Université de Montréal

# Les progressions arithmétiques dans les nombres entiers

par
Antoine Poirier

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

Mémoire présenté à la Faculté des études supérieures
en vue de l'obtention du grade de Maître ès sciences (M.Sc.)
en mathématiques

février , 2012

Université de Montréal
Faculté des études supérieures

Ce mémoire intitulé:

**Les progressions arithmétiques dans les nombres entiers**

présenté par:

Antoine Poirier

a été évalué par un jury composé des personnes suivantes:

| | |
|---|---|
| Matilde Lalin, | président-rapporteur |
| Andrew Granville, | directeur de recherche |
| Mariah Hamel, | membre du jury |

Mémoire accepté le: 22 février 2012

## RÉSUMÉ

Le sujet de cette thèse est l'étude des progressions arithmétiques dans les nombres entiers. Plus précisément, nous nous intéressons à borner inférieurement $v(N)$, la taille du plus grand sous-ensemble des nombres entiers de 1 à $N$ qui ne contient pas de progressions arithmétiques de 3 termes. Nous allons donc construire de grands sous-ensembles de nombres entiers qui ne contiennent pas de telles progressions, ce qui nous donne une borne inférieure sur $v(N)$. Nous allons d'abord étudier les preuves de toutes les bornes inférieures obtenues jusqu'à présent, pour ensuite donner une autre preuve de la meilleure borne. Nous allons considérer les points à coordonnés entières dans un anneau à $d$ dimensions, et compter le nombre de progressions arithmétiques qu'il contient. Pour obtenir des bornes sur ces quantités, nous allons étudier les méthodes pour compter le nombre de points de réseau dans des sphères à plusieurs dimensions, ce qui est le sujet de la dernière section.



**Mots clés: Combinatoire additive, progressions arithmétiques, points de réseau, points entiers contenu dans des sphères.**

## ABSTRACT

The subject of this thesis is the study of arithmetic progressions in the integers. Precisely, we are interested in the size $v(N)$ of the largest subset of the integers from 1 to $N$ that contains no 3 term arithmetic progressions. Therefore, we will construct a large subset of integers with no such progressions, thus giving us a lower bound on $v(N)$. We will begin by looking at the proofs of all the significant lower bounds obtained on $v(N)$, then we will show another proof of the best lower bound known today. For the proof, we will consider points on a large $d$-dimensional annulus, and count the number of integer points inside that annulus and the number of arithmetic progressions it contains. To obtain bounds on those quantities, it will be interesting to look at the theory behind counting lattice points in high dimensional spheres, which is the subject of the last section.



**Keywords: Additive combinatorics, arithmetic progressions, lattice theory, integer points in large spheres.**

## TABLE DES MATIÈRES

**RÉSUMÉ** . . . . . **iii**

**ABSTRACT** . . . . . **iv**

**TABLE DES MATIÈRES** . . . . . **v**

**REMERCIEMENTS** . . . . . **vii**

**CHAPITRE 1 : THÉORÈMES ANTÉRIEURS** . . . . . **1**

Introduction . . . . . 1

1.1 Théorème d'Erdös-Turàn . . . . . 3

1.2 Théorème de Salem-Spencer . . . . . 7

1.3 Théorème de Behrend . . . . . 10

1.4 Théorème d'Elkin . . . . . 15

**CHAPITRE 2 : THÉORÈME PRINCIPAL** . . . . . **25**

**CHAPITRE 3 : LES POINTS ENTIERS DANS UNE *D*-SPHÈRE** . . . . . **36**

3.1 Lemmes sur la fonction $\psi$ d'Euler et sur les sommes exponentielles . . 36

3.2 Les points entiers dans une 4-sphère . . . . . 46

3.3 Les points entiers dans une 5-sphère . . . . . 52

3.4 Les points entiers dans une $d$-sphère . . . . . 60

**BIBLIOGRAPHIE** . . . . . **64**

## REMERCIEMENTS

Je remercie le professeur Andrew Granville, mon directeur de recherche, pour son aide, son soutien, et aussi pour m'avoir montré l'importance des détails en mathématiques.

Je remercie également ma copine et ma famille pour leurs encouragements pendant ces années.

# CHAPITRE 1

# THÉORÈMES ANTÉRIEURS

## Introduction

Le sujet de ce mémoire de maîtrise est l'étude des progressions arithmétiques dans les nombres entiers. Plus précisément, nous étudirons la fonction $v(N)$, pour $N \in \mathbb{N}$, qui représente la taille du plus grand sous-ensemble des nombres entiers de 1 à $N$ qui ne contient pas de progressions arithmétiques de 3 termes, c'est-à-dire la taille du plus grand sous-ensemble qui ne contient pas trois termes de la forme $x, x+d, x+2d$, où $d \neq 0$.

L'étude de cette fonction a débuté en 1936 dans un article d'Erdös et de Turàn [6]. Ils ont découvert que borner cette fonction supérieurement aurait des conséquences profondes sur notre compréhension des nombres premiers. En particulier, s'il était possible de borner supérieurement de manière satisfaisante la fonction la taille du plus grand sous-ensemble de $\{1,...,N\}$ qui ne contient pas de progressions arithmétiques de $k$ termes pour tout $k$, et pour tout $N$ suffisamment grand, on pourrait conclure immédiatement qu'il existe une infinité de progressions arithmétiques arbitrairement longues dans les nombres premiers. La borne supérieure présente n'est pas assez bonne pour pouvoir conclure cela, mais Green et Tao ont, par contre, réussit à prouver qu'il y avait des progressions arithmétiques arbitrairement longue dans les nombres premiers, en utilisant

une autre méthode [7].

Dans ce mémoire, nous allons étudier la question inverse, c'est-à-dire que nous allons borner inférieurement $v(N)$, ce qui consiste en construire de grands sous-ensembles de $\{1,...,N\}$ qui ne contiennent pas de progressions arithmétiques. Dans la première section, nous allons faire l'historique des bornes inférieures obtenues sur $v(N)$, en commençant par celle d'Erdös et de Turàn [6] jusqu'à celle d'Elkin [5][2], en passant par la preuve de Salem et Spencer [3] ainsi que celle de Behrend [1]. Ensuite, nous allons exposer une preuve différente de la meilleure borne connue aujourd'hui. La preuve étant principalement basée sur l'étude du nombre de points entiers contenus dans des sphères, la dernière section sera dédiée à prouver quelques résultats dans ce sujet.

Dans cette section, nous allons prouver toutes les bornes inférieures de $v(N)$ qui ont été trouvés, depuis l'introduction de cette fonction. Nous allons commencer par celle proposée par Erdös et Turàn en 1936 [6].

## 1.1 Théorème d'Erdös-Turàn

**Théorème 1.1.1** (Erdös et Turàn)**.** *Pour tout $N \in \mathbb{N}$,*

$$v(N) \geq \frac{1}{2} N^{\frac{1}{\log_2(3)}}.$$

*Démonstration.* Soit $d$ un nombre entier positif et $N = 3^d$. Considérons l'ensemble $A \subseteq \{0,...,N-1\}$ des nombres qui ne s'écrivent, en base 3, qu'avec des 0 et des 1. Ainsi,

$$A = \left\{ x \in \{0,...,N-1\} : x = \sum_{i=1}^{d} x_i 3^{i-1},\ x_i \in \{0,1\} \right\}.$$

Démontrons que $A$ ne contient pas de progressions arithmétiques de trois termes. Si $x,y,z \in A$ forment une progression arithmétique, soit $x+y=2z$, alors $\sum_{i=1}^{d}(x_i+y_i-2z_i)3^{i-1}=0$. Nous aurons besoin du lemme suivant :

**Lemme 1.1.2.** *Soit $m \geq 2$ un nombre entier, $x,y,z \in \mathbb{N}$ et $(x_1,...,x_d)$, $(y_1,...,y_d)$ et $(z_1,...,z_d)$ leur représentation en base m, soit $x = \sum_{i=1}^{d} x_i m^{i-1}$. Supposons aussi que $0 \leq x_i, y_i, z_i < \frac{m}{2}$. Alors, $x+y=2z$ si et seulement si $x_i+y_i=2z_i$ pour $i=1,...,d$.*

*Démonstration.* Nous n'avons qu'à prouver que $x+y=2z$ implique $x_i+y_i=2z_i$, l'autre

sens de l'équivalence étant trivial. La preuve se fait par induction sur $d$. Si $x+y=2z$, alors $x+y \equiv 2z \mod m$. Les seules composantes de $x, y$ et $z$ qui ne sont pas un multiple de $m$ étant respectivement $x_1, y_1$ et $z_1$, cette dernière égalité implique que $x_1+y_1 \equiv 2z_1 \mod m$. Puisque $0 \leq x_1, y_1, z_1 < \frac{m}{2}$, alors $0 \leq x_1+y_1, 2z_1 < m$ et donc $x_1+y_1=2z_1$. Supposons maintenant, pour l'étape d'induction, que $x_i+y_i=2z_i$ pour tout $i \leq j-1$, où $j \geq 2$. On a encore que $x+y=2z$ implique $x+y \equiv 2z \mod m^j$. Cette dernière égalité, combinée avec l'hypothèse d'induction, nous donne que $(x_j+y_j)m^{j-1} \equiv 2z_j m^{j-1} \mod m^j$, donc que $x_j+y_j \equiv 2z_j \mod m$. Puisque $0 \leq x_j, y_j, z_j < \frac{m}{2}$, alors $0 \leq x_j+y_j, 2z_j < m$ et donc $x_j+y_j=2z_j$. Donc, pour tout $i$, on a que $x_i+y_i=2z_i$, ce qui complète la preuve.

□

Pour la preuve du théorème 1.1.1, on applique le lemme précédent pour $m=3$. Soit $x, y, z \in A$ tels que $x+y=2z$. Alors, on a $x_i+y_i=2z_i$ où $x_i, y_i, z_i \in \{0,1\}$, pour $i=1,2,...,d$. Si $z_i=0$, il n'y a pas d'autres choix que $x_i=y_i=0$. Si $z_i=1$, il n'y a encore pas d'autres choix que $x_i=y_i=1$. Donc, $x_i=y_i=z_i$ pour tout $i$, et alors $x=y=z$. Il n'y a donc pas de progressions arithmétiques dans $A$. Chaque élément de $A$ s'écrit avec $d$ décimales en base 3, chacune d'elles étant soit un 0, soit un 1. Il y a donc $2^d$ éléments dans cet ensemble. En additionnant 1 à chaque élément de $A$, on obtient alors un sous-ensemble de $\{1,...,N\}$ de taille $2^d = N^{\frac{1}{\log_2(3)}}$. Si $3^d < N < 3^{d+1}$, alors

$$v(N) \geq v(3^d) = \frac{2^{d+1}}{2} > \frac{1}{2} N^{\frac{1}{\log_2(3)}}$$

ce qu'il fallait démontrer.

□

Il serait intéressant, à ce point, de vérifier ce qu'on peut obtenir comme borne sur $v(N)$ avec l'algorithme glouton. On commence avec un ensemble vide et on considère, en ordre croissant, chaque nombre de 1 à $N$, et on l'ajoute à l'ensemble s'il ne crée pas de progressions arithmétiques de 3 termes avec les éléments déjà présents dans l'ensemble. Ainsi, pour $N = 27$, l'algorithme glouton nous donnerait l'ensemble $\{1,2,4,5,10,11,13,14\}$. Remarquons que si on soustrait 1 à chaque élément, on obtient $\{0,1,3,4,9,10,12,13\}$, ce qui est exactement l'ensemble $A$ dans le théorème précédent, pour $d = 3$. En effet, si on écrit ces derniers en base 3 on a l'ensemble

$$\{0,1,10,11,100,101,110,111\},$$

ce qui correspond bien à l'ensemble décrit dans le théorème.

**Proposition 1.1.3.** *L'ensemble sans progressions arithmétiques obtenu par l'algorithme glouton est le même que celui obtenu dans le théorème 1.1.1.*

*Démonstration.* La preuve se fait par induction sur le nombre $m$ d'éléments dans l'ensemble. Pour la base d'induction, si $m = 1$, on a comme ensemble $\{0\}$. Supposons maintenant que l'ensemble $A$ de $m-1$ éléments obtenus par l'algorithme glouton contient les $m-1$ premiers nombres qui ne s'écrivent en base 3 qu'avec des 0 et des 1. Considérons $x, y \in A$, $y > x$, et leurs représentation en base 3, soit $(x_1, ..., x_d)$ et $(y_1, ..., y_d)$. Il a déjà

été démontré, dans la preuve du théorème 1.1.1, que $2y - x$ est un nombre qui contient au moins un 2 dans sa représentation en base 3. Il nous reste à montrer que tout nombre ayant un 2 dans sa représentation en base 3 ne peut pas faire partie de l'ensemble obtenu par l'algorithme glouton. En effet, pour $z = (z_1, ..., z_d)$ où au moins un des $z_i$ est égal à 2, on peut trouver $x$ et $y$ inférieurs à $z$, sans 2 dans leurs représentation en base 3, tels que $z = 2y - x$. Si $z_i = 0$, alors on prend $y_i = x_i = 0$. Si $z_i = 1$, alors on prend $y_i = x_i = 1$. Finalement, si $z_i = 2$, on choisit $y_i = 1$ et $x_i = 0$. Puisqu'au moins un des $z_i$ est égal à 2, les trois nombres, $x, y$ et $z$, sont distincts et forment réellement une progression arithmétique. On en conclut que le $m$-ème terme de $A$ sera le plus petit nombre s'écrivant sans 2 en base 3 qui n'est pas encore dans $A$.

□

## 1.2 Théorème de Salem-Spencer

La seconde borne que nous allons exposer est dû à Salem et Spencer [3]. Elle utilise sensiblement la même méthode que celle du théorème 1.1.1, puisqu'elle crée un ensemble sans progressions arithmétiques en ne prenant que les nombres dont les décimales en base $2d-1$ possèdent certaines propriétés. Le passage de la base 3 à une base plus générale, soit la base $2d-1$, va nous permettre d'obtenir une meilleure borne inférieure sur $v(N)$.

**Théorème 1.2.1** (Salem et Spencer)**.** *Pour tout $\varepsilon > 0$, il existe $N_\varepsilon$ tel que pour tout $N \geq N_\varepsilon$,*

$$v(N) \geq N^{1-\frac{\log(2)+\varepsilon}{\log(\log(N))}}.$$

*Démonstration.* Soit $d > 2$ et $k$ un nombre entier divisible par $d$. Soit $S(d,k)$ l'ensemble des points $x$ tels que $x = x_1 + x_2(2d-1) + ... + x_k(2d-1)^{k-1}$ et où les $x_i$ sont répartis également entre les valeurs $0, 1, ..., d-1$. Ainsi, exactement $\frac{k}{d}$ des $x_i$ prennent la valeur $t$, pour $t = 0, 1, ..., d-1$. On peut alors calculer la taille de l'ensemble $S(d,k)$, puisqu'il est égal au nombre de façon de distribuer équitablement $k$ éléments parmis $d$ classes. Pour tout $\varepsilon > 0$, il existe $k_\varepsilon, d_\varepsilon$ tel que pour tout $k \geq k_\varepsilon$ et pour tout $d \geq d_\varepsilon$,

$$|S(d,k)| = \frac{k!}{(\frac{k}{d}!)^d} \geq (1-\varepsilon)\frac{\sqrt{\pi k}}{2\sqrt{2\pi\frac{k}{d}}^d}\left(\frac{k}{e}\right)^k\left(\frac{de}{k}\right)^{\frac{dk}{d}} \geq (1-\varepsilon)\left(\frac{d}{2\pi k}\right)^{\frac{d}{2}} d^k \qquad (1.1)$$

par l'approximation de Stirling. Démontrons que l'ensemble $S(d,k)$ ne contient pas de

progressions arithmétiques. Supposons que, pour $x,y,z \in S(d,k)$, on a $x+y=2z$. Donc, on a $x_1+y_1+...+(x_k+y_k)(2d-1)^{k-1} = 2z_1+...+2z_k(2d-1)^{k-1}$. Chaque $x_i, y_i$ et $z_i$ est inférieur à $d-1$. Alors, le lemme 1.1.2 avec $m=2d-1$ nous indique que $x+y=2z$ implique que $x_i+y_i=2z_i$ pour $i=1,...,k$. Supposons que $z_i=0$ pour un certain $i$. Cela implique que $x_i=y_i=0$. Ainsi, $x_i=y_i=z_i$ pour tout $i$ tel que $z_i=0$. Prenons $j$ tel que $z_j=1$. Puisque $x_j \neq 0$ et $y_j \neq 0$, on en conclut que $x_j=y_j=1$. Ainsi, $x_j=y_j=z_j$ pour tout $j$ tel que $z_j=1$. On peut répéter l'argument pour conclure que si $x+y=2z$, alors $x_i=y_i=z_i$ pour tout $i$, et donc que $x=y=z$. $S(d,k)$ ne contient donc pas de progressions arithmétiques de trois termes. Il ne nous reste qu'à fixer $N$ en fonction des variables $d$ et $k$. Fixons $d = \left\lfloor \frac{\log(N)}{(\log\log(N))^3} \right\rfloor$ et $k=dm$ où $m = \left\lfloor \frac{\log(N)}{d\log(2d-1)} \right\rfloor$. Ainsi, tous les nombres dans $S(d,k)$ étant inférieurs à $(2d-1)^k$, on a que

$$(2d-1)^k \leq (2d-1)^{\frac{\log(N)}{\log(2d-1)}} = N < (2d-1)^{d(m+1)}$$

ce qui nous garantie qu'aucun nombre dans $S(d,k)$ est supérieur au $N$ choisi. Maintenant, on a que

$$dm \leq \frac{\log(N)}{\log(2d-1)} \leq \frac{\log(N)}{\log(d)} \leq \frac{\log(N)}{\log\log(N)-3\log\log\log(N)}.$$

et donc, pour tout $\varepsilon \geq 0$, il existe $N_\varepsilon$ tel que pour tout $N \geq N_\varepsilon$,

$$dm \leq \frac{\log(N)+\varepsilon}{\log\log(N)}. \tag{1.2}$$

Maintenant, puisque $N < (2d-1)^{d(m+1)}$, et par les inégalités (1.1) et (1.2), on a que

$$\begin{aligned}
\frac{|S(d,dm)|}{N} &\geq (1-\varepsilon)\left(\frac{1}{2\pi m}\right)^{\frac{d}{2}} \frac{1}{(2d-1)^d}\left(\frac{d}{2d-1}\right)^{dm} \\
\frac{|S(d,dm)|}{N} &\geq (1-\varepsilon)\left(\frac{\log(2d-1)}{8\pi d\log(N)}\right)^{\frac{d}{2}} \frac{1}{2^{dm}} \\
\frac{|S(d,dm)|}{N} &\geq (1-\varepsilon)\left(\frac{\log(\frac{2\log(N)}{(\log\log(N))^3}-1)}{8\pi\frac{\log(N)}{(\log\log(N))^3}\log(N)}\right)^{\frac{\log(N)}{2(\log\log(N))^3}} N^{-\frac{\log(2)+\varepsilon}{\log\log(N)}} \\
\frac{|S(d,dm)|}{N} &\geq (1-\varepsilon)\left(\frac{\log(\frac{\log(N)}{(\log\log(N))^3})(\log\log(N))^3}{(\log(N))^2}\right)^{\frac{\log(N)}{2(\log\log(N))^3}} N^{-\frac{\log(2)+\varepsilon}{\log\log(N)}-\frac{\log(8\pi)}{2(\log\log(N))^3}} \\
\frac{|S(d,dm)|}{N} &\geq (1-\varepsilon)N^{-\frac{\log(2)+\varepsilon}{\log\log(N)}-\frac{\log(8\pi)}{2(\log\log(N))^3}+\frac{1}{2(\log\log(N))^3}\log\left(\frac{\log(\frac{\log(N)}{(\log\log(N))^3})(\log\log(N))^3}{(\log(N))^2}\right)} \\
|S(d,dm)| &\geq N^{1-\frac{\log(2)+\varepsilon}{\log\log(N)}}.
\end{aligned}$$

□

## 1.3 Théorème de Behrend

Le théorème suivant, dû à Behrend [1], va donner la borne inférieure sur $v(N)$ qui va persister pendant plus de 60 ans. Les méthodes utilisées sont similaires, puisqu'on va toujours faire appel à l'écriture en base $2y-1$ des nombres faisant partie de notre ensemble sans progressions arithmétiques pour exprimer sa taille en fonction de $N$.

**Théorème 1.3.1** (Behrend)**.** *Il exsite une constante C telle que, pour tout N suffisamment grand,*

$$v(N) \geq C\frac{N}{2^{2\sqrt{2}\sqrt{\log_2(N)}}\log_2^{1/4}(N)}$$

*Démonstration.* Fixons d'abord $N \in \mathbb{N}$ et soit $d$ et $y$ des nombres entiers. L'idée est de trouver le cercle qui contient le plus de points entiers parmis l'ensemble de points $\{0,1,...,y-1\}^d$. Ce raffinement, qui n'est pas présent dans la preuve originale de Behrend, va améliorer la borne d'un facteur $\log_2^{\frac{1}{4}}(N)$. Pour ce faire, considérons $Y_1,...,Y_d$ des variables aléatoires où les $Y_i$ sont uniformément distribuées sur les nombres entiers $\{0,1,...,y-1\}$. Soit $Z_i = Y_i^2$ et $Z = \sum_{i=1}^d Z_i$. On remarque alors que $Z$ est le carré de la norme d'un vecteur dans $\{0,1,...,y-1\}^d$. On peut alors calculer l'espérance $\mu$ et l'écart-type $\sigma$ de ces variables aléatoires. On trouve que

$$\mu_{Z_i} = \frac{1}{y}\sum_{j=0}^{y-1} j^2 = \frac{y(y-1)(2y-1)}{6y} = \frac{y^2}{3} - \frac{y}{2} + \frac{1}{6}.$$

Puisque les variables $Z_i$ sont indépendantes et identiquement distribuées, on trouve

que $\mu_Z = d\mu_{Z_i}$. Puisque $Var(Z_i) = \mu_{Z_i^2} - \mu_{Z_i}^2$ et puisque

$$\mu_{Z_i^2} = \frac{1}{y}\sum_{j=0}^{y-1} j^4 = \frac{1}{y}\frac{y(y-1)(2y-1)(y^2-3y-1)}{30} = \frac{y^4}{5} - \frac{y^3}{2} + \frac{y^2}{3} - \frac{1}{30},$$

on a que

$$\sigma_{Z_i}^2 = \frac{4y^4}{45} - \frac{y^3}{6} - \frac{y^2}{36} + \frac{y}{6} - \frac{11}{180} \leq \frac{4y^4}{45}$$

et aussi que $\sigma_Z^2 = d\sigma_{Z_i}^2$. Par l'inégalité de Chebychev, on a, pour tout $a > 0$,

$$\mathbb{P}(|Z - \mu_Z| > a\sigma_Z) \leq \frac{1}{a^2}.$$

Donc, pour un $a > 0$, le nombre de vecteurs $v$ de $\{0, 1, ..., y-1\}^d$ qui satisfont l'inégalité suivante est au moins $(1 - \frac{1}{a^2})y^d$.

$$\mu_Z - a\sigma_Z \leq ||v||^2 \leq \mu_Z + a\sigma_Z.$$

Il y a seulement $2a\sigma_Z + 1$ valeurs entières possibles pour $||v||^2$ parmis les vecteurs qui satisfont l'inégalité ci-dessus. Par le principe du pigeonnier, il existe une valeur $\mu_Z - a\sigma_Z \leq T \leq \mu_Z + a\sigma_Z$ pour laquelle au moins $\frac{1}{2a\sigma_Z+1}(1 - \frac{1}{a^2})y^d$ vecteurs de $\{0, 1, ..., y-1\}^d$ ont une norme carré égale à $T$. Soit $S$ l'ensemble de ces vecteurs. Donc,

$$|S| \geq \frac{1}{2a\sigma_Z + 1}\left(1 - \frac{1}{a^2}\right)y^d. \tag{1.3}$$

**Proposition 1.3.2.** *L'ensemble S ne contient pas de progressions arithmétiques.*

*Démonstration.* Puisque tous les vecteurs de $S$ ont la même norme $\sqrt{T}$, pour tout $a,b,c \in S$, on ne peut pas avoir $a+b=2c$ à moins que $a=b=c$. En effet, en employant l'inégalité du triangle avec les points $a$,$b$ et l'origine, on a que $||a+b|| \leq ||a||+||b||$, avec égalité si et seulement si $a$,$b$ et l'origine sont supportés par une seule droite, avec l'origine suitée entre les points $a$ et $b$. Puisque $||a|| = ||b||$, on ne peut conclure que $a = \pm b$. Dans le cas où $a = -b$, on a que $c = 0$, mais alors $||a|| = ||b|| = ||c||$ et donc $a = b = c = 0$. Sinon, $a = b$ et alors $a = b = c$.

□

Soit maintenant l'injection $\phi : S \longrightarrow \mathbb{Z}$ définit par

$$\phi(x_1, x_2, ..., x_d) = x_1 + x_2(2y-1) + ... + x_d(2y-1)^{d-1}.$$

La fonction $\phi$ fait le lien entre un nombre $x$ et son écriture en base $2y-1$. En prenant $m = 2y-1$ dans le lemme 1.1.2, on a que la fonction $\phi$ préserve les progressions arithmétiques de $S$, de même que $\phi^{-1}$. Alors, puisque $S$ ne contient pas de progressions arithmétiques, on a que l'ensemble $A = \phi(S)$, qui est un sous-ensemble de $\{1,2,...,N\}$, n'a pas de progression arithmétiques. Il ne nous reste qu'à fixer les paramètres $d, y$ et $a$ en fonction de $N$ de manière à optimiser $|A|$, dont la taille est bornée inférieurement dans

(1.3). On choisi $a = \sqrt{3}$, $y = \frac{1}{2}N^{\frac{1}{d}}$ et $d = \lfloor \sqrt{2\log_2(N)} \rfloor$. Ainsi, pour $d \geq 4$, on a que

$$|A| \geq \frac{2}{3} \frac{y^d}{\frac{4\sqrt{3}dy^2}{3\sqrt{5}} + 1} \geq \frac{2}{5\sqrt{d}} y^{d-2}.$$

Supposons d'abord que $y = \frac{1}{2}N^{\frac{1}{d}}$ soit un nombre entier ; le cas contraire sera étudié après. Pour tout $x \in A$, on a que $x \leq (2y)^d \leq N$, donc les variables $y$ et $d$ ont été choisis de manière à ce que tous les éléments de $A$ soient plus petits que $N$. On a que

$$|A| \geq \frac{2}{5\, 2^{\frac{1}{4}} \log_2^{\frac{1}{4}}(N)} \left(\frac{N^{\frac{1}{d}}}{2}\right)^{d-2} \geq \frac{8}{5\, 2^{\frac{1}{4}} \log_2^{\frac{1}{4}}(N)} \frac{N}{2^d N^{\frac{2}{d}}} \geq \frac{4}{5\, 2^{\frac{1}{4}} \log_2^{\frac{1}{4}}(N)} \frac{N}{2^{2\sqrt{2\log_2(N)}}}$$

ce qu'il fallait démontrer. Maintenant, si $y = \frac{1}{2}N^{\frac{1}{d}}$ n'est pas un nombre entier, on prend $\lfloor y \rfloor$ à la place de $y$. Ainsi, on a $N' = (2\lfloor y \rfloor)^d$. Par l'argument précédent, on obtient un ensemble $A$ sans progressions arithmétiques de taille

$$|A| \geq \frac{4}{5\, 2^{\frac{1}{4}} \log_2^{\frac{1}{4}}(N')} \frac{N'}{2^{2\sqrt{2\log_2(N')}}} \geq \frac{4}{5\, 2^{\frac{1}{4}} \log_2^{\frac{1}{4}}(N)} \frac{N'}{2^{2\sqrt{2\log_2(N)}}}.$$

Remarquons maintenant que

$$N' \geq \left(\frac{y-1}{y}\right)^d N \geq \left(1 - \frac{d}{y}\right) N \geq \left(1 - \frac{2\sqrt{2\log_2(N)}}{2^{\frac{\sqrt{\log_2(N)}}{\sqrt{2}}}}\right) N \geq \frac{N}{2}$$

pour $N$ suffisamment grand. On en conclut que, si $\frac{1}{2}N^{\frac{1}{d}}$ n'est pas un nombre entier, alors

$$|A| \geq \frac{C}{\log_2^{\frac{1}{4}}(N)} \frac{N}{2^{2\sqrt{2\log_2(N)}}}$$

avec $C = \frac{2}{5\,2^{\frac{1}{4}}} \geq \frac{1}{3}$, ce qui complète la preuve.

□

## 1.4 Théorème d'Elkin

Le théorème suivant est une amélioration de celui de Behrend. À la place d'une sphère, la preuve du théorème suivant, dû à Elkin [2], utilisera un anneau suffisamment mince, et ensuite, en enlevant certains points, on obtient un ensemble sans progressions arithmétiques. L'idée principale de la preuve est dû à Elkin, mais ici, nous présenterons la preuve de Green et Wolf [5], qui est beaucoup plus brève et qui a une démarche un peu différente des preuves précédentes.

**Théorème 1.4.1** (Green et Wolf)**.** *Il existe une constante c telle que pour tout N suffisamment grand,*

$$v(N) \geq c\frac{N\log^{\frac{1}{4}}(N)}{2^{\left(2\sqrt{2}\sqrt{\log_2(N)}\right)}}.$$

*Démonstration.* Supposons $N$ pair et soit $d \in \mathbb{N}$ et $0 < \delta < 1$. Soit aussi $0 < c < 1 < C$ des constantes absolues et qui pourrait varier au long de la preuve. Pour tout $r \leq \frac{1}{2}\sqrt{d}$, posons $S(r)$ comme l'ensemble

$$S(r) = \{x \in [0,1/2)^d : r - \delta \leq ||x|| \leq r\}$$

où $||x||^2 = \sum_{i=1}^{d} x_i^2$ est la norme au carré de $x$. Soit $x = (x_1, x_2, ..., x_d)$ choisit aléatoirement et uniformément dans $\left[0, \frac{1}{2}\right)^d$. Alors, on calcule l'espérance $\mu$ et la variance $\sigma^2$ de $||x||^2$,

et on obtient que

$$\begin{aligned}\mu &= 2d\int_0^{\frac{1}{2}} x_i^2 dx_i = \frac{d}{12}\\ \sigma^2 &= d\left(2\int_0^{\frac{1}{2}} x^4 dx - \frac{1}{144}\right) = \frac{d}{180} = \frac{\mu}{15}.\end{aligned}$$

**Proposition 1.4.2.** *Il existe $C > 1$ et $c < 1$ tels que pour tout $d$ suffisamment grand,*

$$\mathbb{P}\left(\left|||x|| - \sqrt{\frac{d}{12}}\right| \leq C\right) \geq c$$

*Démonstration.* Soit l'ensemble $B(C,d) = \left\{x \in \left[0,\frac{1}{2}\right)^d : \left|||x|| - \sqrt{\frac{d}{12}}\right| \leq C\right\}$ et l'ensemble $A(C,d) = \left\{x \in \left[0,\frac{1}{2}\right)^d : \left|||x||^2 - \frac{d}{12}\right| \leq C\right\}$. Choisissons d'abord $C > 1$ tel que $2C\sqrt{\frac{d}{12}} - C^2$ soit positif pour tout $d$ suffisamment grand et soit $x \in A\left(2C\sqrt{\frac{d}{12}} - C^2, d\right)$, c'est à dire que

$$C^2 - 2C\sqrt{\frac{d}{12}} \leq ||x||^2 - \frac{d}{12} \leq -C^2 + 2C\sqrt{\frac{d}{12}}.$$

Cela implique que

$$\begin{aligned}C^2 - 2C\sqrt{\frac{d}{12}} &\leq ||x||^2 - \frac{d}{12} \leq C^2 + 2C\sqrt{\frac{d}{12}}\\ C^2 - 2C\sqrt{\frac{d}{12}} + \frac{d}{12} &\leq ||x||^2 \leq C^2 + 2C\sqrt{\frac{d}{12}} + \frac{d}{12}\\ -C + \sqrt{\frac{d}{12}} &\leq ||x|| \leq C + \sqrt{\frac{d}{12}}\\ -C &\leq ||x|| - \sqrt{\frac{d}{12}} \leq C\end{aligned}$$

et donc que $x \in B(C,d)$. Alors, $A\left(2C\sqrt{\frac{d}{12}} - C^2, d\right) \subseteq B(C,d)$, ce qui nous indique, en termes de probabilités, que

$$\mathbb{P}\left(x \in A\left(2C\sqrt{\frac{d}{12}} - C^2, d\right)\right) \leq \mathbb{P}\left(x \in B(C,d)\right).$$

De plus, l'inégalité de Chebychev nous indique que pour tout $a > 0$, on a que

$$\mathbb{P}\left(x \in A\left(a\sqrt{\frac{d}{180}}, d\right)\right) \geq 1 - \frac{1}{a^2}.$$

Il suffit alors de choisir $a > 1$ tel que $a\sqrt{\frac{d}{180}} \leq 2C\sqrt{\frac{d}{12}} - C^2$ pour tout $d$ suffisamment grand, pour obtenir la série d'inégalités suivante :

$$1 - \frac{1}{a^2} \leq \mathbb{P}\left(x \in A\left(a\sqrt{\frac{d}{180}}, d\right)\right) \leq \mathbb{P}\left(x \in A\left(2C\sqrt{\frac{d}{12}} - C^2, d\right)\right) \leq \mathbb{P}\left(x \in B(C,d)\right).$$

Il est certainement possible de choisir un tel $a$, car la condition sur $a$ se réécrit comme $a \leq 2\sqrt{15}\, C - \frac{6\sqrt{5}C^2}{\sqrt{d}}$ et, lorsque $d$ est suffisamment grand, et puisque $C$ est déjà fixé comme étant supérieur à 1, le côté droit de l'inégalité sera strictement plus grand que 1. On en conclut que, pour tout $d$ suffisamment grand,

$$\mathbb{P}\left(x \in B(C,d)\right) = \mathbb{P}\left(\left|\,||x|| - \sqrt{\frac{d}{12}}\,\right| \leq C\right) \geq c$$

ce qu'il fallait démontrer.

□

Ainsi, par le principe du pigeonnier et la proposition précédente, il existe un $r \leq \frac{1}{2}\sqrt{d}$ tel que

$$Vol(S(r)) \geq c\delta 2^{-d}. \tag{1.4}$$

Soit $S = S(r) \subset \left[0, \frac{1}{2}\right)^d$ l'ensemble choisi et $\mathbb{T}^d = \mathbb{R}^d/\mathbb{Z}^d$ le tore à $d$ dimensions. Nous avons que $\mathbb{T}^d \sim [0,1)^d$. Puisque $x_i + z_i < 1$ pour tout $x, z \in S$ et $i = 1, 2, ..., d$, on observe alors que les progressions arithmétiques dans $S$ correspondent avec celles dans $\mathbb{T}^d$. Soit $(x, y)$ un couple tel que $x - y, x, x + y \in S$. Par la loi du parallélogramme, nous avons

$$2||x||^2 + 2||y||^2 = ||x+y||^2 + ||x-y||^2$$

et donc que

$$||y|| \leq \sqrt{r^2 - (r-\delta)^2} = \sqrt{2\delta r - \delta^2}.$$

Alors, si on dénote $B \subset \mathbb{T}^d \times \mathbb{T}^d$ comme l'ensemble contenant toutes les pairs $(x, y)$ décrites ci-dessus, on peut alors en déduire, avec la formule pour le volume d'une sphère à $d$ dimensions et l'approximation de Stirling, que

$$Vol(B) \leq Vol(S)\frac{\pi^{d/2}}{\left(\frac{d}{2}\right)!}(2\delta r - \delta^2)^{d/2} \leq Vol(S)\frac{1}{\sqrt{\pi d}}\left(\frac{2\pi e\delta}{\sqrt{d}}\right)^{\frac{d}{2}}. \tag{1.5}$$

Posons maintenant, pour $\theta, \alpha \in \mathbb{T}^d$, la transformation $\psi_{\theta,\alpha} : \{1, 2, ..., N\} \to \mathbb{T}^d$ de la

manière suivante :

$$\psi_{\theta,\alpha}(n) = \theta n + \alpha (mod\, 1).$$

**Proposition 1.4.3.** *Pour tout $n \in \{1,2,...,N\}$, $\psi_{\theta,\alpha}(n)$ varie uniformément sur $\mathbb{T}^d$ lorsque $\theta$ et $\alpha$ varient uniformément et indépendamment sur $\mathbb{T}^d \times \mathbb{T}^d$.*

*Démonstration.* Soit $C = \prod_{i=1}^{d} [a_i, b_i]$, $0 \leq a_i < b_i < 1$, une boîte quelconque dans $\mathbb{T}^d$. On voudrait que $\mathbb{P}_{\theta,\alpha}\left(\psi_{\theta,\alpha}(n) \in C\right) = Vol(C) = \prod_{i=1}^{d}(b_i - a_i)$. En effet, puisque $\theta$ et $\alpha$ varient uniformément et indépendamment sur $\mathbb{T}^d \times \mathbb{T}^d$, on a, pour chaque coordonnées $\theta_i$ et $\alpha_i$ de $\theta$ et $\alpha$ respectivement, que la fonction de densité $f_{\theta_i}(x) = f_{\alpha_i}(x) = 1$ pour tout $x \in [0,1)$. Alors,

$$\begin{aligned}
\mathbb{P}_{\theta,\alpha}\left(\psi_{\theta,\alpha}(n) \in C\right) &= \prod_{i=1}^{d} \mathbb{P}_{\theta_i,\alpha_i}(a_i \leq \theta_i n + \alpha_i \leq b_i \mod 1) \\
&= \prod_{i=1}^{d} \int_0^1 \mathbb{P}_{\alpha_i}(a_i - \theta_i n \leq \alpha_i \leq b_i - \theta_i n \mod 1) f_{\theta_i}(\theta_i) d\theta_i \\
&= \prod_{i=1}^{d} \int_0^1 (b_i - a_i) d\theta_i = \prod_{i=1}^{d} (b_i - a_i)
\end{aligned}$$

ce qu'il fallait démontrer.

□

Définissons maintenant $A_{\theta,\alpha} = \{n \in \{1,2,...,N\} : \psi_{\theta,\alpha}(n) \in S\}$. Puisque $\psi_{\theta,\alpha}(n)$ varie uniformément sur $\mathbb{T}^d$ lorsque $\theta$ et $\alpha$ varient indépendamment et uniformément, on en conclut que

$$\mathbb{E}_{\theta,\alpha}(|A_{\theta,\alpha}|) = N\, Vol(S).$$

Maintenant, observons que chaque progression arithmétique est de la forme $x-y,x,x+y$. Il y a donc $N-2$ choix possibles pour $x$ (1 et $N$ ne sont pas des valeurs possibles pour $x$) et ensuite $\min\{x-1,N-x\}$ choix pour $y$, résultant en

$$\sum_{x=2}^{\frac{N}{2}}(x-1)+\sum_{x=\frac{N}{2}+1}^{N-1}(N-x)=\frac{N(N-2)}{4}$$

progressions arithmétiques différentes.

**Proposition 1.4.4.** *Pour tout $n,m\in\{1,2,...,N\}$ tel que $n\neq m$, $(\psi_{\theta,\alpha}(m),\psi_{\theta,\alpha}(n))$ varie uniformément sur $\mathbb{T}^d\times\mathbb{T}^d$ lorsque $\theta$ et $\alpha$ varient uniformément et indépendamment sur $\mathbb{T}^d\times\mathbb{T}^d$.*

*Démonstration.* Soit $I\in\mathbb{R}$ un intervalle, et $X$ une variable aléatoire de densité $f_X$. Alors, les lois sur la probabilité conditionnelle d'un évènement $A$ nous indique que

$$\mathbb{P}(A\mid X\in I)=\int_{i\in I}\frac{\mathbb{P}(A\mid X=i)\,f_X(i)}{\mathbb{P}(X\in I)}di \tag{1.6}$$

Maintenant, pour prouver la proposition, il suffit de prouver que, pour toute boîte $C=\prod_{i=1}^{d}[a_i,b_i]\times\prod_{i=1}^{d}[c_i,e_i]$, où $0\leq a_i<b_i<1$ et $0\leq c_i<e_i<1$, que

$$\mathbb{P}_{\theta,\alpha}\left(\left(\psi_{\theta,\alpha}(m),\psi_{\theta,\alpha}(n)\right)\in C\right)=Vol(C)$$

pour tout nombres entiers positifs $n\neq m$. On peut réécrire la condition à satisfaire de la

manière suivante : pour tout $i = 1, ..., d$,

$$\mathbb{P}_{\theta_i,\alpha_i}\left(a_i \leq \psi_{\theta,\alpha}(m) \leq b_i \mid c_i \leq \psi_{\theta,\alpha}(n) \leq e_i\right) \mathbb{P}_{\theta_i,\alpha_i}\left(c_i \leq \psi_{\theta,\alpha}(n) \leq e_i\right) = (b_i - a_i)(e_i - c_i).$$

Par la proposition 1.4.3, on a que la condition à satisfaire est

$$F(m,n) := \mathbb{P}_{\theta_i,\alpha_i}\left(a_i \leq \psi_{\theta,\alpha}(m) \leq b_i \mid c_i \leq \psi_{\theta,\alpha}(n) \leq e_i\right) = (b_i - a_i).$$

On a donc, par l'équation (1.6) et par la proposition 1.4.3, que

$$\begin{aligned} F(m,n) &= \frac{1}{e_i - c_i} \int_{c_i}^{e_i} \mathbb{P}_{\theta_i,\alpha_i}\left(a \leq \theta_i m + \alpha_i \leq b \mod 1 \mid \theta_i n + \alpha_i = y\right) dy. \\ &= \frac{1}{e_i - c_i} \int_{c_i}^{e_i} \mathbb{P}_{\theta_i}\left(a_i - y \leq \theta_i (m-n) \leq b_i - y \mod 1\right) dy \\ &= \frac{1}{e_i - c_i} \int_{c_i}^{e_i} (b_i - a_i) dy = (b_i - a_i) \end{aligned}$$

ce qui complète la démonstration.

□

Soit $n-a, n, n+a$ une progression arithmétique dans $A_{\theta,\alpha}$. Donc, $\psi_{\theta,\alpha}(n-a)$, $\psi_{\theta,\alpha}(n)$ et $\psi_{\theta,\alpha}(n+a)$ sont dans $S$. Alors, le couple $(\psi_{\theta,\alpha}(n), \psi_{\theta,\alpha}(n) - \psi_{\theta,\alpha}(n-a))$ est dans $B$. Donc, à chaque progression arithmétique de $A_{\theta,\alpha}$ correspond un point de $B$. Puisque si $x \neq x'$, on a que $(\psi_{\theta,\alpha}(x), \psi_{\theta,\alpha}(x'))$ varie uniformément sur $\mathbb{T}^d \times \mathbb{T}^d$ lorsque $\theta$ et $\alpha$ varient uniformément et indépendamment, chacune de ces progressions arithmétique a une probabilité $Vol(B)/Vol(\mathbb{T}^d \times \mathbb{T}^d) = Vol(B)$ de se retrouver dans $A_{\theta,\alpha}$, puisque $B$ est

exactement l'ensemble contenant tous les couples $(x,y)$ tels que $x-y,x,x+y \in S$. Donc, si on note par $T(A_{\theta,\alpha})$ le nombre de progressions arithmétiques dans $A_{\theta,\alpha}$, on obtient

$$\mathbb{E}_{\theta,\alpha}(T(A_{\theta,\alpha})) = Vol(B)\frac{N(N-2)}{4}.$$

Nous avons donc un ensemble $A_{\theta,\alpha}$ suffisamment grand, contenant une quantité bornée par $Vol(B)\frac{N(N-2)}{4}$ de progressions arithmétiques. Il suffit maintenant de fixer les paramètres $\delta$ et $d$ en fonction de $N$. Si on choisit ces paramètres de manière à ce que

$$\mathbb{E}_{\theta,\alpha}(T(A_{\theta,\alpha})) \leq \frac{1}{3}\mathbb{E}_{\theta,\alpha}(|A_{\theta,\alpha}|), \tag{1.7}$$

on aura que

$$\mathbb{E}_{\theta,\alpha}\left(\frac{2}{3}|A_{\theta,\alpha}| - T(A_{\theta,\alpha})\right) \geq \frac{1}{3}\mathbb{E}_{\theta,\alpha}(|A_{\theta,\alpha}|) = \frac{1}{3}N\,Vol(S).$$

Il sera possible alors de fixer $\theta$ et $\alpha$ de manière à ce que $A = A_{\theta,\alpha}$ satisfait à

$$T(A) \leq \frac{2}{3}|A|$$

et donc que

$$\frac{2}{3}|A| \geq \frac{1}{3}N\,Vol(S).$$

Ayant une borne supérieure sur le nombre de progressions arithmétiques dans $A$, il

suffira d'enlever au plus $T(A)/|A|$ des éléments de $A$ afin que l'ensemble résultant soit sans progressions arithmétiques. Ainsi, nous aurons, après cette opération, un ensemble sans progressions arithmétiques de taille $\frac{1}{6}N\,Vol(S)$. Pour ce faire, il faut que l'inégalité (1.7) soit vraie, et donc que

$$\frac{1}{3}N\,Vol(S) \geq \frac{N(N-2)}{2}Vol(B).$$

Puisque nous avons déjà obtenu une borne supérieure sur $Vol(B)$ en (1.5), il suffit donc d'avoir

$$\frac{1}{3}N\,Vol(S) \geq \frac{N(N-2)}{2}Vol(S)\frac{1}{\sqrt{\pi d}}\left(\frac{2\pi e\delta}{\sqrt{d}}\right)^{\frac{d}{2}},$$

ce qui est possible en prenant $\delta = \frac{\sqrt{d}N^{-\frac{2}{d}}}{2\pi e}$. En employant cette valeur de $\delta$ dans la borne inférieure sur $Vol(S)$ obtenu en (1.4), on obtient

$$|A| \geq \frac{1}{6}N\,Vol(S) \geq \frac{1}{6}c\frac{\sqrt{d}N^{1-\frac{2}{d}}}{2\pi e}2^{-d}.$$

En prenant ensuite $d = \lfloor\sqrt{2\log_2(N)}\rfloor$, on obtient le résultat voulu de la même façon que dans le théorème 1.3.1, c'est-à-dire

$$|A| \geq c\frac{N\log^{\frac{1}{4}}(N)}{2^{\left(2\sqrt{2}\sqrt{\log_2(N)}\right)}}.$$

□

Dans la preuve précédente, on a considéré les points entiers d'un anneau au lieu de ceux d'une sphère. Par contre, cet ensemble contient des progressions arithmétiques, mais peu par rapport à la taille de l'ensemble. L'argument probabiliste est très utile, puisqu'il nous évite de compter les points de l'ensemble. En effet, si on veux estimer la taille de l'ensemble des points entiers de l'anneau, la meilleure approximation reste le volume de l'anneau. Par contre, il faut borner supérieurement le terme d'erreur de manière satisfaisante. Dans la section suivante, nous prouverons le même théorème, mais, cette fois-ci, sans l'argument probabiliste, et donc en comptant le nombre de points entiers dans l'anneau que nous allons choisir, et aussi en comptant le nombre de progressions arithmétiques qu'il contient.

# CHAPITRE 2

# THÉORÈME PRINCIPAL

Dans cette section, nous obtenons une borne similaire à celle du théorème 1.4.1. Au lieu d'utiliser un argument probabiliste, nous allons borner le nombre de progressions arithmétique dans un anneau à $d$ dimensions.

**Théorème 2.0.5.** *Pour N suffisamment grand,*

$$v(N) \geq \frac{2^{\frac{1}{4}}\sqrt{5}}{21\sqrt{2}} \frac{N(\log_2(N))^{\frac{1}{4}}}{2^{\left(2\sqrt{2}\sqrt{\log_2(N)}\right)}}.$$

*Démonstration.* Soit $d \geq 60$ un entier positif pair et $y = 2^{\frac{d}{2}-1}$. Soit $\mathscr{C} = \{0, 1, ..., y-1\}$. On s'intéresse à la taille de l'anneau $A(r,\delta) = \left\{x \in \mathscr{C}^d : r - \delta \leq ||x-\alpha||^2 < r\right\}$ où $\alpha = \left(\frac{y-1}{2}, ..., \frac{y-1}{2}\right)$, et au nombre de progressions arithmétiques qu'il contient. L'objectif est de trouver un tel anneau qui contient suffisamment de points et peu de progressions arithmétiques par rapport à sa taille, disons au plus $\frac{|A(r,\delta)|}{2}$ progressions arithmétiques. Dans ce cas, il nous est possible d'éliminer au plus la moitié des éléments de $A(r,\delta)$ et de trouver un ensemble de taille $\frac{|A(r,\delta)|}{2}$ sans progressions arithmétiques. Ensuite, une injection de $\mathbb{Z}^d$ vers $\mathbb{N}$ qui préserve la notion de progressions arithmétiques va nous permettre de trouver un sous-ensemble $\{1, ..., N\}$ qui ne contient pas de progressions arithmétiques.

Soit $X_i$ des variables aléatoires distribués uniformément sur $\mathscr{C}$, chacunes indépen-

dantes des autres, pour $i = 1, ..., d$. Soit $Z = \sum_{i=1}^{d} \left( X_i - \frac{y-1}{2} \right)^2$. Ainsi, $Z$ représente le carré de la distance entre un vecteur choisi aléatoirement dans $\mathscr{C}^d$ et le point central $\alpha$. Il sera utile de calculer l'espérance $\mu_Z$ de la variable $Z$, ainsi que son écart-type, $\sigma_Z$ :

$$\mu_Z = d\,\mathbb{E}\left( \left( X_i - \frac{y-1}{2} \right)^2 \right) = \frac{d}{y} \sum_{j=0}^{y-1} \left( j - \frac{y-1}{2} \right)^2 = \frac{d}{12} \left( y^2 - 1 \right) \tag{2.1}$$

$$\sigma_Z^2 = d\,\mathbb{E}\left( \left( X_i - \frac{y-1}{2} \right)^4 \right) - d\,\mathbb{E}\left( \left( X_i - \frac{y-1}{2} \right)^2 \right)^2 = \frac{d}{180} \left( y^4 - 5y^2 + 4 \right) \tag{2.2}$$

et donc,

$$\sigma_Z \leq \frac{\sqrt{d}}{6\sqrt{5}} y^2$$

Considérons maintenant la somme suivante, pour une constante $a > 1$ :

$$\sum_{n=1}^{\left\lceil \frac{2a\sigma_Z}{\delta} \right\rceil} |A(\mu_Z - a\sigma_Z + n\delta, \delta)| \geq \left| \left\{ x \in \mathscr{C}^d : \mu_Z - a\sigma_Z \leq ||x - \alpha||^2 \leq \mu_Z + a\sigma_Z \right\} \right| \tag{2.3}$$

Par l'inégalité de Chebychev appliqué à la variable aléatoire $Z$, on a que pour tout $a > 1$, $\mathbb{P}(|Z - \mu_Z| \leq a\sigma_Z) > 1 - \frac{1}{a^2}$. Alors, pour $a = \sqrt{2}$, parmi les $y^d$ vecteurs de $\mathscr{C}^d$, il y en a au moins $\frac{y^d}{2}$ qui ont une norme carrée comprise entre $\mu_Z - \sqrt{2}\sigma_Z$ et $\mu_Z + \sqrt{2}\sigma_Z$.

Alors on peut borner la somme dans l'équation (2.3) par

$$\sum_{n=1}^{\left\lceil \frac{2\sqrt{2}\sigma_Z}{\delta} \right\rceil} \left| A(\mu_Z - \sqrt{2}\sigma_Z + n\delta, \delta) \right| \geq \frac{y^d}{2}. \tag{2.4}$$

Par le principe du pigeonnier, il nous est possible de choisir $n$ tel que l'ensemble $A(r,\delta)$ correspondant contient beaucoup de points. Cepdenant, chacun des ensembles $A(r,\delta)$ que l'on somme dans l'inégalité (2.4) contient des progressions arithmétiques. Soit $D(r,\delta) = \left\{(x,y,z) \in A(r,\delta)^3 : y-z = x-y\right\}$ l'ensemble des progressions arithmétiques de $A(r,\delta)$. Il est important de pouvoir borner supérieurement les quantités $|D(r,\delta)|$. Soit $x-\Delta, x, x+\Delta$ une progression arithmétique de $A(r,\delta)$, où $\Delta \in \mathbb{Z}^d$. Alors, l'égalité du parallélogramme nous indique que

$$\begin{aligned} ||x-\Delta||^2 + ||x+\Delta||^2 &= 2||x||^2 + 2||\Delta||^2 \\ ||\Delta||^2 &\leq \delta. \end{aligned}$$

De plus, on a que $\left| ||x+\Delta||^2 - ||x-\Delta||^2 \right| \leq \delta$, ce qui entraîne que $|x \cdot \Delta| \leq \frac{\delta}{4}$. Soit $B_\Delta := B(A(r,\delta)) = \{x \in A(r,\delta) : x-\Delta, x, x+\Delta \in A(r,\delta)\}$. Donc, $B_\Delta$ représente toutes les progressions arithmétiques de différence $\Delta$ dans $A(r,\delta)$. L'inégalité du parallélogramme utilisée précédemment nous indique que $B_\Delta \subseteq \left\{x \in A(r,\delta) : |x \cdot \Delta| \leq \frac{\delta}{4}\right\}$. Alors, on peut

écrire que

$$B_\Delta \subseteq \bigcup_{|h|\leq \frac{\delta}{4}} \{x \in A(r,\delta) : x\cdot\Delta = h\}. \tag{2.5}$$

Si on somme $B_\Delta$ sur tous les vecteurs $\Delta$ possibles, on obtient le nombre total de progressions arithmétiques de $A(r,\delta)$. On a donc l'inégalité suivante :

$$|D(r,\delta)| \leq \sum_{1\leq||\Delta||^2\leq\delta} \sum_{|h|\leq\frac{\delta}{4}} |\{x \in A(r,\delta) : x\cdot\Delta = h\}|$$

Similairement à l'équation (2.4), on somme $D(r,\delta)$ pour les même valeurs de $r$, et on obtient que

$$\sum_{n=1}^{\left\lceil\frac{2\sqrt{2}\sigma_Z}{\delta}\right\rceil} \left|D(\mu_Z - \sqrt{2}\sigma_Z + n\delta, \delta)\right| \leq \sum_{1\leq||\Delta||^2\leq\delta} \sum_{|h|\leq\frac{\delta}{4}} |B_\Delta(h)| \tag{2.6}$$

où $B_\Delta(h) = \left\{x \in \mathbb{Z}^d : \mu_Z - \sqrt{2}\sigma_Z \leq ||x||^2 \leq \mu_Z + \sqrt{2}\sigma_Z \ , \ x\cdot\Delta = h\right\}$. Il serait bien de pouvoir borner la taille de l'ensemble $B_\Delta(h)$. En effet, $B_\Delta(h)$ est l'intersection du réseau engendré par l'équation $x\cdot\Delta = h$ et d'un anneau.

**Lemme 2.0.6.**

$$|B_\Delta(h)| \leq \frac{\pi^{\frac{d-1}{2}}}{\Gamma\left(\frac{d+1}{2}\right)} \left(\left(\sqrt{\mu_Z + \sqrt{2}\sigma_Z} + \frac{\rho(\Delta)}{2}\right)^{d-1} - \left(\sqrt{\mu_Z - \sqrt{2}\sigma_Z} - \frac{\rho(\Delta)}{2}\right)^{d-1}\right)$$

*où* $\rho(\Delta) \leq \sqrt{5d}$

*Démonstration.* Soit $x_0 + < \lambda_1, ..., \lambda_{d-1} >_{\mathbb{Z}}$ le réseau définit par l'équation $x \cdot \Delta = h$. Ici, $\lambda_i$ sont des vecteurs à $d$ dimensions et le réseau $< \lambda_1, ..., \lambda_{d-1} >_{\mathbb{Z}}$ correspond à l'équation $x \cdot \Delta = 0$. Le volume du domaine fondamental est d'au moins 1, et d'au plus $||\Delta||$. Pour chaque point $x \in B_\Delta(h)$, considérons le parallélépipède $\prod_{i=1}^{d-1} \left[x - \frac{\lambda_i}{2}, x + \frac{\lambda_i}{2}\right]$, de volume au moins 1. Pour deux valeurs $x \in B_\Delta(h)$ distinctes, ces parallélépipèdes sont disjoints, et sont de volumes au moins 1. En faisant la somme des volumes des parallélépipèdes pour tout $x \in B_\Delta(h)$, on obtient

$$|B_\Delta(h)| \leq \left| \bigcup_{x \in B_\Delta(h)} \prod_{i=1}^{d-1} \left[x - \frac{\lambda_i}{2}, x + \frac{\lambda_i}{2}\right] \right|.$$

Maintenant, rappelons nous que $B_\Delta(h)$ est aussi contenu dans un anneau de $d$ dimensions centré en 0 définit par les rayons carrés $\mu_Z - a\sigma_Z$ et $\mu_Z + a\sigma_Z$. Alors, l'union des parallélépipèdes est contenu dans un anneau à $d-1$ dimensions, centré en 0, définit par les rayons carrés $\left(\sqrt{\mu_Z - \sqrt{2}\sigma_Z} - \frac{\rho(\Delta)}{2}\right)^2$ et $\left(\sqrt{\mu_Z - \sqrt{2}\sigma_Z} + \frac{\rho(\Delta)}{2}\right)^2$ où $\rho(\Delta)$ représente la longueur de la plus grande diagonale du domaine fondamental du réseau, et donc la longueur de la plus grande diagonale des parallélépipèdes. Le volume de l'union des parallélépipèdes est donc bornée supérieurement par la volume de l'anneau définit ci-dessus, ce qui implique que

$$|B_\Delta(h)| \leq \frac{\pi^{\frac{d-1}{2}}}{\Gamma\left(\frac{d+1}{2}\right)} \left( \left(\sqrt{\mu_Z + \sqrt{2}\sigma_Z} + \frac{\rho(\Delta)}{2}\right)^{d-1} - \left(\sqrt{\mu_Z - \sqrt{2}\sigma_Z} - \frac{\rho(\Delta)}{2}\right)^{d-1} \right)$$

ce qu'il fallait démontrer. Il nous suffit alors de trouver une borne pour $\rho(\Delta)$, qui re-

présente la longueur de la plus grande diagonale des parallélépipèdes, en fonction du vecteur $\Delta$. Si $\Delta = (\Delta_1, ..., \Delta_d)$, on peut réarranger les coordonnés de $\Delta$, sans perdre de généralité, et mettre les 0 à la fin, c'est-à-dire $\Delta = (u_1, ..., u_k, 0, ..., 0)$, où $u_i \neq 0$. Alors, les points suivants sont dans l'espace $x \cdot \Delta = 0$ :

$$(u_2, -u_1, 0, 0, 0, ..., 0)$$

$$(0, u_3, -u_2, 0, 0, ..., 0)$$

$$(0, 0, u_4, -u_3, 0, ..., 0)$$

$$...$$

$$(0, ..., 0, u_k, -u_{k-1}, 0, ..., 0)$$

L'ensemble des vecteurs unités $e_i = (0, 0, ..., 0, 1, 0, ..., 0)$ qui est composé de 0 partout et d'un 1 à la $i$-ème position, pour $i = k+1, ..., d$ sont aussi dans l'espace $x \cdot \Delta = 0$. Ces $d-1$ vecteurs sont tous linéairement indépendants, et le domaine fondamental du réseau doit se retrouver dans la boîte créée par les vecteurs ci-dessus. Il s'en suit que $\rho(\Delta)$ est inférieur ou égal à la diagonale de cette boîte, et donc

$$\begin{aligned}
\rho(\Delta)^2 &\leq u_2^2 + \sum_{i=2}^{k-1} (|u_{i-1}| + |u_{i+1}|)^2 + u_{k-1}^2 + \sum_{i=k+1}^{d} 1 \\
&\leq u_2^2 + \sum_{i=2}^{k-1} |u_{i-1}|^2 + \sum_{i=2}^{k-1} |u_{i+1}|^2 + 2\sqrt{\sum_{i=2}^{k-1} |u_{i-1}|^2}\sqrt{\sum_{i=2}^{k-1} |u_{i+1}|^2} + u_{k-1}^2 + d - k \\
&\leq 4||\Delta||^2 + d - k \leq 5d
\end{aligned}$$

Alors, $\rho(\Delta) \leq \sqrt{5d}$.

□

Maintenant que nous avons une borne sur $|B_\Delta(h)|$, indépendante de $h$, il nous faut aussi trouver une borne sur le nombre de vecteurs $\Delta$ admissibles, c'est-à-dire borner $\left|\left\{\Delta \in \mathbb{Z}^d : 1 \leq ||\Delta||^2 \leq \delta\right\}\right|$. Soit $\mathscr{N}_d(t)$ le nombre de points de $\mathbb{Z}^d$ contenus dans une $d$-sphère de rayon carré $t$. On cherche alors à borner supérieurement $\mathscr{N}_d(t) - 1$.

**Lemme 2.0.7.** *Pour tout $\delta < d$,*

$$\mathscr{N}_d(\delta) \leq 2^\delta \delta \binom{\delta + d - 1}{\delta}.$$

*Démonstration.* On cherche à compter la taille de $\left\{\Delta \in \mathbb{Z}^d : \sum_{i=1}^d \Delta_i \leq \delta\right\}$ où le vecteur $\Delta = (\Delta_1, \cdots, \Delta_d)$. Pour ce faire, nous allons considérer $Q(k) = \left\{q \in \mathbb{N}^d : \sum_{i=1}^d q_i = k\right\}$. Calculer la taille de cet ensemble revient à compter les différentes façons de répartir les k unités parmi les $d$ différents $q_i$ Ainsi, $|Q(k)| = \binom{k+d-1}{k}$. À chaque élément de l'ensemble $Q(k)$ correspond au plus $2^\delta$ éléments de $\left\{\Delta \in \mathbb{Z}^d : \sum_{i=1}^d \Delta_i \leq \delta\right\}$. En effet, puisque $\delta < d$ et que $k \leq \delta$, les éléments de $Q(k)$ possèdent au plus $k$ coordonnées non-nulles. Pour chacune de ces coordonnées $q_i$, il y a au plus deux possibilités pour $\Delta_i$, soit $\sqrt{q_i}$ et $-\sqrt{q_i}$. Donc,

$$\mathscr{N}_d(\delta) \leq \sum_{k=1}^{\lfloor \delta \rfloor} 2^\delta \binom{k + d - 1}{k} \leq 2^\delta \delta \binom{\delta + d - 1}{\delta}$$

ce qu'il fallait démontrer.

□

Avec ces bornes obtenus aux lemmes 2.0.6 et 2.0.7, nous sommes en mesure de borner l'expression dans l'inégalité (2.6). Mais avant, tentons de simplifier les expressions obtenus dans les deux lemmes. Premièrement, on a, par les équations (2.1) et par le fait que $d \geq 60$, que

$$\begin{aligned} \mu_Z + \sqrt{2}\sigma_Z &\leq \frac{d}{12}(y^2-1) + \frac{\sqrt{2d}}{6\sqrt{5}}y^2 \leq \frac{7}{72}dy^2. \\ \mu_Z - \sqrt{2}\sigma_Z &\geq \frac{d}{12}(y^2-1) - \frac{\sqrt{2d}}{6\sqrt{5}}y^2 \geq \frac{5}{72}dy^2. \end{aligned}$$

Alors la borne de $|B_\Delta(h)|$ du lemme 2.0.6 devient, avec $\rho(\Delta) \leq \sqrt{5d}$ et l'approximation de Stirling pour $\Gamma\left(\frac{d+1}{2}\right)$,

$$\begin{aligned} |B_\Delta(h)| &\leq \frac{\pi^{\frac{d-1}{2}}}{\Gamma\left(\frac{d+1}{2}\right)} \left( \left( \sqrt{\frac{7d}{72}}y + \frac{\sqrt{5d}}{2} \right)^{d-1} - \left( \sqrt{\frac{5d}{72}}y - \frac{\sqrt{5d}}{2} \right)^{d-1} \right) \\ &\leq 2\frac{\pi^{\frac{d-1}{2}}}{\Gamma\left(\frac{d+1}{2}\right)} \left( \left( \sqrt{\frac{7d}{72}}y \right)^{d-1} - \left( \sqrt{\frac{5d}{72}}y \right)^{d-1} \right) \\ &\leq 2\frac{\pi^{\frac{d-1}{2}}}{\Gamma\left(\frac{d+1}{2}\right)} \left( \sqrt{\frac{d}{72}}y \right)^{d-1} \left( 7^{\frac{d-1}{2}} - 5^{\frac{d-1}{2}} \right) \\ &\leq \frac{4}{\sqrt{2\pi}} \frac{(2\pi e)^{\frac{d-1}{2}}}{(d-1)^{\frac{d}{2}}} \left( \sqrt{\frac{d}{72}}y \right)^{d-1} \left( 7^{\frac{d-1}{2}} - 5^{\frac{d-1}{2}} \right) \\ &\leq \frac{4e}{\sqrt{2\pi}\,(d-1)} \left( \sqrt{\frac{\pi e}{36}}y \right)^{d-1} \left( 7^{\frac{d-1}{2}} - 5^{\frac{d-1}{2}} \right) \end{aligned} \tag{2.7}$$

Par ailleurs, étudions, afin de simplifier la borne du lemme 2.0.7, le coefficient bino-

mial $\binom{\delta+d-1}{\delta}$. On a, par l'approximation de Stirling, que

$$\binom{\delta+d-1}{\delta} = \frac{(\delta+d-1)!}{\delta!(d-1)!} \leq \frac{8}{\sqrt{2\pi}} \frac{(\delta+d-1)^{\delta+d-\frac{1}{2}}}{\delta^{\delta+\frac{1}{2}}(d-1)^{d-\frac{1}{2}}}. \tag{2.8}$$

Avec les inégalités (2.7) et (2.8), et avec l'aide des lemmes 2.0.6 et 2.0.7, on peut borner $\sum_{n=1}^{\left\lceil \frac{2\sqrt{2}\sigma_Z}{\delta} \right\rceil} \left| D(\mu_Z - \sqrt{2}\sigma_Z + n\delta, \delta) \right|$ de l'inégalité (2.6). Alors, on a, après plusieurs simplifications, que

$$\sum_{n=1}^{\left\lceil \frac{2\sqrt{2}\sigma_Z}{\delta} \right\rceil} \left| D(\mu_Z - \sqrt{2}\sigma_Z + n\delta, \delta) \right| \leq \frac{8e}{\pi} \frac{(\delta+d-1)^{\delta+d-\frac{1}{2}}}{\delta^{\delta-\frac{1}{2}}(d-1)^{d+\frac{1}{2}}} \left( \frac{\sqrt{\pi e}}{6} y \right)^{d-1} \left( 7^{\frac{d-1}{2}} - 5^{\frac{d-1}{2}} \right)$$

et si on pose $\delta = \varepsilon d$ pour un certain $\varepsilon < 1$, l'inégalité devient alors

$$D \leq \frac{48\sqrt{e\varepsilon}}{\pi^{\frac{3}{2}}} \sqrt{\frac{d}{(d-1)\left((\varepsilon+1)d-1\right)}} \left( \frac{\sqrt{7\pi e}\left((\varepsilon+1)d-1\right)^{\varepsilon+1}}{6(\varepsilon d)^{\varepsilon}(d-1)} \right)^{d} y^{d-1}. \tag{2.9}$$

Nous sommes maintenant en mesure de borner l'équations inférieurement l'équation suivante :

$$\sum_{n=1}^{\left\lceil \frac{2\sqrt{2}\sigma_Z}{\delta} \right\rceil} \left| A(\mu_Z - \sqrt{2}\sigma_Z + n\delta, \delta) \right| - \left| D(\mu_Z - \sqrt{2}\sigma_Z + n\delta, \delta) \right|$$

La borne inférieure est obtenue à partir des inégalités (2.4) et (2.9). Elle est

$$\begin{aligned} &\geq \frac{y^d}{2} - \frac{48\sqrt{e\varepsilon}}{\pi^{\frac{3}{2}}}\sqrt{\frac{d}{(d-1)\left((\varepsilon+1)d-1\right)}}\left(\frac{\sqrt{7\pi e}\left((\varepsilon+1)d-1\right)^{\varepsilon+1}}{6(\varepsilon d)^{\varepsilon}(d-1)}\right)^d y^{d-1} \\ &= \frac{y^d}{2}\left(1 - \frac{192\sqrt{e\varepsilon}}{\pi^{\frac{3}{2}}}\sqrt{\frac{d}{(d-1)\left((\varepsilon+1)d-1\right)}}\left(\frac{\sqrt{7\pi e}\left((\varepsilon+1)d-1\right)^{\varepsilon+1}}{6\sqrt{2}(\varepsilon d)^{\varepsilon}(d-1)}\right)^d\right). \end{aligned}$$

Si on choisit $\varepsilon = \frac{2}{125}$, on a, pour tout $d \geq 60$, que l'intérieur de la parenthèse de l'inégalité précédente est supérieur à $\frac{1}{2}$. Alors, on a que, pour $\delta = \frac{2d}{125}$,

$$\sum_{n=1}^{\left\lceil \frac{2\sqrt{2}\sigma_Z}{\delta} \right\rceil} \Big|A(\mu_Z - \sqrt{2}\sigma_Z + n\delta, \delta)\Big| - \Big|D(\mu_Z - \sqrt{2}\sigma_Z + n\delta, \delta)\Big| \geq \frac{y^d}{4}. \tag{2.10}$$

Par contre, étant donné que les ensembles $D(\mu_Z - \sqrt{2}\sigma_Z + n\delta, \delta)$ représentent le nombre de progressions arithmétiques dans l'ensemble $A(\mu_Z - \sqrt{2}\sigma_Z + n\delta, \delta)$, l'inégalité précédente nous indique que la somme des tailles de $\left\lceil \frac{2\sqrt{2}\sigma_Z}{\delta} \right\rceil$ ensembles sans progressions arithmétiques est supérieure ou égale à $\frac{y^d}{2}$. Par le principe du pigeonnier, et en rappelant la borne obtenu en (2.3) pour $\sigma_Z$, il en existe un, noté $A$, tel que

$$|A| \geq \frac{y^d}{4\left(\frac{2\sqrt{2}\sigma_Z}{\delta} + 1\right)} \geq \frac{\sqrt{5}}{84\sqrt{2}} y^{d-2}\sqrt{d}.$$

Cet ensemble $A$ est, par contre, un sous-ensemble de $\mathbb{Z}^d$. Soit maintenant $\phi : A \longrightarrow \mathbb{Z}$

définit par

$$\phi(x_1, x_2, ..., x_d) = x_1 + x_2(2y) + ... + x_d(2y)^{d-1}.$$

Par le lemme 1.1.2, on a que la fonction $\phi$ préserve les progressions arithmétiques de $A$, de même que $\phi^{-1}$. Alors, si $A$ ne contient pas de progressions arithmétiques, alors on a que l'ensemble $\phi(A)$, qui est un sous-ensemble de $\{1, 2, ..., N\}$, n'a pas de progression arithmétiques. Bien sûr, $|\phi(A)| = |A|$. Pour tous $n \in \phi(A)$, on a que $n \leq (2y)^d$, que l'on pose comme $N$. Alors, $y = \frac{N^{\frac{1}{d}}}{2}$ et

$$|\phi(A)| \geq \frac{\sqrt{5}}{21\sqrt{2}} \frac{N\sqrt{d}}{2^d N^{\frac{2}{d}}} = \frac{2^{\frac{1}{4}}\sqrt{5}}{21\sqrt{2}} \frac{N\sqrt{d}}{2^{d+\frac{2}{d}\log_2(N)}}. \tag{2.11}$$

On veut alors poser $d$, en fonction de $N$, de manière à minimiser le dénominateur, soit minimiser $d + \frac{2}{d}\log_2(N)$. On pose alors $d = \left\lceil \sqrt{2\ \log_2(N)} \right\rceil$ pour obtenir la borne désirée :

$$|\phi(A)| \geq \frac{2^{\frac{1}{4}}\sqrt{5}}{21\sqrt{2}} \frac{N(\log_2(N))^{\frac{1}{4}}}{2^{\left(2\sqrt{2}\sqrt{\log_2(N)}\right)}}.$$

Cette borne est valide pour $d \geq 60$,et donc pour $N \geq 10^{542}$.

□

# CHAPITRE 3

# LES POINTS ENTIERS DANS UNE $D$-SPHÈRE

Soit $P_d(t) = \mathscr{N}_d(t) - \mathscr{V}_d(t)$, la différence entre le volume et le nombre de points entiers dans une $d$-sphère de rayon carré $t$. Nous avons utilisé certaines méthodes pour estimer la taille de $\mathscr{N}_d(t)$ dans la section précédente, mais ces dernières ne sont pas optimales, quoique suffisantes pour la preuve. Cette section sera consacrée à borner $|P_d(t)|$ le plus optimalement possible. Nous allons d'abord trouver une borne pour une sphère en 4 dimensions, qui est, en fait, la meilleure borne connue. Après, nous allons utiliser la borne obtenue pour trouver une borne pour la différence entre le nombre de points entier et le volume d'une sphère à 5 dimensions. Cette dernière sera la base d'induction pour l'obtention d'une borne sur les sphère à $d$ dimensions, avec $d \geq 5$. Nous allons ensuite montrer à quel point les bornes pour $d \geq 5$ sont optimales. Tout d'abord, il sera important de prouver ces quelques lemmes suivants.

## 3.1 Lemmes sur la fonction $\psi$ d'Euler et sur les sommes exponentielles

Les lemmes de cette section sont tous utiles pour démontrer les théorèmes des sections suivantes. La fonction $\psi$, défini comme $\psi(x) = x - \lfloor x \rfloor - \frac{1}{2}$, sert surtout à faire le lien entre l'intégrale d'une fonction et ses sommes partielles.

**Lemme 3.1.1.** *Soit $f$ une fonction continûment différentiable sur l'intervalle réel $(a,b)$*

*et* $\psi(x) = x - \lfloor x \rfloor - \frac{1}{2}$. *Alors*

$$\sum_{a \leq n \leq b} f(n) - \int_a^b f(x)dx = \psi(a)f(a) - \psi(b)f(b) + \int_a^b \psi(x)f'(x)dx$$

*Démonstration.* Il suffit d'intégrer la fonction $f(x)d\psi(x)$ et d'utiliser la linéarité de l'intégrale de Riemann-Stieltjes pour obtenir

$$\int_a^b f(x)d\psi(x) = \int_a^b f(x)dx - \int_a^b f(x)d\lfloor x \rfloor - \int_a^b f(x)d\frac{1}{2}.$$

On intègre par partie le côté gauche de l'égalité précédente et, du côté droit, on évalue les intégrales de Riemann-Stieltjes :

$$\begin{aligned}
\int_a^b f(x)d\psi(x) &= \int_a^b f(x)dx - \sum_{a \leq n \leq b} f(n) \\
\psi(b)f(b) - \psi(a)f(a) - \int_a^b \psi(x)f'(x)dx &= \int_a^b f(x)dx - \sum_{a \leq n \leq b} f(n). \\
\psi(a)f(a) - \psi(b)f(b) + \int_a^b \psi(x)f'(x)dx &= \sum_{a \leq n \leq b} f(n) - \int_a^b f(x)dx
\end{aligned}$$

ce qu'il fallait démontrer.

□

**Lemme 3.1.2.** *Pour tout* $d \geq 2$, *pour tout* $t \geq 0$ *et pour tout* $\alpha \in \mathbb{R}$,

$$\left| \int_0^{\sqrt{t}} \psi(x-\alpha)x(t-x^2)^{\frac{d}{2}-1}dx \right| \leq \frac{1}{2\sqrt{ed}} t^{\frac{d-1}{2}}$$

*Démonstration.* Posons $f(x) = x(t-x^2)^{\frac{d}{2}-1}$, et $A(T) = \int_0^T \psi(x-\alpha)dx$ pour $0 \leq T \leq \sqrt{t}$. Remarquons que $\psi$ est une fonction de période 1 et, pour tout $n \in \mathbb{Z}$, $\int_n^{n+1} \psi(x-\alpha)dx = \int_n^{n+1} \{x-\alpha\} - \frac{1}{2}dx = 0$. Donc, la fonction $A(T)$ atteint son maximum lorsque $\{T\}$, la partie fractionnaire de $T$, est égale à $\frac{1}{2}$. Alors,

$$|A(T)| = \left| \int_0^{\{T\}} \psi(x-\alpha)dx \right| \leq \left| \int_0^{\frac{1}{2}} \left( x - \frac{1}{2} \right) dx \right| = \frac{1}{8}. \tag{3.1}$$

On intègre par partie la fonction $\psi(x-\alpha)f(x)$ de la manière suivante :

$$\int_0^{\sqrt{t}} \psi(x-\alpha)f(x)dx = A(x)f(x) \mid_0^{\sqrt{t}} - \int_0^{\sqrt{t}} A(x)f'(x)dx = -\int_0^{\sqrt{t}} A(x)f'(x)dx,$$

où $f'(x) = (t-x^2)^{\frac{d}{2}-2}(t-(d-1)x^2)$. Remarquons que cette fonction est positive si et seulement si $x^2 \leq \frac{t}{d-1}$. Alors, on utilise (3.1) pour obtenir

$$\begin{aligned}
\left| \int_0^{\sqrt{t}} \psi(x-\alpha)f(x)dx \right| &\leq \frac{1}{8}\int_0^{\sqrt{t}} \left| f'(x) \right| dx = \frac{1}{8}\int_0^{\sqrt{\frac{t}{d-1}}} f'(x)dx - \frac{1}{8}\int_{\sqrt{\frac{t}{d-1}}}^{\sqrt{t}} f'(x)dx \\
&\leq \frac{1}{8}\left( 2f\left( \sqrt{\frac{t}{d-1}} \right) - f(\sqrt{t}) - f(0) \right) = \frac{1}{4}\sqrt{\frac{t}{d-1}} \left( \frac{d-1}{d-2}t \right)^{\frac{d}{2}-1} \\
&\leq \frac{1}{4}t^{\frac{d-1}{2}} \left( \frac{(d-2)^{d-2}}{(d-1)^{d-1}} \right)^{\frac{1}{2}} \leq \frac{t^{\frac{d-1}{2}}}{2\sqrt{ed}}
\end{aligned}$$

ce qu'il fallait démontrer.

□

**Lemme 3.1.3.**

$$\psi(x) = -\frac{1}{2\pi\imath} \sum_{\substack{m=-\infty \\ m\neq 0}}^{\infty} \frac{e^{2\pi\imath mx}}{m}$$

*Démonstration.* Par la série de Fourier de $\{x\} = x - \lfloor x \rfloor$ , on trouve que

$$\psi(x) = \frac{1}{2}a_0 + \sum_{m=1}^{\infty} a_m \cos(2m\pi x) + \sum_{m=1}^{\infty} b_m \sin(2m\pi x) - \frac{1}{2}$$

où

$$\begin{aligned}
a_0 &= 2\int_0^1 \{x\}dx = 1 \\
a_m &= 2\int_0^1 \{x\}\cos(2m\pi x)dx = \frac{\cos(2m\pi) - 1 + 2m\pi\sin(2m\pi)}{2m^2\pi^2} = 0 \\
b_m &= 2\int_0^1 \{x\}\sin(2m\pi x)dx = \frac{\sin(2m\pi) - 2m\pi\cos(2m\pi)}{2m^2\pi^2} = -\frac{1}{m\pi}
\end{aligned}$$

ce qui implique que

$$\begin{aligned}
\psi(x) &= \frac{1}{2} - \sum_{m=1}^{\infty} \frac{\sin(2\pi mx)}{m\pi} - \frac{1}{2} = -\frac{1}{\pi}\sum_{m=1}^{\infty} \frac{\sin(2\pi mx)}{m} \\
&= -\frac{1}{2\pi\imath}\sum_{m=1}^{\infty} \frac{e^{2\pi\imath mx} - e^{-2\pi\imath mx}}{m} = -\frac{1}{2\pi\imath}\sum_{\substack{m=-\infty \\ m\neq 0}}^{\infty} \frac{e^{2\pi\imath mx}}{m}
\end{aligned}$$

ce qu'il fallait démontrer.

□

Soit, pour $x \in \mathbb{R}$, la fonction $D_{\mathbb{Z}}(x) = \min_{n\in\mathbb{Z}} |n - x|$ qui représente la distance entre un nombre réel $x$ et le plus proche nombre entier. Les deux théorèmes suivants, qui

portent sur les sommes exponentielles, sont tirés de [4].

**Théorème 3.1.4** (Kusmin-Landau)**.** *Soit $a,b \in \mathbb{Z}$ et $f : \mathbb{R} \to \mathbb{R}$ une fonction continûment différentiable sur $[a,b]$ telle que $f'$ est monotone et qu'il existe $0 < \lambda \leq \frac{1}{2}$ tel que $D_{\mathbb{Z}}(f'(x)) \geq \lambda > 0$ pour tout $x \in [a,b]$. Alors,*

$$\left| \sum_{n=a}^{b} e^{2\pi\imath f(n)} \right| \leq \frac{2}{\lambda} + 1$$

*Démonstration.* Étant donné que $\left|\sum_{n=a}^{b} e^{2\pi\imath f(n)}\right| = \left|\sum_{n=a}^{b} e^{-2\pi\imath f(n)}\right|$, on peut supposer, sans perdre de généralité, que $f'$ est croissante. Puisque $D_{\mathbb{Z}}(f'(x)) \geq \lambda$, on a qu'il existe $k \in \mathbb{Z}$ tel que $k + \lambda \leq f'(x) \leq k + 1 - \lambda$. Cependant, puisque $e^{2\pi\imath f(n)} = e^{2\pi\imath(f(n)-kn)}$ et que $(f(n) - kn)' = f'(n) - k$, on peut aussi supposer, sans perdre de généralité, que $\lambda \leq f'(x) \leq 1 - \lambda$. Soit la fonction $g(n) = f(n+1) - f(n)$, pour $n \in [a,b]$. on sait, par le théorème de la moyenne, qu'il existe $x_n \in [n, n+1]$ tel que $g(n) = f'(x_n)$. Alors, $g$ est aussi croissante et $\lambda \leq g \leq 1 - \lambda$. Maintenant, on peut réécrire le terme principal de la somme de la manière suivante :

$$e^{2\pi\imath f(n)} = \frac{e^{2\pi\imath f(n)} - e^{2\pi\imath f(n+1)}}{1 - e^{2\pi\imath g(n)}} = \left(e^{2\pi\imath f(n)} - e^{2\pi\imath f(n+1)}\right) C_n$$

où $C_n = \frac{1}{2}(1 + \imath \cot(\pi g(n)))$. La somme à borner devient alors

$$\begin{aligned}
\left|\sum_{n=a}^{b} e^{2\pi\imath f(n)}\right| &= \left|\sum_{n=a}^{b-1}\left(e^{2\pi\imath f(n)} - e^{2\pi\imath f(n+1)}\right)C_n + e^{2\pi\imath f(b)}\right| \\
&= \left|\sum_{n=a+1}^{b-1} e^{2\pi\imath f(n)}(C_n - C_{n-1}) + e^{2\pi\imath f(a)}C_a + e^{2\pi\imath f(b)}(1 - C_{b-1})\right| \\
&\leq \sum_{n=a+1}^{b-1} |C_n - C_{n-1}| + |C_a| + |1 - C_{b-1}| \\
&\leq \frac{1}{2}\sum_{n=a+1}^{b-1} |\cot(\pi g(n-1)) - \cot(\pi g(n))| + |C_a| + |1 - C_{b-1}|. \quad (3.2)
\end{aligned}$$

Puisque $0 < \lambda \leq g(n) \leq 1 - \lambda < 1$, on a que $0 < \pi g(n) < \pi$, et alors tous les $\cot(\pi g(n))$ se retrouve dans la même période de la fonction cotagente, pour $n \in [a,b]$. Puisque la fonction cot est décroissante sur sa période et que $g(n)$ est croissante, on peut se débarrasser des valeurs absolues dans la somme de (3.2) pour obtenir

$$\begin{aligned}
\left|\sum_{n=a}^{b} e^{2\pi\imath f(n)}\right| &\leq \frac{1}{2}\sum_{n=a+1}^{b-1} (\cot(\pi g(n-1)) - \cot(\pi g(n))) + |C_a| + |1 - C_{b-1}| \\
&\leq \frac{1}{2}(\cot(\pi g(a)) - \cot(\pi g(b-1))) + |C_a| + |1 - C_{b-1}| \quad (3.3) \\
&\leq \frac{1}{2}(\cot(\pi g(a)) - \cot(\pi g(b-1)) + |\cot(\pi g(a))| + |\cot(\pi g(b-1))|) + 1
\end{aligned}$$

On peut alors appliquer la borne $|\cot(\pi x)| \leq D_{\mathbb{Z}}(x)^{-1}$, en se rappelant aussi que $D_{\mathbb{Z}}(g(n)) \geq \lambda$. On obtient, de l'inégalité (3.3),

$$\left|\sum_{n=a}^{b} e^{2\pi\imath f(n)}\right| \leq \frac{2}{\lambda} + 1$$

ce qu'il fallait démontrer.

□

**Théorème 3.1.5** (van der Corput)**.** *Soit $a,b \in \mathbb{Z}$ et une fonction $f \in C^2[a,b]$ telle que $|f''(x)| = \lambda > 0$ pour tout $x \in [a,b]$. Alors,*

$$\left| \sum_{n=a}^{b} e^{2\pi\imath f(n)} \right| \leq 5\sqrt{\lambda}(b-a) + \frac{10}{\sqrt{\lambda}}$$

*Démonstration.* Supposons, sans perdre de généralité, que $f''(x) = \lambda$, et donc que $f'(x)$ est croissante. Soit $0 < \beta \leq \frac{1}{2}$. On peut séparer l'intervalle $[a,b]$ en au plus $\lambda(b-a)+2$ intervalles sur lesquels $D_{\mathbb{Z}}(f'(x)) \geq \beta$, et en au plus $\lambda(b-a)+2$ intervalles sur les lesquels $D_{\mathbb{Z}}(f'(x)) < \beta$, mais ces derniers sont de longueur au plus $\frac{2\beta}{\lambda}$. On applique le théorème 3.1.4 à la première classe d'intervalle et l'inégalité du triangle à la deuxième classe. On obtient

$$\begin{aligned} \left| \sum_{n=a}^{b} e^{2\pi\imath f(n)} \right| &\leq (\lambda(b-a)+2)\left(\frac{2}{\beta}+1+\frac{2\beta}{\lambda}+1\right) \\ &\leq 2(\lambda(b-a)+2)\left(\frac{1}{\beta}+\frac{\beta}{\lambda}+1\right) \end{aligned}$$

On pose $\beta = \sqrt{\lambda}$ afin de minimiser le côté droit de l'inégalité précédente, et on obtient, pour $\lambda \leq \frac{1}{4}$,

$$\left| \sum_{n=a}^{b} e^{2\pi\imath f(n)} \right| \leq \frac{4}{\sqrt{\lambda}}(\lambda(b-a)+2)\left(1+\frac{\sqrt{\lambda}}{2}\right) \leq 5\sqrt{\lambda}(b-a)+\frac{10}{\sqrt{\lambda}}.$$

Si $\lambda > \frac{1}{4}$, le résultat découle simplement de l'inégalité du triangle.

□

**Lemme 3.1.6** (Walfisz [9]). *Pour tout $X, Y \in \mathbb{Z}$, $X \leq Y$, pour toute fonction $f \in C^2[X,Y]$ telle que $|f''(r)| = \varepsilon \leq 1$ pour tout $r \in [X,Y]$,*

$$\left| \sum_{r=X}^{Y} \psi(f(r)) \right| \leq (Y-X) \left( \frac{2^{\frac{4}{3}} 15}{\pi} \varepsilon^{\frac{1}{6}} + 2^{-\frac{7}{3}} \varepsilon^{\frac{1}{3}} \right) + \frac{30}{\pi} \varepsilon^{-\frac{1}{2}}.$$

*Démonstration.* La première observation à faire est que $\psi(y_1) - \psi(y_2) = y_1 - y_2 - (\lfloor y_1 \rfloor - \lfloor y_2 \rfloor)$, et donc que $\psi(y_1) - \psi(y_2) \leq y_1 - y_2$ si $y_1 \geq y_2$. Ceci entraîne que, pour tout $T \geq 1$,

$$T \sum_{r=X}^{Y} \int_0^{\frac{1}{T}} \psi(f(r)+\theta) - \psi(f(r))\, d\theta \;\; \leq \;\; T \sum_{r=X}^{Y} \int_0^{\frac{1}{T}} \theta d\theta \leq \frac{Y-X+1}{2T}. \quad (3.4)$$

Similairement, on a

$$T \sum_{r=X}^{Y} \int_{-\frac{1}{T}}^{0} \psi(f(r)) - \psi(f(r)+\theta)\, d\theta \leq \frac{Y-X+1}{2T}. \quad (3.5)$$

De plus, par le lemme 3.1.3, on a que pour tout $z \in \mathbb{R}$,

$$T \int_0^{\frac{1}{T}} \psi(z+\theta) d\theta = \sum_{\substack{m=-\infty \\ m \neq 0}}^{\infty} \omega_m^+ e^{2\pi \imath m z} \quad (3.6)$$

où $\omega_m^+ = \frac{-T}{2\pi\imath m}\int_0^{\frac{1}{T}} e^{2\pi\imath m\theta}d\theta$. Similairement, on a

$$T\int_{-\frac{1}{T}}^{0}\psi(z+\theta)d\theta = \sum_{\substack{m=-\infty\\ m\neq 0}}^{\infty}\omega_m^- e^{2\pi\imath mz}. \tag{3.7}$$

où $\omega_m^- = \frac{-T}{2\pi\imath m}\int_{-\frac{1}{T}}^{0} e^{2\pi\imath m\theta}d\theta$. L'inégalité du triangle sur les intégrales dans la définition de $|\omega_m^-|, |\omega_m^+|$ nous donne que $|\omega_m^-|, |\omega_m^+| \leq \frac{1}{2\pi|m|}$, et si on évalue l'intégrale, on en arrive à $|\omega_m^-|, |\omega_m^+| \leq \frac{T}{2\pi m^2}$, ce qui implique que $|\omega_m^-|, |\omega_m^+| \leq \frac{1}{2\pi}\min\left(\frac{1}{|m|}, \frac{T}{m^2}\right)$. Les inégalités (3.4), (3.5), (3.6) et (3.7) combinées impliquent que

$$\left|T\sum_{r=X}^{Y}\int_0^{\frac{1}{T}}\psi\left(f(r)+\theta\right)d\theta\right| \leq \frac{1}{\pi}\sum_{m=1}^{\infty}\left|\sum_{r=X}^{Y}e^{2\pi\imath mf(r)}\right|\min\left(\frac{1}{m}, \frac{T}{m^2}\right) \tag{3.8}$$

Il est maintenant temps d'appliquer le théorème 3.1.5 à l'inégalité (3.8), pour la fonction $mf(r)$. On obtient alors que la deuxième dérivée est $m\varepsilon$ et alors

$$\begin{aligned}\left|T\sum_{r=X}^{Y}\int_0^{\frac{1}{T}}\psi\left(f(r)+\theta\right)d\theta\right| &\leq \frac{1}{\pi}\sum_{m=1}^{\infty}\left(5\sqrt{m\varepsilon}(Y-X)+\frac{10}{\sqrt{m\varepsilon}}\right)\min\left(\frac{1}{m}, \frac{T}{m^2}\right)\\ &\leq \frac{5}{\pi}\sqrt{\varepsilon}\,(Y-X)\,T\sum_{m=1}^{\infty}\frac{1}{m^{\frac{3}{2}}}+\frac{10}{\pi\sqrt{\varepsilon}}\sum_{m=1}^{\infty}\frac{1}{m^{\frac{3}{2}}}\\ &\leq \frac{15}{\pi}\sqrt{\varepsilon}\,(Y-X)\,T+\frac{30}{\pi\sqrt{\varepsilon}}.\end{aligned} \tag{3.9}$$

Finalement, puisque $T\int_0^{\frac{1}{T}}\sum_{r=X}^{Y}\psi\left(f(r)\right) = T\int_{-\frac{1}{T}}^{0}\sum_{r=X}^{Y}\psi\left(f(r)\right) = \psi\left(f(r)\right)$, on peut isoler $\sum_{r=X}^{Y}\psi\left(f(r)\right)$ dans les équations (3.4) et (3.5), et on applique la borne (3.9), et on

obtient que

$$\left|\sum_{r=X}^{Y}\psi(f(r))\right| \leq \frac{15}{\pi}\sqrt{\varepsilon}\,(Y-X)\,T+\frac{30}{\pi\sqrt{\varepsilon}}+\frac{Y-X+1}{2T}$$

On choisit alors $T=2^{\frac{4}{3}}\varepsilon^{-\frac{1}{3}}$. De cette façon, on a $T\geq 1$ si et seulement $\varepsilon\leq 2$. On obtient alors comme borne

$$\left|\sum_{r=X}^{Y}\psi(f(r))\right| \leq (Y-X)\left(\frac{2^{\frac{4}{3}}15}{\pi}\varepsilon^{\frac{1}{6}}+2^{-\frac{7}{3}}\varepsilon^{\frac{1}{3}}\right)+\frac{30}{\pi}\varepsilon^{-\frac{1}{2}}$$

ce qu'il fallait démontrer.

□

## 3.2 Les points entiers dans une 4-sphère

Dans cette section, nous nous intéresserons à borner $|P_4(t)|$, puisque c'est la base qui nous permettra ensuite de borner $|P_5(t)|$, qui, à son tour, sera la base d'induction pour borner $|P_d(t)|$ pour tout $d \geq 5$. Nous commençons notre analyse à $d = 4$ puisqu'il existe un théorème sur la représentation de nombre entier comme somme de 4 carrés, dû à Jacobi [8]. La preuve de la borne pour $d = 4$ est dû à Walfisz [9], mais sa preuve ne se préoccupe pas de la constante. Il nous sera utile de trouver une constante explicite pour la borne, au lieu de simplement citer qu'il existe une constante qui fait l'affaire.

**Théorème 3.2.1** (Jacobi)**.** *Soit* $r_d(n) = |\{\bar{x} \in \mathbb{Z}^d : ||x||^2 = n\}|$*, où* $n \in \mathbb{N}$*,* $n \geq 1$*. Alors,*

$$r_4(n) = 8 \sum_{4 \nmid m \,:\, m \mid n} m.$$

**Corollaire 3.2.2.** *Pour tout nombre impair* $\nu$*,*

$$r_4(2^a \nu) = \begin{cases} 8 \quad \sigma(\nu) & si\, a = 0 \\ 24 \quad \sigma(\nu) & si\, a > 0 \end{cases}$$

*où* $\sigma(n)$ *est la somme des diviseurs de n.*

*Démonstration.* Si $a = 0$, alors $2^a \nu$ est impair et on utilise le théorème 3.2.1 pour obtenir

le résultat, car $m \mid \nu$ implique que $4 \nmid m$ et

$$\sum_{4\nmid m\mid \nu} m = \sum_{m\mid \nu} m = \sigma(\nu).$$

Sinon, $a > 0$ et $2^a\nu$ est pair. Par le théorème 3.2.1, on a

$$r_4(2^a\nu) = 8 \sum_{4\nmid m\mid 2^a\nu} m = 8 \sum_{m\mid 2\nu} m = 8 \left( \sum_{2\mid m\mid 2\nu} m + \sum_{2\nmid m\mid 2\nu} m \right) = 8\left(2\sigma(\nu) + \sigma(\nu)\right) = 24\sigma(\nu)$$

ce qu'il fallait démontrer.

□

**Lemme 3.2.3** (Walfisz)**.** *Pour tout $t \geq 4$,*

$$|P_4(t)| \leq 14t\log(t).$$

*Démonstration.* Premièrement, on exprime $\mathcal{N}_4(t)$ en fonction de $r_4(n)$, grâce au théorème 3.2.1. On obtient que

$$\mathcal{N}_4(t) = 1 + \sum_{1\leq n\leq t} r_4(n).$$

On ajoute 1 pour le point $(0,0,0,0)$, car la fonction $r_4(0) = 1$. Dans les équations suivantes, $\mu$ et $\nu$ représente des nombres impairs exclusivement, et $n$ est strictement positif. On sépare la somme précédente en deux somme : une pour les $n$ impairs et l'autre pour

les $n$ pairs.

$$\mathscr{N}_4(t) = 1 + 8\sum_{\mu\le t}\sum_{d|\mu} d + 24\sum_{2n\le t}\sum_{\nu|n}\nu. \tag{3.10}$$

Afin d'analyser les deux sommes de (3.10), posons $S(t) = \sum_{n\le t}\sigma(n)$. Alors,

$$\begin{aligned}\sum_{2n\le t}\sum_{\nu|n}\nu &= \sum_{n\le\frac{t}{2}}\left(\sum_{d|n} d - \sum_{2d|n} 2d\right) = \sum_{n\le\frac{t}{2}}\sigma(n) - 2\sum_{2n\le\frac{t}{2}}\sum_{2d|2n} d \\ &= \sum_{n\le\frac{t}{2}}\sigma(n) - 2\sum_{n\le\frac{t}{4}}\sigma(n) = S\left(\frac{t}{2}\right) - 2S\left(\frac{t}{4}\right). \end{aligned}\tag{3.11}$$

Pour l'autre somme dans (3.10), on a

$$\begin{aligned}\sum_{\mu\le t}\sum_{d|\mu} d &= \sum_{n\le t}\sum_{d|n} d - \sum_{2n\le t}\sum_{d|2n} d = S(t) - \sum_{2n\le t}\left(\sum_{2d|2n} 2d + \sum_{\nu|n}\nu\right) \\ &= S(t) - 2\sum_{n\le\frac{t}{2}}\sum_{d|n} d - \sum_{2n\le t}\sum_{\nu|n}\nu = S(t) - 2S\left(\frac{t}{2}\right) - S\left(\frac{t}{2}\right) + 2S\left(\frac{t}{4}\right) \\ &= S(t) - 3S\left(\frac{t}{2}\right) + 2S\left(\frac{t}{4}\right). \end{aligned}\tag{3.12}$$

où on obtient l'égalité $\sum_{2n\le t}\sum_{\nu|n}\nu = S\left(\frac{t}{2}\right) - 2S\left(\frac{t}{4}\right)$ de l'équation (3.11). En combinant (3.11) et (3.12) dans (3.10), on a que

$$\mathscr{N}_4(t) = 1 + 8S(t) - 32S\left(\frac{t}{4}\right). \tag{3.13}$$

Il nous reste à borner $S(t)$ en fonction de $t$. La proposition suivante, tirée de [9], nous donne une borne convenable pour $S(t)$.

**Proposition 3.2.4.** *Pour tout $t \geq 1$,*

$$\left| S(t) - \frac{\pi^2}{12} t^2 \right| \leq \frac{1}{2} t \log(t) + t.$$

*Démonstration.* Soit $q$ un nombre entier positif.

$$S(t) = \sum_{n \leq t} \sum_{n=dq} d = \sum_{dn \leq t} d = \sum_{n \leq t} \sum_{d \leq \frac{t}{n}} d$$

Rappelons-nous que $\psi(x) = x - \lfloor x \rfloor - \frac{1}{2}$. Puisque $\sum_{d \leq \frac{t}{n}} d = \frac{1}{2}\left( \left\lfloor \frac{t}{n} \right\rfloor^2 + \left\lfloor \frac{t}{n} \right\rfloor \right)$, on a que

$$\begin{aligned} S(t) &= \frac{1}{2} \sum_{n \leq t} \left( \left\lfloor \frac{t}{n} \right\rfloor^2 + \left\lfloor \frac{t}{n} \right\rfloor \right) \\ &= \sum_{n \leq t} \left( \frac{t^2}{2n^2} - \frac{t}{n} \psi\left(\frac{t}{n}\right) + \frac{1}{2}\left( \left\lfloor \frac{t}{n} \right\rfloor - \frac{t}{n} \right) + \frac{1}{2}\left( \left\lfloor \frac{t}{n} \right\rfloor - \frac{t}{n} \right)^2 \right) \qquad (3.14) \\ &= \frac{t^2}{2} \left( \sum_{n=1}^{\infty} \frac{1}{n^2} - \sum_{n>t} \frac{1}{n^2} \right) - t \sum_{n \leq t} \frac{1}{n} \psi\left(\frac{t}{n}\right) + \frac{1}{2} \sum_{n \leq t} \left\lfloor \frac{t}{n} \right\rfloor - \frac{t}{n} + \left( \left\lfloor \frac{t}{n} \right\rfloor - \frac{t}{n} \right)^2. \end{aligned}$$

Remarquons que $0 \leq \left| \left\lfloor \frac{t}{n} \right\rfloor - \frac{t}{n} \right| \leq 1$ pour tout $n$ et pour tout $t$. De plus, on a que $|\psi(x)| \leq \frac{1}{2}$ pour tout $x \in \mathbb{R}$, et que la somme des inverses des carrés des nombres entiers est $\zeta(2) = \frac{\pi^2}{6}$. Ainsi, pour tout $t \geq 2$,

$$-\frac{t^2}{2} \sum_{n>t} \frac{1}{n^2} - \frac{1}{2} t \log(t) \leq S(t) - \frac{\pi^2}{12} t^2 \leq \frac{1}{2} t \log(t) + t.$$

Remarquons maintenant que

$$\frac{t^2}{2}\sum_{n>t}\frac{1}{n^2} \leq \frac{t^2}{2}\int_{t-1}^{\infty}\frac{dn}{n^2} \leq \frac{t^2}{2(t-1)} \leq t$$

et on a, par conséquence, pour tout $t \geq 2$,

$$|S(t) - \frac{\pi^2}{12}t^2| \leq \frac{1}{2}t\log(t) + t$$

ce qu'il fallait démontrer. Il nous reste à étudier le cas où $1 \leq t \leq 2$. On a que $S(1) = 1$ et donc que, pour tout $1 \leq t \leq \frac{2\sqrt{3}}{\pi}$, on a que $|S(t) - \frac{\pi^2}{12}t^2| = 1 - \frac{\pi^2}{12}t^2 \leq 1 \leq \frac{1}{2}t\log(t) + t$. Si $\frac{2\sqrt{3}}{\pi} < t \leq 2$, on a que $|S(t) - \frac{\pi^2}{12}t^2| = \frac{\pi^2}{12}t^2 - 1 \leq \frac{1}{2}t\log(t) + t$ car la fonction $\frac{\pi^2}{12}t^2 - 1 - \frac{1}{2}t\log(t) - t$ est croissante lorsque $\frac{2\sqrt{3}}{\pi} < t \leq 2$ et est négative lorsque $t = 2$. Donc, pour tout $1 \leq t \leq 2$, on a encore que $|S(t) - \frac{\pi^2}{12}t^2| \leq \frac{1}{2}t\log(t) + t$, ce qui complète la preuve.

□

On utilise alors le résultat de la proposition 3.2.4 dans l'équation (3.13) pour obtenir comme borne inférieure

$$\mathscr{N}_4(t) \geq 1 + \frac{2\pi^2}{3}t^2 + \frac{\pi^2}{6}t^2 - 4t(\log(t) + \log(\frac{t}{4}) + 3) = 1 + \frac{\pi^2}{2}t^2 - 4t(2\log(t) - \log(4) + 3)$$

et aussi, comme borne supérieure,

$$\mathscr{N}_4(t) \leq 1 + \frac{\pi^2}{2}t^2 + 4t(2\log(t) - \log(4) + 3).$$

À partir des deux dernières inégalités, on remarque que la borne supérieure est plus grande, en valeur absolue, que la borne inférieure. On en conclut que

$$\left| \mathscr{N}_4(t) - \frac{\pi^2}{2} t^2 \right| \leq 1 + 8t(\log(t) + 1)$$

et si $t \geq d = 4$, on a que

$$\left| \mathscr{N}_4(t) - \frac{\pi^2}{2} t^2 \right| \leq 14t \log(t).$$

Puisque $\mathscr{V}_4(t) = \frac{\pi^2}{2} t^2$, on a ce qu'il fallait démontrer.

□

### 3.3 Les points entiers dans une 5-sphère

**Théorème 3.3.1** (Walfisz)**.** *Pour tout $t \geq 1$,*

$$|P_5(t)| \leq 9195 t^{\frac{3}{2}}.$$

*Démonstration.* Notre point de départ sera les équations (3.13) et (3.14). En effet, on a que $\mathscr{N}_5(t) = \sum_{|l| \leq \sqrt{t}} \mathscr{N}_4(t-l^2)$, où $\mathscr{N}_4(t)$ est exprimée en fonction de $S(t)$. Si on reprend maintenant l'équation (3.14) pour déterminer $S(t)$, on a que

$$S(t) = \frac{t^2}{2}\left(\sum_{n=1}^{\infty}\frac{1}{n^2} - \sum_{n>t}\frac{1}{n^2}\right) - t\sum_{n\leq t}\frac{1}{n}\psi\left(\frac{t}{n}\right) + \frac{1}{2}\sum_{n\leq t}\left(\left(\left\lfloor\frac{t}{n}\right\rfloor - \frac{t}{n}\right) + \left(\left\lfloor\frac{t}{n}\right\rfloor - \frac{t}{n}\right)^2\right).$$

Puisque le dernier terme, en valeur absolue, est inférieur ou égal à $t$, on a que

$$\left|S(t) - \frac{\pi^2}{12}t^2 - tF(t)\right| \leq 2t$$

où $F(t) = \sum_{n\leq t}\frac{1}{n}\psi\left(\frac{t}{n}\right)$. On utilise alors l'équation (3.13) et l'inégalité précédente pour obtenir, pour tout $t \geq 1$

$$\begin{aligned}\left|\mathscr{N}_4(t) - \frac{\pi^2}{2}t^2 - 8tF(t) + 8tF\left(\frac{t}{4}\right)\right| &\leq 1 + \left|8S(t) - \frac{2\pi^2}{3}t^2 - 8tF(t)\right| \\ &+ \left|-32S\left(\frac{t}{4}\right) + \frac{\pi^2}{6}t^2 + 8tF\left(\frac{t}{4}\right)\right| \\ &\leq 1 + 16t + 16t \leq 33t. \qquad (3.15)\end{aligned}$$

On utilise maintenant le fait que $\mathscr{N}_5(t) = \sum_{|l|\leq\sqrt{t}} \mathscr{N}_4(t-l^2)$ pour en arriver à

$$\left| \mathscr{N}_5(t) - \frac{\pi^2}{2} \sum_{|l|\leq\sqrt{t}} \left(t-l^2\right)^2 + 8H(t) - 8G(t) \right| \leq 33 \sum_{|l|\leq\sqrt{t}} (t-l^2) \tag{3.16}$$

où $G(t) = \sum_{|l|\leq\sqrt{t}} (t-l^2)F(t-l^2)$ et $H(t) = \sum_{|l|\leq\sqrt{t}} (t-l^2)F\left(\frac{t-l^2}{4}\right)$. On peut approximer, grâce à la proposition suivante, les tailles de $\sum_{|l|\leq\sqrt{t}} \left(t-l^2\right)^2$ et de $\sum_{|l|\leq\sqrt{t}} (t-l^2)$.

**Proposition 3.3.2.** *Pour tout $t > 0$, pour tout $d \geq 4$ et pour tout $\alpha \in [0,1)$,*

$$\left| \mathscr{V}_{d+1}(t) - \sum_{\substack{|r|\leq\sqrt{t} \\ r-\lfloor r \rfloor = \alpha}} \mathscr{V}_d(t-r^2) \right| \leq \frac{\sqrt{d}\pi^{\frac{d}{2}}}{\sqrt{e}\Gamma\left(\frac{d}{2}+1\right)} t^{\frac{d-1}{2}}.$$

*Démonstration.* Nous allons utiliser les lemmes 3.1.1 et 3.1.2 pour trouver une borne appropriée. Effectuons d'abord un changement de variable sur la somme, afin qu'on somme sur des nombres entiers $r$. On a que

$$\sum_{\substack{|r|\leq\sqrt{t} \\ r-\lfloor r \rfloor = \alpha}} \mathscr{V}_d(t-r^2) = \sum_{\substack{-\sqrt{t}-\alpha \leq r \leq \sqrt{t}-\alpha \\ r\in\mathbb{Z}}} \mathscr{V}_d(t-(r+\alpha)^2).$$

On prend, pour le lemme 3.1.1, $f(x) = \mathscr{V}_d(t-(x+\alpha)^2)$, $a = -\sqrt{t}-\alpha$ et $b = \sqrt{t}-\alpha$, on a que $f(a) = f(b) = 0$ et aussi que $f'(x) = -\frac{d\pi^{\frac{d}{2}}}{\Gamma\left(\frac{d}{2}+1\right)}(x+\alpha)(t-(x+\alpha)^2)^{\frac{d}{2}-1}$. Remarquons aussi que

$$\int_{-\sqrt{t}-\alpha}^{\sqrt{t}-\alpha} \mathscr{V}_d(t-(x+\alpha)^2)\,dx = \int_{-\sqrt{t}}^{\sqrt{t}} \mathscr{V}_d(t-x^2)\,dx = \mathscr{V}_{d+1}(t).$$

Donc, par le lemme 3.1.1, on a que

$$\begin{aligned}\left|\mathscr{V}_{d+1}(t)-\sum_{\substack{|r|\leq\sqrt{t}\\ r-\lfloor r\rfloor=\alpha}}\mathscr{V}_d(t-r^2)\right| &\leq \left|\int_a^b \psi(x)f'(x)\,dx\right| \\ &\leq \left|-\frac{d\pi^{\frac{d}{2}}}{\Gamma\left(\frac{d}{2}+1\right)}\int_{-\sqrt{t}-\alpha}^{\sqrt{t}-\alpha}\psi(x)(x+\alpha)(t-(x+\alpha)^2)^{\frac{d}{2}-1}dx\right| \\ &\leq \left|-\frac{d\pi^{\frac{d}{2}}}{\Gamma\left(\frac{d}{2}+1\right)}\int_{-\sqrt{t}}^{\sqrt{t}}\psi(x-\alpha)x\,(t-x^2)^{\frac{d}{2}-1}dx\right|\end{aligned}$$

et, par le lemme 3.1.2, on obtient

$$\begin{aligned}\left|\mathscr{V}_{d+1}(t)-\sum_{\substack{|r|\leq\sqrt{t}\\ r-\lfloor r\rfloor=\alpha}}\mathscr{V}_d(t-r^2)\right| &\leq \frac{\sqrt{d}\pi^{\frac{d}{2}}}{\sqrt{e}\Gamma\left(\frac{d}{2}+1\right)}t^{\frac{d-1}{2}} \\ &\leq \frac{\sqrt{d}\pi^{\frac{d}{2}}}{\sqrt{e}\Gamma\left(\frac{d}{2}+1\right)}t^{\frac{d-1}{2}}\end{aligned} \tag{3.17}$$

ce qui complète la preuve.

□

En effet, on obtient que

$$\left|\frac{\pi^2}{2}\sum_{|l|\leq\sqrt{t}}\left(t-l^2\right)^2-\mathscr{V}_5(t)\right|\leq\frac{\pi^2}{\sqrt{e}}t^{\frac{3}{2}} \tag{3.18}$$

et

$$33\sum_{|l|\leq t}(t-l^2)\leq 44t^{\frac{3}{2}}+\frac{66\sqrt{2}}{\sqrt{e}}\sqrt{t}.$$

Il ne nous reste qu'à montrer qu'il existe une constante $c$ telle que $G(t),H(t)\leq ct^{\frac{3}{2}}$, et on a la borne désirée. Pour ce faire, il nous faudra borner $\sum_{|l|\leq\sqrt{t}}F\left(t-l^2\right)$, et, par la définition de $F$, cela revient à borner correctement $\sum_{|l|\leq\sqrt{t}}\psi\left(\frac{t-l^2}{n}\right)$. C'est pour cela que le lemme 3.1.6, dû à Walfisz [9], sera utile. Remarquons que les fonctions $G(t)$ et $H(t)$ sont très similaires. En effet, nous allons d'abord prouver la borne sur $G(t)$, et nous allons ensuite remarquer que la preuve pour $H(t)$ est identique à un détail près.

**Proposition 3.3.3.** *Pour tout $t\geq 1$,*

$$|G(t)|\leq 624t^{\frac{3}{2}}.$$

*Démonstration.* Tout d'abord, remarquons que $(t-l^2)F(t-l^2)$ est symmétrique par rapport à 0, et donc que

$$G(t)=2\sum_{l=1}^{\lfloor\sqrt{t}\rfloor}(t-l^2)F(t-l^2)+tF(t)$$

et, puisqu'on sait déjà que $|F(t)|\leq\log(t)$, on obtient que

$$\left|G(t)-2\sum_{l=1}^{\lfloor\sqrt{t}\rfloor}(t-l^2)F(t-l^2)\right|\leq t\log(t). \tag{3.19}$$

Analysons maintenant la somme. Il sera utile de séparer $(t-l^2)$ et $F(t-l^2)$ dans la somme, et le lemme suivant fera l'affaire.

**Lemme 3.3.4.** *Soit* $(x_i)_{i=1}^{\infty}, (y_i)_{i=1}^{\infty} \in \mathbb{R}$ *deux suites de nombres réels. Alors, pour tout* $a,b \in \mathbb{N}$ *où* $a \leq b$*, on a*

$$\sum_{i=a}^{b} x_i y_i = \sum_{i=a}^{b} X_i(y_i - y_{i+1}) + X_b y_{b+1}$$

*où* $X_i = \sum_{j=a}^{i} x_j$.

*Démonstration.* Pour $a \leq n \leq b$, remarquons que le coefficient de $y_n$, du côté droit de l'égalité, est $X_n - X_{n-1} = x_n$, ce qui correspond au coefficient de $y_n$ du côté gauche de l'égalité. De plus, le coefficient de $y_{b+1}$ du côté droit est $-X_b + X_b = 0$, ce qui correspond encore au coefficient de $y_{b+1}$ du côté gauche. On en conclut que l'égalité est vraie.

□

On applique le lemme 3.3.4, avec $a=1$, $b = \lfloor \sqrt{t} \rfloor$, $x_i = F(t-i^2)$ et $y_i = (t-i^2)$. On obtient que

$$\begin{aligned} \sum_{l=1}^{\sqrt{t}} (t-l^2)F(t-l^2) &= \sum_{l=1}^{\sqrt{t}} X_l \left( (t-l^2) - (t-(l+1)^2) \right) + X_{\lfloor \sqrt{t} \rfloor} \left( t - (\lfloor \sqrt{t} \rfloor + 1)^2 \right) \\ &= \sum_{l=1}^{\sqrt{t}} X_l (2l+1) + X_{\lfloor \sqrt{t} \rfloor} \left( t - (\lfloor \sqrt{t} \rfloor + 1)^2 \right) \end{aligned} \tag{3.20}$$

où $X_l = \sum_{r=1}^{l} F(t-r^2)$. Remarquons que $-2\sqrt{t} - 1 \leq t - (\lfloor \sqrt{t} \rfloor + 1)^2 \leq 0$, et donc que $\left| t - (\lfloor \sqrt{t} \rfloor + 1)^2 \right| \leq 2\sqrt{t}$. Nous avons maintenant besoin de borner $X_l$, et la proposition

suivante nous sera utile.

**Proposition 3.3.5.** *Pour tout $x \leq \sqrt{t}$, pour tout $q \geq 1$,*

$$\left| \sum_{r=1}^{x} F\left(\frac{t-r^2}{q}\right) \right| \leq \left(89q^{-\frac{1}{6}} + q^{-\frac{1}{3}} + 14\right)\sqrt{t}$$

*Démonstration.* On utilise la définition de $F$, et on a

$$\sum_{r=1}^{x} F\left(\frac{t-r^2}{q}\right) = \sum_{r=1}^{x} \sum_{n=1}^{\frac{t-r^2}{q}} \frac{1}{n}\psi\left(\frac{t-r^2}{qn}\right) = \sum_{n=1}^{\frac{t-1}{q}} \frac{1}{n} \sum_{r=1}^{\min\{x,\sqrt{t-qn}\}} \psi\left(\frac{t-r^2}{qn}\right).$$

On applique alors le lemme 3.1.6 avec $X = 1$, $Y = \min\{x, \sqrt{t-qn}\}$ et $f(r) = \frac{t-r^2}{qn}$, ce qui implique que $f'(r) = -\frac{2r}{qn}$ et $|f''(r)| = \frac{2}{qn} = \varepsilon \leq 2$. On trouve alors que

$$\begin{aligned}
\left| \sum_{n=1}^{\frac{t-1}{q}} \frac{1}{n} \sum_{r=1}^{\min\{x,\sqrt{t-qn}\}} \psi\left(\frac{t-r^2}{qn}\right) \right| &\leq \sum_{n=1}^{\frac{t-1}{q}} \frac{1}{n}\left((Y-X)\left(\frac{2^{\frac{4}{3}}15}{\pi}\varepsilon^{\frac{1}{6}} + 2^{-\frac{7}{3}}\varepsilon^{\frac{1}{3}}\right) + \frac{30}{\pi}\varepsilon^{-\frac{1}{2}}\right) \\
&\leq \sum_{n=1}^{\frac{t-1}{q}} \frac{\sqrt{t}2^{\frac{3}{2}}15}{\pi q^{\frac{1}{6}} n^{\frac{7}{6}}} + \frac{\sqrt{t}}{4q^{\frac{1}{3}}n^{\frac{4}{3}}} + \frac{30\sqrt{q}}{\pi\sqrt{2n}} \\
&\leq \frac{\sqrt{t}2^{\frac{3}{2}}15\zeta\left(\frac{7}{6}\right)}{\pi q^{\frac{1}{6}}} + \frac{\sqrt{t}\zeta\left(\frac{4}{3}\right)}{4q^{\frac{1}{3}}} + \frac{30\sqrt{2t}}{\pi} \\
&\leq \left(89q^{-\frac{1}{6}} + q^{-\frac{1}{3}} + 14\right)\sqrt{t} \qquad (3.21)
\end{aligned}$$

car $\sum_{n=1}^{\frac{t-1}{q}} \frac{1}{n^s} \leq \sum_{n=1}^{\infty} n^{-s} = \zeta(s)$ pour $s > 1$, et $\sum_{n=1}^{\frac{t-1}{q}} n^{-\frac{1}{2}} \leq 2\sqrt{\frac{t}{q}}$, ce qui complète la preuve.

□

On utilise alors la proposition 3.3.5 dans l'inégalité (3.20) pour obtenir que

$$\left|\sum_{l=1}^{\sqrt{t}}(t-l^2)F(t-l^2)\right| \leq C\sqrt{t}\sum_{l=1}^{\sqrt{t}}(2l+1)+Ct$$

où la constante $C = 104$ est celle obtenue à la proposition 3.3.5 avec $q = 1$. On effectue la sommme et on trouve que

$$\left|\sum_{l=1}^{\sqrt{t}}(t-l^2)F(t-l^2)\right| \leq C\sqrt{t}\left(\sqrt{t}+1\right)\sqrt{t}+3Ct \leq 5Ct^{\frac{3}{2}}$$

ce qui implique, avec l'inégalité (3.19), que

$$|G(t)| \leq 5Ct^{\frac{3}{2}}+t\log(t) \leq 6Ct^{\frac{3}{2}} = 624t^{\frac{3}{2}}$$

ce qu'il fallait démontrer.

□

**Proposition 3.3.6.** *Pour tout $t \geq 1$,*

$$|H(t)| \leq 512t^{\frac{3}{2}}.$$

*Démonstration.* La preuve de la borne pour $|H(t)|$ est très similaire à celle pour $|G(t)|$ de la proposition 3.3.3. En effet, la seule différence dans la preuve est qu'on choisi $q = 4$ lorsqu'on applique la proposition 3.3.5, ce qui nous donne la constante différente.

□

Retournons maintenant à l'inégalité (3.16). Les propositions 3.3.3 et 3.3.6 nous indique que

$$\left| \mathscr{N}_5(t) - \frac{\pi^2}{2} \sum_{|l| \leq \sqrt{t}} \left(t - l^2\right)^2 \right| \leq 44 t^{\frac{3}{2}} + \frac{66\sqrt{2}}{\sqrt{e}} \sqrt{t} + 8\,(624 + 512)\, t^{\frac{3}{2}}.$$

L'inégalité précédente, combinée avec l'inégalité (3.18), nous donne que

$$|\mathscr{N}_5(t) - \mathscr{V}_5(t)| \leq 44 t^{\frac{3}{2}} + \frac{66\sqrt{2}}{\sqrt{e}} \sqrt{t} + 8\,(624 + 512)\, t^{\frac{3}{2}} + \frac{\pi^2}{\sqrt{e}} t^{\frac{3}{2}} \leq 9195 t^{\frac{3}{2}}$$

ce qui complète la preuve du théorème 3.3.1.

□

## 3.4 Les points entiers dans une $d$-sphère

Dans cette section, nous allons finalement prouver une borne sur la différence entre le nombre de points entiers et le volume d'une $d$-sphère. Le point de départ sera le théorème 3.3.1 de la section précédente, qui servira de base d'induction.

**Théorème 3.4.1.** *Pour tout $t > 0$, pour tout $d \geq 5$,*

$$|P_d(t)| \leq 440d \prod_{i=1}^{d-2} \left(1 + \frac{i}{t\sqrt{2\pi e}}\right) \mathscr{V}_{d-2}(t).$$

*Démonstration.* La preuve se fait par induction sur $d$. Pour $d = 5$, le théorème 3.3.1 nous donne que pour tout $t \geq 1$,

$$|P_5(t)| \leq 9195t^{\frac{3}{2}} \leq 2200 \prod_{i=1}^{3} \left(1 + \frac{i}{t\sqrt{2\pi e}}\right) \frac{4\pi}{3} t^{\frac{3}{2}}. \tag{3.22}$$

Pour l'étape d'induction, supposons que, pour $d \geq 5$ fixe, pour tout $t \geq 1$,

$$|P_d(t)| \leq 440d \prod_{i=1}^{d-2} \left(1 + \frac{i}{t\sqrt{2\pi e}}\right) \mathscr{V}_{d-2}(t).$$

Ainsi, on a, pour $d+1$,

$$\begin{aligned}
|P_{d+1}(t)| &= |\mathscr{N}_{d+1}(t) - \mathscr{V}_{d+1}(t)| = \left| \sum_{|r|\leq\sqrt{t}} \mathscr{N}_d(t-r^2) - \mathscr{V}_{d+1}(t) \right| \\
&\leq \sum_{|r|\leq\sqrt{t}} \left| \mathscr{N}_d(t-r^2) - \mathscr{V}_d(t-r^2) \right| + \left| \mathscr{V}_{d+1}(t) - \sum_{|r|\leq\sqrt{t}} \mathscr{V}_d(t-r^2) \right| \qquad (3.23) \\
&\leq 440d \prod_{i=1}^{d-2} \left(1 + \frac{i}{t\sqrt{2\pi e}}\right) \sum_{|r|\leq\sqrt{t}} \mathscr{V}_{d-2}(t-r^2) + \left| \mathscr{V}_{d+1}(t) - \sum_{|r|\leq\sqrt{t}} \mathscr{V}_d(t-r^2) \right|.
\end{aligned}$$

Il nous reste à borner supérieurement la somme $\sum_{|r|\leq\sqrt{t}} \mathscr{V}_{d-2}(t-r^2)$ et la valeur absolue $\left| \mathscr{V}_{d+1}(t) - \sum_{|r|\leq\sqrt{t}} \mathscr{V}_d(t-r^2) \right|$. La proposition 3.3.2 est exactement ce que nous avons besoin. L'équation (3.23) devient

$$\begin{aligned}
|P_{d+1}(t)| &\leq 440d \prod_{i=1}^{d-2} \left(1 + \frac{i}{t\sqrt{2\pi e}}\right) \left( \mathscr{V}_{d-1}(t) + \frac{\sqrt{d-2}\pi^{\frac{d-2}{2}}}{\sqrt{e}\Gamma\left(\frac{d}{2}\right)} t^{\frac{d-3}{2}} \right) + \frac{\sqrt{d}\pi^{\frac{d}{2}}}{\sqrt{e}\Gamma\left(\frac{d}{2}+1\right)} t^{\frac{d-1}{2}} \\
&\leq 440d \prod_{i=1}^{d-2} \left(1 + \frac{i}{t\sqrt{2\pi e}}\right) \left(1 + \frac{\sqrt{(d-2)d}}{t\sqrt{2\pi e}}\right) \mathscr{V}_{d-1}(t) + \frac{\sqrt{\pi d}\Gamma\left(\frac{d+1}{2}\right)}{\sqrt{e}\Gamma\left(\frac{d}{2}+1\right)} \mathscr{V}_{d-1}(t) \\
&\leq 440 \prod_{i=1}^{d-1} \left(1 + \frac{i}{t\sqrt{2\pi e}}\right) \left( d\mathscr{V}_{d-1}(t) + \frac{\sqrt{\pi d}\Gamma\left(\frac{d+1}{2}\right)}{440\sqrt{e}\Gamma\left(\frac{d}{2}+1\right)} \mathscr{V}_{d-1}(t) \right).
\end{aligned}$$

Si $d \geq 4$, alors $\frac{\sqrt{\pi d}\Gamma\left(\frac{d+1}{2}\right)}{440\sqrt{e}\Gamma\left(\frac{d}{2}+1\right)} \leq 1$ et on obtient que

$$|P_{d+1}(t)| \leq 440(d+1) \prod_{i=1}^{d-1} \left(1 + \frac{i}{t\sqrt{2\pi e}}\right) \mathscr{V}_{d-1}(t)$$

ce qu'il fallait démontrer.

□

Le théorème suivant nous indique que la borne obtenue sur $|P_d(t)|$ est presque optimale asymptotiquement. Cela nous indique donc que la puissance de $t$ dans l'expression de la borne pour $|P_d(t)|$, pour $d \geq 5$, est la meilleure possible.

**Théorème 3.4.2.** *Pour tout $d \geq 2$, il existe $c_d > 0$ telle que pour tout $t \geq 1$, il existe $t_0 \geq t$ tel que*

$$|P_d(t_0)| \geq c_d \frac{\pi^{\frac{d}{2}}}{\Gamma\left(\frac{d}{2}+1\right)} t_0^{\frac{d-2}{2}}.$$

*Démonstration.* Supposons le contraire, c'est-à-dire que pour tout $c_d > 0$, il existe $t_{c_d}$ tel que pour tout $t \geq t_{c_d}$, on a que

$$|P_d(t)| < c_d \frac{\pi^{\frac{d}{2}}}{\Gamma\left(\frac{d}{2}+1\right)} t^{\frac{d-2}{2}}.$$

Fixons $c$, et soit $t_c$ correspondant au choix de $c$. Alors, pour tout nombre entier $n$ tel que $n > t_c$,

$$|P_d(n)| < c \frac{\pi^{\frac{d}{2}}}{\Gamma\left(\frac{d}{2}+1\right)} n^{\frac{d-2}{2}}.$$

$$\left|P_d\left(n+\frac{1}{2}\right)\right| < c \frac{\pi^{\frac{d}{2}}}{\Gamma\left(\frac{d}{2}+1\right)} \left(n+\frac{1}{2}\right)^{\frac{d-2}{2}}.$$

et donc, en combinant les deux inégalités précédentes, on obtient que

$$\left|P_d(n) - P_d\left(n+\frac{1}{2}\right)\right| < c \frac{\pi^{\frac{d}{2}}}{\Gamma\left(\frac{d}{2}+1\right)} \left(n^{\frac{d-2}{2}} + \left(n+\frac{1}{2}\right)^{\frac{d-2}{2}}\right).$$

et pour $n$ suffisamment grand,

$$\left|P_d(n) - P_d\left(n+\frac{1}{2}\right)\right| < k\frac{\pi^{\frac{d}{2}}}{\Gamma\left(\frac{d}{2}+1\right)}\left(2n^{\frac{d-2}{2}}\right). \tag{3.24}$$

où $k \geq c$. Par contre, on a

$$P_d(n) - P_d\left(n+\frac{1}{2}\right) = \mathscr{N}_d(n) - \mathscr{V}_d(n) - \mathscr{N}_d\left(n+\frac{1}{2}\right) + \mathscr{V}_d\left(n+\frac{1}{2}\right)$$

et, puisque $\mathscr{N}_d(t)$ représente la taille de l'ensemble des points entiers de norme au carré au plus $t$, on a que $\mathscr{N}_d(n) = \mathscr{N}_d(n+\frac{1}{2})$. Donc,

$$P_d(n) - P_d\left(n+\frac{1}{2}\right) = \frac{\pi^{\frac{d}{2}}}{\Gamma\left(\frac{d}{2}+1\right)}\left(\left(n+\frac{1}{2}\right)^{\frac{d}{2}} - n^{\frac{d}{2}}\right)$$

et, en développant $(n+\frac{1}{2})^{\frac{d}{2}}$, on remarque que le terme dominant, $n^{\frac{d}{2}}$, s'annule avec l'autre $n^{\frac{d}{2}}$, et donc,

$$\left|P_d(n) - P_d\left(n+\frac{1}{2}\right)\right| > \frac{d\pi^{\frac{d}{2}}}{4\Gamma\left(\frac{d}{2}+1\right)}n^{\frac{d-2}{2}}$$

ce qui contredit (3.24), et par conséquent, l'hypothèse de départ. L'hypothèse contredite étant l'énoncé contraire du théorème, on ne peut conclure que ce dernier est vrai.

□

## BIBLIOGRAPHIE


[1] F.A. Behrend. On sets of integers which contain no three terms in arithmetical progression. Dans *Proceedings of the National Academy of Sciences of the United States of America*, pages 331–332, 1946.

[2] M. Elkin. An improved construction of progression-free sets. *Israeli Journal of Mathematics*, 184(1):93–128, 2011.

[3] R. Salem et D. Spencer. On sets of integers which contain no three terms in arithmetic progression. Dans *Proceedings of the National Academy of Sciences of the United States of America*, pages 561–563, 1942.

[4] S.H. Graham et G. Kolesnik. *Van der Corput's method of exponential sums*. Cambridge University Press, 1991.

[5] B. Green et J. Wolf. A note on elkin's improvement of behrend's constructions. *Additive Number Theory*, 1:141–144, 2010.

[6] P. Erdös et P. Turàn. On some sequences of integers. *Journal of the London Mathematical Society*, s1-11:261–264, 1936.

[7] B. Green et T.Tao. The primes contain arbitrarily long arithmetic progressions. *Annals of Mathematics*, 167-2:481–547, 2008.

[8] M.D. Hischhorn. A simple proof of jacobi's four-square theorem. Dans *Proceedings of the American Mathematical Society*, pages 436–438, 1987.

[9] A. Walfisz. *Gitterpunkte in mehrdimensionalen Kugeln*. Panstwowe Wydawnictwo Naukowe, 1957.