$$

Dans ce qui suit, pour un sextuplé racine $v_{\mathcal{P}}^t$, on note $\mathcal{O}_d$ l'orbite $\tilde{\mathcal{A}}.v_{\mathcal{P}}^t$ réduite mod d. Zhang, dans [**Zha13**], donne une description de $\mathcal{O}_d$, résumée dans les deux propositions suivantes :

Proposition 3.1.2. *Soit $d = \prod_i p_i^{n_i}$. Alors, la projection suivante est surjective :*

$$\mathcal{O}_d \longrightarrow \prod_i \mathcal{O}_{p_i^{n_i}}\,.$$

Proposition 3.1.3. *Pour $p \geq 3$ et $m \geq 1$,*

$$\mathcal{O}_{p^m} = \{v^t \in (\mathbb{Z}/p^m\mathbb{Z})^4 - \{0\} \text{ tel que } Q(v) \equiv 0 \bmod p^m\}\,.$$

Lemme 3.1.1. *Soit $v_{\mathcal{P}}^t$ le sextuplé racine d'un empilement primitif. Alors, tous les vecteurs de l'orbite $\mathcal{A}.v_{\mathcal{P}}^t$ ont la même réduction* mod 2 *qui est l'une des suivantes :*

$$(0,1,0,1)^t \quad ou \quad (1,0,0,1)^t \quad ou \quad (0,0,1,1)^t\,.$$

Démonstration. Pour le sextuplé racine $v_{\mathcal{P}}^t = (a_0, b_0, c_0, w_0)^t$, l'équation (3.1.1) regardée mod 2 nous donne trois possibilités :

- toutes les entrées de $v_{\mathcal{P}}^t$ sont paires. Mais c'est impossible par primitivité de l'empilement.
- toutes les entrées de $v_{\mathcal{P}}^t$ sont impaires. Mais alors $2w_0(a_0 + b_0 + c_0) \equiv 0 \bmod 4$, ce qui est impossible puisque les quatre entrées sont impaires.
- $v_{\mathcal{P}}^t$ possède deux entrées paires et deux entrées impaires.

Ainsi, $v_{\mathcal{P}}^t$ possède deux entrées paires et deux entrées impaires. Mais, si w_0 est pair, on a $a_0^2 + b_0^2 + c_0^2 \equiv 0 \bmod 4$, ce qui est impossible. Donc $v_{\mathcal{P}}^t$ est l'un des trois vecteurs donnés dans le lemme et, puisque $\tilde{\mathcal{A}}$ est trivial mod 2, on obtient le résultat. □

Lemme 3.1.2. *Pour d sans facteur carré,*

$$|\mathcal{O}_d| = \prod_{\substack{p|d \\ p \equiv 1,3 \bmod 8}} \left(p^3 + p^2 - p - 1\right) \prod_{\substack{p|d \\ p \equiv 5,7 \bmod 8}} \left(p^3 - p^2 + p - 1\right)\,.$$

DÉMONSTRATION. Par la proposition 3.1.3, pour $p \geq 3$,

$$\mathcal{O}_p = \{v^t \in (\mathbb{Z}/p\mathbb{Z})^4 - \{0\} \text{ tel que } Q(v) \equiv 0 \bmod p\}\,.$$

Or, il est classique (voir par exemple [**BS66**]) que, pour une forme quadratique f en $2k$ variables de discriminant $\Delta \not\equiv 0 \bmod p$,

$$|\{x \in (\mathbb{Z}/p\mathbb{Z})^{2k} \text{ tel que } f(x) \equiv 0 \bmod p\}| = p^{2k-1} + (p-1)\left(\frac{(-1)^k\Delta}{p}\right)p^{k-1}\,,$$

où $\left(\frac{\cdot}{\cdot}\right)$ dénote le symbole de Legendre. Ainsi, dans le cas présent $\Delta = -2$ et on obtient :

$$|\mathcal{O}_p| = \begin{cases} p^3 + p^2 - p - 1 \text{ si } p \equiv 1, 3 \bmod 8\,, \\ p^3 - p^2 + p - 1 \text{ si } p \equiv 5, 7 \bmod 8\,. \end{cases}$$

Puisque $|\mathcal{O}_2| = 1$ par le lemme 3.1.1, on obtient le résultat escompté, en vertu de la proposition 3.1.2. □

Définition 3.1.2. *Pour $v \in \mathbb{R}^4$, soit $\max_1(v) = \max \tilde{v}$. Soient $\max_2(v)$ la deuxième plus grande entrée de $\tilde{v}$ et $\max_3(v)$ la troisième plus grande entrée de $\tilde{v}$. Soient*

$$B_1(T) = \left\{v \in \mathbb{R}^4 \text{ tel que } \max_1(v) \leq T\right\}\,,$$
$$B_i(T) = \left\{v \in \mathbb{R}^4 \text{ tel que } \max_i(v) \leq T \text{ et } \max_1(v) \leq 3T\right\} \text{ pour } i = 2, 3\,.$$

Remarque 13 : $\max_1(.)$ est une norme sur $\mathbb{R}^4$.

Remarque 14 : Si $v \in B_i(T)$ est tel que $Q(v) = 0$, alors la condition $\max_1(v) \leq 3T$ est automatiquement vérifiée. En effet, supposons, quitte à considérer $-v$, que $v_4 \geq 0$. Il est facile de voir que $\max_3(v) \geq v_4$. Sans perte de généralité, on peut supposer que $|v_1| = \max_1(v)$. Alors, $\max_1(v) \leq 2|v_4| + |2v_4 - v_1| \leq 3\max_3(v)$ puisque, par exemple pour des raisons géométriques (puisque v annule Q), $|2v_4 - v_1| \neq \max_2(v)$ (sauf si tous les $\max_i(v)$ sont égaux) et donc $|2v_4 - v_1| \leq \max_3(v)$.

Lemme 3.1.3. *Pour deux vecteurs u et v de $\mathbb{R}^4$ tels que $\max_1(v-u) \leq M$, on a*

$$|\max_1(v) - \max_1(u)| \leq M\,,\ |\max_2(v) - \max_2(u)| \leq 3M\,,\ |\max_3(v) - \max_3(u)| \leq 9M\,.$$

DÉMONSTRATION. Le résultat est trivial pour $\max_1$ par l'inégalité triangulaire. Supposons, sans perte de généralité, que $|u_1| = \max_2(u)$. On distingue trois cas :

- $|v_1| = \max_2(v)$. Or, $||v_1| - |u_1|| \leq |v_1 - u_1| \leq \max_1(v-u) \leq M$.
- $|v_1| = \max_1(v)$. Alors, $|\max_1(v) - \max_2(u)| = ||v_1| - |u_1|| \leq \max_1(v-u) \leq M$ et $|\max_1(v) - \max_1(u)| \leq M$. Notons $\tilde{u}'$ et $\tilde{v}'$ les vecteurs obtenus en supprimant la première ligne de $\tilde{u}$ et $\tilde{v}$. Alors, $|\max(\tilde{v}') - \max(\tilde{u}')| \leq \max_1(v-u) \leq M$ et $\max(\tilde{u}') = \max_1(u)$, $\max(\tilde{v}') = \max_2(v)$.

Ainsi,

$$|\max_2(v) - \max_2(u)| \leq |\max_2(v) - \max_1(u)| + |\max_1(v) - \max_1(u)| \\ + |\max_1(v) - \max_2(u)| \leq 3M\,.$$

• $|v_1|$ n'est ni $\max_1(v)$ ni $\max_2(v)$. Si $\max_2(v)$ et $\max_1(u)$ sont sur la même ligne dans $\tilde{u}$ et $\tilde{v}$, on est ramené au cas précédent. Sinon, on note $\tilde{u}'$ et $\tilde{v}'$ les vecteurs obtenus en supprimant la où les lignes de $\tilde{u}$ et $\tilde{v}$ contenant $\max_1(u)$ et $\max_1(v)$. Alors, $\max(\tilde{u}') = \max_2(u)$, $\max(\tilde{v}') = \max_2(v)$ et $|\max(\tilde{v}') - \max(\tilde{u}')| \leq \max_1(v-u) \leq M$.

La preuve pour $\max_3$ est semblable. □

Par la proposition 3.1.1, l'ensemble des courbures des cercles de l'empilement $\mathcal{P}$ (avec multiplicité) est exactement l'ensemble consistant en les trois entrées maximales de $\tilde{v}$ où v^t parcourt l'orbite $\tilde{\mathcal{A}}.v_{\mathcal{P}}^t$, en les trois entrées maximales de $\tilde{v}$ où v^t parcourt l'orbite $\tilde{\mathcal{A}}.S_{123}v_{\mathcal{P}}^t$ et en les entrées a_0, b_0, c_0 du sextuplé racine.

Définition 3.1.3. *Pour $T > 0$, on définit $N_{\mathcal{P}}(T)$ le nombre de cercles de courbures plus petites que T dans l'empilement.*

Alors, en utilisant les notations précédentes, on a :

Proposition 3.1.4.

$$N_{\mathcal{P}}(T) = \sum_{i=1}^{3} \left(\left| \tilde{\mathcal{A}}.v_{\mathcal{P}}^t \cap B_i(T) \right| + \left| \tilde{\mathcal{A}}.S_{123}v_{\mathcal{P}}^t \cap B_i(T) \right| \right) + 3\,.$$

3.2. Dénombrement dans les empilements apolloniens généralisés de cercles

Dans cette section, nous allons estimer $\left|\tilde{\mathcal{A}}.v_{\mathcal{P}}^t \cap B_i(T)\right|$. Nous pourrons en déduire une asymptotique pour $N_{\mathcal{P}}(T)$, l'estimation pour $\left|\tilde{\mathcal{A}}.S_{123}v_{\mathcal{P}}^t \cap B_i(T)\right|$ étant semblable. Il est à noter qu'un résultat similaire peut sans doute être déduit du travail de Mohammadi et Oh [**MO15**] et peut être obtenu à partir du travail effectué dans [**Vin14**].

Pour l'étude du groupe $\tilde{\mathcal{A}}$ et de sa préimage dans le double recouvrement spin, nous référons au travail de Zhang [**Zha13**] dont nous utiliserons les résultats comme outils.

Dans ce qui suit, on note δ la dimension de Hausdorff de l'empilement, c'est-à-dire la dimension de Hausdorff de son espace résiduel. D'après Larman, dans [**Lar67**], $\delta > 1,03$.

Remarque 15 : Expérimentalement, il semble que $\delta \approx 1,33$.

Remarque 16 : $\tilde{\mathcal{A}}$ étant d'indice fini dans $\mathcal{A}$, $\tilde{\mathcal{A}}$ et $\mathcal{A}$ ont la même dimension de Hausdorff.

Soit $G = \mathrm{PSL}_2(\mathbb{C})$ et sa décomposition d'Iwasawa $G = NAK$ (ou, de façon équivalente, $G = KAN$) avec

$$N = \left\{ n_x = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \text{ avec } x \in \mathbb{C} \right\} \quad , \quad A = \left\{ a_y = \begin{pmatrix} \sqrt{y} & 0 \\ 0 & \frac{1}{\sqrt{y}} \end{pmatrix} \text{ avec } y > 0 \right\} ,$$
$$K = PSU(2) = \left\{ M \in M_2(\mathbb{C}) \text{ telle que } {}^t\overline{M}M = I_2 \right\} .$$

Soit M le centralisateur de A dans K. Dans le cas présent,

$$M = \left\{ \begin{pmatrix} \mathrm{e}^{i\theta} & 0 \\ 0 & \mathrm{e}^{-i\theta} \end{pmatrix} \text{ avec } \theta \in [0, \pi) \right\} .$$

On note $H(x_1, x_2, x_3, x_4) = x_1^2 + x_2^2 + x_3^2 - x_4^2$ la forme de Lorentz. En procédant comme dans le chapitre 13.9 de [**Cas78**], on obtient l'isomorphisme suivant ρ de G dans le groupe de Lorentz restreint $\mathrm{SO}_H(\mathbb{R}) = \mathrm{SO}^+(1,3)$:

$$\begin{array}{ccc} \mathrm{PSL}_2(\mathbb{C}) & \xrightarrow{\rho} & \mathrm{SO}_H(\mathbb{R}) \\ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} & \longmapsto & \begin{pmatrix} \Re(\alpha\overline{\delta} + \beta\overline{\gamma}) & \Im(\alpha\overline{\delta} + \overline{\beta}\gamma) & \Re(-\alpha\overline{\gamma} + \beta\overline{\delta}) & \Re(\alpha\overline{\gamma} + \beta\overline{\delta}) \\ \Im(-\alpha\overline{\delta} - \beta\overline{\gamma}) & \Re(\alpha\overline{\delta} - \beta\overline{\gamma}) & \Im(\alpha\overline{\gamma} - \beta\overline{\delta}) & \Im(-\alpha\overline{\gamma} - \beta\overline{\delta}) \\ \Re(-\alpha\overline{\beta} + \gamma\overline{\delta}) & \Im(-\alpha\overline{\beta} + \gamma\overline{\delta}) & \frac{|\alpha|^2 - |\beta|^2 - |\gamma|^2 + |\delta|^2}{2} & \frac{-|\alpha|^2 - |\beta|^2 + |\gamma|^2 + |\delta|^2}{2} \\ \Re(\alpha\overline{\beta} + \gamma\overline{\delta}) & \Im(\alpha\overline{\beta} + \gamma\overline{\delta}) & \frac{-|\alpha|^2 + |\beta|^2 - |\gamma|^2 + |\delta|^2}{2} & \frac{|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2}{2} \end{pmatrix} \end{array} .$$

Or, $\mathrm{SO}_H(\mathbb{R})$ et $\mathrm{SO}_Q(\mathbb{R})$ sont isomorphes, l'isomorphisme ψ étant donné par

$$\begin{array}{ccc} \psi : \mathrm{SO}_H(\mathbb{R}) & \longrightarrow & \mathrm{SO}_Q(\mathbb{R}) \\ M & \longmapsto & J^{-1}MJ \end{array}$$

où

$$J = \begin{pmatrix} 1 & 0 & 0 & -1 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & \sqrt{2} \end{pmatrix} .$$

Soit $j : \mathrm{PSL}_2(\mathbb{C}) \to \mathrm{SO}_Q(\mathbb{R})$ tel que $j(B) = \psi(\rho(\mathfrak{m}B\mathfrak{m}^{-1}))$ où

$$\mathfrak{m} = \begin{pmatrix} 1+i & -\sqrt{2} \\ \sqrt{2} & 1+i \end{pmatrix} .$$

Comme observé dans [**Zha13**], la préimage de $\tilde{\mathcal{A}}$ par j est contenue dans $\mathrm{PSL}_2(\mathbb{Z}[i\sqrt{2}])$ et est géométriquement finie. Notons Υ cette préimage, et, pour un entier $q \in \mathbb{Z}$, on note $\Upsilon(q) = \{M \in \Upsilon \text{ telle que } M \equiv I_2 \bmod (q)\}$. Υ et les $\Upsilon(q)$ sont des sous-groupes discrets de $\mathrm{PSL}_2(\mathbb{C})$ (qu'on appelle groupes kleiniens).

Remarquons que les $\Upsilon(q)$ étant d'indice fini dans Υ, leurs ensembles limites ont la même dimension de Hausdorff que celui de Υ, c'est-à-dire δ, la dimension de Hausdorff de l'espace résiduel de l'empilement.

Soit Δ l'opérateur de Laplace associé à la métrique $\mathrm{d}\,s^2 = \frac{\mathrm{d}\,x^2+\mathrm{d}\,y^2+\mathrm{d}\,z^2}{z^2}$ sur $\mathbb{H}^3$,

$$\Delta = -z^2\left(\frac{\partial^2}{\partial x^2}+\frac{\partial^2}{\partial y^2}+\frac{\partial^2}{\partial z^2}\right)+z\frac{\partial}{\partial z}\,.$$

Puisque la dimension de Hausdorff $\delta > 1$, le travail de Sullivan [**Sul79a**] et Lax et Phillips [**LP82**] donne que la plus petite valeur propre de l'opérateur de Laplace sur $L^2\left(\Upsilon(q)\setminus\mathbb{H}^3\right)$ est $\lambda_0(q) = \delta(2-\delta)$ et est isolée. Si $\lambda_1(q)$ dénote la seconde plus petite valeur propre, alors le théorème 1.5 de [**Zha13**] donne :

Théorème 3.2.1 (Théorème du trou spectral)**.** *Il existe $\delta_0 > 0$ tel que, pour tout entier naturel q,*

$$\lambda_1(q) - \lambda_0(q) > \delta_0\,.$$

En notant $\lambda_1(q) = s_1(2-s_1)$, tout nombre positif $s_{\Upsilon(q)}$ tel que $0 < s_{\Upsilon(q)} < \delta - s_1$ sera appelé un trou spectral pour $\Upsilon(q)$. Le théorème 3.2.1 nous indique qu'un tel trou spectral peut être choisi uniformément en q.

Pour d sans facteur carré, soit $\tilde{\mathcal{A}}_{v_\mathcal{P}}(d) = \left\{\alpha\in\tilde{\mathcal{A}} \text{ tel que } \alpha v_\mathcal{P}^t \equiv v_\mathcal{P}^t \bmod d\right\}$. Notons $\Upsilon_{v_\mathcal{P}}(d)$ la préimage de $\tilde{\mathcal{A}}_{v_\mathcal{P}}(d)$ par j. Il est facile de vérifier que $\Upsilon(d)$ est contenu dans $\Upsilon_{v_\mathcal{P}}(d)$. Alors, puisque $\Upsilon(d)$ est d'indice fini dans $\Upsilon_{v_\mathcal{P}}(d)$, un trou spectral de $\Upsilon_{v_\mathcal{P}}(d)$ peut être choisi uniformément en d (puisque le spectre de l'opérateur de Laplace sur $L^2\left(\Upsilon_{v_\mathcal{P}}(d)\setminus\mathbb{H}^3\right)$ est contenu dans celui de l'opérateur de Laplace sur $L^2\left(\Upsilon(d)\setminus\mathbb{H}^3\right)$).

Remarquons qu'il existe un unique vecteur (à multiplication par un scalaire près) stabilisé par l'image de NM par j, et qu'il appartient au cone isotrope de Q. En effet, il est aisé de vérifier que $(0,0,-1,1)^t$ est le seul vecteur propre associé à la valeur propre 1 commun à toutes les matrices de l'image de NM par ρ. Or, le groupe orthogonal de Q agissant transitivement sur le cône isotrope, il existe donc un élément $R\in O_Q(\mathbb{R})$ tel que le stabilisateur de $Rv_\mathcal{P}^t$ par j soit NM. Quitte à remplacer $v_\mathcal{P}^t = (a_0,b_0,c_0,\omega_0)^t$ par $(b_0,a_0,c_0,\omega_0)^t$ (pour lequel les propriétés de la section 3.1 sont toujours vraies), on peut supposer que $R\in \mathrm{SO}_Q(\mathbb{R})$. Soit $\mathfrak{r}$ la préimage de R par j. On note :

$$\begin{array}{rccc} i : & \mathrm{PSL}_2(\mathbb{C}) & \longrightarrow & \mathrm{SO}_Q(\mathbb{R}) \\ & B & \longmapsto & j(\mathfrak{r}B\mathfrak{r}^{-1}) \end{array}\,.$$

Alors, i est un isomorphisme tel que $v_{\mathcal{P}}^t$ est stabilisé par NM. On note Γ la préimage de $\tilde{\mathcal{A}}$ dans G. Pour d sans facteur carré, on note $\Gamma_{v_{\mathcal{P}}}(d)$ la préimage de $\tilde{\mathcal{A}}_{v_{\mathcal{P}}}(d)$ dans G. Par ce qui précède, il existe s_0 un trou spectral de $\Gamma_{v_{\mathcal{P}}}(d)$, pour tout d sans facteur carré. Notons que les $\Gamma_{v_{\mathcal{P}}}(d)$ étant d'indices finis dans Γ, leurs ensembles limites ont la même dimension de Hausdorff que celle de $\tilde{\mathcal{A}}$, c'est-à-dire δ.

Afin de simplifier la notation, pour un vecteur ligne $v \in \mathbb{R}^4$ et pour $g \in G$, on notera vg en lieu et place de $i(g)v^t$. Dans ce contexte, estimer $\left|\tilde{\mathcal{A}}.v_{\mathcal{P}}^t \cap B_i(T)\right|$ revient à estimer $|v_{\mathcal{P}}\Gamma \cap B_i(T)|$. Nous allons en fait ici estimer, pour $\alpha \in \tilde{\mathcal{A}}$, la quantité $\left|\alpha\tilde{\mathcal{A}}_{v_{\mathcal{P}}}(d).v_{\mathcal{P}}^t \cap B_i(T)\right|$. Ainsi, ceci revient à estimer, pour $\gamma_0 \in \Gamma$, la quantité $|v_{\mathcal{P}}\Gamma_{v_{\mathcal{P}}}(d)\gamma_0 \cap B_i(T)|$.

Soit ν_o^Γ la mesure de Patterson-Sullivan sur l'ensemble limite $\Lambda(\Gamma)$ associée au point de base $o = (0, 0, 1) \in \mathbb{H}^3$, normalisée telle que $\|\phi_0\|_2 = 1$, où ϕ_0 est la fonction propre

$$\phi_0(n_x a_y) = \int_{u \in \Lambda(\Gamma)\setminus\{\infty\}} \left(\frac{(\|u\|^2+1)y}{\|x-u\|^2+y^2}\right)^\delta \mathrm{d}\,\nu_o^\Gamma(u)\,,$$

où $\Lambda(\Gamma)$ est vu comme un sous-ensemble de $\mathbb{C}\cup\{\infty\}$ (ϕ_0 est le vecteur propre de l'opérateur de Laplace associé à la valeur propre λ_0 précédente). Rappelons que cette mesure est finie et unique. Pour plus de détails sur la mesure de Patterson-Sullivan et sa construction, il est possible de se référer à la généralisation du travail de Patterson par Sullivan dans [**Sul79b**]. Comme K/M peut être identifié avec $\partial(\mathbb{H}^3)$, on peut considérer la mesure de Patterson-Sullivan sur K via la projection $K \to K/M$. Pour $f \in C(K)$,

$$\nu_o^\Gamma(f) = \int_{k\in K/M}\int_{m\in M} f(km)\,\mathrm{d}\,m\,\mathrm{d}\,\nu_o^\Gamma(k)$$

pour la mesure de probabilité de Haar $\mathrm{d}\,m$ sur M (M étant compact, toute mesure de Haar est finie et peut donc être normalisée). Pour une fonction $\psi \in C_c(G/M)$, on définit

$$\tilde{m}_{N,\Gamma}^{BR}(\psi) = \int_{KAN} \psi(ka_y n_x) y^{\delta-1}\,\mathrm{d}\,x\,\mathrm{d}\,y\,\mathrm{d}\,\nu_o^\Gamma(k)\,. \tag{3.2.1}$$

La mesure de Burger-Roblin $m_{N,\Gamma}^{BR}$ (associée au sous-groupe N) est la mesure sur $\Gamma\setminus G/M$ induite par $\tilde{m}_{N,\Gamma}^{BR}$.

Lemme 3.2.1.

$$\nu_o^{\Gamma_{v_{\mathcal{P}}}(d)} = \frac{1}{\sqrt{[\Gamma : \Gamma_{v_{\mathcal{P}}}(d)]}}\nu_o^\Gamma$$

Démonstration. Puisque $\Gamma_{v_{\mathcal{P}}}(d)$ est d'indice fini dans Γ, on a $\Lambda(\Gamma_{v_{\mathcal{P}}}(d)) = \Lambda(\Gamma)$. Le résultat suit alors de l'unicité et de la normalisation choisie de la mesure de Patterson-Sullivan. □

Soit $\mathcal{U}_\varepsilon = i^{-1}(B(\varepsilon))$, où $B(\varepsilon)$ est la boule de rayon ε autour de l'identité pour la norme sur les matrices 4×4 induite par $\max_1$, que l'on notera $\|.\|$. Nous aurons besoin du lemme suivant, que l'on peut par exemple trouver dans [**GOS10**] et qui donne l'uniforme continuité de la décomposition d'Iwasawa :

Lemme 3.2.2 (Strong wave front lemma)**.** *Il existe $0 < l < 1$ tel que, si $g = n_x a_y k$, alors*

$$gU_{l\varepsilon} \subset (n_x N_\varepsilon)(a_y A_\varepsilon)(kK_\varepsilon)$$

où $N_\varepsilon = N \cap U_\varepsilon$, $A_\varepsilon = A \cap U_\varepsilon$ et $K_\varepsilon = K \cap U_\varepsilon$.

Lemme 3.2.3. *Il existe $l > 0$ tel que, pour $i = 1, 2, 3$ on ait :*

$$B_i(T)\mathcal{U}_{l\varepsilon} \subset B_i((1+\varepsilon)T) \quad \text{et} \quad B_i((1-\varepsilon)T) \subset \cap_{g \in \mathcal{U}_{l\varepsilon}} B_i(T)g\,. \tag{3.2.2}$$

Démonstration. D'après le lemme 3.1.3, si $\max_1(v-u) \leq M$, alors

$$|\max_1(v) - \max_1(u)| \leq M\,,\ |\max_2(v) - \max_2(u)| \leq 3M\,,\ |\max_3(v) - \max_3(u)| \leq 9M\,.$$

Alors, pour $u \in B_i(T)$, $g \in \mathcal{U}_{l\varepsilon}$ et $v = ug$, on a

$$|\max_i(v) - \max_i(u)| \leq 3^{i-1} \max_1(v-u) \leq 3^{i-1} \max_1(u)\|g - e\|\,.$$

Ainsi, $\max_i(v) \leq (1 + 27l\varepsilon)T$ et donc $B_i(T)\mathcal{U}_{l\varepsilon} \subset B_i((1+\varepsilon)T)$ si $l \leq \frac{1}{27}$. Soit maintenant $v \in B_i((1-\varepsilon)T)$. Par continuité de $g \mapsto g^{-1}$, il existe l_0 tel que, pour tout $g \in \mathcal{U}_{l_0\varepsilon}$, on ait $g^{-1} \in \mathcal{U}_{l'\varepsilon}$ avec $l' \leq \frac{1}{27}$. Alors,

$$vg^{-1} \in B_i((1-\varepsilon)T)\mathcal{U}_{l'\varepsilon} \subset B_i((1-\varepsilon^2)T)\,. \tag{3.2.3}$$

Il suffit maintenant de prendre $l = \min(\frac{1}{27}, l_0)$. □

Un des éléments clés de la preuve sera le théorème suivant, prouvé dans [**LO13**] et ici appliqué à Γ, que nous appliquerons par la suite à $\Gamma_{v_\mathcal{P}}(d)$:

Théorème 3.2.2. *Pour tout $\psi \in C_c^\infty(\Gamma \setminus G)^M$, quand $y \to 0$,*

$$\int_{(N\cap\Gamma)\setminus N} \psi(n_x a_y)\,\mathrm{d}\,x = \kappa_\Gamma m_N^{BR}(\psi) y^{2-\delta} + O(\mathcal{S}_5(\psi) y^{2-\delta+\frac{2}{7}s_\Gamma})$$

où s_Γ est un trou spectral pour Γ,

$$\kappa_\Gamma = \int_{x\in\mathbb{R}^2} \frac{\mathrm{d}\,x}{(1+|x|^2)^\delta} \int_{n_x \in (N\cap\Gamma)\setminus N} (1+|x|^2)^\delta\,\mathrm{d}\,\nu_o(x)$$

et $\mathcal{S}_5(\psi)$ est la norme de Sobolev

$$\mathcal{S}_5(\psi) = \max\{\|Z_{i_1} \dots Z_{i_5}(\psi)\|_2, 1 \leq i_j \leq 6\}$$

pour $Z_1, \dots, Z_6$ une base orthonormale de l'algèbre de Lie de G.

Remarque 17 : Par ce qui précède, $\Gamma_{v_\mathcal{P}}(d)$ admet un trou spectral s_0 indépendant de d sans facteur carré. Ainsi, nous utiliserons ce trou spectral lorsque nous appliquerons le théorème précédent à $\Gamma_{v_\mathcal{P}}(d)$.

Proposition 3.2.1. *Pour tout $\gamma_0 \in \Gamma$,*

$$|v_\mathcal{P}\Gamma_{v_\mathcal{P}}(d)\gamma_0 \cap B_i(T)| = \frac{1}{\delta}\frac{\kappa_\Gamma}{[\Gamma : \Gamma_{v_\mathcal{P}}(d)]}T^\delta \int_{k\in K} \frac{\mathrm{d}\,\nu_o^\Gamma(k)}{\max_i(v_\mathcal{P}k)^\delta} + O(T^{\delta-\frac{2s_0}{63}})$$

où la constante impliquée est indépendante de d et γ_0.

Démonstration. G étant de dimension 6, il existe $\psi_\varepsilon \in C_c^\infty(G)$, supportée dans $U_{l\varepsilon}$, d'intégrale 1 et telle que $\mathcal{S}_5(\psi_\varepsilon) = O(\varepsilon^{-8})$ (en utilisant par exemple la construction classique à l'aide de $\exp(-\frac{1}{1-\|x\|^2})$ d'une unité approchée). On définit une unité approchée sur $\Gamma_{v_\mathcal{P}}(d) \setminus G$ par

$$\Psi_{\Gamma_{v_\mathcal{P}}(d),\varepsilon}(g) = \sum_{\gamma\in\Gamma_{v_\mathcal{P}}(d)} \psi_\varepsilon(\gamma g)\,.$$

Comme $N \cap \Gamma_{v_\mathcal{P}}(d) = N \cap \Gamma$, on peut définir $F_T^i(g) = \sum_{\gamma\in N\cap\Gamma\setminus\Gamma_{v_\mathcal{P}}(d)} \chi_{B_i(T)}(v_\mathcal{P}\gamma g)$. Alors,

$$|v_\mathcal{P}\Gamma_{v_\mathcal{P}}(d)\gamma_0 \cap B_i(T)| = F_T^i(\gamma_0)$$

et, par le lemme 3.2.3, pour tout $g \in U_{l\varepsilon}$,

$$F^i_{(1-\varepsilon)T}(\gamma_0 g) \le F_T^i(\gamma_0) \le F^i_{(1+\varepsilon)T}(\gamma_0 g)\,.$$

Ainsi, pour $\mathrm{d}\,g = y^{-3}\,\mathrm{d}\,x\,\mathrm{d}\,y\,\mathrm{d}\,k$ la mesure de Haar de G, avec $g = n_x a_y k$, on a :

$$\int_{\Gamma_{v_\mathcal{P}}(d)\setminus G} F^i_{(1-\varepsilon)T}(\gamma_0 g)\Psi_{\Gamma_{v_\mathcal{P}}(d),\varepsilon}(g)\,\mathrm{d}\,g \le F_T^i(\gamma_0) \le \int_{\Gamma_{v_\mathcal{P}}(d)\setminus G} F^i_{(1+\varepsilon)T}(\gamma_0 g)\Psi_{\Gamma_{v_\mathcal{P}}(d),\varepsilon}(g)\,\mathrm{d}\,g\,.$$

Nous allons seulement évaluer le terme de droite, le terme de gauche pouvant être traité de façon analogue.

$$\begin{aligned}
\int_{\Gamma_{v_\mathcal{P}}(d)\setminus G} F^i_{(1+\varepsilon)T}(\gamma_0 g)\Psi_{\Gamma_{v_\mathcal{P}}(d),\varepsilon}(g)\,\mathrm{d}\,g &= \int_{\Gamma_{v_\mathcal{P}}(d)\setminus G} F^i_{(1+\varepsilon)T}(g)\Psi_{\Gamma_{v_\mathcal{P}}(d),\varepsilon}(\gamma_0^{-1}g)\,\mathrm{d}\,g \\
&= \int_{\Gamma_{v_\mathcal{P}}(d)\setminus G} \sum_{\gamma\in N\cap\Gamma\setminus\Gamma_{v_\mathcal{P}}(d)} \chi_{B_i((1+\varepsilon)T)}(v_\mathcal{P}\gamma g)\Psi_{\Gamma_{v_\mathcal{P}}(d),\varepsilon}(\gamma_0^{-1}g)\,\mathrm{d}\,g \\
&= \int_{N\cap\Gamma\setminus G} \chi_{B_i((1+\varepsilon)T)}(v_\mathcal{P} g)\Psi_{\Gamma_{v_\mathcal{P}}(d),\varepsilon}(\gamma_0^{-1}g)\,\mathrm{d}\,g \\
&= \int_{a_yk\in AK} \chi_{B_i((1+\varepsilon)T)}(v_\mathcal{P} a_y k)\left(\int_{N\cap\Gamma\setminus N} \Psi^{\gamma_0}_{\Gamma_{v_\mathcal{P}}(d),\varepsilon}(n_x a_y k)\,\mathrm{d}\,x\right) y^{-3}\,\mathrm{d}\,y\,\mathrm{d}\,k
\end{aligned}$$

où $\Psi^{\gamma_0}_{\Gamma_{v_\mathcal{P}}(d),\varepsilon}(g) = \Psi_{\Gamma_{v_\mathcal{P}}(d),\varepsilon}(\gamma_0^{-1}g)$. Or, comme $v_\mathcal{P} a_y n_x m = v_\mathcal{P} n_{xy^{-1}} m a_y$, on a que $v_\mathcal{P} a_y$ est stabilisé par NM. Ainsi, $v_\mathcal{P} a_y$ est proportionnel à $v_\mathcal{P}$. Il est facile de vérifier que les valeurs propres de $i(a_y)$ sont $1, y$ et y^{-1} et que seul le vecteur propre associé à y^{-1} est stabilisé par NM.

D'où $v_{\mathcal{P}} a_y = y^{-1} v_{\mathcal{P}}$ et

$$\begin{aligned}
&\int_{\Gamma_{v_{\mathcal{P}}}(d)\backslash G} F^i_{(1+\varepsilon)T}(\gamma_0 g)\Psi_{\Gamma_{v_{\mathcal{P}}}(d),\varepsilon}(g)\,\mathrm{d}\,g \\
&\quad = \int_{k\in M\backslash K}\int_{(1+\varepsilon)Ty\geq \max_i(v_{\mathcal{P}}k)} \left(\int_{N\cap\Gamma\backslash N}\int_{m\in M} \Psi^{\gamma_0}_{\Gamma_{v_{\mathcal{P}}}(d),\varepsilon}(n_x a_y m k)\,\mathrm{d}\,m\,\mathrm{d}\,x\right) y^{-3}\,\mathrm{d}\,y\,\mathrm{d}\,k
\end{aligned}$$

puisque, comme noté dans la remarque 14, $v_{\mathcal{P}}k$ vérifie automatiquement la condition $\max_1(v) \leq 3T$, car $Q(v_{\mathcal{P}}) = 0$ et $i(k) \in \mathrm{SO}_Q(\mathbb{R})$. Soient

$$\Psi^{\gamma_0,k}_{\Gamma_{v_{\mathcal{P}}}(d),\varepsilon}(g) = \int_{m\in M} \Psi^{\gamma_0}_{\Gamma_{v_{\mathcal{P}}}(d),\varepsilon}(gmk)\,\mathrm{d}\,m \quad \text{et} \quad \psi^{\gamma_0,k}_{\varepsilon}(g) = \int_{m\in M} \psi^{\gamma_0}_{\varepsilon}(gmk)\,\mathrm{d}\,m\,.$$

À l'aide du théorème 3.2.2, on peut remplacer l'intégrale intérieure, pour obtenir

$$\begin{aligned}
&\int_{\Gamma_{v_{\mathcal{P}}}(d)\backslash G} F^i_{(1+\varepsilon)T}(\gamma_0 g)\Psi_{\Gamma_{v_{\mathcal{P}}}(d),\varepsilon}(g)\,\mathrm{d}\,g \\
&\quad = \frac{\kappa_{\Gamma_{v_{\mathcal{P}}}(d)}}{\delta}\left(\int_{k\in M\backslash K} \frac{m^{BR}_{N,\Gamma_{v_{\mathcal{P}}}(d)}(\Psi^{\gamma_0,k}_{\Gamma_{v_{\mathcal{P}}}(d),\varepsilon})}{\max_i(v_{\mathcal{P}}k)^\delta}\,\mathrm{d}\,k\right)(1+\varepsilon)^\delta T^\delta + O(\mathcal{S}_5(\psi_\varepsilon)T^{\delta-\frac{2}{7}s_0})\,.
\end{aligned}$$

Mais, d'après le lemme 3.2.1,

$$\kappa_{\Gamma_{v_{\mathcal{P}}}(d)} = \frac{\kappa_\Gamma}{\sqrt{[\Gamma:\Gamma_{v_{\mathcal{P}}}(d)]}}$$

et, par la Γ-invariance de $\tilde{m}^{BR}_{N,\Gamma}$,

$$\begin{aligned}
m^{BR}_{N,\Gamma_{v_{\mathcal{P}}}(d)}(\Psi^{\gamma_0,k}_{\Gamma_{v_{\mathcal{P}}}(d),\varepsilon}) &= \tilde{m}^{BR}_{N,\Gamma_{v_{\mathcal{P}}}(d)}(\psi^{\gamma_0,k}_\varepsilon) \\
&= \frac{1}{\sqrt{[\Gamma:\Gamma_{v_{\mathcal{P}}}(d)]}}\tilde{m}^{BR}_{N,\Gamma}(\psi^{\gamma_0,k}_\varepsilon) = \frac{1}{\sqrt{[\Gamma:\Gamma_{v_{\mathcal{P}}}(d)]}}\tilde{m}^{BR}_{N,\Gamma}(\psi^{k}_\varepsilon)\,.
\end{aligned}$$

Ainsi,

$$\begin{aligned}
\int_{k\in M\backslash K} \frac{m^{BR}_{N,\Gamma_{v_{\mathcal{P}}}(d)}(\Psi^{\gamma_0,k}_{\Gamma_{v_{\mathcal{P}}}(d),\varepsilon})}{\max_i(v_{\mathcal{P}}k)^\delta}\,\mathrm{d}\,k &= \frac{1}{\sqrt{[\Gamma:\Gamma_{v_{\mathcal{P}}}(d)]}}\int_{k'\in K}\int_{ANK} \frac{\psi_\varepsilon(k'a_y n_x k)}{\max_i(v_{\mathcal{P}}k)^\delta} y^{\delta-1}\,\mathrm{d}\,x\,\mathrm{d}\,y\,\mathrm{d}\,k\,\mathrm{d}\,\nu^\Gamma_o(k') \\
&= \frac{1}{\sqrt{[\Gamma:\Gamma_{v_{\mathcal{P}}}(d)]}}\int_{k'\in K}\int_G \frac{\psi_\varepsilon(k'g)}{\max_i(v_{\mathcal{P}}k(g))^\delta} y(g)^{\delta+2}\,\mathrm{d}\,g\,\mathrm{d}\,\nu^\Gamma_o(k') \\
&= \frac{1}{\sqrt{[\Gamma:\Gamma_{v_{\mathcal{P}}}(d)]}}\int_{k'\in K}\int_G \frac{\psi_\varepsilon(g)}{\max_i(v_{\mathcal{P}}k(k'^{-1}g))^\delta} y(k'^{-1}g)^{\delta+2}\,\mathrm{d}\,g\,\mathrm{d}\,\nu^\Gamma_o(k') \\
&= \frac{1}{\sqrt{[\Gamma:\Gamma_{v_{\mathcal{P}}}(d)]}}\int_{U_{l\varepsilon}} \psi_\varepsilon(g)\int_{k'\in K} \frac{y(k'^{-1}g)^{\delta+2}}{\max_i(v_{\mathcal{P}}k(k'^{-1}g))^\delta}\,\mathrm{d}\,\nu^\Gamma_o(k')\,\mathrm{d}\,g\,,
\end{aligned}$$

où $k(g)$ et $y(g)$ désignent les composantes en K et A de g dans la décomposition d'Iwasawa. D'après le lemme 3.2.2, les applications $g \mapsto k(g)$ et $g \mapsto y(g)$ sont uniformément continues sur G. De plus, comme $|\max_i(v) - \max_i(u)| \leq 3^{i-1}\max_1(v-u)$, l'application

$k \mapsto \max_i(v_{\mathcal{P}}k)$ est continue sur l'ensemble compact K. Ainsi, elle y est uniformément continue. Donc, il existe l tel que, si $g \in U_{l\varepsilon}$,

$$\frac{y(k'^{-1}g)^{\delta+2}}{\max_i(v_{\mathcal{P}}k(k'^{-1}g))^{\delta}} = \frac{1}{\max_i(v_{\mathcal{P}}k'^{-1})^{\delta}} + O(\varepsilon)\,.$$

Alors, puisque la mesure de Patterson-Sullivan est finie,

$$\int_{k\in M\backslash K} \frac{m^{BR}_{N,\Gamma_{v_{\mathcal{P}}}(d)}(\Psi^{\gamma_0,k}_{\Gamma_{v_{\mathcal{P}}}(d),\varepsilon})}{\max_i(v_{\mathcal{P}}k)^{\delta}}\,\mathrm{d}\,k = \frac{1}{\sqrt{[\Gamma:\Gamma_{v_{\mathcal{P}}}(d)]}}\int_{k\in K}\frac{\mathrm{d}\,\nu^{\Gamma}_o(k)}{\max_i(v_{\mathcal{P}}k)^{\delta}} + O(\varepsilon)$$

et

$$\begin{aligned}
&\int_{\Gamma_{v_{\mathcal{P}}}(d)\backslash G} F^i_{(1+\varepsilon)T}(\gamma_0 g)\Psi_{\Gamma_{v_{\mathcal{P}}}(d),\varepsilon}(g)\,\mathrm{d}\,g \\
&\qquad = \frac{1}{\delta}\frac{\kappa_\Gamma}{[\Gamma:\Gamma_{v_{\mathcal{P}}}(d)]}T^{\delta}\int_{k\in K}\frac{\mathrm{d}\,\nu^{\Gamma}_o(k)}{\max_i(v_{\mathcal{P}}k)^{\delta}} + O(\varepsilon T^{\delta} + \mathcal{S}_5(\psi_\varepsilon)T^{\delta-\frac{2}{7}s_0}) \\
&\qquad = \frac{1}{\delta}\frac{\kappa_\Gamma}{[\Gamma:\Gamma_{v_{\mathcal{P}}}(d)]}T^{\delta}\int_{k\in K}\frac{\mathrm{d}\,\nu^{\Gamma}_o(k)}{\max_i(v_{\mathcal{P}}k)^{\delta}} + O(\varepsilon T^{\delta} + \varepsilon^{-8}T^{\delta-\frac{2}{7}s_0}) \\
&\qquad = \frac{1}{\delta}\frac{\kappa_\Gamma}{[\Gamma:\Gamma_{v_{\mathcal{P}}}(d)]}T^{\delta}\int_{k\in K}\frac{\mathrm{d}\,\nu^{\Gamma}_o(k)}{\max_i(v_{\mathcal{P}}k)^{\delta}} + O(T^{\delta-\frac{2s_0}{63}})
\end{aligned}$$

puisque $\mathcal{S}_5(\psi_\varepsilon) = O(\varepsilon^{-8})$, en prenant ε tel que $\varepsilon T^{\delta} = \varepsilon^{-8}T^{\delta-\frac{2}{7}s_0}$. Ainsi,

$$F^i_T(\gamma_0) = \frac{1}{\delta}\frac{\kappa_\Gamma}{[\Gamma:\Gamma_{v_{\mathcal{P}}}(d)]}T^{\delta}\int_{k\in K}\frac{\mathrm{d}\,\nu^{\Gamma}_o(k)}{\max_i(v_{\mathcal{P}}k)^{\delta}} + O(T^{\delta-\frac{2s_0}{63}})\,.$$

□

Corollaire 3.2.1. *Soit $\alpha \in \tilde{\mathcal{A}}$. Alors,*

$$\begin{aligned}
\left|\alpha\tilde{\mathcal{A}}_{v_{\mathcal{P}}}(d).v^t_{\mathcal{P}} \cap B_i(T)\right| &= \frac{1}{\delta}\frac{\kappa_\Gamma}{[\Gamma:\Gamma_{v_{\mathcal{P}}}(d)]}T^{\delta}\int_{k\in K}\frac{\mathrm{d}\,\nu^{\Gamma}_o(k)}{\max_i(v_{\mathcal{P}}k)^{\delta}} + O(T^{\delta-\frac{2s_0}{63}})\,, \\
\left|\alpha\tilde{\mathcal{A}}_{v_{\mathcal{P}}}(d).S_{123}v^t_{\mathcal{P}} \cap B_i(T)\right| &= \frac{1}{\delta}\frac{\kappa_\Gamma}{[\Gamma:\Gamma_{v_{\mathcal{P}}}(d)]}T^{\delta}\int_{k\in K}\frac{\mathrm{d}\,\nu^{\Gamma}_o(k)}{\max_i(v_{\mathcal{P}}S^t_{123}k)^{\delta}} + O(T^{\delta-\frac{2s_0}{63}})\,,
\end{aligned}$$

où les constantes impliquées sont indépendantes de d et α.

Démonstration. De manière analogue à ce qui précède, il nous faut fixer une représentation $i' : G \to \mathrm{SO}_Q(\mathbb{R})$ telle que le stabilisateur de $S_{123}v^t_{\mathcal{P}}$ dans G soit NM. Or, clairement, puisque i était telle que le stabilisateur de $v_{\mathcal{P}}$ dans G était NM, on peut prendre i' telle que $i'(g) = S_{123}i(g)S_{123}$. Mais alors, puisque $S_{123}\tilde{\mathcal{A}}S_{123} = \tilde{\mathcal{A}}$, la préimage de $\tilde{\mathcal{A}}$ par i' est à nouveau Γ. De plus, $\tilde{\mathcal{A}}_{S_{123}v_{\mathcal{P}}}(d) = S_{123}\tilde{\mathcal{A}}_{v_{\mathcal{P}}}(d)S_{123}$. Ainsi, la proposition 3.2.1 nous donne le résultat. □

De ce qui précède, on obtient immédiatement le corollaire suivant :

Corollaire 3.2.2.

$$N_{\mathcal{P}}(T) = \frac{\kappa_\Gamma}{\delta} T^\delta \int_{k\in K} \sum_{i=1}^{3} \left(\frac{1}{\max_i(v_{\mathcal{P}}k)^\delta} + \frac{1}{\max_i(v_{\mathcal{P}}S_{123}^t k)^\delta} \right) \mathrm{d}\,\nu_o^\Gamma(k) + O(T^{\delta-\frac{2s_0}{63}})\,.$$

Afin de dénombrer les nombres premiers apparaissant comme courbures dans l'empilement, nous allons utiliser le corollaire qui suit :

Corollaire 3.2.3. *Par le lemme 3.1.1, $v_{\mathcal{P}}^t$ a exactement deux de ses trois premières entrées paires. Notons j_1 et j_2 leurs indices. Soient d sans facteur carré et $1 \leq j \leq 6$. Soit $M_{\mathcal{P}}^{j,d}(T)$ le nombre de vecteurs v^t de $\mathcal{A}.v_{\mathcal{P}}^t \cap B_3(T)$ tels que la j-ième coordonnée de $\tilde{v}$ soit divisible par d. Alors, si d est pair et $j \neq j_1, j_2, j_1+3, j_2+3$, $M_{\mathcal{P}}^{j,d}(T) = 0$. Sinon,*

$$M_{\mathcal{P}}^{j,d}(T) = \frac{\kappa_\Gamma}{\delta} g(d) T^\delta \int_{k\in K} \left(\frac{1}{\max_3(v_{\mathcal{P}}k)^\delta} + \frac{1}{\max_3(v_{\mathcal{P}}S_{123}^t k)^\delta} \right) \mathrm{d}\,\nu_o^\Gamma(k) + O(d^2 T^{\delta-\frac{2s_0}{63}})$$

avec

$$g(d) = \prod_{\substack{p\mid d \\ p\equiv 1,3 \bmod 8}} \left(\frac{1}{p+1}\right) \prod_{\substack{p\mid d \\ p\equiv 5,7 \bmod 8}} \left(\frac{p+1}{p^2+1}\right)\,.$$

Démonstration. On note

$$f_j(v^t) = \begin{cases} v_j \text{ si } 1 \leq j \leq 3\,, \\ 2v_4 - v_{j-3} \text{ si } 4 \leq j \leq 6\,. \end{cases}$$

Alors,

$$M_{\mathcal{P}}^{j,d}(T) = \sum_{\substack{\alpha\in\tilde{\mathcal{A}}_{v_{\mathcal{P}}}(d)\backslash\tilde{\mathcal{A}} \\ f_j(\alpha v_{\mathcal{P}}^t)\equiv 0 \bmod d}} \left|\alpha\tilde{\mathcal{A}}_{v_{\mathcal{P}}}(d).v_{\mathcal{P}}^t \cap B_3(T)\right| + \sum_{\substack{\alpha\in\tilde{\mathcal{A}}_d\backslash\tilde{\mathcal{A}} \\ f_j(\alpha S_{123}v_{\mathcal{P}}^t)\equiv 0 \bmod d}} \left|\alpha\tilde{\mathcal{A}}_{v_{\mathcal{P}}}(d).S_{123}v_{\mathcal{P}}^t \cap B_3(T)\right|$$

et, en utilisant le corollaire 3.2.1, on est ainsi amené à étudier les quantités suivantes :

$$[\Gamma : \Gamma_{v_{\mathcal{P}}}(d)] \quad , \quad \sum_{\substack{\alpha\in\tilde{\mathcal{A}}_{v_{\mathcal{P}}}(d)\backslash\tilde{\mathcal{A}} \\ f_j(\alpha v_{\mathcal{P}}^t)\equiv 0 \bmod d}} 1 \quad , \quad \sum_{\substack{\alpha\in\tilde{\mathcal{A}}_d\backslash\tilde{\mathcal{A}} \\ f_j(\alpha S_{123}v_{\mathcal{P}}^t)\equiv 0 \bmod d}} 1\,.$$

Par le lemme 3.1.2,

$$[\Gamma : \Gamma_{v_{\mathcal{P}}}(d)] = |\mathcal{O}_d| = \prod_{\substack{p\mid d \\ p\equiv 1,3 \bmod 8}} \left(p^3+p^2-p-1\right) \prod_{\substack{p\mid d \\ p\equiv 5,7 \bmod 8}} \left(p^3-p^2+p-1\right)\,.$$

On s'intéresse maintenant à la somme

$$\sum_{\substack{\alpha\in\tilde{\mathcal{A}}_{v_\mathcal{P}}(d)\backslash\tilde{\mathcal{A}}\\ f_j(\alpha v_\mathcal{P}^t)\equiv 0 \bmod d}} 1 = \left|\left\{v\in\mathcal{O}_d \text{ tel que } f_j(v^t)\equiv 0 \bmod d\right\}\right|.$$

On définit :

$$\alpha_j(p) = \begin{cases} \left|\left\{v\in(\mathbb{Z}/p\mathbb{Z})^4-\{0\} \text{ tel que } f_j(v^t)\equiv 0 \bmod p \text{ et } Q(v)\equiv 0 \bmod p\right\}\right| & \text{si } p\neq 2\,,\\ 1 \text{ si } p=2 \text{ et } j=j_1,j_2,j_1+3,j_2+3\,,\\ 0 \text{ sinon}\,. \end{cases}$$

Pour $p\neq 2$, on a $\alpha_j(p)=p^2-1$ et, par les propositions 3.1.2 et 3.1.3,

$$\sum_{\substack{\alpha\in\tilde{\mathcal{A}}_{v_\mathcal{P}}(d)\backslash\tilde{\mathcal{A}}\\ f_j(\alpha v_\mathcal{P}^t)\equiv 0 \bmod d}} 1 = \prod_{p|d}\alpha_j(p)\,.$$

Ainsi,

$$\frac{1}{[\Gamma:\Gamma_{v_\mathcal{P}}(d)]}\sum_{\substack{\alpha\in\tilde{\mathcal{A}}_{v_\mathcal{P}}(d)\backslash\tilde{\mathcal{A}}\\ f_j(\alpha v_\mathcal{P}^t)\equiv 0 \bmod d}} 1 = g(d) \quad \text{et} \quad \sum_{\substack{\alpha\in\tilde{\mathcal{A}}_{v_\mathcal{P}}(d)\backslash\tilde{\mathcal{A}}\\ f_j(\alpha v_\mathcal{P}^t)\equiv 0 \bmod d}} 1 \ll d^2\,.$$

On s'intéresse maintenant à la somme

$$\sum_{\substack{\alpha\in\tilde{\mathcal{A}}_{S_{123}v_\mathcal{P}}(d)\backslash\tilde{\mathcal{A}}\\ f_j(\alpha v_\mathcal{P}^t)\equiv 0 \bmod d}} 1\,.$$

Mais, puisque $\tilde{\mathcal{A}}.S_{123}v_\mathcal{P}^t = S_{123}\tilde{\mathcal{A}}.v_\mathcal{P}^t$, l'orbite $\tilde{\mathcal{A}}.S_{123}v_\mathcal{P}^t \bmod d$ est simplement $S_{123}\mathcal{O}_d$. Donc, par les propositions 3.1.2, 3.1.3, le lemme 3.1.1 et le fait que S_{123} est trivial modulo 2, on a, pour d sans facteur carré,

$$S_{123}\mathcal{O}_d \simeq \mathcal{O}_2\prod_{\substack{p|d\\ p\neq 2}}\mathcal{C}_p$$

où $\mathcal{C}_p$ est le cône $\{v\in(\mathbb{Z}/p\mathbb{Z})^4-\{0\} \text{ tel que } Q(v)\equiv 0 \bmod p\}$. Ainsi, comme précédemment,

$$\frac{1}{[\Gamma:\Gamma_{v_\mathcal{P}}(d)]}\sum_{\substack{\alpha\in\tilde{\mathcal{A}}_{S_{123}v_\mathcal{P}}(d)\backslash\tilde{\mathcal{A}}\\ f_j(\alpha v_\mathcal{P}^t)\equiv 0 \bmod d}} 1 = g(d)$$

et

$$\sum_{\substack{\alpha\in\tilde{\mathcal{A}}_{S_{123}v_\mathcal{P}}(d)\backslash\tilde{\mathcal{A}}\\ f_j(\alpha v_\mathcal{P}^t)\equiv 0 \bmod d}} 1 \ll d^2\,.$$

□

3.3. Applications

3.3.1. Dénombrement des courbures premières

Des résultats précédents, il est possible d'obtenir très simplement une borne sur le nombre de courbures premières de l'empilement plus petites que T. Pour ce faire, nous utilisons le crible de Selberg, rappelé ci-dessous (voir par exemple [**IK04**] pour plus de détails) :

Théorème 3.3.1 (Le crible de Selberg)**.** *Soient $A = (a_n)_n$ une suite de nombres réels positifs et P un produit fini de nombres premiers. Soient*

$$S(A,P) = \sum_{\text{pgcd}\,(n,P)=1} a_n$$

et, pour tout entier $d|P$, $A_d = \{a_n \text{ tel que } n \equiv 0 \bmod d\}$. Supposons qu'il existe $\chi > 1$ et une fonction multiplicative g définie sur les entiers sans facteur carré avec $0 < g(p) < 1$ pour $p|P$ telle que, pour tout entier sans facteur carré $d|P$,

$$|A_d| = g(d)\chi + r_d(A)\,.$$

Soit h la fonction multiplicative définie par $h(p) = \frac{g(p)}{1-g(p)}$.

Alors, pour tout $D > 1$,

$$S(A,P) \leq \chi \left(\sum_{\substack{d<\sqrt{D} \\ d|P}} h(d) \right)^{-1} + \sum_{\substack{d<D \\ d|P}} \tau_3(d)|r_d(A)|\,,$$

où $\tau_3(d)$ dénote le nombre de représentations de d comme produit de trois entiers.

Proposition 3.3.1. *Soit $\pi_{\mathcal{P}}(T)$ le nombre de cercles de l'empilement de courbures premières et $\leq T$. Alors,*

$$\pi_{\mathcal{P}}(T) \ll \frac{T^\delta}{\log T}\,.$$

Démonstration. Soit $A^j = A^j(T) = (a_n^j)_n$ où

$$a_n^j = \begin{cases} |v \in \mathcal{A}.v_{\mathcal{P}}^t \cap B_3(T) \text{ tel que } \tilde{v}_j = n|\,, \\ 0 \text{ sinon}\,. \end{cases}$$

Alors, pour d sans facteur carré, le corollaire 3.2.3 donne

$$\left|A_d^j\right| = g_j(d)\chi + r_d(A^j)$$

avec

$$g_j(d) = \begin{cases} 0 \text{ si } d \text{ est pair et } j \neq j_1, j_2, j_1+3, j_2+3\,, \\ \displaystyle\prod_{\substack{p\mid d \\ p\equiv 1,3 \bmod 8}} \left(\frac{1}{p+1}\right) \prod_{\substack{p\mid d \\ p\equiv 5,7 \bmod 8}} \left(\frac{p+1}{p^2+1}\right) \text{ sinon}\,, \end{cases}$$

$$r_d(A^j) = O(d^2 T^{\delta - \frac{2s_0}{63}})$$

et

$$\chi = \frac{\kappa_\Gamma}{\delta} T^\delta \int_{k\in K} \left(\frac{1}{\max_3(v_{\mathcal{P}} k)^\delta} + \frac{1}{\max_3(v_{\mathcal{P}} S_{123}^t k)^\delta} \right) \mathrm{d}\,\nu_o^\Gamma(k)\,.$$

Alors, pour $D = T^{\frac{2s_0}{252}}$ et $P = \prod_{p\leq D} p$,

$$\sum_{\substack{d<D \\ d\mid P}} \tau_3(d) |r_d(A^j)| \ll \left(D^3 \log^2 D\right) T^{\delta - \frac{2s_0}{63}} \ll \frac{T^\delta}{\log T}\,.$$

Puisque $g_j(p) = \frac{1}{p} + O\left(\frac{1}{p^2}\right)$, on a

$$\sum_{p\leq x} g_j(p) \log p = \log x + O(1)\,,$$
$$\sum_{p} g_j(p)^2 \log p < \infty\,,$$

et donc, en utilisant par exemple le chapitre 6.6 de [**IK04**], on obtient

$$\sum_{\substack{d<\sqrt{D} \\ d\mid P}} h_j(d) \gg \log D \gg \log T\,.$$

Ainsi, le théorème 3.3.1 donne :

$$S(A^j(T), P) \ll \frac{T^\delta}{\log T}\,.$$

Mais,

$$\pi_{\mathcal{P}}(T) \leq \sum_{j=1}^{6} S(A^j(T), P) \ll \frac{T^\delta}{\log T}\,.$$

□

Remarque 18 : Il serait plus précis d'utiliser la suite $A^j = A^j(T) = (a_n^j)_n$ où

$$a_n^j = \begin{cases} |v \in \mathcal{A}.v_{\mathcal{P}}^t \cap B_3(T) \text{ tel que } \tilde{v}_j = n| \text{ si } n \leq T\,, \\ 0 \text{ sinon}\,. \end{cases}$$

Pour obtenir une asymptotique du type

$$\left|A_d^j\right| = g_j(d)\chi + r_d(A^j)\,, \tag{3.3.1}$$

on peut procéder comme dans la preuve de la section précédente, en calculant le cardinal $\left|v_{\mathcal{P}}\Gamma_{v_{\mathcal{P}}}(d)\gamma_0 \cap B_3^j(T)\right|$, où $B_3^j(T)$ est l'ensemble des vecteurs $v \in B_3(T)$ tels que $\tilde{v}_j \leq T$. Alors,

$$\left|v_{\mathcal{P}}\Gamma_{v_{\mathcal{P}}}(d)\gamma_0 \cap B_3^j(T)\right| = \frac{1}{\delta}\frac{\kappa_\Gamma}{[\Gamma : \Gamma_{v_{\mathcal{P}}}(d)]}T^\delta \int_{k\in K} \frac{\mathrm{d}\,\nu_o^\Gamma(k)}{\max\left(\max_3(v_{\mathcal{P}}k), (\widetilde{v_{\mathcal{P}}k})_j\right)^\delta} + O(T^{\delta-\frac{2s_0}{63}})$$

et donc une égalité du type (3.3.1) existe avec g_j et r_d comme dans le corollaire 3.2.3 et

$$\chi = \frac{\kappa_\Gamma}{\delta}T^\delta \int_{k\in K} \frac{\mathrm{d}\,\nu_o^\Gamma(k)}{\max\left(\max_3(v_{\mathcal{P}}k), (\widetilde{v_{\mathcal{P}}k})_j\right)^\delta}\,.$$

Toutefois, cela n'améliorerait pas le résultat de la proposition 3.3.1.

3.3.2. Un résultat du type Erdős-Kac

L'un des objectifs initiaux de l'auteur de cette thèse était d'obtenir un théorème du type Erdős-Kac pour les empilements généralisés, à savoir déterminer la distribution de la fonction ω sur les courbures d'un empilement. Comme nous le verrons plus tard, le résultat escompté n'a pas pu être prouvé, toutefois un résultat analogue au résultat de Djanković sur les empilements de cercles apolloniens dans [**Dja11**] est démontré ici. Plus précisément, il est possible d'obtenir une estimation, bien moins éclairante, sur la distribution des facteurs premiers des entrées des vecteurs de l'orbite $\mathcal{A}.v_{\mathcal{P}}^t$. On dénote $B\mathcal{P}_j(T) = \{\tilde{v}_j, v^t \in \mathcal{A}.v_{\mathcal{P}}^t \cap B_3(T)\}$ (avec multiplicité).

Proposition 3.3.2. *Pour tout $\alpha \leq \beta$,*

$$\lim_{T\to\infty} \frac{1}{|B\mathcal{P}_j(T)|}|a \in B\mathcal{P}_j(T) \text{ tel que } \alpha \leq \frac{\omega(a) - \log\log T}{\sqrt{\log\log T}} \leq \beta| = \frac{1}{\sqrt{2\pi}}\int_\alpha^\beta \mathrm{e}^{-\frac{t^2}{2}}\,\mathrm{d}\,t\,.$$

On peut espérer mener la preuve d'un tel résultat en procédant à la manière de Granville et Soundararajan dans [**GS07**]. Dans cet article, les auteurs étudient la distribution de la fonction ω sur des suites dans un contexte de crible. On rappelle ci-dessous leur proposition 3, adaptée ici aux notations utilisées précédemment dans l'énoncé du crible de Selberg (théorème 3.3.1).

Soit $A = (a_n)_n$ une suite de nombres réels positifs et P un produit fini de nombres premiers. Pour tout entier d, on définit $A_d = \{a_n \text{ tel que } n \equiv 0 \bmod d\}$. Supposons qu'il existe $\chi > 1$ et une fonction multiplicative g définie sur les entiers sans facteur carré telle

que, pour tout entier sans facteur carré d,

$$|A_d| = g(d)\chi + r_d\,.$$

On définit

$$\mu_P = \sum_{p|P} g(p) \quad \text{et} \quad \sigma_P^2 = \sum_{p|P} g(p)(1-g(p))\,.$$

Soit $\omega_P(a)$ le nombre de facteurs premiers de P qui divisent a.

Proposition 3.3.3 (Granville-Soundararajan)**.** *Uniformément pour tous les entiers naturels $k \leq \sigma_P^{\frac{2}{3}}$, on a :*

$$\sum_{a\in A} (\omega_P(a) - \mu_P)^k = C_k \chi \sigma_P^k \left(1 + O\left(\frac{k^3}{\sigma_P^2}\right)\right) + O\left(\mu_P^k \sum_{d\in D_k(P)} |r_d|\right)$$

si k est pair, et

$$\sum_{a\in A} (\omega_P(a) - \mu_P)^k \ll C_k \chi \sigma_P^k \frac{k^{\frac{3}{2}}}{\sigma_P} + \mu_P^k \sum_{d\in D_k(P)} |r_d|$$

si k est impair, où $D_k(P)$ dénote l'ensemble des entiers sans facteur carré produits d'au plus k nombres premiers divisant P et $C_k = \Gamma(k+1)/\left(2^{k/2}\Gamma(k/2+1)\right)$.

Preuve de la proposition 3.3.2. À l'aide du corollaire 3.2.3, on obtient

$$|B\mathcal{P}_j(T)| = c_{\mathcal{P}} N_{\mathcal{P}}(T) + O(T^{\delta - \frac{2s_0}{63}})$$

avec

$$c_{\mathcal{P}} = \left(\int_{k\in K} \left(\frac{1}{\max_3(v_{\mathcal{P}}k)^\delta} + \frac{1}{\max_3(v_{\mathcal{P}}S_{123}^t k)^\delta}\right) \mathrm{d}\,\nu_o^\Gamma(k)\right) \times \left(\int_{k\in K} \sum_{i=1}^{3} \left(\frac{1}{\max_i(v_{\mathcal{P}}k)^\delta} + \frac{1}{\max_i(v_{\mathcal{P}}S_{123}^t k)^\delta}\right) \mathrm{d}\,\nu_o^\Gamma(k)\right)^{-1}.$$

Le corollaire 3.2.3 nous donne donc

$$\sum_{\substack{a\in B\mathcal{P}_j(T)\\ d|a}} 1 = g_j(d)|B\mathcal{P}_j(T)| + r_d$$

avec

$$g_j(d) = \begin{cases} 0 \text{ si } d \text{ est pair et } j \neq j_1, j_2, j_1+3, j_2+3\,, \\ \displaystyle\prod_{\substack{p|d\\ p\equiv 1,3 \bmod 8}} \left(\frac{1}{p+1}\right) \prod_{\substack{p|d\\ p\equiv 5,7 \bmod 8}} \left(\frac{p+1}{p^2+1}\right) \text{ sinon}\,, \end{cases}$$

$$r_d = O(d^2 T^{\delta - \frac{2s_0}{63}})\,.$$

Soit $P = \prod_{p \leq z} p$. On désire appliquer la proposition 3.3.3 avec $z = T^{1/s}$ pour un certain $s > 0$. On remarque que

$$\mu_P = \sum_{p \leq z} g_j(p) = \log\log z + O(1)\,,$$
$$\sigma_P^2 = \sum_{p \leq z} g_j(p)\,(1 - g_j(p)) = \log\log z + O(1)\,,$$

et que, pour $a \in B\mathcal{P}_j(T)$ (et donc $a \leq 3T$),

$$\omega(a) - \log\log T = \omega_P(a) - \mu_P + O(s)\,.$$

Donc, pour une certaine constante c positive,

$$\sum_{a \in B\mathcal{P}_j(T)} (\omega(a) - \log\log T)^k = \sum_{a \in B\mathcal{P}_j(T)} (\omega_P(a) - \mu_P)^k + O\left(\sum_{l=0}^{k-1} \binom{l}{k} (cs)^{k-l} \Big| \sum_{a \in B\mathcal{P}_j(T)} (\omega_P(a) - \mu_P)^l \Big|\right)\,.$$

Alors, la proposition 3.3.3 permet d'estimer chacune des sommes en jeu. Pour k fixé, on obtient, pour $0 \leq l \leq k$, si l est pair :

$$\sum_{a \in B\mathcal{P}_j(T)} (\omega_P(a) - \mu_P)^l = C_l (\log\log T)^{l/2} |B\mathcal{P}_j(T)| + O\left(\left(\frac{\log\log T}{\log T}\right)^l T^{\delta - \frac{2s_0}{63} + \frac{3l}{s}}\right)$$

et si l est impair :

$$\sum_{a \in B\mathcal{P}_j(T)} (\omega_P(a) - \mu_P)^l \ll (\log\log T)^{(l-1)/2} T^\delta + \left(\frac{\log\log T}{\log T}\right)^l T^{\delta - \frac{2s_0}{63} + \frac{3l}{s}}\,.$$

Alors, si $s = \frac{189k}{2s_0} - \varepsilon$ pour un $\varepsilon > 0$,

(3.3.2)

$$\sum_{a \in B\mathcal{P}_j(T)} (\omega(a) - \log\log T)^k = \begin{cases} O\left((\log\log T)^{(k-1)/2} T^\delta\right) & \text{si } k \text{ est impair}\,, \\ C_k (\log\log T)^{k/2} |B\mathcal{P}_j(T)| + O((\log\log T)^{(k-1)/2} T^\delta) & \text{sinon}\,, \end{cases}$$

et donc

$$\frac{1}{|B\mathcal{P}_j(T)|} \sum_{a \in B\mathcal{P}_i(T)} \left(\frac{\omega(a) - \log\log T}{\sqrt{\log\log T}}\right)^k \to \begin{cases} \frac{k!}{2^{k/2}\left(\frac{k}{2}\right)!} \text{ si } k \text{ est pair}\,, \\ 0 \text{ si } k \text{ est impair}\,. \end{cases}$$

quand $T \to \infty$. La méthode des moments permet alors de conclure au théorème. □

Le résultat de la proposition 3.3.2 est évidemment bien plus faible que celui escompté, puisque l'ensemble $B\mathcal{P}_j(T)$ peut contenir, à priori, beaucoup de répétitions des courbures apparaissant en j-ième coordonnée. Toutefois, notons que l'équation (3.3.2) donne

$$\sum_{a\in B\mathcal{P}_j(T)} (\omega(a) - \log\log T)^2 = O\left((\log\log T)T^{\delta}\right) .$$

En particulier, on obtient qu'avec au plus $o\left(N_{\mathcal{P}}(T)\right)$ exceptions, pour tout $a \in B\mathcal{P}_j(T)$, on a $|\omega(a) - \log\log T| < \varepsilon \log\log T$.

On note $A\mathcal{P}(T)$ le multiensemble des courbures plus petites que T apparaissant dans $\mathcal{P}$. Puisque $A\mathcal{P}(T)$ est contenu dans l'union des $B\mathcal{P}_j(T)$, on peut en déduire un résultat du type Hardy–Ramanujan pour les empilements généralisés :

Proposition 3.3.4. *Avec au plus $o\left(N_{\mathcal{P}}(T)\right)$ exceptions, pour tout cercle C de l'empilement de courbure $a(C) \leq T$, on a $|\omega(a(C)) - \log\log T| < \varepsilon \log\log T$.*

Pour $1 \leq j \leq 6$, on note $A\mathcal{P}_j(X)$ le multiensemble des entrées plus petites que T apparaissant comme $\max_1$, $\max_2$ ou $\max_3$ en position j dans $\tilde{v}$, pour v parcourant l'orbite $\mathcal{A}.v^t_{\mathcal{P}}$. Alors,

$$A\mathcal{P}(T) = \biguplus_{j=1}^{6} A\mathcal{P}_j(T)$$

où $\uplus$ désigne l'union des multiensembles (avec répétition des éléments communs). Afin d'obtenir pour les empilements généralisés un résultat du type Erdős-Kac véritablement significatif, il nous faudrait être capable d'estimer le nombre d'éléments de $A\mathcal{P}_j(T)$ divisibles par d.

On s'attendrait naturellement à ce qu'il n'y ait pas de biais particulier en ce qui concerne les positions où apparaissent les $\max_i$ et que ces évènements soient indépendants du fait d'être divisible par d et plus petit que T. Ainsi, on espèrerait pouvoir trouver un résultat du type

$$\sum_{\substack{a\in A\mathcal{P}_j(T)\\ d|a}} 1 = \frac{f_j(d)}{6} N_{\mathcal{P}}(T) + r_d \tag{3.3.3}$$

avec r_d petit et $f_j(d)$ multiplicative. Alors,

$$\sum_{\substack{a\in A\mathcal{P}(T)\\ d|a}} 1 = \frac{N_{\mathcal{P}}(T)}{6} \sum_{j=1}^{6} f_j(d) + r_d\,.$$

Soit $\mu_P = \frac{1}{6}\sum_{p\leq z}\sum_{j=1}^{6} f_j(p)$ et $\sigma_P^2 = \frac{1}{6}\sum_{p\leq z}\sum_{j=1}^{6} f_j(p)\left(1-f_j(p)\right)$. Appliquer la proposition 3.3.3 permet d'estimer les sommes $\sum_{a\in A\mathcal{P}(T)}\left(\omega_P(a)-\mu_P\right)^k$ pour $k \leq \sigma_P^{\frac{2}{3}}$. Mais, si z est une puissance de T, μ_P et σ_P^2 devraient être proches de $\log\log T$. Ainsi, des calculs similaires à ceux qui précèdent devraient ainsi permettre de conclure à un théorème du type Erdős-Kac.

Malheureusement, l'auteur de cette thèse n'a pas été en mesure d'obtenir un résultat du type de l'équation (3.3.3).

Deuxième partie

Distribution angulaire dans les extensions quadratiques imaginaires

Chapitre 4

NOMBRES IDÉAUX ET THÉORÈME DES NOMBRES IDÉAUX PREMIERS DANS LES SECTEURS

Le concept de *nombres idéaux*, introduit par Hecke dans [**Hec18**, **Hec20**], est basé sur une idée issue du travail de Kummer sur les corps cyclotomiques. Celle-ci est d'associer à un corps de nombres $\mathbb{K}$ un système $\mathbb{K}^*(\omega_1, \ldots, \omega_k)$ de nombres idéaux (dont la construction est explicitée ci-dessous), tel que $\mathbb{K}^*(\omega_1, \ldots, \omega_k)/\mathbb{K}^*$ est isomorphe au groupe des classes d'idéaux de $\mathbb{K}$ et tel que tout idéal de $\mathbb{K}$ est principal dans l'anneau des entiers de $\mathbb{K}(\omega_1, \ldots, \omega_k)$.

Soit $\mathbb{K}$ un corps de nombres de degré $n = r_1 + 2r_2$, où r_1 est le nombre de plongements réels et r_2 le nombre de plongements complexes. Soit h son nombre de classes, soit $\mathcal{O}_\mathbb{K}$ son anneau des entiers et soit $\mathcal{U}$ l'ensemble des unités de $\mathcal{O}_\mathbb{K}$. Dans ce qui suit, tous les idéaux (entiers ou fractionnaires) considérés sont des idéaux de $\mathcal{O}_\mathbb{K}$. Il est classique que les classes d'idéaux de $\mathcal{O}_\mathbb{K}$ forment un groupe abélien fini d'ordre h, appelé le groupe des classes d'idéaux.

Si $h > 1$, le groupe des classes d'idéaux possède une base, disons les classes $B_1, \ldots, B_k$, d'ordres respectifs $c_1, \ldots, c_k$. Dans chaque classe B_i, on choisit un idéal $\mathfrak{b}_i$. Par définition d'une base, tout idéal est équivalent à un unique produit $\mathfrak{b}_1^{m_1} \ldots \mathfrak{b}_k^{m_k}$ avec $0 \leq m_i < c_i$. Ainsi, pour tout idéal $\mathfrak{a}$, il existe $c \in \mathbb{K}$ tel que

$$\mathfrak{a} = c\mathfrak{b}_1^{m_1} \ldots \mathfrak{b}_k^{m_k}.$$

Pour tout $1 \leq i \leq k$, il existe $\beta_i \in \mathcal{O}_\mathbb{K}$ tel que $\mathfrak{b}_i^{c_i} = (\beta_i)$. Soit $\omega_i = \sqrt[c_i]{\beta_i}$, où l'on fait un choix sur la racine c_i-ème de β_i à considérer. On définit

$$\alpha = c\omega_1^{m_1} \ldots \omega_k^{m_k}.$$

Alors, α est appelé un nombre idéal associé à l'idéal $\mathfrak{a}$.

Si $h = 1$, alors tout idéal est principal. Si $\mathfrak{a} = (a)$ est un idéal, l'ensemble des nombres idéaux associés à $\mathfrak{a}$ est défini comme étant l'ensemble des éléments de la forme ua, où u parcourt les unités de $\mathcal{O}_{\mathbb{K}}$.

Pour chacun des β_i définis ci-dessus, on note $\beta_i^{(m)}$, $1 \leq m \leq r_1 + r_2$, les éléments conjugués de β_i. On définit alors les nombres idéaux conjugués à ω_i comme

$$\omega_i^{(m)} = \sqrt[c_i]{\beta_i^{(m)}} \quad \text{pour } 1 \leq m \leq r_1 + r_2\,,$$

où l'on fait un choix sur la racine c_i-ème des $\beta_i^{(m)}$ à considérer.

Il est aisé d'étendre la multiplication de l'ensemble des idéaux à l'ensemble des nombres idéaux. Remarquons que l'application de l'ensemble des nombres idéaux vers l'ensemble des idéaux, donnée par

$$c\omega_1^{m_1} \dots \omega_k^{m_k} \longmapsto \mathfrak{a} = c\mathfrak{b}_1^{m_1} \dots \mathfrak{b}_k^{m_k} \tag{4.0.4}$$

est un homomorphisme surjectif de noyau $\mathcal{U}$. Si $|\mathcal{U}|$ est fini (ce qui sera majoritairement le cas dans nos applications futures), ce morphisme est alors $|\mathcal{U}|$-pour-1.

Définition 4.0.1. *Le groupe $\mathbb{K}^*(\omega_1, \dots, \omega_k)$ est appelé un système de nombres idéaux de $\mathbb{K}$ et le corps $\mathbb{K}(\omega_1, \dots, \omega_k)$, noté $H_{\mathbb{K}}$, est appelé le corps de Hecke de $\mathbb{K}$ associé au système de nombres idéaux $\mathbb{K}^*(\omega_1, \dots, \omega_k)$ de $\mathbb{K}$.*

Remarque 19 : Le corps de Hecke d'un corps de nombres $\mathbb{K}$ dépend du choix d'un système de nombres idéaux. Il est toutefois uniquement déterminé à $\mathbb{K}$-isomorphisme près.

Notons que le morphisme donné en (4.0.4) induit un morphisme surjectif entre le groupe des classes d'idéaux de $\mathbb{K}$ et $\mathbb{K}^*(\omega_1, \dots, \omega_k)/\mathbb{K}^*$. Il est possible de montrer (voir [**AN95**]) que cette application est en fait un isomorphisme :

$$\text{Groupe des classes de } \mathbb{K} \simeq \mathbb{K}^*(\omega_1, \dots, \omega_k)/\mathbb{K}^*\,. \tag{4.0.5}$$

Les nombres idéaux se divisent en h classes distinctes, qui correspondent aux h classes d'idéaux. Il est aisé de prouver que l'ensemble des nombres idéaux associés à $\overline{\mathfrak{a}}$ est l'ensemble des conjugués des nombres idéaux associés à $\mathfrak{a}$.

Un nombre idéal α est dit entier si α est un entier algébrique, c'est-à-dire si et seulement si l'idéal correspondant est un idéal entier. La norme d'un nombre idéal entier α est définie comme la norme de l'idéal correspondant, c'est-à-dire $N(\alpha) = |\mathcal{O}_{\mathbb{K}}/\mathfrak{a}|$. Un nombre idéal entier α est un nombre idéal premier si l'idéal correspondant est un idéal premier.

Remarquons que, de la propriété correspondante sur les idéaux, l'ensemble des nombres idéaux entiers hérite de la propriété de factorisation en produit de nombres idéaux premiers. Cette factorisation n'est pas unique, puisque chaque nombre idéal premier peut être choisi à une unité près. Toutefois, dans le cas où $|\mathcal{U}|$ est fini, si on impose que le nombre idéal premier ait un argument dans $[0, \frac{2\pi}{|\mathcal{U}|})$, la factorisation devient unique.

Notons également les deux propriétés remarquables suivantes des nombres idéaux, dont les preuves peuvent être trouvées dans [**AN95**] :

Théorème 4.0.2.

$$[H_{\mathbb{K}} : \mathbb{K}] = h\,.$$

Proposition 4.0.5. *Soit $\mathcal{C}$ une classe d'idéaux dans le groupe des classes, d'ordre m, et α un représentant de son image par l'isomorphisme (4.0.5). Alors, $[\mathbb{K}(\alpha) : \mathbb{K}] = m$ et tout idéal de $\mathcal{C}$ est principal dans $\mathbb{K}(\alpha)$.*

Remarque 20 : En d'autres termes, toute classe d'ordre m devient principale dans un corps intermédiaire de degré m sur $\mathbb{K}$.

4.1. Le cas des extensions quadratiques imaginaires

4.1.1. Argument d'un nombre idéal entier d'une extension quadratique

Soit $d > 0$ tel que $-d$ soit un discriminant fondamental. Soit $\mathcal{O}_d$ l'anneau des entiers de $\mathbb{K} = \mathbb{Q}(i\sqrt{d})$ et, comme précédemment, h son nombre de classes et $\mathcal{U}$ son ensemble des unités. Nous rappelons que :

$$\mathcal{U} = \{u^k\} \text{ avec } \begin{cases} u = i \text{ et } 0 \leq k \leq 3 \text{ si } d = 1, \\ u = \mathrm{e}^{i\frac{\pi}{3}} \text{ et } 0 \leq k \leq 5 \text{ si } d = 3, \\ u = -1 \text{ et } 0 \leq k \leq 1 \text{ sinon }. \end{cases} \tag{4.1.1}$$

Soit n un entier,

$$n = \prod_{\left(\frac{-d}{p}\right)=1} p^{\alpha_p} \prod_{\left(\frac{-d}{q}\right)=0} q^{\beta_q} \prod_{\left(\frac{-d}{r}\right)=-1} r^{\gamma_r}$$

où $\left(\frac{-d}{\cdot}\right)$ dénote le symbole de Kronecker. Il est classique que :

$$[p] = \mathcal{P}\overline{\mathcal{P}} \text{ avec } \mathcal{P} \text{ un idéal premier tel que } \mathcal{P} \neq \overline{\mathcal{P}} \text{ si } \left(\frac{-d}{p}\right) = 1\,,$$

$$[q] = \mathcal{Q}^2 \text{ avec } \mathcal{Q} \text{ un idéal premier (on a } \mathcal{Q} = \overline{\mathcal{Q}}) \text{ si } \left(\frac{-d}{q}\right) = 0\,,$$

$$[r] \text{ est un idéal premier si } \left(\frac{-d}{r}\right) = -1\,.$$

On en déduit facilement que, si n est la norme d'un idéal de $\mathcal{O}_d$, il faut que γ_r soit pair. On note $\gamma_r = 2\gamma'_r$.

Les nombres idéaux premiers correspondant à $\overline{\mathcal{P}}$ sont les conjugués de ceux correspondant à $\mathcal{P}$. Ainsi, parmi les nombres idéaux premiers correspondant à $\mathcal{P}$ et $\overline{\mathcal{P}}$, il en existe exactement un dont l'argument est dans $[0, \frac{\pi}{|\mathcal{U}|})$. On le note π_p et on note ϕ_p son argument.

Notons η_q le nombre idéal premier correspondant à $\mathcal{Q}$ dont l'argument est dans $[0, \frac{2\pi}{|\mathcal{U}|})$. Puisque $\mathcal{Q} = \overline{\mathcal{Q}}$, η_q a pour argument 0. Ainsi, tout nombre idéal entier de norme n est de la forme

$$u^k \prod_{(\frac{-d}{p})=1} \pi_p^{\delta_p} \overline{\pi_p}^{\alpha_p - \delta_p} \prod_{(\frac{-d}{q})=0} \eta_q^{\beta_q} \prod_{(\frac{-d}{r})=-1} r^{\gamma'_r}$$

où $0 \leq k \leq |\mathcal{U}| - 1$ et réciproquement, tout élément de cette forme est un nombre idéal entier de norme n.

Définition 4.1.1. *On définit $r(n)$ comme le nombre de nombres idéaux entiers de norme n. On note $\mathbb{G}$ l'ensemble des entiers n avec $r(n) > 0$.*

Remarque 21 : Par ce qui précède, $r(n) > 0$ si et seulement si n est de la forme

$$n = \prod_{(\frac{-d}{p})=1} p^{\alpha_p} \prod_{(\frac{-d}{q})=0} q^{\beta_q} \prod_{(\frac{-d}{r})=-1} r^{2\gamma'_r}$$

et, dans ce cas,

$$r(n) = |\mathcal{U}| \sum_{\delta_p} 1 = |\mathcal{U}| \prod_{(\frac{-d}{p})=1} (\alpha_p + 1)$$

où la somme porte sur tous les choix possibles de $0 \leq \delta_p \leq \alpha_p$.

Lemme 4.1.1. *Soit $n \in \mathbb{G}$, $n = \prod_{(\frac{-d}{p})=1} p^{\alpha_p} \prod_{(\frac{-d}{q})=0} q^{\beta_q} \prod_{(\frac{-d}{r})=-1} r^{2\gamma'_r}$. Soit α un nombre idéal entier de norme n, c'est-à-dire*

$$\alpha = u^k \prod_{(\frac{-d}{p})=1} \pi_p^{\delta_p} \overline{\pi_p}^{\alpha_p - \delta_p} \prod_{(\frac{-d}{q})=0} \eta_q^{\beta_q} \prod_{(\frac{-d}{r})=-1} r^{\gamma'_r}$$

pour certains $0 \leq \delta_p \leq \alpha_p$ et $0 \leq k \leq |\mathcal{U}| - 1$. Alors,

$$arg(\alpha) = \sum_{(\frac{-d}{p})=1} (2\delta_p - \alpha_p)\phi_p + k arg(u) \bmod 2\pi \,.$$

Réciproquement, tout angle de cette forme est angle d'un nombre idéal entier de norme n.

4.1.2. Théorème des nombres idéaux premiers angulaire

La distribution des nombres premiers est une question classique en théorie des nombres, trouvant réponse notamment dans le théorème des nombres premiers, dans sa version plus générale qu'est le théorème de Siegel–Walfisz ou encore dans le théorème de Bombieri–Vinogradov.

Une question similaire peut être posée dans le cas des nombres idéaux premiers. Plus précisément, il est légitime de désirer estimer la distribution asymptotique des nombres idéaux premiers, que ce soit dans une classe donnée, un secteur angulaire donné, ou de norme dans une progression arithmétique fixée.

Avec le théorème 4 de [**Kub52**], Kubilyus adresse certaines de ces questions. La version énoncée ici est moins générale que celle de l'article original (qui est en fait un analogue au théorème de Siegel–Walfisz, étudiant les nombres idéaux premiers dans des progressions arithmétiques), et propose un moins bon terme d'erreur, qui sera toutefois suffisant pour la suite.

Théorème 4.1.1 (Kubilyus)**.** *Pour tout nombre idéal α, on définit $\lambda(\alpha) = \left(\frac{\alpha}{|\alpha|}\right)^{|\mathcal{U}|}$. Soient $x > 3$ et $0 \leq \theta_1 \leq \theta_2 \leq 2\pi$. Pour une classe de nombres idéaux $\mathcal{C}$, soit $\Pi_{\mathcal{C}}(\theta_1, \theta_2, x)$ le nombre de nombres idéaux premiers de $\mathbb{Q}(i\sqrt{d})$ de norme inférieure ou égale à x, dans la classe $\mathcal{C}$ et avec $\arg \lambda(\alpha)$ entre θ_1 et θ_2. Alors,*

$$\Pi_{\mathcal{C}}(\theta_1, \theta_2, x) = \frac{(\theta_2 - \theta_1)|\mathcal{U}|}{2\pi h} \int_2^x \frac{\mathrm{d}\, u}{\log u} + O\left\{x \exp\left(-c\sqrt{\log x}\right)\right\}$$

pour une certaine constante positive c.

Ce théorème n'adresse pas directement la question de la distribution angulaire des nombres idéaux premiers, puisque la fonction λ indifférencie un nombre idéal α et les $u\alpha$ pour $u \in \mathcal{U}$. Il est toutefois aisé d'en déduire le corollaire suivant, qui montre une équidistribution des nombres idéaux à la fois angulairement et parmi les classes.

Corollaire 4.1.1. *Soient $x > 3$ et $0 \leq \theta_1 \leq \theta_2 \leq 2\pi$ tels que $\theta_2 - \theta_1 \leq \frac{2\pi}{|\mathcal{U}|}$. Alors, le nombre de nombres idéaux premiers de $\mathbb{Q}(i\sqrt{d})$ de norme inférieure ou égale à x, dans la classe $\mathcal{C}$ et d'argument entre θ_1 et θ_2 est*

$$\frac{(\theta_2 - \theta_1)|\mathcal{U}|}{2\pi h} \int_2^x \frac{\mathrm{d}\, u}{\log u} + O\left\{x \exp\left(-c\sqrt{\log x}\right)\right\}$$

pour une certaine constante positive c.

Afin de simplifier les notations, on note, classiquement,

$$\mathrm{Li}(x) = \int_2^x \frac{\mathrm{d}\, u}{\log u}\,.$$

Définition 4.1.2. *Soit $\varphi'(q)$ le nombre d'entiers $1 \leq l \leq q-1$, $(l,q)=1$ tels qu'il existe un idéal principal $\mathfrak{a}$ de norme $N\mathfrak{a} \equiv l \bmod q$.*

Remarque 22 : Comme prouvé dans [Fog62], pour toute classe $\mathcal{C}$, le nombre d'entiers $1 \leq l \leq q-1$, $(l,q)=1$ tels qu'il existe un idéal $\mathfrak{a}$ dans $\mathcal{C}$ avec $N\mathfrak{a} \equiv l \bmod q$ est le même. Ainsi, $\varphi'(q)$ pourrait en fait être défini en utilisant une autre classe que la classe principale. Notons également que $\varphi'(q)$ est une fonction multiplicative.

Lemme 4.1.2. *Soit q un entier sans facteur carré. Alors,*

$$\varphi'(q) = \frac{\varphi(q)}{2^{\omega(\operatorname{pgcd}(d,q))}}$$

Démonstration. Soit $1 \leq l \leq q-1$, $(l,q)=1$. Puisque q est sans facteur carré, par le théorème des restes chinois, il existe un idéal principal $\mathfrak{a}$ avec $N\mathfrak{a} \equiv l \bmod q$ si et seulement si, pour tout p divisant q, il existe $\alpha_p \in \mathcal{O}_d$ tel que $N(\alpha_p) \equiv l \bmod p$. Soit $p|q$. Pour $(p,d)=1$, il est facile de voir qu'un tel α_p existe toujours. Pour $(p,d) \neq 1$, un tel α_p existe si et seulement si $\left(\frac{l}{p}\right)=1$. Ainsi,

$$\begin{aligned}
\varphi'(q) &= \left| \left\{ 1 \leq l \leq q-1, (l,q)=1 \text{ et } \left(\frac{l}{p}\right)=1 \text{ pour tout } p|\operatorname{pgcd}(d,q) \right\} \right| \\
&= \frac{1}{2^{\omega(\operatorname{pgcd}(d,q))}} \sum_{\substack{1\leq l\leq q-1 \\ (l,q)=1}} \prod_{p|\operatorname{pgcd}(d,q)} \left[\left(\frac{l}{p}\right) + 1 \right] \\
&= \frac{1}{2^{\omega(\operatorname{pgcd}(d,q))}} \sum_{\substack{1\leq l\leq q-1 \\ (l,q)=1}} \sum_{n|\operatorname{pgcd}(d,q)} \left(\frac{l}{n}\right) \\
&= \frac{1}{2^{\omega(\operatorname{pgcd}(d,q))}} \sum_{n|\operatorname{pgcd}(d,q)} \sum_{\substack{1\leq l\leq q-1 \\ (l,q)=1}} \left(\frac{l}{n}\right) .
\end{aligned}$$

Mais $\left(\frac{\cdot}{n}\right)$ est un caractère mod n. Alors, pour $n|q$ et $n \neq 1$, on obtient par orthogonalité :

$$\sum_{\substack{1\leq l\leq q-1 \\ (l,q)=1}} \left(\frac{l}{n}\right) = 0 .$$

Par conséquent,

$$\varphi'(q) = \frac{\varphi(q)}{2^{\omega(\operatorname{pgcd}(d,q))}} .$$

□

Définition 4.1.3. *On appelle secteur angulaire d'angle θ un intervalle $[\theta_1, \theta_2] \subset [0, 2\pi)$ avec $\beta_2 - \beta_1 = \theta$.*

Il est à remarquer que le théorème 4.1.1 ne permet l'étude que dans le cas de secteurs d'angles de taille $O(1)$. Il est toutefois possible de remédier à ce problème, en utilisant par exemple le résultat suivant, de Koval'chik [**Kov75**] :

Théorème 4.1.2. *Soient $x > 3$ et S un secteur d'angle θ. Pour une classe de nombres idéaux $\mathcal{C}$, soit $\Pi_{\mathcal{C}}(S, x)$ le nombre de nombres idéaux premiers de $\mathbb{Q}(i\sqrt{d})$ de norme inférieure ou égale à x, dans la classe $\mathcal{C}$ et avec $\arg \lambda(\alpha)$ dans S. Alors,*

$$\Pi_{\mathcal{C}}(S, x) = \frac{|\mathcal{U}|}{2\pi h} \frac{\theta x}{\log x} (1 + o(1)) + O\left(x^{3/4+\varepsilon}\right)$$

pour tout nombre $\varepsilon > 0$. Les o et O ne dépendent que de ε et d.

Remarque 23 : Ce théorème n'est évidemment non trivial que lorsque le secteur est d'angle plus grand que $x^{-1/4+\varepsilon}$.

Le théorème suivant, également prouvé par Koval'chik dans [**Kov75**], propose un analogue au théorème de Bombieri-Vinogradov dans le cas des nombres idéaux.

Théorème 4.1.3. *Soit S un secteur angulaire de taille θ. Pour $(k, q) = 1$, soit $\Pi(x, k, q, \mathcal{C}, S)$ le nombre de nombres idéaux premiers π dans la classe $\mathcal{C}$ dont la norme est inférieure ou égale à x, tels que $\arg \lambda(\pi) \in S$ et $N(\pi) \equiv k \bmod q$. Alors,*

$$\sum_{q \leq \theta x^{\frac{1}{4}-\varepsilon}} \max_{\mathcal{C}} \max_{(k,q)=1} \left| \Pi(x, k, q, \mathcal{C}, S) - \frac{\theta |\mathcal{U}|}{2\pi h \varphi'(q)} \operatorname{Li}(x) \right| = O\left(\frac{\theta x}{\log^A x}\right)$$

où ε est un nombre positif arbitraire plus petit que $\frac{1}{4}$ et A est arbitrairement grand, mais fixé.

Dans ce qui suit, nous aurons également besoin de deux propriétés additionnelles de l'ensemble $\mathbb{G}$. La première, due à Bernays [**Ber12**], donne la formule asymptotique du cardinal des éléments de $\mathbb{G}$ plus petits que x, tandis que la seconde renseigne sur le nombre de diviseurs premiers des entiers de $\mathbb{G}$.

Lemme 4.1.3 (Bernays)**.** *Il existe une constante κ_d, ne dépendant que de d, telle que*

$$|\mathbb{G} \cap [0, x]| = \kappa_d \frac{x}{\sqrt{\log x}} + O\left(\frac{x}{\log^{3/4} x}\right).$$

Lemme 4.1.4. *Soit $\omega(n)$ le nombre de diviseurs premiers de n. Alors,*

$$\sum_{\substack{n \in \mathbb{G} \\ n \leq x}} \omega(n) = \kappa_d \frac{x}{\sqrt{\log x}} \left(\frac{1}{2} \log \log x + O(1)\right),$$

$$\sum_{\substack{n \in \mathbb{G} \\ n \leq x}} \omega(n)^2 = \kappa_d \frac{x}{\sqrt{\log x}} \left(\frac{1}{4} (\log \log x)^2 + O(\log \log x)\right),$$

Démonstration. On peut par exemple montrer ce résultat en utilisant la proposition 3.3.3 du chapitre 3 de la partie 1. Soient

$$A = \{n \leq x \text{ tel que } n \in \mathbb{G}\}\,,$$
$$A_m = \{n \leq x \text{ tel que } n \in \mathbb{G} \text{ et } n \equiv 0 \bmod m\}\,.$$

Pour m sans facteur carré, on a $|A_m| = \left|\{n \leq \frac{x}{m_1 m} \text{ tel que } n \in \mathbb{G}\}\right|$, où $m_1 = \prod_{\substack{p|m \\ (\frac{-d}{p})=-1}} p$.

Ainsi, en utilisant le lemme 4.1.3, pour m sans facteur carré, on obtient :

$$|A_m| = \kappa_d \frac{x}{m_1 m\sqrt{\log x}} + O\left(\frac{x}{m_1 m \log^{3/4} x}\right)\,.$$

Soit alors $P = \prod_{p\leq x} p$, de sorte que $\omega_P(n) = \omega(n)$ si $n \leq x$. On peut appliquer la proposition 3.3.3, avec

$$g(p) = \begin{cases} \frac{1}{p} \text{ si } \left(\frac{-d}{p}\right) = 0 \text{ ou } \left(\frac{-d}{p}\right) = 1\,, \\ \frac{1}{p^2} \text{ si } \left(\frac{-d}{p}\right) = -1\,. \end{cases}$$

On a donc

$$\mu_P = \sum_{p\leq x} g(p) = \sum_{\substack{p\leq x \\ (\frac{-d}{p})=1}} \frac{1}{p} + O(1) = \frac{1}{2}\log\log x + O(1)\,, \tag{4.1.2}$$

$$\sigma_P^2 = \sum_{p\leq x} g(p)(1-g(p)) = \sum_{\substack{p\leq x \\ (\frac{-d}{p})=1}} \frac{1}{p} + O(1) = \frac{1}{2}\log\log x + O(1)\,.$$

On déduit alors facilement de la proposition 3.3.3 que

$$\sum_{\substack{n\in\mathbb{G} \\ n\leq x}} (\omega(n) - \mu_P) \ll \frac{x}{\sqrt{\log x}}\,,$$
$$\sum_{\substack{n\in\mathbb{G} \\ n\leq x}} (\omega(n) - \mu_P)^2 \ll \frac{x\log\log x}{\sqrt{\log x}}\,,$$

ce qui suffit à conclure. □

Remarque 24 : La proposition 3.3.3 donne en fait bien plus que le simple lemme 4.1.4. On obtient en réalité un résultat sur la distribution de la fonction ω sur $\mathbb{G}$ du type Erdős-Kac, à savoir :

$$\lim_{x\to\infty} \frac{1}{|\mathbb{G}\cap[0,x]|}|n \in \mathbb{G}, n \leq x \text{ tel que } \alpha \leq \frac{\omega(a) - \frac{1}{2}\log\log x}{\sqrt{\log\log x}} \leq \beta| = \frac{1}{\sqrt{2\pi}}\int_\alpha^\beta \mathrm{e}^{-\frac{t^2}{2}}\,\mathrm{d}\,t\,.$$

En effet, d'après (4.1.2), pour un entier k fixé,

$$\sum_{\substack{n\in\mathbb{G}\\ n\leq x}}\left(\omega(n)-\frac{1}{2}\log\log x\right)^k=\sum_{\substack{n\in\mathbb{G}\\ n\leq x}}\left(\omega(n)-\mu_P\right)^k+O\left(\sum_{m=0}^{k-1}\binom{m}{k}|\sum_{\substack{n\in\mathbb{G}\\ n\leq x}}\left(\omega(n)-\mu_P\right)^m|\right).$$

Pour $m\leq k-1$, par la proposition 3.3.3, on obtient

$$\sum_{\substack{n\in\mathbb{G}\\ n\leq x}}\left(\omega(n)-\mu_P\right)^m\ll\frac{x(\log\log x)^{m/2}}{\sqrt{\log x}}$$

et donc

$$\sum_{\substack{n\in\mathbb{G}\\ n\leq x}}\left(\omega(n)-\frac{1}{2}\log\log x\right)^k=\sum_{\substack{n\in\mathbb{G}\\ n\leq x}}\left(\omega(n)-\mu_P\right)^k+O\left(\frac{x(\log\log x)^{(k-1)/2}}{\sqrt{\log x}}\right).$$

Ainsi, en utilisant à nouveau la proposition 3.3.3 on a, pour tout entier k, quand $x\to\infty$,

$$\frac{\sqrt{\log x}}{\kappa_d x}\sum_{\substack{n\in\mathbb{G}\\ n\leq x}}\left(\frac{\omega(n)-\frac{1}{2}\log\log x}{\sqrt{\log\log x}}\right)^k\to\begin{cases}\frac{k!}{2^{k/2}\left(\frac{k}{2}\right)!}\text{ si }k\text{ est pair},\\ 0\text{ si }k\text{ est impair}.\end{cases}$$

La méthode des moments donne alors le résultat.

Lemme 4.1.5.

$$\sum_{\substack{n\in\mathbb{G}\\ n\leq x}}(\omega(n)-\frac{1}{2}\log\log x)^2=O\left(\frac{x\log\log x}{\sqrt{\log x}}\right).$$

Démonstration. C'est une conséquence immédiate du lemme 4.1.4. □

On peut alors déduire du lemme 4.1.5 le résultat suivant :

Lemme 4.1.6. *Avec au plus* $o\left(\frac{x}{\sqrt{\log x}}\right)$ *exceptions, pour tout entier* n *plus petit que* x *dans* $\mathbb{G}$, *on a* $\omega(n)>\left(\frac{1}{2}-\varepsilon\right)\log\log x$.

4.2. Le cas de la dimension supérieure

Les résultats précédents portaient sur les extensions quadratiques, mais il est également légitime de se demander ce qu'il en est des extensions de degré supérieur.

Nous adoptons ici les notations suivantes. $\mathbb{K}$ est un corps de nombres de degré $n=r_1+2r_2$, où r_1 est le nombre de plongements réels et r_2 le nombre de plongements complexes. Pour un nombre idéal ω, on note $\omega^{(m)}$, $1\leq m\leq r_1+r_2$, ses conjugués, avec la convention que le (r_1+1)-ème conjugué corresponde à l'application identité. On note $r=r_1+r_2-1$, $\mathcal{O}_{\mathbb{K}}$ l'anneau des entiers de $\mathbb{K}$, $w_{\mathbb{K}}$ son nombre de racines de l'unité, h son nombre de classes et R son régulateur.

Alors, une généralisation du théorème 4.1.1 aux extensions de degrés quelconques existe, comme donnée dans le théorème suivant, dû à Mitsui [**Mit56**] (comme précédemment, la version présentée ici est une version simplifiée, le théorème d'origine étant encore une fois un analogue au théorème de Siegel–Walfisz).

Théorème 4.2.1. *Soit $\mathcal{C}$ une classe de nombres idéaux. Soient $Y_1, \dots, Y_n$ des nombres réels positifs tels que $Y_m = Y_{m+r_2}$ pour $m \geq r_1 + 1$ et $Y_i \leq Y_j^a$ pour un certain nombre positif a fixé. Soient $\theta_{r_1+1}, \dots, \theta_{r_1+r_2}$ des nombres réels positifs tels que $0 < \theta_m \leq 1$ pour $r_1 + 1 \leq m \leq r_1 + r_2$. Soit $\Pi_{\mathcal{C}}(Y_1, \dots, Y_n, \theta_{r_1+1}, \dots, \theta_{r_1+r_2}) = \Pi_{\mathcal{C}}(Y_i, \theta_i)$ le nombre de nombres idéaux premiers ω de $\mathcal{O}_{\mathbb{K}}$ de la classe $\mathcal{C}$ avec*

$$|\omega^{(m)}| \leq Y_m \text{ pour } m = 1, \dots, r+1\,,$$
$$0 \leq \arg(\omega^{(m)}) < 2\pi\theta_m \text{ pour } m = r_1+1, \dots, r_1+r_2\,.$$

Alors,

$$\Pi_{\mathcal{C}}(Y_i, \theta_i) = \frac{\theta_{r_1+1} \dots \theta_{r_1+r_2} w_{\mathbb{K}}}{hR} \int_2^{Y_1^{e_1}} \mathrm{d}\, t_1 \dots \int_2^{Y_r^{e_r}} \mathrm{d}\, t_r \int_2^{Y_{r+1}^{e_{r+1}}} \frac{\mathrm{d}\, t_{r+1}}{\log(t_1 \dots t_{r+1})} + O\left(Y_1 \dots Y_n\, \mathrm{e}^{-c\sqrt{\log(Y_1 \dots Y_n)}}\right)$$

pour une constante positive c, $e_i = 1$ si $i \leq r_1$, $e_i = 2$ si $i \geq r_1 + 1$ et le terme d'erreur ne dépend que de a et $\mathbb{K}$.

À l'aide de ce théorème, on peut, par exemple, prouver le résultat suivant, qui généralise au cas des extensions de degrés quelconques le fait que l'ensemble des quotients de nombres premiers est dense dans l'ensemble des nombres réels positifs :

Théorème 4.2.2. *Soit $\mathbb{K}$ un corps de nombres et $\mathcal{O}_{\mathbb{K}}$ son anneau des entiers. Si $\mathbb{K}$ n'est pas totalement réel, alors, l'ensemble des quotients des premiers de $\mathcal{O}_{\mathbb{K}}$ est dense dans $\mathbb{C}$. Si $\mathbb{K}$ est totalement réel, alors l'ensemble des quotients des premiers de $\mathcal{O}_{\mathbb{K}}$ est dense dans $\mathbb{R}$.*

La preuve se base sur le corollaire au théorème 4.2.1 suivant :

Corollaire 4.2.1. *Supposons que $\mathbb{K}$ ne soit pas totalement réel. Alors, pour tout $B > A > 0$, pour tout secteur d'angle θ, il existe N_0 ne dépendant que de $\mathbb{K}$, θ, A et B tel que, pour tout $N > N_0$, il existe un premier π_2 de $\mathcal{O}_{\mathbb{K}}$ dans le secteur avec $\frac{N}{B} < |\pi_2| < \frac{N}{A}$.*

Supposons que $\mathbb{K}$ soit totalement réel. Alors, pour tout $B > A > 0$, il existe N_0 ne dépendant que de $\mathbb{K}$, A et B tel que, pour tout $N > N_0$, il existe un premier π_2 de $\mathcal{O}_{\mathbb{K}}$ avec $\frac{N}{B} < |\pi_2| < \frac{N}{A}$.

Démonstration. Supposons que $\mathbb{K}$ ne soit pas totalement réel. Soit $S = [\alpha, \beta]$ un secteur avec $\beta - \alpha = \theta$ et $\mathcal{C}$ la classe principale. Soient

$$Y_{r_1+1} = \frac{N_0}{B}\,, \quad Y'_{r_1+1} = \frac{N_0}{A}\,,$$
$$\theta_{r_1+1} = \frac{\alpha}{2\pi}\,, \quad \theta'_{r_1+1} = \frac{\beta}{2\pi}\,,$$
$$Y_i = Y'_i = N_0 \text{ et } \theta_i = \theta'_i = 1 \text{ pour } i \neq r_1 + 1\,.$$

D'après le théorème 4.2.1, il suffit maintenant de choisir N_0 suffisamment grand pour que

$$\Big(\Pi_{\mathcal{C}}(Y'_i, \theta'_i) - \Pi_{\mathcal{C}}(Y'_i, \theta_i)\Big) - \Big(\Pi_{\mathcal{C}}(Y_i, \theta'_i) - \Pi_{\mathcal{C}}(Y_i, \theta_i)\Big) =$$
$$\frac{\theta w_{\mathbb{K}}}{hR} \int_2^{N_0} \mathrm{d}\, t_1 \ldots \int_2^{N_0} \mathrm{d}\, t_{r_1} \int_{\left(\frac{N_0}{B}\right)^2}^{\left(\frac{N_0}{A}\right)^2} \mathrm{d}\, t_{r_1+1} \int_2^{N_0^2} \mathrm{d}\, t_{r_1+2} \ldots \int_2^{N_0^2} \frac{\mathrm{d}\, t_{r+1}}{\log(t_1 \ldots t_{r+1})}$$
$$+ O\left(N_0^n\, \mathrm{e}^{-c\sqrt{n \log N_0}}\right) \geq 2\,.$$

Un tel N_0 existe puisque la partie gauche de l'équation tend vers l'infini et N_0 ne dépend que de $\mathbb{K}$, θ, A et B puisque le terme d'erreur du théorème 4.2.1 ne dépend que de $\mathbb{K}$.

La preuve du cas totalement réel est semblable. □

Preuve du théorème 4.2.2. Supposons que $\mathbb{K}$ ne soit pas totalement réel. Soient $z_0 \in \mathbb{C}$ et $\varepsilon > 0$. Soient $\varepsilon_1, \varepsilon_2 > 0$ tels que $\varepsilon_1 < |z_0|$ et

$$\{z \in \mathbb{C} \text{ tel que } ||z_0| - |z|| < \varepsilon_1 \text{ et } |\arg(z_0) - \arg(z)| \leq \varepsilon_2\} \subset \{z \in \mathbb{C} \text{ tel que } |z_0 - z| < \varepsilon\}\,.$$

Soit N_0 donné par le corollaire 4.2.1 pour un secteur d'angle $2\varepsilon_2$ et

$$B = |z_0| + \varepsilon_1\,, \quad A = |z_0| - \varepsilon_1\,.$$

À l'aide du théorème 4.2.1, on choisit π_1 un premier de $\mathcal{O}_{\mathbb{K}}$ avec $|\pi_1| > N_0$. D'après le corollaire 4.2.1 pour le choix précédent de A, B et le secteur

$$S = [\arg(\pi_1) - \arg(z_0) - \varepsilon_2, \arg(\pi_1) - \arg(z_0) + \varepsilon_2]\,,$$

il existe un premier π_2 de $\mathcal{O}_{\mathbb{K}}$ avec $\arg(\pi_2) \in S$ et $\frac{|\pi_1|}{|z_0|+\varepsilon_1} < |\pi_2| < \frac{|\pi_1|}{|z_0|-\varepsilon_1}$. Cela implique

$$\left||z_0| - \left|\frac{\pi_1}{\pi_2}\right|\right| < \varepsilon_1 \quad \text{et} \quad \left|\arg(z_0) - \arg\left(\frac{\pi_1}{\pi_2}\right)\right| \leq \varepsilon_2\,.$$

Supposons que $\mathbb{K}$ soit totalement réel. Soit $z_0 \in \mathbb{R}$ et $\varepsilon > 0$. Soit N_0 donné par le corollaire 4.2.1 pour

$$B = |z_0| + \varepsilon\,, \quad A = |z_0| - \varepsilon\,.$$

À l'aide du théorème 4.2.1, on choisit π_1 un premier de $\mathcal{O}_{\mathbb{K}}$ avec $|\pi_1| > N_0$. D'après le corollaire 4.2.1 pour le choix précédent de A et B, il existe un premier π_2 de $\mathcal{O}_{\mathbb{K}}$ avec $\frac{|\pi_1|}{|z_0|+\varepsilon_1} < |\pi_2| < \frac{|\pi_1|}{|z_0|-\varepsilon_1}$. Cela implique

$$\left| |z_0| - \left| \frac{\pi_1}{\pi_2} \right| \right| < \varepsilon$$

et, comme $-\pi_1$ est également un premier,

$$\left| z_0 - \frac{\pi_1}{\pi_2} \right| < \varepsilon \,.$$

□

Remarque 25 : Il est en réalité possible d'obtenir un résultat plus général que le théorème 4.2.2. Plus précisément, par une preuve semblable à ce qui précède, on peut obtenir la densité des quotients des nombres idéaux premiers d'une classe donnée.

Chapitre 5

DISTRIBUTION DES NOMBRES IDÉAUX ENTIERS DE NORME DONNÉE

Dans [EH99], Erdős et Hall étudient la distribution angulaire des entiers de Gauss de norme donnée, ce qui, géométriquement, revient à étudier la distribution des points à coordonnées entières sur un cercle. Il est aisé de voir que les entiers de Gauss de norme donnée ne sont pas uniformément distribués sur le cercle, par exemple avec la proposition suivante (que l'on peut trouver dans [Cil93]) :

Proposition 5.0.1. *Pour tout $\varepsilon > 0$ et tout entier k, il existe un cercle $x^2 + y^2 = n$ dont tous les points à coordonnées entières sont situés sur des arcs d'angles plus petits que ε*

Démonstration. D'après le corollaire 4.1.1, il est possible de trouver un premier π de $\mathbb{Z}[i]$ d'argument dans $(0, \frac{\varepsilon}{k})$ avec $N(\pi) = p$ un premier de $\mathbb{Z}$. Alors, les entiers de Gauss de norme p^k sont de la forme $u\pi^m\overline{\pi}^{k-m}$ avec $0 \leq m \leq k$ et $u = \pm 1, \pm i$. Or, tous ces entiers de Gauss ont un argument dans un des quatre secteurs d'angle 2ε que sont $(-\varepsilon, \varepsilon)$ et ses rotations par des multiples de $\frac{\pi}{2}$. □

Toutefois, même si les arguments des entiers de Gauss de norme donnée ne sont pas uniformément distribués dans $[0, 2\pi)$, Erdős et Hall montrent que leur discrépance est relativement faible. L'objet de ce chapitre est d'étendre ce résultat à une extension quadratique imaginaire générale.

$\mathbb{Z}[i]$ étant un anneau principal, le résultat mentionné précédemment peut être vu comme une étude de l'argument des générateurs des idéaux entiers de $\mathbb{Z}[i]$ de norme donnée. Malheureusement, dans une extension quadratique imaginaire quelconque, l'anneau des entiers n'est en général pas un anneau principal. Toutefois, comme vu dans le chapitre 4, tout idéal devient principal dans l'anneau des entiers du corps de Hecke. Ainsi, nous allons ici étudier la distribution de nombres idéaux entiers de norme donnée.

Il est à noter qu'un tel résultat est bien l'analogue du résultat de Erdős et Hall puisque, dans le cas d'une extension dont l'anneau des entiers est principal, générateurs des idéaux entiers et nombres idéaux entiers coïncident.

5.1. Sur la distribution des nombres idéaux entiers de norme donnée

On reprend ici les notations de la section 4.1. Soit $d > 0$ tel que $-d$ soit un discriminant fondamental. Soit $\mathcal{O}_d$ l'anneau des entiers de $\mathbb{K} = \mathbb{Q}(i\sqrt{d})$, h son nombre de classes et $\mathcal{U}$ son ensemble des unités. Soit $r(n)$ le nombre de nombres idéaux entiers de norme n et $\mathbb{G}$ l'ensemble des entiers n avec $r(n) > 0$.

Définition 5.1.1. *Soit Φ_n l'ensemble des arguments des nombres idéaux entiers de norme n. La discrépance $\Delta(n)$ de l'ensemble Φ_n est*

$$\Delta(n) = \max\left\{ |\operatorname{card}^*\{\phi \in \Phi_n, \phi \in [\theta_1, \theta_2] \bmod 2\pi\} - \frac{(\theta_2 - \theta_1)}{2\pi} r(n)|, 0 \leq \theta_1 < \theta_2 \leq 2\pi \right\}$$

où l'astérisque dénote que si l'angle est θ_1 ou θ_2, alors il compte pour $\frac{1}{2}$.

Nous allons prouver la borne supérieure suivante :

Théorème 5.1.1. *Soit $\varepsilon > 0$. Alors, pour tous les entiers plus petits que x de $\mathbb{G}$, avec au plus $o(|\mathbb{G} \cap [0, x]|)$ exceptions,*

$$\Delta(n) \leq \frac{r(n)}{(\log x)^{\frac{1}{2}\log\left(\frac{\pi}{2}\right)-\varepsilon}}.$$

Remarque 26 : La borne triviale sur la discrépance $\Delta(n)$ est $r(n)$. Ainsi, le théorème 5.1.1 est une amélioration de la borne triviale par une puissance de log, moyennant un ensemble d'exceptions. $r(n)$ étant lui-même d'ordre une puissance de log, c'est une amélioration substantielle. Plus précisément, pour tout $n \in \mathbb{G}$, $r(n) \leq d(n)$, la fonction diviseur. Soit $\Omega(n)$ le nombre de diviseurs premiers de n comptés avec multiplicité. De manière analogue au lemme 4.1.6, il est possible de prouver que $\Omega(n) < (\frac{1}{2} + \varepsilon) \log\log x$ pour presque tout $n \in \mathbb{G} \cap [0, x]$. Ainsi, $r(n) \leq d(n) \leq 2^{\Omega(n)} \leq (\log x)^{(\frac{1}{2}+\varepsilon)\log 2}$ pour presque tous les entiers n de $\mathbb{G}$ plus petits que x.

Afin d'obtenir la borne désirée pour $\Delta(n)$, pour un nombre réel positif fixé y, on étudie la moyenne de $\frac{\Delta(n)}{r(n)} y^{\omega(n)}$ sur l'ensemble $\mathbb{G}$ en montrant qu'elle est « petite ». L'outil principal de la preuve sera la borne classique de la discrépance, uniforme en T, prouvée par Erdős et Turán [**ET48a**, **ET48b**],

$$\Delta(n) \ll \frac{r(n)}{T} + \sum_{t \leq T} \frac{|Z_t(n)|}{t} \quad \text{où} \quad Z_t(n) = \sum_{\phi \in \Phi_n} \mathrm{e}^{it\phi}.$$

Remarque 27 : À l'aide du lemme 4.1.1, on a :

$$Z_t(n) = \sum_{\phi\in\Phi_n} \mathrm{e}^{it\phi} = \sum_{k=0}^{|\mathcal{U}|-1} u^{tk} \sum_{\delta_p} \mathrm{e}^{it\sum(2\delta_p-\alpha_p)\phi_p}$$

où la somme porte sur tous les choix possibles de $0 \leq \delta_p \leq \alpha_p$. Ainsi,

$$Z_t(n) = \begin{cases} |\mathcal{U}| \sum_{\delta_p} \mathrm{e}^{it\sum(2\delta_p-\alpha_p)\phi_p} & \text{si } t \equiv 0 \bmod |\mathcal{U}|, \\ 0 \text{ si } t \not\equiv 0 \bmod |\mathcal{U}|. \end{cases}$$

Notons que $\frac{|Z_t(n)|}{|\mathcal{U}|}$ est multiplicative. $\frac{r(n)}{|\mathcal{U}|}$ étant également multiplicative, $\frac{|Z_t(n)|}{r(n)}$ est ainsi une fonction multiplicative sur $\mathbb{G}$.

À l'aide de la borne supérieure précédente,

$$\sum_{\substack{n\in\mathbb{G}\\ n\leq x}} \frac{\Delta(n)}{r(n)} y^{\omega(n)} \ll \frac{1}{T} \sum_{\substack{n\in\mathbb{G}\\ n\leq x}} y^{\omega(n)} + \sum_{\substack{t\leq T\\ t\equiv 0 \bmod |\mathcal{U}|}} \frac{1}{t} \sum_{\substack{n\in\mathbb{G}\\ n\leq x}} \frac{|Z_t(n)|}{r(n)} y^{\omega(n)}.$$

Les deux sommes précédentes vont être estimées à l'aide de l'inégalité suivante, prouvée par Kátai [**Kát76**] :

Lemme 5.1.1. *Soit $f(n)$ une fonction multiplicative positive, avec $f(p^k) \leq Ck$ pour toute puissance première p^k. Alors,*

$$\sum_{n\leq x} f(n) \leq c \frac{x}{\log x} \exp\left(\sum_{p\leq x} \frac{f(p)}{p}\right)$$

où la constante c ne dépend que de la constante C.

Cette inégalité peut être aisément appliquée aux deux sommes précédentes. Pour $p^k \in \mathbb{G}$, par la remarque 21 et la remarque 27, nous avons, pour $t \equiv 0 \bmod |\mathcal{U}|$,

$$\frac{|Z_t(p^k)|}{r(p^k)} y^{\omega(p^k)} \leq y \quad \text{et} \quad \frac{|Z_t(p)|}{r(p)} y^{\omega(p)} = \begin{cases} y|\cos(t\phi_p)| \text{ si } \left(-\frac{d}{p}\right) = 1, \\ y \text{ si } \left(-\frac{d}{p}\right) = 0, \\ 0 \text{ si } \left(-\frac{d}{p}\right) = -1. \end{cases}$$

On applique maintenant le lemme 5.1.1 aux première et deuxième sommes. On obtient alors :

$$\sum_{\substack{n\in\mathbb{G}\\ n\leq x}} \frac{\Delta(n)}{r(n)} y^{\omega(n)} \ll \frac{1}{T} \frac{x}{\log x} \exp\left(y \sum_{\substack{p\leq x\\ (-\frac{d}{p})=1}} \frac{1}{p}\right) + \frac{x}{\log x} \sum_{\substack{t\leq T\\ t\equiv 0 \bmod |\mathcal{U}|}} \frac{1}{t} \exp\left(y \sum_{\substack{p\leq x\\ (-\frac{d}{p})=1}} \frac{|\cos(t\phi_p)|}{p} + O(y)\right)$$

$$\ll \frac{1}{T}x(\log x)^{\frac{y}{2}-1} + \frac{x}{\log x}\sum_{\substack{t\leq T\\ t\equiv 0 \bmod |\mathcal{U}|}}\frac{1}{t}\exp\left(y\sum_{\substack{p\leq x\\ (-\frac{d}{p})=1}}\frac{|\cos(t\phi_p)|}{p}+O(y)\right).$$

Il reste maintenant à estimer

$$\sum_{\substack{p\leq x\\ (-\frac{d}{p})=1}}\frac{|\cos(t\phi_p)|}{p}.$$

Pour tout p avec $\left(-\frac{d}{p}\right)=1$, $\phi_p\in(0,\frac{\pi}{|\mathcal{U}|})$. On divise cet intervalle en intervalles E_j de longueur $\frac{\pi}{t}$ de sorte que, sur chacun de ces intervalles, $\cos(t\theta)$ soit de signe constant. Plus précisément, soit

$$E_j=\left[\frac{(2j+1)\pi}{2t},\frac{(2j+3)\pi}{2t}\right) \text{ avec } 0\leq j\leq \frac{t}{|\mathcal{U}|}-2\,.$$

Remarquons que j est bien un nombre entier, puisque $t\equiv 0 \bmod |\mathcal{U}|$. Alors, pour tout nombre réel k,

$$\sum_{p\leq k}^{*}|\cos(t\phi_p)| = \sum_{\substack{p\leq k\\ \phi_p\in(0,\frac{\pi}{2t})}}^{*}\cos(t\phi_p)+(-1)^{\frac{t}{|\mathcal{U}|}-1}\sum_{\substack{p\leq k\\ \phi_p\in[\frac{\pi}{|\mathcal{U}|}-\frac{\pi}{2t},\frac{\pi}{|\mathcal{U}|})}}^{*}\cos(t\phi_p)+\sum_{j=0}^{\frac{t}{|\mathcal{U}|}-2}(-1)^{j+1}\sum_{\substack{p\leq k\\ \phi_p\in E_j}}^{*}\cos(t\phi_p)$$

où l'astérisque dénote que la somme est restreinte aux premiers satisfaisant $\left(-\frac{d}{p}\right)=1$. Du corollaire 4.1.1 (où l'égalité est multipliée par h, puisqu'on ne considère pas une classe de nombres idéaux en particulier), on obtient :

$$\begin{aligned}\sum_{\substack{p\leq k\\ \phi_p\in E_j}}^{*}\cos(t\phi_p) &= \sum_{\substack{p\leq k\\ \phi_p\in E_j}}^{*}\int_{\phi_p}^{\frac{(2j+3)\pi}{2t}} t\sin(t\theta)\,\mathrm{d}\,\theta = \int_{E_j}\sum_{\substack{p\leq k\\ \frac{(2j+1)\pi}{2t}<\phi_p\leq\theta}}^{*} t\sin(t\theta)\,\mathrm{d}\,\theta\\ &= \frac{|\mathcal{U}|}{2\pi}\int_2^k\frac{\mathrm{d}\,v}{\log v}\int_{E_j}\left(\theta-\frac{(2j+1)\pi}{2t}\right)t\sin(t\theta)\,\mathrm{d}\,\theta+O\left(k\exp(-c\sqrt{\log k})\right)\\ &= (-1)^{j+1}\frac{|\mathcal{U}|}{\pi t}\int_2^k\frac{\mathrm{d}\,v}{\log v}+O\left(k\exp(-c\sqrt{\log k})\right).\end{aligned}$$

En estimant les deux autres sommes de façon semblable, on en déduit que, pour tout $2\leq\omega\leq x$,

$$\begin{aligned}\sum_{p\leq x}^{*}\frac{|\cos(t\phi_p)|}{p} &\leq \sum_{p\leq w}^{*}\frac{1}{p}+\sum_{w<p\leq x}^{*}\frac{|\cos(t\phi_p)|}{p}\\ &\leq \frac{1}{2}\log\log w+O(1)+\frac{1}{\pi}\log\left(\frac{\log x}{\log w}\right)+O\left(t\exp(-c\sqrt{\log w})\right)\end{aligned}$$

en utilisant la formule d'Abel pour la seconde somme. Maintenant, soit $\log w = (c^{-1}\log t)^2$ (afin de rendre égaux les deux termes d'erreur). Alors, uniformément en t,

$$\sum_{p\le x}^{*}\frac{|\cos(t\phi_p)|}{p} \le \frac{1}{\pi}\log\log x + \left(1-\frac{2}{\pi}\right)\log\log t + O(1)\,.$$

Ainsi,

$$\begin{aligned}\sum_{\substack{n\in\mathbb{G}\\ n\le x}}\frac{\Delta(n)}{r(n)}y^{\omega(n)} &\ll \frac{x(\log x)^{\frac{y}{2}-1}}{T} + x(\log x)^{\frac{y}{\pi}-1}(\log T)^{y(1-\frac{2}{\pi})+1}\\ &\ll \frac{x}{\sqrt{\log x}}(\log\log x)^{\frac{\pi}{2}}\end{aligned}$$

en prenant $T=(\log x)^{y(\frac{1}{2}-\frac{1}{\pi})}$ et $y=\frac{\pi}{2}$. Par le lemme 4.1.6,

$$y^{\omega(n)} > y^{\left(\frac{1}{2}-\varepsilon\right)\log\log x} = (\log x)^{(\frac{1}{2}-\varepsilon)\log y}$$

pour tous les entiers de $\mathbb{G}$, avec au plus $o\left(\frac{x}{\sqrt{\log x}}\right)$ exceptions. Ceci donne le résultat souhaité.

5.2. Angle d'une représentation par une forme quadratique

Dans ce qui suit, on considère uniquement des formes quadratiques binaires entières définies positives de discriminant $-d$, c'est-à-dire des formes quadratiques binaires entières de la forme $f(x,y)=ax^2+bxy+cy^2$ avec $-d=b^2-4ac<0$ et $a>0$ (en d'autres termes, $f(x,y)>0$ pour tout $(x,y)\neq(0,0)$). On appelle forme quadratique binaire primitive réduite toute forme quadratique binaire définie positive avec $a,b,c\in\mathbb{Z}$, $\mathrm{pgcd}(a,b,c)=1$ et $|b|\le a\le c$, ou $b\ge 0$ si $|b|=a$ ou $a=c$. On appelle représentation de n par f une solution sur les entiers de l'équation $f(x,y)=n$.

Il est classique qu'il existe un isomorphisme entre l'espace des classes des formes quadratiques binaires primitives de discriminant $-d$ et les classes d'idéaux de $\mathcal{O}_d$, qui associe l'idéal $[a,\frac{-b+i\sqrt{d}}{2}]$ à la forme $ax^2+bxy+cy^2$.

Dans cette section, nous utiliserons de manière indifférenciée la notation suivante pour dénoter les classes de formes ou les classes d'idéaux : si f est une forme quadratique binaire primitive réduite de discriminant $-d$, on note $\mathcal{C}_f$ la classe des formes équivalentes à f et la classe d'idéaux de $\mathcal{O}_d$ correspondante. On note également $\mathcal{C}_f^{-1}$ son inverse dans le groupe des classes (et $\mathcal{C}_f^{-1}=\mathcal{C}_{f^{-1}}$, où f^{-1} est appelée la forme opposée, et si $f(x,y)=ax^2+bxy+cy^2$, alors f^{-1} est la forme réduite correspondant à $ax^2-bxy+cy^2$).

Définition 5.2.1. *Soit $f(x,y) = ax^2 + bxy + cy^2$ une forme quadratique binaire primitive réduite de discriminant $-d$ et soit n un entier représenté par f. Soit*

$$f(x_0, y_0) = \frac{N(\alpha_{x_0,y_0})}{a} = n$$

où N est la norme dans $\mathcal{O}_d$, $\tau_f = \frac{-b+i\sqrt{d}}{2a}$ et $\alpha_{x_0,y_0} = a(x_0 - \overline{\tau_f} y_0)$, une représentation de n par f. On définit l'angle de cette représentation de n par f par

$$\arg(f(x_0, y_0) = n) = \arg(\alpha_{x_0,y_0})\,.$$

Remarque 28 : Géométriquement, l'équation $f(x,y) = n$ définit une ellipse. L'application $(x,y) \mapsto (ax + \frac{b}{2}y, \frac{\sqrt{d}}{2})$ envoie l'ellipse sur un cercle de rayon $\sqrt{n}$, en complétant les carrés, à partir duquel on peut paramétriser l'ellipse. L'angle de la représentation $f(x_0, y_0) = n$ est la valeur de ce paramètre.

Pour une forme quadratique binaire primitive réduite $f(x,y) = ax^2 + bxy + cy^2$ de discriminant $-d$ et pour un entier positif n représenté par f, il existe une correspondance $|\mathcal{U}|$-pour-un entre les représentations de n par f et les idéaux de norme n dans $\mathcal{C}_f$. Plus précisément, (voir, par exemple, [Cox89] pour plus de détails), soit $f(x_0, y_0) = n$ une représentation de n par f. Pour toute unité u^k de $\mathcal{O}_d$, il existe un unique couple (x_0', y_0') tel que $u^k \alpha_{x_0,y_0} = \alpha_{x_0',y_0'}$. Alors,

$$f(x_0', y_0') = \frac{N(\alpha_{x_0',y_0'})}{a} = \frac{N(\alpha_{x_0,y_0})}{a} = n$$

est une autre représentation de n par f. On appellera une telle représentation une représentation équivalente à $f(x_0, y_0) = n$. On peut grouper ensemble ces $|\mathcal{U}|$ représentations équivalentes et associer à ces $|\mathcal{U}|$ représentations l'idéal $\alpha_{x_0,y_0}[1, \tau_f]$.

Remarque 29 : Les $|\mathcal{U}|$ choix possibles pour α_{x_0,y_0} diffèrent par des unités. Toutefois, l'idéal associé est unique.

Lemme 5.2.1. *Soit $\mathcal{I}$ l'idéal associé à un ensemble de $|\mathcal{U}|$ représentations équivalentes à $f(x_0, y_0) = n$. Soit $\mathfrak{b}_f = a[1, \overline{\tau_f}]$ l'idéal de plus petite norme dans $\mathcal{C}_{f^{-1}}$. Alors,*

$$\left\{ \begin{matrix} \textit{arguments des nombres} \\ \textit{idéaux associés à } \mathcal{I} \end{matrix} \right\} = \left\{ \begin{matrix} \textit{angles des } |\mathcal{U}| \textit{ représentations} \\ \textit{équivalentes à } f(x_0, y_0) = n \end{matrix} \right\} - \arg(\omega_{\mathfrak{b}_f}) \bmod 2\pi$$

où $\omega_{\mathfrak{b}_f}$ est n'importe quel nombre idéal associé à $\mathfrak{b}_f$.

DÉMONSTRATION. On a $\mathcal{I} = \alpha_{x_0,y_0}[1, \tau_f]$. Alors,

$$\begin{aligned} \alpha_{x_0,y_0}[1, \tau_f]\mathfrak{b}_f &= \alpha_{x_0,y_0}[1, \tau_f] a[1, \overline{\tau_f}] \\ &= [a\alpha_{x_0,y_0}, b\alpha_{x_0,y_0}, c\alpha_{x_0,y_0}, a\alpha_{x_0,y_0}\tau_f] \\ &= [\alpha_{x_0,y_0}] \end{aligned}$$

puisque la norme de l'idéal $[\alpha_{x_0,y_0}]$ est an, la même que celle de $\alpha_{x_0,y_0}[1,\tau_f]\mathfrak{b}_f$. Ainsi, l'ensemble des nombres idéaux de $\mathcal{I}\mathfrak{b}_f$ est l'ensemble des éléments de la forme $u^k\alpha_{x_0,y_0}$. Cela prouve le résultat. □

Géométriquement, les représentations de n par f sont les points à coordonnées entières sur l'ellipse $f(x,y)=n$. Par le lemme 5.2.1, on peut immédiatement déduire que la distribution de tels points est la même que la distribution angulaire des nombres idéaux de norme n dans la classe $\mathcal{C}_f$.

Supposons $h>1$ (puisque, s'il y a seulement une classe, il n'y a rien de plus à prouver que le théorème 5.1.1).

Définition 5.2.2. *Pour une forme quadratique binaire primitive f de discriminant $-d$ et $n\in\mathbb{G}$, n representé par f, soit Φ_n^f l'ensemble des arguments des nombres idéaux entiers de norme n dans $\mathcal{C}_f$ et $r_f(n)$ le nombre de nombres idéaux entiers de norme n dans $\mathcal{C}_f$. On définit la discrépance de Φ_n^f comme*

$$\Delta_f(n)=\max\Big\{|\operatorname{card}^*\{\phi\in\Phi_n^f,\phi\in[\theta_1,\theta_2] \bmod 2\pi\}-(\theta_2-\theta_1)r_f(n)|, 0\le\theta_1<\theta_2\le 2\pi\Big\}$$

où l'astérisque dénote que si l'angle est θ_1 ou θ_2, alors il compte pour $\frac{1}{2}$.

Nous aimerions pouvoir utiliser la même technique que dans la première section, en utilisant la borne

$$\Delta_f(n)\ll\frac{r_f(n)}{T}+\sum_{t\le T}\frac{|Z_t^f(n)|}{t}$$

où $Z_t^f(n)=\sum_{\phi\in\Phi_n^f}\mathrm{e}^{it\phi}$.

Malheureusement, la fonction $\frac{|Z_t^f(n)|}{r_f(n)}$ n'est généralement pas multiplicative. Toutefois, dans le cas (très restrictif) où il n'y a qu'une seule classe par genre, l'étude précédente permet de borner la discrépance $\Delta_f(n)$, puisqu'elle sera égale à $\Delta(n)$.

5.2.1. Une classe par genre

On rappelle que deux formes de discriminant $-d$ sont dans le même genre si elles représentent les mêmes valeurs dans $\mathbb{Z}/d\mathbb{Z}$. Ainsi, deux formes de la même classe seront toujours dans le même genre, et en fait, chaque genre consiste en le même nombre de classes de formes.

Il est connu qu'il n'y a qu'un nombre fini de discriminants fondamentaux $-d$ avec une classe par genre. Les valeurs de d correspondantes sont données dans la liste qui suit. Cette liste est complète, si ce n'est pour une éventuelle valeur supplémentaire, plus grande que 5460 (voir [**Wei73**]).

$$3, 4, 7, 8, 11, 15, 19, 20, 24, 35, 40, 43, 51,52, 67, 84, 88, 91, 115, 120, 123, 132, 148,$$
$$163, 168, 187, 195, 228, 232, 235, 267, 280, 312, 340, 372, 403, 408, 420, 427, 435, 483,$$
$$520, 532, 555, 595, 627, 660, 708, 715, 760, 795, 840, 1012, 1092, 1155, 1320,$$
$$1380, 1428, 1435, 1540,1848, 1995, 3003, 3315, 5460\,.$$

Définition 5.2.3. *Soient $p_1, \ldots, p_k$ les facteurs premiers impairs de d. On définit :*

$$\chi_i(m) = \left(\frac{m}{p_i}\right) \text{ si } m \text{ est copremier à } p_i, 1 \leq i \leq k\,,$$

$$\delta(m) = (-1)^{\frac{m-1}{2}} \text{ si } m \text{ est impair} \quad , \quad \varepsilon(m) = (-1)^{\frac{m^2-1}{8}} \text{ si } m \text{ est impair}.$$

Si $-d \equiv 1 \bmod 4$, on définit les caractères assignés comme étant le uplet $\chi_1, \ldots, \chi_k$. Si $-d \equiv 0 \bmod 4$, on écrit $-d = -4\Delta$ et on définit les caractères assignés comme les uplets donnés dans le tableau suivant :

Δ	*caractères assignés*
$\Delta \equiv 3 \bmod 4$	$\chi_1, \ldots, \chi_k$
$\Delta \equiv 1 \bmod 4$	$\chi_1, \ldots, \chi_k, \delta$
$\Delta \equiv 2 \bmod 8$	$\chi_1, \ldots, \chi_k, \delta\varepsilon$
$\Delta \equiv 6 \bmod 8$	$\chi_1, \ldots, \chi_k, \varepsilon$
$\Delta \equiv 4 \bmod 8$	$\chi_1, \ldots, \chi_k, \delta$
$\Delta \equiv 0 \bmod 8$	$\chi_1, \ldots, \chi_k, \delta, \varepsilon$

Alors, on a (voir par exemple le lemme 3.20 de [**Cox89**]) :

Lemme 5.2.2. *Soit $f(x, y)$ une forme de discriminant $-d$. Alors, pour tout entier m premier à d et représenté par f, le uplet des caractères assignés évalués en m est le même. On appelle cet uplet le caractère complet de $f(x, y)$. De plus, deux formes de discriminant $-d$ sont dans le même genre si et seulement si leurs caractères complets sont les mêmes.*

Ainsi, on peut en déduire le corollaire suivant :

Corollaire 5.2.1. *Supposons qu'il n'y ait qu'une seule classe par genre. Soit m un entier copremier avec $2d$. Alors, il existe une, et une seulement, classe de formes quadratiques de déterminant $-d$ qui représente m.*

Démonstration. Puisqu'il n'y a qu'une classe par genre, chaque forme réduite a, d'après le lemme 5.2.2, un caractère complet différent. Ainsi, m ne peut pas être représenté par des formes de classes distinctes. □

Remarque 30 : Ainsi, si m est copremier à $2d$, il existe une unique classe de nombres idéaux contenant un nombre idéal entier de norme m.

Théorème 5.2.1. *Supposons que d soit dans la liste précédente. Soit $\mathbb{G}_f$ l'ensemble des $n \in \mathbb{G}$ avec $r_f(n) > 0$. Soit $\varepsilon > 0$. Alors, pour tout entier de $\mathbb{G}_f$ plus petit que x, avec au plus $o(|\mathbb{G}_f \cap [0,x]|)$ exceptions, on a*

$$\Delta_f(n) \leq \frac{r_f(n)}{(\log x)^{\frac{1}{2}\log\left(\frac{\pi}{2}\right)-\varepsilon}}\,.$$

Remarque 31 : Dans [Ber12], Bernays prouve en fait un résultat plus fort que celui énoncé dans le lemme 4.1.3. Il prouve que

$$|\mathbb{G}_f \cap [0,x]| = \frac{\kappa_d}{h}\frac{x}{\sqrt{\log x}} + O\left(\frac{x}{\log^{3/4} x}\right)\,.$$

Démonstration. Il suffit de prouver que, si $r_f(n) > 0$, on a $r_f(n) = r(n)$. Alors, on aura $\Delta_f(n) = \Delta(n)$ si $n \in \mathbb{G}_f$, ce qui donnera le résultat désiré. Soit $n = mk$ avec

$$m = \prod_{\left(\frac{-d}{p}\right)=1} p^{\alpha_p} \quad \text{et} \quad k = \prod_{\left(\frac{-d}{q}\right)=0} q^{\beta_q} \prod_{\left(\frac{-d}{r}\right)=-1} r^{2\gamma'_r}\,.$$

Si $\mathcal{C}_g$ dénote la classe $\mathcal{C}_f \prod_{\left(\frac{-d}{q}\right)=0} \mathcal{C}_q^{-\beta_q}$, où $\mathcal{C}_q$ est la classe de $\mathcal{Q}$, avec $[q] = \mathcal{Q}^2$, alors $r_f(n) = r_g(m)$.

Si $n \in \mathbb{G}_f$, alors $r_g(m) > 0$. Si $(m,2) = 1$, comme alors $(m,2d) = 1$ et qu'il n'y a qu'une classe par genre, $r_g(m) = r(m) = r(n)$. Ainsi, $r_f(n) = r(n)$.

Si $2|m$, alors $\left(\frac{-d}{2}\right) = 1$, c'est-à-dire $d \equiv \pm 1 \bmod 8$. Le seul cas de la liste avec $h > 1$ est alors $d = 15$. Dans ce cas, $h = 2$ et les deux formes réduites de discriminant -15 sont :

$$f_0(x,y) = x^2 + xy + 4y^2 \quad \text{et} \quad f_1(x,y) = 2x^2 + xy + 2y^2\,.$$

Comme $h = 2$, $\mathcal{C}_{f_i}^{-1} = \mathcal{C}_{f_i}$ pour $i \in \{0,1\}$. Si $m \in \mathbb{G}_{f_i}$ avec $m = 2^l s$, s impair, un idéal $\mathcal{I}$ de norme m dans $\mathcal{C}_{f_i}$ est de la forme

$$\mathcal{I} = [2, \frac{1+i\sqrt{15}}{2}]^{\alpha_2}[2, \frac{1-i\sqrt{15}}{2}]^{l-\alpha_2}\mathcal{J}$$

où $\mathcal{J}$ est un idéal de norme s dans la classe $\mathcal{C}_{f_i}\mathcal{C}_{f_1}^l$. Réciproquement, pour tout idéal $\mathcal{J}$ de norme s dans la classe $\mathcal{C}_{f_i}\mathcal{C}_{f_1}^l$ et pour tout choix de $0 \leq \alpha_2 \leq l$, un tel idéal est un idéal de norme m dans $\mathcal{C}_{f_i}$. Ainsi, si $m = 2^l s$, s impair, on a

$$r_{f_i}(2^l r) = (l+1)r(s) = r(m)\,.$$

□

Chapitre 6

ÉCARTS ENTRE LES NOMBRES IDÉAUX PREMIERS DANS DES SECTEURS

Le théorème des nombres premiers a pour conséquence que l'écart moyen entre deux nombres premiers consécutifs p_1 et p_2 est environ $\log p_1$. La célèbre conjecture des nombres premiers jumeaux déclare pourtant qu'il devrait exister une infinité de nombres premiers p tels que $p+2$ soit également un nombre premier.

Cette conjecture est toujours inattaquable de nos jours et c'est ainsi vers une version plus faible que la recherche s'est tournée. Plus précisément, si l'on croit en la conjecture des premiers jumeaux, il est légitime d'essayer de prouver l'existence d'une constante C et d'une infinité de couples de premiers p_1, p_2 vérifiant $|p_2 - p_1| \leq C$.

Cette question a été, au fil des ans, l'objet d'intensives études, dont l'une des pistes les plus probantes est à mettre au crédit de Goldston, Pintz et Yıldırım dans [**GPY09**]. Dans cet article séminal, les auteurs développent ce qui est aujourd'hui communément dénommé comme la méthode GPY et qui leur permet de prouver que

$$\liminf_{n\to\infty} \frac{p_{n+1} - p_n}{\log n} = 0\,,$$

où p_n dénote le n-ième nombre premier.

Ce résultat est toujours bien évidemment loin de celui escompté, mais, en se basant sur des méthodes similaires, Zhang dans [**Zha14**] montre que

$$\liminf_{n\to\infty} p_{n+1} - p_n \leq 7 \cdot 10^7\,,$$

prouvant ainsi l'existence d'une infinité de couples de nombres premiers à une distance bornée.

Loin de marquer la fin de l'histoire, de cette avancée s'ensuivent de nombreuses publications poussant plus loin l'étude de ce problème. Ainsi, quelques mois plus tard, Maynard, dans [May15], et Tao et le projet PolyMath8 [Pol13], proposent, encore une fois en se basant sur la méthode GPY, une preuve d'une incroyable simplicité. Leurs améliorations permettent alors de descendre la borne précédente à 246, mais offrent surtout une réponse à la question des écarts bornés entre les m-uplets de nombres premiers.

Un k-uplet $\mathcal{H} = (h_1, \dots, h_k)$ d'entiers positifs est dit admissible si, pour tout nombre premier p, l'ensemble $\{h_1, \dots, h_k\}$ ne couvre pas tout $\mathbb{Z}/p\mathbb{Z}$. Alors, le travail de Maynard et Tao aboutit au théorème suivant :

Théorème 6.0.2. *Soit $m \geq 2$. Il existe une constante $k_0 = k_0(m)$ telle que, pour tout k-uplet admissible $\mathcal{H} = (h_1, \dots, h_k)$ avec $k \geq k_0$, il existe une infinité d'entiers n tels que au moins m éléments parmi $n + h_1, \dots, n + h_k$ soient des nombres premiers.*

Remarque 32 : Pour tout entier k, il existe toujours un k-uplet admissible. Il suffit de prendre, par exemple, $\mathcal{H} = (p_{\pi(k)+1}, \dots, p_{\pi(k)+k})$. Alors, aucun de ces éléments n'est multiple d'un entier plus petit que k et, modulo tout premier plus grand que k, cet ensemble ne peut couvrir toutes les classes de congruences puisqu'il possède exactement k éléments.

Dans la section suivante, nous expliquons brièvement la façon dont Maynard dans [May15] conduit sa preuve, basée sur la méthode GPY, et qui sera à la base du résultat principal de ce chapitre.

6.1. Écarts entre les premiers après Maynard

On rappelle que ϕ est la fonction indicatrice d'Euler, que $\Pi(x) = |\{p \leq x, p \text{ premier}\}|$ et que $\Pi(x, q, a) = |\{p \leq x, p \equiv a \bmod q, p \text{ premier}\}|$. On appelle niveau de distribution pour les premiers tout nombre réel strictement positif θ tel que, pour tout $A > 0$,

$$\sum_{q \leq Q} \max_{(a,q)=1} \left| \Pi(x, q, a) - \frac{\Pi(x)}{\phi(q)} \right| \ll_A \frac{x}{\log^A x}$$

pour tout $Q \leq x^\theta$.

Afin de prouver le théorème 6.0.2, Maynard fournit une amélioration spectaculaire à la méthode GPY, provenant d'un choix plus général dans les poids utilisés pour le crible. Alors, là où la méthode GPY permet de déduire l'existence de premiers à distance bornée à condition que les premiers aient un niveau de distribution $\theta > 1/2$ (résultat toujours inaccessible de nos jours), Maynard n'a besoin que d'un niveau de distribution strictement positif. Or, un tel résultat est connu, par le théorème de Bombieri-Vinogradov dont l'énoncé est le suivant :

Théorème 6.1.1 (Bombieri-Vinogradov)**.** *Pour tout $A > 0$, on a*

$$\sum_{q \leq Q} \max_{(a,q)=1} \left| \Pi(x,q,a) - \frac{\Pi(x)}{\phi(q)} \right| \ll \frac{x}{\log^A x}$$

où $Q = \sqrt{x}(\log x)^{-B}$ pour $B = B(A) > 0$ et la constante impliquée ne dépend que de A.

Remarque 33 : Le théorème de Bombieri-Vinogradov donne un niveau de distribution $1/2 - \varepsilon$ pour tout $\varepsilon > 0$.

Dans ce qui suit, $\mathcal{H} = (h_1, \ldots, h_k)$ est un k-uplet admissible et $\mathbb{P}$ désigne l'ensemble des nombres premiers. Pour w_n des poids positifs (dont le choix est un élément clé de la preuve) et $W = \prod_{p \leq P_0} p$ avec $P_0 = \log\log\log N$, on définit

$$S_1(N) = \sum_{\substack{N \leq n < 2N \\ n \equiv v_0 \bmod W}} w_n \,,$$

$$S_2(N) = \sum_{\substack{N \leq n < 2N \\ n \equiv v_0 \bmod W}} \left(\sum_{i=1}^{k} \chi_{\mathbb{P}}(n + h_i) \right) w_n \,,$$

où v_0 est tel que $v_0 + h_i$ est copremier à W pour tout i (un tel v_0 existe, car $\mathcal{H}$ est admissible).

Soit $\rho > 0$. L'idée de la méthode GPY est que, si pour N assez grand, la quantité $S_2(N) - \rho S_1(N)$ est strictement positive, alors il existe $n \in [N, 2N)$ tel qu'au moins $\lfloor \rho + 1 \rfloor$ éléments parmi les $n + h_i$, $1 \leq i \leq k$, sont des nombres premiers. Le but est alors de montrer que, pour tout N assez grand, $S_2(N) - \rho S_1(N) > 0$.

Le choix des poids est primordial et se fait de la façon suivante. Soit $R = N^{\theta/2 - \varepsilon}$ pour un certain $\varepsilon > 0$ petit, où θ est le niveau de distribution des nombres premiers et est strictement positif, et soit $\mathcal{R}_k = \left\{ x \in [0,1]^k \text{ tel que } \sum_{i=1}^{k} x_i \leq 1 \right\}$. Pour une fonction $F : [0,1]^k \to \mathbb{R}^k$, infiniment différentiable, à support dans $\mathcal{R}_k$, on définit :

$$\lambda_{d_1,\ldots,d_k} = \left(\prod_{i=1}^{k} \mu(d_i) d_i \right) \sum_{\substack{r_1,\ldots,r_k \\ d_i | r_i \forall i \\ (r_i, W) = 1 \forall i}} \frac{\mu\left(\prod_{i=1}^{k} r_i \right)^2}{\prod_{i=1}^{k} \varphi(r_i)} F\left(\frac{\log(r_1)}{\log(R)}, \ldots, \frac{\log(r_k)}{\log(R)} \right).$$

Soit $d = \prod_{i=1}^{k} d_i$. Supposons que les $\lambda_{d_1,\ldots,d_k}$ soient à support dans $d < R$, d sans facteur carré et $(d, W) = 1$. On définit les poids w_n comme suit :

$$w_n = \left(\sum_{d_i | n + h_i \forall i} \lambda_{d_1,\ldots,d_k} \right)^2 .$$

Alors, dans le but d'établir sa preuve, Maynard obtient les propositions suivantes :

Proposition 6.1.1.

$$S_1 = (1+o(1))\frac{\varphi(W)^k N(\log R)^k}{W^{k+1}} I_k(F)\,,$$
$$S_2 = (1+o(1))\frac{\varphi(W)^k N(\log R)^{k+1}}{W^{k+1}\log N}\sum_{m=1}^{k} J_k^{(m)}(F)\,,$$

à condition que $I_k(F) \neq 0$ *et* $J_k^{(m)}(F) \neq 0$ *pour tout* m*, où*

$$I_k(F) = \int_0^1 \dots \int_0^1 F(t_1,\dots,t_k)^2 \,\mathrm{d}\,t_1 \dots \mathrm{d}\,t_k,$$
$$J_k^{(m)}(F) = \int_0^1 \dots \int_0^1 \left(\int_0^1 F(t_1,\dots,t_k)\,\mathrm{d}\,t_m\right)^2 \mathrm{d}\,t_1 \dots \mathrm{d}\,t_{m-1}\,\mathrm{d}\,t_{m+1}\dots\mathrm{d}\,t_k\,.$$

Proposition 6.1.2. *Soit* $\mathcal{S}_k$ *l'ensemble des fonctions intégrables au sens de Riemann* $F : [0,1]^k \to \mathbb{R}$ *à support dans* $\mathcal{R}_k$ *avec* $I_k(F) \neq 0$ *et* $J_k^{(m)}(F) \neq 0$ *pour tout* m*. Soient*

$$M_k = \sup_{F\in\mathcal{S}_k} \frac{\sum_{m=1}^k J_k^{(m)}(F)}{I_k(F)} \quad \textit{et} \quad r_k = \left\lceil \frac{\theta M_k}{2} \right\rceil .$$

Alors, il existe une infinité d'entiers n *tels qu'au moins* r_k *éléments parmi les* $n+h_i$ *(*$1 \leq i \leq k$*) soient premiers. En particulier,*

$$\liminf_n (p_{n+r_k-1} - p_n) \leq \max_{1\leq i,j\leq k}(h_i - h_j)\,.$$

Proposition 6.1.3. *On a*

$$M_5 > 2\,, \quad M_{105} > 4\,.$$

Pour $k \in \mathbb{N}$ *suffisamment grand, on a*

$$M_k > \log k - 2\log\log k - 2\,.$$

Ces propositions suffisent à conclure la preuve du théorème 6.0.2. En effet, du théorème de Bombieri-Vinogradov, on peut choisir $\theta = \frac{1}{2} - \varepsilon$. Il suffit alors de choisir $k_0 = k_0(m)$ tel que $r_{k_0} > m$ (ce qui est évidemment possible puisque $M_k \to \infty$). Et, comme expliqué dans la remarque 32, un ensemble admissible de longueur k_0 existe toujours.

6.2. Écarts entre les nombres idéaux premiers dans des secteurs

Dans tout ce qui suit, d est un entier > 0 tel que $-d$ est un discriminant fondamental. Soit $\mathcal{O}_d$ l'anneau des entiers de $\mathbb{K} = \mathbb{Q}(i\sqrt{d})$, h son nombre de classes et $\mathcal{U}$ son ensemble des unités. On rappelle que pour tout nombre idéal α, on définit $\lambda(\alpha) = \left(\frac{\alpha}{|\alpha|}\right)^{|\mathcal{U}|}$.

Définition 6.2.1. *Afin de simplifier les notations, pour un nombre idéal α, on note* $\mathrm{Arg}(\alpha) = \arg\lambda(\alpha)$. *Pour un secteur angulaire S, on note $P(\mathcal{C}, S)$ l'ensemble des normes des nombres idéaux premiers α de la classe $\mathcal{C}$ tels que* $\mathrm{Arg}(\alpha) \in S$.

Lemme 6.2.1. *Soit $\mathcal{C}$ une classe de nombres idéaux et S un secteur dans $[0, \pi)$. Alors, pour tout $n \in P(\mathcal{C}, S)$, il y a exactement $|\mathcal{U}|$ nombres idéaux premiers de norme n tels que* Arg *est dans S.*

Démonstration. Si $n \in P(\mathcal{C}, S)$, alors $n = p^2$ avec $\left(\frac{-d}{p}\right) = -1$ ou $n = p$ avec $\left(\frac{-d}{p}\right) = 0$ ou 1. On distingue donc trois cas :

• Si $n = p^2 \in P(\mathcal{C}, S)$ (et donc $0 \in S$), alors, d'après les préliminaires de la section 4, l'ensemble des nombres idéaux de norme n est l'ensemble des up avec $u \in \mathcal{U}$, et tous sont d'Arg $= 0$.

• Si $n = p \in P(\mathcal{C}, S)$ et $\left(\frac{-d}{p}\right) = 0$ (et donc $0 \in S$), alors il existe $\alpha \in \mathbb{R}$ tel que l'ensemble des nombres idéaux de norme n est l'ensemble des $u\alpha$ avec $u \in \mathcal{U}$. Tous ces nombres idéaux sont d'Arg $= 0$.

• Si $n = p \in P(\mathcal{C}, S)$ et $\left(\frac{-d}{p}\right) = 1$, alors il existe α tel que l'ensemble des nombres idéaux de norme n est l'ensemble des $u\alpha$ avec $u \in \mathcal{U}$ union l'ensemble $u\overline{\alpha}$ avec $u \in \mathcal{U}$. Comme $\mathrm{Arg}(\overline{\alpha}) = -\mathrm{Arg}(\alpha)$, exactement $|\mathcal{U}|$ de ces nombres sont tels que Arg $\in S$. □

L'objectif de cette section est de montrer le théorème suivant, analogue au théorème 6.0.2.

Théorème 6.2.1. *Soient S un secteur d'angle Ψ et $\mathcal{C}$ une classe de nombres idéaux. Soit $m \geq 2$. Alors, il existe une constante $k_0 = k_0(m, \mathbb{K}, \Psi)$ telle que, pour tout k-uplet admissible $\mathcal{H} = (h_1, \ldots, h_k)$ avec $k \geq k_0$, il existe une infinité d'entiers n tels qu'au moins m éléments parmi $n + h_1, \ldots, n + h_k$ soient la norme d'un nombre idéal premier dans la classe $\mathcal{C}$ dont l'argument est dans S.*

Remarque 34 : La preuve de ce théorème permet de trouver explicitement une valeur de k_0 qui convient. Plus précisément, on trouve que

$$k_0 = \lceil C \left(\frac{4\pi h}{2^{\omega(d)}\Psi} m\right)^2 \exp\left(\frac{16\pi h}{2^{\omega(d)}\Psi} m\right) \rceil$$

convient, pour une certaine constante absolue C.

Alors, du théorème 6.2.1, on peut déduire les corollaires suivants :

Corollaire 6.2.1. *Dans toute classe de nombres idéaux, pour tout secteur angulaire S de taille Ψ, il existe une constante $c(\mathbb{K}, \Psi)$ et une infinité de couples de nombres idéaux premiers π_1, π_2 tels que* $\mathrm{Arg}(\pi_j) \in S$, $j = 1, 2$ *et* $|N(\pi_1) - N(\pi_2)| \leq c(\mathbb{K}, \Psi)$.

Démonstration. On choisit notre ensemble admissible pour le théorème 6.2.1 de la forme $\mathcal{H} = (p_{\pi(k)+1}, \ldots, p_{\pi(k)+k})$. Cet ensemble est bien admissible, puisqu'aucun de ses

éléments n'est multiple d'un premier plus petit que k et il contient k éléments, qui ne peuvent donc couvrir toutes les classes de congruence modulo tout premier plus grand que k.

Pour cet ensemble, $\max_{1\leq i,j\leq k}(h_i-h_j) = p_{\pi(k)+k}-p_{\pi(k)+1} \ll k\log k$. On choisit maintenant $k = k_0(2,\mathbb{K},\Psi)$ pour la valeur de k_0 donnée par le théorème 6.2.1. Alors, par ce même théorème, il existe une infinité d'entiers n tels qu'au moins deux éléments parmi $n+h_1,\ldots,n+h_k$ soient la norme d'un nombre idéal premier dans la classe $\mathcal{C}$ dont l'argument est dans S, et donc une infinité de couples de nombres idéaux premiers π_1, π_2 de $\mathcal{C}$ tels que $\mathrm{Arg}(\pi_j)\in S$, $j=1,2$ et $|N(\pi_1)-N(\pi_2)|\leq k_0\log k_0$. □

Remarque 35 : Ce résultat est évidemment également vrai avec arg au lieu de Arg.

Corollaire 6.2.2. *Dans toute extension quadratique imaginaire $\mathbb{K}$, pour tout secteur angulaire S de taille Ψ, il existe une constante $c(\mathbb{K},\Psi)$ et une infinité de couples de nombres premiers π_1, π_2 de $\mathcal{O}_\mathbb{K}$ tels que* $\arg(\pi_j)\in S$, $j=1,2$ *et* $|N(\pi_1)-N(\pi_2)|\leq c(\mathbb{K},\Psi)$.

Démonstration. On utilise simplement le corollaire précédent (dans sa version pour arg) pour la classe principale. En effet, si α est un nombre idéal premier dans la classe principale, alors α est un premier de $\mathcal{O}_\mathbb{K}$. □

Corollaire 6.2.3. *Soit $f(x,y)$ une forme quadratique réduite définie positive. Alors, pour tout secteur angulaire S de taille Ψ, il existe une constante $c(f,\Psi)$ et une infinité de couples de nombres premiers p_1, p_2 tels que $|p_1-p_2|\leq c(f,\Psi)$ et $p_i = f(x_i,y_i)$ avec $x_i,y_i\in\mathbb{Z}$ et $(x_i,y_i)\in S$.*

Démonstration. Quitte à réduire la taille du secteur, on peut supposer que $0\notin S$. On utilise alors le lemme 5.2.1 et le corollaire 6.2.1 appliqués à la classe $\mathcal{C}_f$ et à un secteur $S'-\arg(\omega_{\mathfrak{b}_f})$ tel que, si $(ax+\frac{b}{2}y,\frac{\sqrt{d}}{2}y)\in S'$, alors $(x,y)\in S$. □

Dans ce qui suit, on note θ le niveau de distribution de l'ensemble des nombres idéaux premiers. D'après le théorème 4.1.3, on peut prendre $\theta = 1/4-\varepsilon$ pour tout $\varepsilon>0$. De façon analogue à la section précédente, on définit $\mathcal{R}_k = \left\{x\in[0,1]^k \text{ tel que } \sum_{i=1}^k x_i\leq 1\right\}$ et $R = N^{\theta/2-\varepsilon}$ pour un certain $\varepsilon>0$ petit. Pour une fonction $F:[0,1]^k\to\mathbb{R}^k$, infiniment différentiable, à support dans $\mathcal{R}_k$, on définit :

$$\lambda_{d_1,\ldots,d_k} = \left(\prod_{i=1}^k \mu(d_i)d_i\right) \sum_{\substack{r_1,\ldots,r_k\\ d_i|r_i\forall i\\ (r_i,W)=1\forall i}} \frac{\mu\left(\prod_{i=1}^k r_i\right)^2}{\prod_{i=1}^k\varphi(r_i)} F\left(\frac{\log(r_1)}{\log(R)},\ldots,\frac{\log(r_k)}{\log(R)}\right).$$

Soit $D=\prod_{i=1}^k d_i$. Supposons que les $\lambda_{d_1,\ldots,d_k}$ soient à support dans $D<R$, D sans facteur carré et $(D,W)=1$.

Soit $W = \prod_{p \le P_0} p$ avec $P_0 = \log\log\log N$. En particulier, $W \ll (\log\log N)^2$. On choisit N grand, tel que le plus grand facteur premier de d soit plus petit que P_0 (ainsi, $d|W$). On définit

$$S_1 = \sum_{\substack{N \le n < 2N \\ n \equiv v_0 \bmod W}} \left(\sum_{d_i | n+h_i \forall i} \lambda_{d_1,\dots,d_k} \right)^2,$$

$$S_2 = \sum_{\substack{N \le n < 2N \\ n \equiv v_0 \bmod W}} \left(\sum_{i=1}^{k} \chi_{P(\mathcal{C},S)}(n+h_i) \right) \left(\sum_{d_i | n+h_i \forall i} \lambda_{d_1,\dots,d_k} \right)^2,$$

où v_0 est tel que v_0+h_i est copremier à W pour tout i (un tel v_0 existe, car $\mathcal{H}$ est admissible). Comme précédemment, l'idée est de montrer que pour un certain $\rho > 1$, $S_2 - \rho S_1 > 0$ pour tout N assez grand, et ainsi qu'il existe une infinité d'entiers n tels que $\lfloor \rho + 1 \rfloor$ éléments parmi les $n + h_i$ appartiennent à $P(\mathcal{C}, S)$.

Proposition 6.2.1.

$$S_1 = (1+o(1)) \frac{\varphi(W)^k N (\log R)^k}{W^{k+1}} I_k(F),$$

$$S_2 = (1+o(1)) \frac{2^{\omega(d)}\Psi}{2\pi h} \frac{\varphi(W)^k N (\log R)^{k+1}}{W^{k+1} \log N} \sum_{m=1}^{k} J_k^{(m)}(F),$$

à condition que $I_k(F) \neq 0$ *et* $J_k^{(m)}(F) \neq 0$ *pour tout* m, *où*

$$I_k(F) = \int_0^1 \dots \int_0^1 F(t_1,\dots,t_k)^2 \,\mathrm{d}\, t_1 \dots \mathrm{d}\, t_k,$$

$$J_k^{(m)}(F) = \int_0^1 \dots \int_0^1 \left(\int_0^1 F(t_1,\dots,t_k) \,\mathrm{d}\, t_m \right)^2 \mathrm{d}\, t_1 \dots \mathrm{d}\, t_{m-1} \,\mathrm{d}\, t_{m+1} \dots \mathrm{d}\, t_k .$$

Démonstration. Pour S_1, nous référons à la preuve de la proposition 4.1 de [**May15**], dont nous rappelons simplement les grandes étapes ci-dessous. On a :

$$S_1 = \sum_{\substack{d_1,\dots,d_k \\ e_1,\dots,e_k}} \lambda_{d_1,\dots,d_k} \lambda_{e_1,\dots,e_k} \sum_{\substack{N \le n < 2N \\ n \equiv v_0 \bmod W \\ [d_i,e_i] | n+h_i \forall i}} 1 .$$

Si les $[d_i, e_i]$ sont premiers deux à deux, la somme intérieure peut être écrite comme une somme sur une unique classe de congruence modulo $q = W \prod_{i=1}^k [d_i, e_i]$ et dans le cas contraire la somme est vide. Ainsi,

$$S_1 = \frac{N}{W} \sum_{\substack{d_1,\dots,d_k \\ e_1,\dots,e_k}}{}' \frac{\lambda_{d_1,\dots,d_k} \lambda_{e_1,\dots,e_k}}{\prod_{i=1}^k [d_i, e_i]} + O\Big(\sum_{\substack{d_1,\dots,d_k \\ e_1,\dots,e_k}}{}' |\lambda_{d_1,\dots,d_k} \lambda_{e_1,\dots,e_k}| \Big)$$

où $\sum'$ indique que les $[d_i, e_i]$ sont premiers deux à deux.

Alors, en effectuant le changement de variables (inversible)

$$y_{r_1,\dots,r_k} = \left(\prod_{i=1}^{k} \mu(r_i)\varphi(r_i)\right) \sum_{\substack{d_1,\dots,d_k \\ r_i | d_i \forall i}} \frac{\lambda_{d_1,\dots,d_k}}{\prod_{i=1}^{k} d_i}$$

et en remarquant que la contribution principale provient des termes diagonaux, on obtient

$$S_1 = \frac{N}{W} \sum_{u_1,\dots,u_k} \frac{y_{u_1,\dots,u_k}^k}{\prod_{i=1}^{k} \varphi(u_i)} + O\left(\frac{y_{\max}^2 \varphi(W)^k N (\log R)^k}{W^{k+1} P_0}\right),$$

où $y_{\max} = \sup_{r_1,\dots,r_k} |y_{r_1,\dots,r_k}|$. Le résultat découlera alors du choix des $y_{u_1,\dots,u_k}$, dont nous reparlerons lors du traitement de la somme S_2.

Pour S_2, on écrit $S_2 = \sum_{m=1}^{k} S_2^{(m)}$, où

$$S_2^{(m)} = \sum_{\substack{N \le n < 2N \\ n \equiv v_0 \bmod W}} \chi_{P(\mathcal{C},S)}(n + h_m) \left(\sum_{d_i | n + h_i \forall i} \lambda_{d_1,\dots,d_k}\right)^2.$$

En développant le carré et en changeant l'ordre de sommation, on obtient

$$S_2^{(m)} = \sum_{\substack{d_1,\dots,d_k \\ e_1,\dots,e_k}} \lambda_{d_1,\dots,d_k} \lambda_{e_1,\dots,e_k} \sum_{\substack{N \le n < 2N \\ n \equiv v_0 \bmod W \\ [d_i,e_i] | n + h_i \forall i}} \chi_{P(\mathcal{C},S)}(n + h_m).$$

Si les $[d_i, e_i]$ sont premiers deux à deux, la somme intérieure peut être écrite comme une somme sur une unique classe de congruence modulo $q = W \prod_{i=1}^{k} [d_i, e_i]$. Remarquons que, puisque $n + h_m \in P(\mathcal{C}, S)$, $n + h_m$ est un nombre premier ou le carré d'un nombre premier p. Dans les deux cas, supposons que $d_m \neq 1$. Alors, $d_m = p \ge \sqrt{N + h_m}$. Mais $\prod_{i=1}^{k} d_i < R = N^{\frac{\theta}{2} - \varepsilon}$ et $\theta < 1$. Ainsi, $d_m = e_m = 1$.

Si les $[d_i, e_i]$ ne sont pas premiers deux à deux, alors la somme est vide. En effet, le plus grand facteur premier du diviseur commun devrait diviser $h_i - h_j$, qui est une quantité bornée, mais ce facteur premier doit également être $> \log\log\log N$ car $(W, \prod_{i=1}^{k} d_i) = 1$. Ceci ne peut évidemment pas arriver si N est assez grand.

Alors,

$$S_2^{(m)} = \sum_{\substack{d_1,\dots,d_k \\ e_1,\dots,e_k \\ d_m = e_m = 1}}' \lambda_{d_1,\dots,d_k} \lambda_{e_1,\dots,e_k} \sum_{\substack{N \le n < 2N \\ n \equiv c \bmod q}} \chi_{P(\mathcal{C},S)}(n + h_m),$$

où $\sum'$ indique que les $[d_i, e_i]$ sont premiers deux à deux. Or, par le lemme 6.2.1,

$$\begin{aligned}\sum_{\substack{N\leq n<2N\\ n\equiv c \bmod q}} \chi_{P(\mathcal{C},S)}(n+h_m) &= \frac{1}{|\mathcal{U}|} \sum_{\substack{\pi\in\mathcal{C},\mathrm{Arg}(\pi)\in S\\ N+h_m\leq N(\pi)<2N+h_m\\ N(\pi)\equiv c+h_m \bmod q}} 1\\ &= \frac{\Psi}{2\pi h\varphi'(q)}\int_{N+h_m}^{2N+h_m}\frac{\mathrm{d}\,u}{\log u}+O(E(N,q,h_m))\,,\end{aligned}$$

où

$$E(N,q,h_m)=1+\max_{(a,q)=1}\left|\sum_{\substack{\pi\in\mathcal{C},\mathrm{Arg}(\pi)\in S\\ N+h_m\leq N(\pi)<2N+h_m\\ N(\pi)\equiv a \bmod q}} 1-\frac{\Psi|\mathcal{U}|}{2\pi h\varphi'(q)}\int_{N+h_m}^{2N+h_m}\frac{\mathrm{d}\,u}{\log u}\right|.$$

En remplaçant dans l'expression de $S_2^{(m)}$, on a

$$\begin{aligned}S_2^{(m)} &= \frac{\Psi}{2\pi h\varphi'(W)}\int_{N+h_m}^{2N+h_m}\frac{\mathrm{d}\,u}{\log u}\sum_{\substack{d_1,\dots,d_k\\ e_1,\dots,e_k\\ d_m=e_m=1}}'\frac{\lambda_{d_1,\dots,d_k}\lambda_{e_1,\dots,e_k}}{\varphi'(\prod_{i=1}^k[d_i,e_i])}+O(\lambda_{\max}^2\sum_{\substack{d_1,\dots,d_k\\ e_1,\dots,e_k}}'E(N,q,h_m))\\ &= \frac{2^{\omega(d)}\Psi}{2\pi h\varphi(W)}\int_{N+h_m}^{2N+h_m}\frac{\mathrm{d}\,u}{\log u}\sum_{\substack{d_1,\dots,d_k\\ e_1,\dots,e_k\\ d_m=e_m=1}}'\frac{\lambda_{d_1,\dots,d_k}\lambda_{e_1,\dots,e_k}}{\varphi(\prod_{i=1}^k[d_i,e_i])}+O(\lambda_{\max}^2\sum_{\substack{d_1,\dots,d_k\\ e_1,\dots,e_k}}'E(N,q,h_m))\end{aligned}$$

en utilisant le lemme 4.1.2 et le fait que, puisque N est grand, $d|W$.

On s'intéresse maintenant au terme d'erreur. Étant donné le support de $\lambda_{d_1,\dots,d_k}$, il nous suffit de considérer les $q<R^2W$ sans facteur carré. Étant donné un entier r sans facteur carré, il y a au plus τ_{3k} choix de $d_1,\dots,d_k,e_1,\dots,e_k$ pour lesquels $W\prod_{i=1}^k[d_i,e_i]=r$. Ainsi, pour un $A>0$ fixé,

$$\begin{aligned}\sum_{\substack{d_1,\dots,d_k\\ e_1,\dots,e_k}}'E(N,q,h_m) &\ll \sum_{r<R^2W}\mu(r)^2\tau_{3k}(r)E(N,r,h_m)\\ &\ll \left(\sum_{r<R^2W}\mu(r)^2\tau_{3k}(r)^2\frac{N}{\varphi(r)}\right)^{\frac12}\left(\sum_{r<R^2W}\mu(r)^2E(N,r,h_m)\right)^{\frac12}\\ &\ll \frac{N}{\log^A N}\end{aligned}$$

en utilisant l'inégalité de Cauchy-Schwarz, l'estimation triviale $E(N,r,h_m)\ll\frac{N}{\varphi(r)}$ et le théorème 4.1.3 (puisque $R^2W\leq N^{\theta-\varepsilon}$ par notre choix de R et W).

Ainsi,

$$S_2^m = \frac{2^{\omega(d)}\Psi}{2\pi h\varphi(W)} \int_{N+h_m}^{2N+h_m} \frac{\mathrm{d}\, u}{\log u} \sideset{}{'}\sum_{\substack{d_1,\dots,d_k\\ e_1,\dots,e_k}} \frac{\lambda_{d_1,\dots,d_k}\lambda_{e_1,\dots,e_k}}{\varphi(\prod_{i=1}^k [d_i,e_i])} + O(\lambda_{\max}^2 \frac{N}{\log^A N}) .$$

La somme du terme principal est la même que celle traitée dans [**May15**]. On termine alors la preuve de façon similaire aux preuves des lemmes 5.2 et 6.3 de cet article, que l'on esquisse ci-dessous, en rappelant que

$$\int_{N+h_m}^{2N+h_m} \frac{\mathrm{d}\, u}{\log u} = \frac{N}{\log N} + O\left(\frac{N}{\log^2 N}\right) .$$

On effectue le changement de variables (inversible)

$$y^{(m)}_{r_1,\dots,r_k} = \left(\prod_{i=1}^k \mu(r_i) g(r_i)\right) \sum_{\substack{d_1,\dots,d_k\\ r_i | d_i \forall i\\ d_m = 1}} \frac{\lambda_{d_1,\dots,d_k}}{\prod_{i=1}^k \varphi(d_i)} ,$$

où g est totalement multiplicative avec $g(p) = p-2$. Alors la contribution principale vient des termes diagonaux et on obtient :

$$S_2^m = \frac{2^{\omega(d)}\Psi}{2\pi h\varphi(W)} \int_{N+h_m}^{2N+h_m} \frac{\mathrm{d}\, u}{\log u} \sum_{u_1,\dots,u_k} \frac{(y^{(m)}_{u_1,\dots,u_k})^2}{\prod_{i=1}^k g(u_i)} + O\left(\frac{(y^{(m)}_{\max})^2 \varphi(W)^{k-2} N (\log R)^{k-2}}{P_0 W^{k-1}}\right) + O\left(y_{\max}^2 \frac{N}{\log^A N}\right) .$$

Or, si $r_m = 1$, il est possible de montrer que

$$y^{(m)}_{r_1,\dots,r_k} = \sum_{a_m} \frac{y_{r_1,\dots,r_{m-1},a_m,r_{m+1},\dots,r_k}}{\varphi(a_m)} + O\left(\frac{y_{\max}\varphi(W)\log R}{W P_0}\right) .$$

Il reste alors à choisir les $y_{r_1,\dots,r_k}$. Pour $r = \prod_{i=1}^k r_i$ sans facteur carré satisfaisant $(r, W) = 1$, on choisit

$$y_{r_1,\dots,r_k} = F\left(\frac{\log(r_1)}{\log(R)}, \dots, \frac{\log(r_k)}{\log(R)}\right)$$

pour une fonction $F : [0,1]^k \to \mathbb{R}^k$, infiniment différentiable, à support dans $\mathcal{R}_k$ où $\mathcal{R}_k = \left\{x \in [0,1]^k \text{ tel que } \sum_{i=1}^k x_i \leq 1\right\}$ (l'objectif sera ensuite d'optimiser le choix de la fonction F). $y_{r_1,\dots,r_k}$ est pris comme nul en dehors de cet ensemble.

Alors, en utilisant le lemme 4 de [**GGPY09**], qui permet de réécrire les sommes de $y_{r_1,\dots,r_k}$ comme des intégrales de la fonction F, on obtient le résultat escompté. □

Proposition 6.2.2. *Soit $\mathcal{H} = (h_1, \dots, h_k)$ un k-uplet admissible. Soient $I_k(F)$ et $J_k^{(m)}(F)$ comme définis dans la proposition 6.2.1 et soit $\mathcal{S}_k$ l'ensemble des fonctions intégrables au sens de Riemann $F : [0,1]^k \to \mathbb{R}$ à support dans $\mathcal{R}_k$ avec $I_k(F) \neq 0$ et $J_k^{(m)}(F) \neq 0$ pour tout m. Soient*

$$M_k = \sup_{F \in \mathcal{S}_k} \frac{\sum_{m=1}^k J_k^{(m)}(F)}{I_k(F)} \quad \text{et} \quad r_k = \left\lceil \frac{2^{\omega(d)}\Psi}{2\pi h} \frac{\theta M_k}{2} \right\rceil .$$

Alors, il existe une infinité d'entiers n tels qu'au moins r_k éléments parmi les $n + h_i$ $(1 \leq i \leq k)$ appartiennent à $P(\mathcal{C}, S)$.

Démonstration. Soit $S = S_2 - \rho S_1$. Comme expliqué précédemment, si $S > 0$ pour tout N assez grand, alors il existe une infinité d'entiers n tels qu'au moins $\lfloor \rho + 1 \rfloor$ éléments parmi les $n + h_i$ appartiennent à $P(\mathcal{C}, S)$.

Rappelons que $R = N^{\theta/2-\varepsilon}$ pour un $\varepsilon > 0$ petit. Par définition de M_k, on peut choisir $F_0 \in \mathcal{S}_k$ tel que $\sum_{m=1}^k J_k^{(m)}(F_0) > (M_k - \varepsilon) I_k(F_0) > 0$. F_0 étant intégrable au sens de Riemann, il existe une fonction lisse F_1 telle que $\sum_{m=1}^k J_k^{(m)}(F_1) > (M_k - 2\varepsilon) I_k(F_1) > 0$.

À l'aide de la proposition 6.2.1, on a

$$\begin{aligned} S &= \frac{\varphi(W)^k N (\log R)^k}{W^{k+1}} \left(\frac{2^{\omega(d)}\Psi}{2\pi h} \frac{\log R}{\log N} \sum_{m=1}^k J_k^{(m)}(F_1) - \rho I_k(F_1) + o(1) \right) \\ &\geq \frac{\varphi(W)^k N (\log R)^k}{W^{k+1}} I_k(F_1) \left[\frac{2^{\omega(d)}\Psi}{2\pi h} \left(\frac{\theta}{2} - \varepsilon \right) (M_k - 2\varepsilon) - \rho + o(1) \right] . \end{aligned}$$

Soient

$$\delta > 0 \quad \text{et} \quad \rho = \left(\frac{2^{\omega(d)}\Psi}{4\pi h} \theta - \delta \right) M_k .$$

En choisissant ε suffisamment petit, on a $S > 0$ pour tout N assez grand. Ainsi, il existe une infinité d'entiers n tels qu'au moins $\lfloor \rho + 1 \rfloor$ éléments parmi les $n + h_i$ appartiennent à $P(\mathcal{C}, S)$. Mais, si δ est suffisamment petit,

$$\lfloor \rho + 1 \rfloor = \lceil \frac{2^{\omega(d)}\Psi}{4\pi h} \theta M_k \rceil .$$

□

Proposition 6.2.3. *Pour k suffisamment grand, on a*

$$M_k \geq \log k - 2 \log \log k - 2 .$$

Démonstration. C'est la section 7 [May15], dont nous rappelons rapidement ici l'idée principale. Le but est d'optimiser le choix de la fonction F pour maximiser la quantité

$$\frac{\sum_{m=1}^{k} J_k^{(m)}(F)}{I_k(F)}\,.$$

On va chercher F sous la forme

$$F(t_1,\dots,t_k) = \begin{cases} \prod_{i=1}^{k} g(kt_i) \text{ si } \sum_{i=1}^{k} t_i \leq 1\,, \\ 0 \text{ sinon}\,, \end{cases}$$

pour une fonction lisse g supportée dans $[0,T]$ (pour un T que l'on choisira par la suite), de second moment strictement positif et telle que le centre de masse de g^2 soit strictement plus petit que $1-\frac{T}{k}$. Alors, maximiser M_k donne g de la forme $1/(1+At)$ pour $t\in[0,T]$, pour une constante positive A. En optimisant T et A, on obtient le résultat. □

On peut maintenant prouver le théorème 6.2.1.

Preuve du théorème 6.2.1. Par la proposition 6.2.2, il suffit de trouver k tel que $r_k \geq m$, c'est-à-dire

$$\frac{2^{\omega(d)}\Psi}{2\pi h}\frac{\theta M_k}{2} > m-1\,.$$

Par la proposition 6.2.3, il suffit donc de trouver k tel que

$$\frac{2^{\omega(d)}\Psi}{2\pi h}\frac{\theta(\log k - 2\log\log k - 2)}{2} > m-1\,.$$

D'après le théorème 4.1.3, on sait que θ peut être choisi aussi grand que $\frac{1}{4}-\varepsilon$, pour tout $\varepsilon>0$. Pour $\varepsilon=\frac{1}{2k}$, après calcul il est possible de montrer que l'équation précédente est vraie si

$$k \geq k_0 = \lceil C\left(\frac{4\pi h}{2^{\omega(d)}\Psi}m\right)^2 \exp\left(\frac{16\pi h}{2^{\omega(d)}\Psi}m\right)\rceil$$

pour une certaine constante absolue C. □

Remarque 36 : L'énoncé du théorème 6.2.1 n'est pas totalement satisfaisant. Il serait intéressant de pouvoir étudier le problème des écarts bornés entre les premiers dans des secteurs étroits. Plus précisément, on aimerait pouvoir obtenir la positivité de la quantité $S_2(N)-\rho S_1(N)$ pour un secteur d'angle $\Psi = N^{-\alpha}$, avec α strictement positif, qu'on pourrait espérer aller possiblement jusqu'à $\frac{1}{4}$ pour être cohérent avec le niveau de distribution donné par le théorème 4.1.3. L'auteur de cette thèse n'a malheureusement pas été en mesure d'obtenir un tel résultat.

BIBLIOGRAPHIE

[Alb03] Toma Albu : *Cogalois theory*, volume 252 de *Monographs and Textbooks in Pure and Applied Mathematics*. Marcel Dekker, Inc., New York, 2003.

[AN95] Toma Albu et Florin Nicolae : Heckesche Systeme idealer Zahlen und Knesersche Körpererweiterungen. *Acta Arith.*, 73(1):43–50, 1995.

[Bea83] Alan F. Beardon : *The geometry of discrete groups*, volume 91 de *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1983.

[Ber12] Paul Bernays : *Über die Darstellung von positiven, ganzen Zahlen durch die primitiven, binären quadratischen Formen einer nicht-quadratischen Diskriminante*. Dieterich, 1912.

[BF11] Jean Bourgain et Elena Fuchs : A proof of the positive density conjecture for integer Apollonian circle packings. *J. Amer. Math. Soc.*, 24(4):945–967, 2011.

[BK14] Jean Bourgain et Alex Kontorovich : On the local-global conjecture for integral Apollonian gaskets. *Invent. Math.*, 196(3):589–650, 2014. With an appendix by Péter P. Varjú.

[Boy82] David W. Boyd : The sequence of radii of the Apollonian packing. *Math. Comp.*, 39(159):249–254, 1982.

[Bru92] A. M. Brunner : A two-generator presentation for the Picard group. *Proc. Amer. Math. Soc.*, 115(1):45–46, 1992.

[BS66] A. I. Borevich et I. R. Shafarevich : *Number theory*. Translated from the Russian by Newcomb Greenleaf. Pure and Applied Mathematics, Vol. 20. Academic Press, New York-London, 1966.

[Cas78] J. W. S. Cassels : *Rational quadratic forms*, volume 13 de *London Mathematical Society Monographs*. Academic Press Inc. [Harcourt Brace Jovanovich Publishers], London, 1978.

[Cil93] Javier Cilleruelo : The distribution of the lattice points on circles. *J. Number Theory*, 43(2):198–202, 1993.

[Cox89] David A. Cox : *Primes of the form $x^2 + ny^2$*. A Wiley-Interscience Publication. John Wiley & Sons Inc., New York, 1989. Fermat, class field theory and complex multiplication.

[Dja11] Goran Djanković : The Erdős-Kac theorem for curvatures in integral Apollonian circle packings. *Publ. Inst. Math. (Beograd) (N.S.)*, 89(103):11–17, 2011.

[EGM98] J. Elstrodt, F. Grunewald et J. Mennicke : *Groups acting on hyperbolic space*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 1998. Harmonic analysis and number theory.

[EH99] P. Erdős et R. R. Hall : On the angular distribution of Gaussian integers with fixed norm. *Discrete Math.*, 200(1-3):87–94, 1999. Paul Erdős memorial collection.

[ET48a] P. Erdös et P. Turán : On a problem in the theory of uniform distribution. I. *Nederl. Akad. Wetensch., Proc.*, 51:1146–1154 Indagationes Math. 10, 370–378 (1948), 1948.

[ET48b] P. Erdös et P. Turán : On a problem in the theory of uniform distribution. II. *Nederl. Akad. Wetensch., Proc.*, 51:1262–1269 Indagationes Math. 10, 406–413 (1948), 1948.

[FN87] Benjamin Fine et Morris Newman : The normal subgroup structure of the Picard group. *Trans. Amer. Math. Soc.*, 302(2):769–786, 1987.

[Fog62] E. Fogels : On the distribution of prime ideals. *Acta Arith.*, 7:255–269, 1961/1962.

[FS11] Elena Fuchs et Katherine Sanden : Some experiments with integral Apollonian circle packings. *Exp. Math.*, 20(4):380–399, 2011.

[Fuc11] Elena Fuchs : Strong approximation in the Apollonian group. *J. Number Theory*, 131(12):2282–2302, 2011.

[GGPY09] D. A. Goldston, S. W. Graham, J. Pintz et C. Y. Yildirim : Small gaps between products of two primes. *Proc. Lond. Math. Soc. (3)*, 98(3):741–774, 2009.

[GLM+03] Ronald L. Graham, Jeffrey C. Lagarias, Colin L. Mallows, Allan R. Wilks et Catherine H. Yan : Apollonian circle packings : number theory. *J. Number Theory*, 100(1):1–45, 2003.

[GM10] Gerhard Guettler et Colin Mallows : A generalization of Apollonian packing of circles. *J. Comb.*, 1(1, [ISSN 1097-959X on cover]):1–27, 2010.

[Gos37] Thorold Gosset : The kiss precise (generalized). *Nature*, (139):62, 1937.

[GOS10] Alexander Gorodnik, Hee Oh et Nimish Shah : Strong wavefront lemma and counting lattice points in sectors. *Israel J. Math.*, 176:419–444, 2010.

[GPY09] Daniel A. Goldston, János Pintz et Cem Y. Yildirim : Primes in tuples. I. *Ann. of Math. (2)*, 170(2):819–862, 2009.

[GS07] Andrew Granville et K. Soundararajan : Sieving and the Erdős-Kac theorem. *In Equidistribution in number theory, an introduction*, volume 237 de *NATO Sci. Ser. II Math. Phys. Chem.*, pages 15–27. Springer, Dordrecht, 2007.

[HB96] D. R. Heath-Brown : A new form of the circle method, and its application to quadratic forms. *J. Reine Angew. Math.*, 481:149–206, 1996.

[Hec18] E. Hecke : Eine neue Art von Zetafunktionen und ihre Beziehungen zur Verteilung der Primzahlen. *Math. Z.*, 1(4):357–376, 1918.

[Hec20] E. Hecke : Eine neue Art von Zetafunktionen und ihre Beziehungen zur Verteilung der Primzahlen. *Math. Z.*, 6(1-2):11–51, 1920.

[Hir67] K. E. Hirst : The Apollonian packing of circles. *J. London Math. Soc.*, 42:281–291, 1967.

[IK04] Henryk Iwaniec et Emmanuel Kowalski : *Analytic number theory*, volume 53 de *American Mathematical Society Colloquium Publications*. American Mathematical Society, Providence, RI, 2004.

[Kát76] I. Kátai : The distribution of divisors mod1. *Acta Math. Acad. Sci. Hungar.*, 27(1–2):149–152, 1976.

[KO11] Alex Kontorovich et Hee Oh : Apollonian circle packings and closed horospheres on hyperbolic 3-manifolds. *J. Amer. Math. Soc.*, 24(3):603–648, 2011. With an appendix by Oh and Nimish Shah.

[Kon12] A. Kontorovich : The Local-Global Principle for Integral Soddy Sphere Packings. *ArXiv e-prints*, août 2012.

[Kov75] F. B. Koval'chik : Density theorems for sectors and progressions. *Litovsk. Mat. Sb.*, 15(4):133–151, 245, 1975.

[Kub52] I. P. Kubilyus : On some problems of the geometry of prime numbers. *Mat. Sbornik N.S.*, 31(73):507–542, 1952.

[Lar67] D. G. Larman : On the Besicovitch dimension of the residual set of arbitrarily packed disks in the plane. *J. London Math. Soc.*, 42:292–302, 1967.

[LO13] Min Lee et Hee Oh : Effective circle count for Apollonian packings and closed horospheres. *Geom. Funct. Anal.*, 23(2):580–621, 2013.

[LP82] Peter D. Lax et Ralph S. Phillips : The asymptotic distribution of lattice points in Euclidean and non-Euclidean spaces. *J. Funct. Anal.*, 46(3):280–350, 1982.

[May15] James Maynard : Small gaps between primes. *Ann. of Math. (2)*, 181(1):383–413, 2015.

[McM98] Curtis T. McMullen : Hausdorff dimension and conformal dynamics. III. Computation of dimension. *Amer. J. Math.*, 120(4):691–721, 1998.

[Mit56] Takayoshi Mitsui : Generalized prime number theorem. *Jap. J. Math.*, 26:1–42, 1956.

[MO15] Amir Mohammadi et Hee Oh : Matrix coefficients, counting and primes for orbits of geometrically finite groups. *J. Eur. Math. Soc. (JEMS)*, 17(4):837–897, 2015.

[Nak14] K. Nakamura : The local-global principle for integral bends in orthoplicial Apollonian sphere packings. *ArXiv e-prints*, janvier 2014.

[Pol13] PolyMath8 : Bounded gaps between primes. http://michaelnielsen.org/polymath1/index.php?title=Bounded_gaps_between_primes, 2013.

[Sar08] Peter Sarnak : Letter to lagarias on apollonian circle packings, 2008.

[Sie35] Carl Ludwig Siegel : Über die analytische Theorie der quadratischen Formen. *Ann. of Math. (2)*, 36(3):527–606, 1935.

[Sod36] Frederick Soddy : The kiss precise. *Nature*, (137):1021, 1936.

[Sul79a] Dennis Sullivan : The density at infinity of a discrete group of hyperbolic motions. *Inst. Hautes Études Sci. Publ. Math.*, (50):171–202, 1979.

[Sul79b] Dennis Sullivan : The density at infinity of a discrete group of hyperbolic motions. *Inst. Hautes Études Sci. Publ. Math.*, (50):171–202, 1979.

[Vin14] Ilya Vinogradov : Effective bisector estimate with application to Apollonian circle packings. *Int. Math. Res. Not. IMRN*, (12):3217–3262, 2014.

[Wei73] P. J. Weinberger : Exponents of the class groups of complex quadratic fields. *Acta Arith.*, 22:117–124, 1973.

[Wil81] J. B. Wilker : Inversive geometry. *In The geometric vein*, pages 379–442. Springer, New York-Berlin, 1981.

[Zha13] X. Zhang : On the Local-Global Principle for Integral Apollonian-3 Circle Packings. *ArXiv e-prints*, décembre 2013.

[Zha14] Yitang Zhang : Bounded gaps between primes. *Ann. of Math. (2)*, 179(3):1121–1174, 2014.

Annexe A

THE KISS PRECISE

The Kiss Precise

For pairs of lips to kiss maybe
Involves no trigonometry.
This not so when four circles kiss
Each one the other three.
To bring this off the four must be
As three in one or one in three.
If one in three, beyond a doubt
Each gets three kisses from without.
If three in one, then is that one
Thrice kissed internally.

Four circles to the kissing come.
The smaller are the benter.
The bend is just the inverse of
The distance form the center.
Though their intrigue left Euclid dumb
There's now no need for rule of thumb.
Since zero bend's a dead straight line
And concave bends have minus sign,
The sum of the squares of all four bends
Is half the square of their sum.

Frederick Soddy

The Kiss Precise (Extended)

To spy out spherical affairs
An oscular surveyor
Might find the task laborious,
The sphere is much the gayer,
And now besides the pair of pairs
A fifth sphere in the kissing shares.
Yet, signs and zero as before,
For each to kiss the other four
The square of the sum of all five bends
Is thrice the sum of their squares.

Frederick Soddy

The Kiss Precise (Generalized)

And let us not confine our cares
To simple circles, planes and spheres,
But rise to hyper flats and bends
Where kissing multiple appears,
In n-ic space the kissing pairs
Are hyperspheres, and Truth declares,
As $n + 2$ such osculate
Each with an $n + 1$ fold mate
The square of the sum of all the bends
Is n times the sum of their squares.

Thorold Gosset