Le problème de Waring

Alfonso CEVALLOS, Paul DARTHOS, Manuel DURIEZ

18 mai 2010

Table des matières

Chapitre 1

Introduction

Dans cet exposé, nous allons étudier le problème dit « de Waring », énoncé par Edward Waring en 1770 dans son ouvrage *Meditationes Algebraicae*, et dont David Hilbert a montré la véracité 1909, c'est pourquoi il lui a donné son nom. La conjecture est la suivante :

Théorème (Théorème de Waring-Hilbert)**.** *Pour tout entier naturel k , il existe un entier naturel s tel que tout entier naturel peut s'écrire comme somme d'au plus s puissances k-ièmes de nombres entiers naturels.*

En voici une autre formulation, plus explicite :

$$\forall k \in \mathbb{N}, \exists s \in \mathbb{N} \mid \forall N \in \mathbb{N}, \exists x_1, ..., x_s \in \mathbb{N} \mid N = x_1^k + ... + x_s^k$$

Nous allons montrer ce résultat, et également montrer que, pour tous les entiers N suffisamment grands, le plus petit s vérifiant cette condition pour un k donné sera majoré de la façon suivante : $s \leq 2^k + 1$.

Chapitre 2

La méthode du cercle

Cette méthode, introduite par John Edensor Littlewood (1885-1977), Godfrey Harold Hardy (1877-1947) et Srinivâsa Aiyangâr Râmânujan (1887-1920) en 1917, a été d'une grande importance dans les recherches en théorie des nombres du vingtième siècle, notamment dans la preuve du théorème de Waring (elle permet d'en avoir une preuve simplifiée par rapport à celle de Hilbert). Elle permit également à Hardy et Littlewood de faire progresser la démonstration de la conjecture faible de Goldbach :

Théorème (Conjecture faible de Goldbach)**.** *Chaque nombre impair plus grand que 5 peut être exprimé comme une somme de trois nombres premiers.*

Ivan Matveievitch Vinogradov (1891-1983) a perfectionné cette méthode du cercle en 1934, et a ainsi obtenu une avancée conséquente dans la démonstration de la conjecture de Goldbach, en la prouvant pour les nombres « assez grands »(en fait, pour tout $n > 3^{3^{15}}$), et son approche légèrement différente de celle de Hardy et Littlewood a apporté une meilleure étude du problème de Waring.

2.1 Définitions

Nous allons ici définir quelques fonctions utilisées dans cette étude. Au cours de ce travail, k désignera toujours la puissance à laquelle sont élevés les entiers dans la somme de Waring.

Définissons dans un premier temps la fonction r :

Définition (La fonction r). *Pour tous s, k entiers naturels fixés (respectivement la puissance et le nombre d'entiers élevés à la puissance k), soit $r_{s,k}$, définie pour tout entier naturel N :*

$$r_{s,k}(N) = \#\{(x_1, ...x_s) \in \mathbb{N}^s \mid x_1^k + ... + x_s^k = N\}$$

$r(N)$ est donc le nombre de représentations de N en somme de s puissances k-ièmes.

Par la suite, $r_{s,k}$ sera notée r.

Définissons ensuite les fonctions g et G :

Définition (La fonction g). *Pour tout entier naturel k, soit $g(k)$ le plus petit entier naturel s vérifiant la conjecture de Waring.*

$$g(k) = \min\{s \in \mathbb{N}^* | \forall N \in \mathbb{N}^*, r_{s,k}(N) > 0\}$$

Définition (La fonction G). *Pour tout entier naturel k, soit $G(k)$:*

$$G(k) = \min\{s \in \mathbb{N}^* | \exists N_0 \in \mathbb{N}^* | \forall N > N_0, r_{s,k}(N) > 0\}$$

Remarque. *On a toujours : $G(k) \leq g(k)$, et on a le résultat suivant (qui ne sera pas montré ici) :*

$$\frac{G(k)}{g(k)} \overset{k\to\infty}{\to} 0$$

Enfin, définissons une notation qui simplifiera grandement les écritures mathématiques que nous allons employer dans cette étude :

Notation (La fonction e). *Pour tout t réel, posons $e(t) = e^{2i\pi t}$*

2.2 La méthode de Hardy-Littlewood

Nous allons reprendre ici l'ébauche de démonstration qui a été celle de Hardy et Littlewood. Dans cette section, s et k sont fixés. Définissons d'abord la série génératrice :

Définition (La série génératrice f). *Pour tout nombre complexe z, soit :*

$$f(z) = \sum_{n=0}^{\infty} r(n) z^n$$

Puis intéressons-nous à son rayon de convergence :

Lemme. *Le rayon de convergence de cette série est supérieur ou égal à* 1.

Démonstration. En effet, comme on remarque que chacun des x_i vérifie trivialement : $x_i \leq n$, il y a donc au plus n choix pour chaque x_i, et on a s variables x_i, d'où :

$$\forall n \in \mathbb{N}^*, r(n) \leq n^s$$

Comme la série $\sum_{n=0}^{\infty} n^s z^n$ a pour rayon de convergence 1 (en application de la formule d'Hadamard au terme général n^s), la série génératrice a bien pour rayon de convergence $R \geq 1$. □

Notons maintenant $D = \{z \in \mathbb{C} : |z| < 1\}$ le disque unité ouvert.

Proposition. $\forall z \in D, f(z) = (\sum_{n=0}^{\infty} z^{n^k})^s$

Démonstration. La convergence absolue de la série sur l'ouvert D nous permet d'écrire :

$$(\sum_{n=0}^{\infty} z^{n^k})^s = \sum_{n_1 \ldots n_s \geq 0} z^{n_1^k + \ldots + n_s^k}$$

Puis, en regroupant tous les s-uplets $\{n_1, \ldots n_s\}$ tels que $n_1^k + \ldots + n_s^k = N$ pour chaque entier naturel N, et en utilisant le fait que $r(N)$ désigne le nombre de tels s-uplets, on obtient bien :

$$\sum_{n_1 \ldots n_s \geq 0} z^{n_1^k + \ldots + n_s^k} = \sum_{N=0}^{\infty} r(N) z^N$$

D'où l'égalité recherchée. □

Nous allons ensuite intégrer cette fonction génératrice sur un cercle, et obtenir l'expression de la fonction r qui fut le point de départ de Hardy et Littlewood :

Proposition. $\forall N \in \mathbb{N}^*, \forall \rho \in]0,1[, r(N) = \frac{1}{2\pi\rho^N} \int_0^{2\pi} f(\rho e^{it}) e^{-iNt} dt$

Démonstration. Partons de l'élément de droite, et cherchons à l'exprimer explicitement à l'aide de la définition de f :

$$\frac{1}{2\pi\rho^N} \int_0^{2\pi} f(\rho e^{it}) e^{-iNt} dt = \frac{1}{2\pi\rho^N} \int_0^{2\pi} (\sum_{n=0}^{\infty} (r(n)(\rho e^{it})^n)) e^{-iNt} dt$$

On fait rentrer tous les termes dans la somme :

$$\frac{1}{2\pi\rho^N} \int_0^{2\pi} f(\rho e^{it}) e^{-iNt} dt = \frac{1}{2\pi\rho^N} \int_0^{2\pi} (\sum_{n=0}^{\infty} (r(n)(\rho e^{it})^n e^{-iNt})) dt$$

La série singulière étant uniformément convergente sur D, elle l'est a fortiori sur tout cercle de rayon ρ, on peut donc intervertir les signes somme et intégrale :

$$\frac{1}{2\pi\rho^N}\int_0^{2\pi} f(\rho e^{it})e^{-iNt}dt = \frac{1}{2\pi\rho^N}\sum_{n=0}^{\infty}\int_0^{2\pi}(r(n)(\rho e^{it})^n e^{-iNt})dt$$

On réécrit l'expression obtenue de manière à ne garder que ce qui dépend de t dans l'intégrale :

$$\frac{1}{2\pi\rho^N}\int_0^{2\pi} f(\rho e^{it})e^{-iNt}dt = \frac{1}{2\pi\rho^N}\sum_{n=0}^{\infty}(r(n)\rho^n\int_0^{2\pi} e^{it(n-N)}dt\,)$$

On va préciser la valeur de l'intégrale. Notons-la :

$$I = \int_0^{2\pi} e^{it(n-N)}dt$$

- Si $n \neq N$, $I = [\frac{1}{i(n-N)}e^{it(n-N)}]_0^{2\pi} = \frac{1}{i(n-N)} - \frac{1}{i(n-N)} = 0$
- Si $n = N$, $I = \int_0^{2\pi} 1dt = 2\pi$

Dans la somme, tous les termes sauf celui en N sont donc nuls, on obtient donc :

$$\frac{1}{2\pi\rho^N}\int_0^{2\pi} f(\rho e^{it})e^{-iNt}dt = \frac{1}{2\pi\rho^N}r(N)\rho^N 2\pi$$

D'où, au final, l'égalité recherchée :

$$\frac{1}{2\pi\rho^N}\int_0^{2\pi} f(\rho e^{it})e^{-iNt}dt = r(N)$$

□

2.3 L'approche de Vinogradov

Au cours de ses travaux sur la méthode du cercle, Vinogradov a introduit une variante de la fonction $r(n)$, en bornant les éléments du s-uplet. On fixe $P \in \mathbb{N}$ qui sera la borne en question. Voici la définition de la fonction :

Définition (La fonction r'_P)**.** *Pour tout $m \in \mathbb{N}$:*

$$r'_P(m) = \#\{(x_1, ..., x_s) \in [|1; P|] \mid x_1^k + ... + x_s^k = m\}$$

Remarque. *On remarque que comme $x_1^k + ... + x_s^k = m$, alors $\forall i \in [|1, s|], x_i \leq \lfloor m^{1/k} \rfloor$. On en déduit que si $P \geq m^{1/k}$, on a $r'_P(m) = r(m)$*

Définissons ensuite la fonction T :

Définition. $\forall \alpha \in \mathbb{R}, T(\alpha) = \sum_{x=1}^{P} e(\alpha x^k)$

On montre ensuite le résultat obtenu par Vinogradov sur ces fonctions :

Proposition 1. $\forall \alpha \in \mathbb{R}, (T(\alpha))^s = \sum_{m \geq 0} e(\alpha m) r'_P(m)$,*ce qui implique :*

$$r'_P(M) = \int_0^1 (T(\alpha))^s e(-\alpha M) d\alpha$$

Démonstration. Montrons d'abord :

$$(\sum_{x=1}^{P} e(\alpha x^k))^s = \sum_{m \geq 0} e(\alpha m) r'_P(m)$$

On a :

$$\begin{aligned}(\sum_{x=1}^{P} e(\alpha x^k))^s &= (\sum_{x=1}^{P} e(\alpha)^{x^k})^s \\ &= \sum_{x_1,\dots x_s=1}^{P} (e(\alpha))^{x_1^k+\dots+x_s^k} \\ &= \sum_{m=0}^{\infty} e(\alpha)^m r'_P(m) \qquad \text{qui est le premier résultat.}\end{aligned}$$

Montrons ensuite le second résultat ; posons pour cela :

$$I = \int_0^1 (T(\alpha)^s e(-\alpha M) d\alpha\,)$$

$$I = \int_0^1 (\sum_{m \geq 0} e(\alpha m) r'_P(m)) e(-\alpha M) d\alpha$$

$$I = \sum_{m \geq 0} (r'_P(m) \int_0^1 e(\alpha m) e(-\alpha M) d\alpha\,)$$

$$I = r'_P(M) \qquad \text{car } \int_0^1 e(\alpha m) e(-\alpha M) d\alpha = \int_0^1 1 d\alpha = 1 \text{ si } m = M \text{ et } 0 \text{ sinon.}$$

□

On pose donc, pour toute la suite de l'étude, $P = \lfloor m^{1/k} \rfloor$ et, d'après la remarque ci-dessus, on a donc :

$$r(m) = \int_0^1 (T(\alpha)^s e(-\alpha m) d\alpha\,)$$

Chapitre 3

Les inégalités fondamentales

Ici, nous supposerons toujours $k \in \mathbb{N}^*$ fixé.

3.1 L'inégalité de Weyl

Ici, on pose : $f \in \mathbb{R}[x]$ qui s'écrit : $f(x) = \alpha x^k + \alpha_1 x^{k-1} + ... + \alpha_k$, et l'on suppose vraie l'existence d'un couple $(a, q) \in \mathbb{Z} \times \mathbb{N}^*$ vérifiant : $a \wedge q = 1$ et $|\frac{a}{q} - \alpha| \leq \frac{1}{q^2}$.

On a alors l'inégalité de Weyl, qui est la suivante :

Théorème. *Si l'on pose $K = 2^{k-1}$, alors on a l'inégalité :*

$$\forall \epsilon > 0, |\sum_{x=1}^{P} e(f(x))| \ll P^{1+\epsilon}(P^{-\frac{1}{K}} + q^{-\frac{1}{K}} + (\frac{P^k}{q})^{-\frac{1}{K}})$$

Pour prouver ce théorème, démontrons d'abord le résultat préliminaire suivant :

Proposition. *Soient $P_1, P_2 \in \mathbb{Z}$ tels que $0 \leq P_2 - P_1 \leq P$, et soit $S_k(f) = \sum_{x=P_1+1}^{P_2} e(f(x))$.*

$$\text{Alors : } |S_k(f)|^{2^\nu} \ll P^{2^\nu - 1} + P^{2^\nu - \nu - 1} \sum_{y_1=1}^{P} ... \sum_{y_\nu=1}^{P} |S_{k-\nu}(\Delta_{y_1,...y_\nu} f)|,$$
$$\text{où } (\Delta_y(f))(x) = f(x+y) - f(x).$$

Démonstration. On va procéder par récurrence sur ν. Étudions le cas de base $\nu = 1$:

$$\begin{aligned}
|S_k(f)|^2 &= S_k(f) \cdot \overline{S_k(f)} \\
&= (\sum_{x=P_1+1}^{P_2} e(f(x))) \cdot (\sum_{x=P_1+1}^{P_2} e(-f(x))) \\
&= \sum_{x_1,x_2=P_1+1}^{P_2} e(f(x_2) - f(x_1)) \\
&= \sum_{x=P_1+1}^{P_2} e(0) + \sum_{\substack{x_1,x_2=P_1+1 \\ x_1 \neq x_2}}^{P_2} e(f(x_2) - f(x_1)) \\
&= P_2 - P_1 + \sum_{P_1+1 \leq x_1 < x_2 \leq P_2} (e(f(x_2) - f(x_1)) + e(f(x_1) - f(x_2))) \\
&= P_2 - P_1 + 2 \cdot \Re(\sum_{P_1+1 \leq x_1 < x_2 \leq P_2} (e(f(x_2) - f(x_1)))) \\
&= P_2 - P_1 + 2 \cdot \Re(\sum_{y=1}^{P} \sum_{x} e((\Delta_y f)(x)))
\end{aligned}$$

en sommant x sur des intervalles dépendant de y mais restant inclus dans $[|P_1 + 1, P_2|]$.

Remarquons que $\Delta_y f$ est un polynôme de degré $k - 1$. En effet,

$$(\Delta_y f)(x) = f(x + y) - f(x) = \alpha(x + y)^k + ... + \alpha_k - \alpha x^k - ... - \alpha_k$$

et les termes en x^k s'éliminent.

On a alors :

$$\begin{aligned}
\Re(\sum_{x} e((\Delta_y f)(x))) &\leq |\sum_{x} e((\Delta_y f)(x))| \quad \text{(comparaison partie réelle - module d'un complexe)} \\
&\leq |S_{k-1}\Delta_y f|
\end{aligned}$$

Et, comme on a $P_2 - P_1 \leq P$, on obtient

$$|S_k(f)|^2 \leq P + 2\sum_{y=1}^{P} |S_{k-1}(\Delta_y f)|$$

Par conséquent :

$$|S_k(f)|^2 \ll P + \sum_{y=1}^{P} |S_{k-1}(\Delta_y f)| \ll P^{2^1-1} + P^{2^1-1-1} \sum_{y_1=1}^{P} |S_{k-1}(\Delta_{y_1} f)|$$

qui est l'inégalité recherchée pour $\nu = 1$.

Montrons maintenant l'hérédité de la récurrence. Supposons l'hypothèse de récurrence vraie au rang $\nu \leq k$.

On a :

$$|S_k(f)|^{2^\nu} \ll P^{2^\nu - 1} + P^{2^\nu - \nu - 1} \sum_{y_1=1}^{P} ... \sum_{y_\nu=1}^{P} |S_{k-\nu}(\Delta_{y_1,...y_\nu} f)|$$

On élève cette formule au carré :

$$|S_k(f)|^{2^\nu+1} \ll P^{2\cdot(2^\nu-1)} + P^{2(2^\nu-\nu-1)}(\sum_{y_1=1}^{P} ... \sum_{y_\nu=1}^{P} |S_{k-\nu}(\Delta_{y_1,...y_\nu} f)|)^2$$

En effet, on a « inclus »le double produit dans les deux termes carrés de la majoration en utilisant le fait qu'un produit de deux facteurs est majoré par la somme des carrés des deux facteurs.

Appliquons maintenant au carré des ν sommes emboîtées l'inégalité de Cauchy-Schwartz :

$$\begin{aligned}(\sum_{y_1=1}^{P} ... \sum_{y_\nu=1}^{P} |S_{k-\nu}(\Delta_{y_1,...y_\nu} f)| \cdot 1)^2 &\leq (\sum_{y_1=1}^{P} 1^2)(\sum_{y_1=1}^{P}(\sum_{y_2=1}^{P} ... \sum_{y_\nu=1}^{P} |S_{k-\nu}(\Delta_{y_1,...y_\nu} f)|)^2) \\ &\leq P(\sum_{y_1=1}^{P}(\sum_{y_2=1}^{P} ... \sum_{y_\nu=1}^{P} |S_{k-\nu}(\Delta_{y_1,...y_\nu} f)|)^2)\end{aligned}$$

On réitère sur chaque somme emboîtée, et l'on obtient :

$$(\sum_{y_1=1}^{P} ... \sum_{y_\nu=1}^{P} |S_{k-\nu}(\Delta_{y_1,...y_\nu} f)|)^2 \leq P^\nu \sum_{y_1=1}^{P} ... \sum_{y_\nu=1}^{P} |S_{k-\nu}(\Delta_{y_1,...y_\nu} f)|^2$$

Or, dans le cas de base, on a vu que :

$$|S_k(f)|^2 \leq P + 2\sum_{y=1}^{P} |S_{k-1}(\Delta_y f)|$$

donc :

$$|S_{k-\nu}(\Delta_{y_1,...y_\nu} f)|^2 \leq P + 2 \sum_{y_{\nu+1}=1}^{P} |S_{k-\nu-1}(\Delta_{y_1,...y_{\nu+1}} f)|$$

Et, en remplaçant dans le terme de droite, on trouve :

$$(\sum_{y_1=1}^{P} ... \sum_{y_\nu=1}^{P} |S_{k-\nu}(\Delta_{y_1,...y_\nu} f)|)^2 \leq P^\nu (P^{\nu+1} + 2 \sum_{y_1=1}^{P} ... \sum_{y_{\nu+1}=1}^{P} |S_{k-\nu-1}(\Delta_{y_1,...y_{\nu+1}} f)|)$$

Au final, on a :

$$\begin{aligned}|S_k(f)|^{2^{\nu}+1} &\ll P^{2^{\nu+1}-2} + P^{2^{\nu+1}-2\nu-2}(P^{2\nu+1} + 2P^{\nu}\sum_{y_1=1}^{P}...\sum_{y_{\nu+1}=1}^{P}|S_{k-\nu-1}(\Delta_{y_1,...y_{\nu+1}}f)|)\\ &\ll P^{2^{\nu+1}-2} + P^{2^{\nu+1}-1} + 2P^{2^{\nu+1}-\nu-2}\sum_{y_1=1}^{P}...\sum_{y_{\nu+1}=1}^{P}|S_{k-\nu-1}(\Delta_{y_1,...y_{\nu+1}}f)|\\ &\ll P^{2^{\nu+1}-1} + P^{2^{\nu+1}-(\nu+1)-1}\sum_{y_1=1}^{P}...\sum_{y_{\nu+1}=1}^{P}|S_{k-(\nu+1)}(\Delta_{y_1,...y_{\nu+1}}f)|\end{aligned}$$

Et l'on a la relation recherchée, ce qui termine la récurrence et prouve le résultat. □

Montrons maintenant un résultat général qui servira également dans la preuve :

Lemme. *Pour tout $m \in \mathbb{N}^*$, en notant $d(m)$ le nombre de diviseurs (pas nécessairement premiers) de m, on a : $\forall \epsilon > 0, d(m) \ll m^{\epsilon}$*

Démonstration. Écrivons la décomposition de m en facteurs premiers : $m = p_1^{\alpha_1}...p_n^{\alpha_n}$.
D'autre part, par récurrence immédiate, on montre : $d(m) = (\alpha_1 + 1)...(\alpha_n + 1)$.
On a donc :

$$\frac{d(m)}{m^{\epsilon}} = \prod_{i=1}^{n}\frac{\alpha_i + 1}{p_i^{\epsilon\alpha_i}}$$

Or, pour $x \geq 2^{\frac{1}{\epsilon}}$, on a

$$x^{\epsilon\alpha_i} \geq 2^{\alpha_i}$$

et donc

$$\frac{\alpha_i + 1}{x^{\epsilon\alpha_i}} \leq (\alpha_i + 1)2^{-\alpha_i} \leq 1$$

si $x \geq 1$. On obtient :

$$\forall p_i \geq 2^{\frac{1}{\epsilon}}, \frac{\alpha_i + 1}{p_i^{\epsilon\alpha_i}} \leq 1$$

On peut donc majorer le produit de départ par le produit des termes restants :

$$\frac{d(m)}{m^{\epsilon}} \leq \prod_{p_i \leq 2^{\frac{1}{\epsilon}}}\frac{\alpha_i + 1}{p_i^{\epsilon\alpha_i}} \leq \prod_{p_i \leq 2^{\frac{1}{\epsilon}}}\frac{\alpha_i + 1}{2^{\epsilon\alpha_i}}$$

car tout premier p vérifie $p \geq 2$. De plus, pour α quelconque, $2^{-\epsilon\alpha}(\alpha + 1)$ est borné par une constante dépendant de ϵ, notée C_{ϵ}. D'où : $\frac{d(m)}{m^{\epsilon}} \leq C_{\epsilon}$, autrement dit :

$$\forall \epsilon > 0, d(m) \ll m^{\epsilon}$$

□

À l'aide de ces résultats, nous pouvons commencer à démontrer l'inégalité de Weyl :

Démonstration. Appliquons la proposition à $\nu = k-1$:

$$|S_k(f)|^{2^{k-1}} \ll P^{2^{k-1}-1} + P^{2^{k-1}-k} \sum_{y_1=1}^{P} ... \sum_{y_{k-1}=1}^{P} |S_1(\Delta_{y_1,...y_{k-1}} f)|$$

où l'on somme un polynôme en x de degré 1. En effet, on a :

$$\begin{aligned}(\Delta_y f)(x) &= \alpha((x+y)^k - x^k) + ... + \alpha_{k-1}(x+y-x) + \alpha_k - \alpha_k \\ &= \alpha k y x^{k-1} + ... + \alpha y^k + ... + \alpha_{k-1} y\end{aligned}$$

On réitère $k-1$ fois, et l'on trouve :

$$(\Delta_{y_1,...y_{k-1}} f)(x) = \alpha k! y_1 ... y_{k-1} x + \beta \qquad \text{où } \beta \in \mathbb{Z} \text{ ne dépend pas de } x.$$

On peut simplifier :

$$\begin{aligned}|S_1(\Delta_{y_1,...y_{k-1}} f)| &= |\sum_x e(\alpha k! y_1 ... y_{k-1} x + \beta)| \\ &= |e(-\beta)||\sum_x e(\alpha k! y_1 ... y_{k-1} x)| \\ &= |\sum_x e(\alpha k! y_1 ... y_{k-1} x)|\end{aligned}$$

Or on a vu que x était sommé sur un intervalle $I \subset [|P_1+1, P_2|]$. Notons-le $I = [|x_1, x_2 - 1|]$, de longueur au plus P. On a alors, en posant $\lambda = \alpha k! y_1 ... y_{k-1}$, et en supposant $\lambda \notin \mathbb{Z}$,

$$\begin{aligned}|\sum_{x=x_1}^{x_2-1} e(\lambda x)| &= |e(\lambda x_1)||\sum_{x=0}^{x_2-x_1-1} (e(\lambda))^x| \\ &= |e(\lambda x_1)||\frac{e(\lambda)^{x_2-x_1}-1}{e(\lambda)-1}| && \text{(somme d'une série géométrique)} \\ &= |e(\lambda x_1)||\frac{e(\lambda\frac{x_2-x_1}{2})}{e(\frac{\lambda}{2})}||\frac{e(\lambda\frac{x_2-x_1}{2}) - e(-\lambda\frac{x_2-x_1}{2})}{e(\frac{\lambda}{2}) - e(-\frac{\lambda}{2})}| && \text{(angle moitié)} \\ &= |e(\lambda\frac{x_1+x_2-1}{2})||\frac{sin(\pi\lambda(x_2-x_1))}{sin(\pi\lambda)}| && \text{(formule exponentielle du sinus)}\end{aligned}$$

On en déduit :

$$|S_1(\Delta_{y_1,...y_{k-1}} f)| \ll \frac{1}{sin(\pi\lambda)}$$

Notons maintenant $\|\lambda\| = d(\lambda, \mathbb{Z}) = \min\{\lambda - \lfloor\lambda\rfloor, \lfloor\lambda+1\rfloor - \lambda\}$. Comme $\lambda \notin \mathbb{Z}$, on a $\|\lambda\| \in]0, \frac{1}{2}]$, et soit alors l tel que $\|\lambda\| = |\lambda - l|$. On notera qu'on a alors $l \in \{\lfloor\lambda\rfloor, \lfloor\lambda+1\rfloor\}$. Donc :

$$\begin{aligned}|sin(\pi\lambda)| &= |sin(\pi(\lambda-l) + \pi l)| \\ &= |sin(\pi(\lambda-l)| \gg |\lambda - l| && \text{car } |\lambda - l| \in]0, \frac{1}{2}]\end{aligned}$$

D'où le résultat :

$$|sin(\pi\lambda)| \gg \|\lambda\|$$

et donc :

$$\frac{1}{|sin(\pi\lambda)|} \ll \frac{1}{\|\lambda\|}$$

D'autre part, si $\lambda \in \mathbb{Z}$,

$$\sum_{x=x_1}^{x_2-1} e(\lambda x) = x_2 - x_1 \ll P$$

On injecte ce résultat dans l'expression suivante :

$$|S_1(\Delta_{y_1,...y_{k-1}} f)| \ll \min\{P, \frac{1}{\|\lambda\|}\}$$

Appliquons ce résultat à l'expression de départ :

$$|S_k(f)|^{2^{k-1}} \ll P^{2^{k-1}-1} + P^{2^{k-1}-k} \sum_{y_1=1}^{P} ... \sum_{y_{k-1}=1}^{P} \min\{P, \frac{1}{\|\lambda\|}\}$$

$$|S_k(f)|^{K} \ll P^{K-1} + P^{K-k} \sum_{y_1=1}^{P} ... \sum_{y_{k-1}=1}^{P} \min\{P, \frac{1}{\|\lambda\|}\}$$

On va ensuite regrouper les termes de ces sommes, en regroupant les $(k-1)$-uplets qui vérifient : $y_1...y_{k-1} = m$. D'après le lemme, on sait déjà que l'on a :

$$\forall \epsilon > 0, \#\{(y_1, ...y_{k-1}) \in [|1, P|]^{k-1} \mid y_1...y_{k-1} = m\} \ll m^{\epsilon}$$

car l'ensemble de tels $(k-1)$-uplets est inclus dans l'ensemble des diviseurs de m. A fortiori,

$$\forall \epsilon > 0, \forall m \in [|1, k!P^{k-1}|], \#\{(y_1, ...y_{k-1}) \in [|1, P|]^{k-1} \mid k!y_1...y_{k-1} = m\} \ll m^{\epsilon} \ll P^{\epsilon}$$

En appliquant ceci à la majoration précédente, on a :

$$\begin{aligned} |S_k(f)|^{K} &\ll P^{K-1} + P^{K-k} \sum_{m=1}^{k!P^{k-1}} P^{\epsilon} \min\{P, \frac{1}{\|\alpha m\|}\} \\ &\ll P^{K-1} + P^{K-k+\epsilon} \sum_{m=1}^{k!P^{k-1}} \min\{P, \frac{1}{\|\alpha m\|}\} \end{aligned}$$

Intéressons-nous à la somme restante dans le terme de droite. Rappelons l'hypothèse énoncée dans le théorème :

$$\exists (a, q) \in \mathbb{Z} \times \mathbb{N}^* \ tq \ a \wedge q = 1 \ et \ |\frac{a}{q} - \alpha| \leq \frac{1}{q^2}$$

Séparons alors la somme en plusieurs sommes de q termes consécutifs, i.e. des sommes de la forme suivante :

$$\sum_{m=0}^{q-1} \min\{P, \frac{1}{\|\alpha(m_1+m)\|}\}$$

Il y a $\lfloor \frac{k!P^{k-1}}{q} \rfloor + 1 \ll \frac{P^{k-1}}{q} + 1$ blocs de ce type (le dernier pouvant être incomplet). Simplifions l'intérieur de ces blocs :

$$\begin{aligned}\alpha(m_1+m) &= \alpha m_1 + \frac{am}{q} + (\alpha - \frac{a}{q})m \\ &= \alpha m_1 + \frac{am}{q} + O(\frac{1}{q}) \qquad \text{car } |\frac{a}{q} - \alpha| \leq \frac{1}{q^2} \text{ et } m \in [|0,q|].\end{aligned}$$

De plus, comme $a \wedge q = 1$ et que m parcourt $[|0, q-1|]$, alors $(am \mod q)$ parcourt $[|0, q-1|]$. Écrivons alors $r = (am \mod q)$. Notons que l'on peut éliminer les termes entiers de la norme, par définition de celle-ci. On a donc :

$$\sum_{m=0}^{q-1} \min\{P, \frac{1}{\|\alpha(m_1+m)\|}\} = \sum_{r=0}^{q-1} \min\{P, \frac{1}{\|\alpha m_1 + \frac{r}{q} + O(\frac{1}{q})\|}\}$$

En posant b comme l'entier le plus proche de $q\alpha m_1$, on a

$$|\frac{b}{q} - \alpha m_1| \leq \frac{1}{q}$$

et donc :

$$\sum_{m=0}^{q-1} \min\{P, \frac{1}{\|\alpha(m_1+m)\|}\} = \sum_{r=0}^{q-1} \min\{P, \frac{1}{\|\frac{r+b}{q} + O(\frac{1}{q})\|}\}$$

Notons maintenant :

$$\|\frac{r+b}{q} + O(\frac{1}{q})\| = \|\frac{s}{q} + \gamma\|$$

où $\gamma = O(\frac{1}{q})$, i.e. : $\exists C > 0 \ tq \ |\gamma| \leq \frac{C}{q}$, et en supposant $s \in [|-\frac{q}{2}+1, \frac{q}{2}|]$.

Alors, si $|s| \geq 2C$,

$$\|\frac{s}{q} + \gamma\| \geq \frac{1}{2}|\frac{s}{q}| \tag{1}$$

En effet : supposons $s > 0$ (la démonstration pour $s \leq 0$ est similaire. Alors :

$$|\gamma| \leq \frac{s}{2} \ et \ \frac{s}{2q} \leq \frac{s}{q} + |\gamma| \leq \frac{3}{2}\frac{s}{q}$$

On note que

$$0 \leq \frac{s}{q} \leq \frac{1}{2} \ \ et \ \ \frac{s}{2q} \leq \frac{s}{q} + \gamma \leq \frac{3}{4}$$

En particulier,

$$\|\frac{s}{q} + \gamma\| \geq \min\{\frac{1}{4}, \frac{s}{2q}\}$$

Mais $\frac{s}{2q} \leq \frac{1}{4}$ donc on a démontré (1).

On a donc :

Si $|s| < 2C$, on majore le terme de la somme de droite par P.

Si $|s| \geq 2C$, on le majore par $\frac{2q}{|s|}$.

Et comme il y a $O(1)$ valeurs de s pour lesquelles $s \geq 2C$, on a :

$$\sum_{m=0}^{q-1} \min\{P, \frac{1}{\|\alpha(m_1+m)\|}\} \ll (4C+1)P + 2\sum_{|s|\geq 2C} \frac{q}{|s|}$$
$$\ll P + \sum_{s=1}^{\frac{q}{2}} \frac{q}{s} \ll P + q\log q$$

Remplaçons dans l'expression globale :

$$|S_k(f)|^K \ll P^{K-1} + P^{K-k+\epsilon}(\frac{P^{k-1}}{q} + 1)(P + q\log q)$$

Remarquons que si $q > P^k$, l'inégalité de Weyl est triviale. En effet, on a alors :

$$\frac{P^k}{q} < 1$$

Et donc :

$$(\frac{P^k}{q})^{-\frac{1}{K}} > 1$$
$$P^{1+\epsilon}(P^{-\frac{1}{K}} + q^{-\frac{1}{K}} + (\frac{P^k}{q})^{-\frac{1}{K}}) > P^{1+\epsilon} > P > |S_k(f)|$$

Supposons donc $q \leq P^k$, ce qui nous permet d'écrire :

$$\log q \ll P^\epsilon$$

Développons alors :

$$|S_k(f)|^K \ll P^{K-1} + P^{K-k+\epsilon}(\frac{P^{k-1}}{q} + 1)(P+q)$$
$$\ll P^{K-1} + (\frac{P^{K-1+\epsilon}}{q} + P^{K-k+\epsilon})(P+q)$$
$$\ll P^{K+\epsilon}(P^{-1} + (\frac{P^{-1}}{q} + P^{-k})(P+q))$$
$$\ll P^{K+\epsilon}(P^{-1} + \frac{1}{q} + qP^{-k})$$

On en tire le résultat final :

$$|S_k(f)| \ll P^{1+\epsilon}(P^{-\frac{1}{K}} + q^{-\frac{1}{K}} + (\frac{P^k}{q})^{-\frac{1}{K}})$$

Et l'on remarque qu'en prenant $P_2 = P$ et $P_1 = 0$ il s'agit exactement de la majoration énoncée.

□

3.2 L'inégalité de Hua

Abordons maintenant l'inégalité de Hua, qui est liée à la fonction T de Vinogradov, dont nous rappelons la définition :

Définition. $\forall \alpha \in \mathbb{R}, T(\alpha) = \sum_{x=1}^{P} e(\alpha x^k)$

Voici l'inégalité que nous allons démontrer :

Théorème. $\forall \epsilon > 0, \int_0^1 |T(\alpha)|^{2^k} d\alpha \ll P^{2^k - k + \epsilon}$

Démonstration. Posons

$$I_\nu = \int_0^1 |T(\alpha)|^{2^\nu} d\alpha$$

et montrons l'inégalité de Hua par récurrence sur ν, où $\nu \in [|0, k|]$:

$$\forall \epsilon > 0, I_\nu \ll P^{2^k - k + \epsilon}$$

Montrons d'abord le cas de base, à savoir $\nu = 1$:

$$\begin{aligned}
I_1 &= \int_0^1 |T(\alpha)|^2 d\alpha \\
I_1 &= \int_0^1 (\sum_{x=1}^{P} e(\alpha x^k)) * (\sum_{x=1}^{P} e(-\alpha x^k)) d\alpha \\
I_1 &= \int_0^1 \sum_{x_1, x_2 = 1}^{P} e(\alpha(x_1^k - x_2^k)) d\alpha \\
I_1 &= \int_0^1 (\sum_{\substack{x_1, x_2 = 1 \\ x_1 \neq x_2}}^{P} e(\alpha(x_1^k - x_2^k)) + \sum_{x=1}^{P} 1) d\alpha \\
I_1 &= \sum_{x=1}^{P} (\int_0^1 1 d\alpha) + \sum_{\substack{x_1, x_2 = 1 \\ x_1 \neq x_2}}^{P} (\int_0^1 e(\alpha(x_1^k - x_2^k)) d\alpha)
\end{aligned}$$

Or, si $x_1 \neq x_2$, on a, comme vu au chapitre 1 :

$$\int_0^1 e(\alpha(x_1^k - x_2^k)) d\alpha = 0$$

On a donc :

$$I_1 = P \ll P^{1+\epsilon}$$

ce qui conclut le cas de base. Supposons maintenant l'inégalité vraie au rang $\nu \leq k-1$.
Appliquons la proposition de la section précédente en prenant $S_k(f) = T(\alpha)$, i.e. $f(x) = \alpha x^k$:

$$\begin{aligned}|T(\alpha)|^{2^\nu} = |\sum_{x=1}^{P} e(f(x))|^{2^\nu} &\ll P^{2^\nu-1} + P^{2^\nu-\nu-1} \sum_{y_1=1}^{P} ... \sum_{y_\nu=1}^{P} \sum_{x} \Re(e(\alpha \Delta_{y_1,...y_\nu} x^k)) \\ &\ll P^{2^\nu-1} + P^{2^\nu-\nu-1} \Re(\sum_{y_1=1}^{P} ... \sum_{y_\nu=1}^{P} (S_{k-\nu}(\Delta_{y_1,...y_\nu} f)))\end{aligned}$$

On observera qu'il s'agit en fait de la version « forte »de la proposition, énoncée au cours de la preuve de celle-ci, le résultat final étant similaire, à l'exception de la partie réelle qui est majorée par le module.
Multiplions de part et d'autre de la majoration par $|T(\alpha)|^{2^\nu}$:

$$|T(\alpha)|^{2^{\nu+1}} \ll |T(\alpha)|^{2^\nu} P^{2^\nu-1} + |T(\alpha)|^{2^\nu} P^{2^\nu-\nu-1} \Re(\sum_{y_1=1}^{P} ... \sum_{y_\nu=1}^{P} (S_{k-\nu}(\Delta_{y_1,...y_\nu} f)))$$

Puis intégrons de 0 à 1 par rapport à α :

$$I_{\nu+1} \ll I_\nu P^{2^\nu-1} + P^{2^\nu-\nu-1} \sum_{y_1,...,y_\nu} \Re(\int_0^1 |T(\alpha)|^{2^\nu} S_{k-\nu}(\Delta_{y_1,...y_\nu} f) d\alpha\,)$$

Précisons la dernière intégrale, en développant son intégrande :

$$\begin{aligned}|T(\alpha)|^{2^\nu} S_{k-\nu}(\Delta_{y_1,...y_\nu} f) =& |T(\alpha)|^2 ... |T(\alpha)|^2 \cdot \sum_x e(\alpha \Delta_{y_1,...,y_\nu}(x^k)) \\ =& (\sum_{u_1=1}^{P} e(\alpha u_1^k))(\sum_{v_1=1}^{P} e(-\alpha v_1^k)) ... (\sum_{u_{2^{\nu-1}}=1}^{P} e(\alpha u_{2^{\nu-1}}^k))(\sum_{v_{2^{\nu-1}}=1}^{P} e(-\alpha v_{2^{\nu-1}}^k)) \\ & \times \sum_x e(\alpha \Delta_{y_1,...,y_\nu}(x^k)) \\ =& \sum_x \sum_{\substack{u_1,...,u_{2^{\nu-1}}=1 \\ v_1,...v_{2^{\nu-1}}=1}}^{P} e(\alpha(\Delta_{y_1,...,y_\nu}(x^k) + u_1^k + ... + u_{2^{\nu-1}}^k - v_1^k - ... - v_{2^{\nu-1}}^k))\end{aligned}$$

L'intégrale s'écrit donc ainsi :

$$\begin{aligned}&\int_0^1 |T(\alpha)|^{2^\nu} S_{k-\nu}(\Delta_{y_1,...y_\nu} f) d\alpha = \\ &\qquad \sum_x \sum_{\substack{u_1,...,u_{2^{\nu-1}}=1 \\ v_1,...v_{2^{\nu-1}}=1}}^{P} \int_0^1 e(\alpha(\Delta_{y_1,...,y_\nu}(x^k) + u_1^k + ... + u_{2^{\nu-1}}^k - v_1^k - ... - v_{2^{\nu-1}}^k)) d\alpha\end{aligned}$$

L'intégrale est donc égale au nombre de solutions de l'équation :

$$\Delta_{y_1,...,y_\nu}(x^k) + u_1^k + ... + u_{2^{\nu-1}}^k - v_1^k - ... - v_{2^{\nu-1}}^k = 0$$

où $y_i \in [|1, P|]$, $u_i \in [|1, P|]$, $v_i \in [|1, P|]$, $x \in [|1, P|]$. Notons le nombre de ces solutions N. On obtient alors :

$$I_{\nu+1} \ll P^{2^\nu - 1} I_\nu + P^{2^\nu - \nu - 1} N$$

On va majorer N, en remarquant que $\Delta_{y_1,...,y_\nu}(x^k)$ est strictement positif et est divisible par $y_1, ...y_\nu$. En fixant certains $u_1, ...u_{2^{\nu-1}}, v_1, ...v_{2^{\nu-1}}$, comme chacun de ces nombres est dans $[|1, P|]$, en application du lemme sur les diviseurs, on obtient que $\Delta_{y_1,...,y_\nu}(x^k)$ peut avoir un nombre $2^{\nu-1}P^k \ll P^\epsilon$ de valeurs, pour tout $\epsilon > 0$.

En effet, une fois les y_i fixés, x ne peut avoir qu'une seule valeur, car $\Delta_{y_1,...,y_\nu}(x^k)$ est strictement croissante en x.

On remarque enfin que chaque u_i peut prendre P valeurs, et qu'il y en a $2^{\nu-1}$; de même pour chaque v_i. On a donc $P^{2^{\nu-1}} \cdot P^{2^{\nu-1}} = P^{2^\nu}$ choix pour $(u_1, ..., u_{2^{\nu-1}}, v_1, ..., v_{2^{\nu-1}})$.

On obtient :

$$\forall \epsilon > 0, N \ll P^{2^\nu} \cdot P^\epsilon \cdot 1 = P^{2^\nu + \epsilon}$$

d'où :

$$I_{\nu+1} \ll P^{2^\nu} \cdot I_\nu + P^{2^\nu - \nu - 1} \cdot P^{2^\nu + \epsilon} I_{\nu+1} \ll P^{2^{\nu+1} - \nu + \epsilon} + P^{2^{\nu+1} - (\nu+1) + \epsilon}$$

Et l'on conclut :

$$I_{\nu+1} \ll P^{2^{\nu+1} - (\nu+1) + \epsilon}$$

Cela termine la récurrence, et démontre l'inégalité de Hua. □

Chapitre 4

Arcs mineurs, Arcs majeurs

Dans toute cette partie, la variable N correspondra au m de la section 2.3, et $P = \lfloor N^{\frac{1}{k}} \rfloor + 1$.

On va commencer par faire les hypothèses suivantes : $s \geq 2^k + 1$ et on suppose vraie l'existence de I sous-ensemble mesurable de $[0;1]$ tel que :

$$\exists \delta > 0, \qquad \forall \alpha \in I, \qquad |T(\alpha)| << P^{1-\delta}$$

Alors on trouve :

$$\begin{aligned} \forall \epsilon > 0, \int_I |T(\alpha)|^s d\alpha &= \int_I |T(\alpha)|^{s-2^k} \cdot |T(\alpha)|^{2^k} d\alpha \\ &\ll (P^{1-\delta})^{s-2^k} \cdot P^{2^k-k+\epsilon} \qquad \text{(inégalité de Hua)} \\ &\ll P^{s-k+(\epsilon-\delta(s-2^k))} \\ &\ll P^{s-k+\epsilon-\delta} \end{aligned}$$

Donc en particulier, si on prend ϵ assez petit, on obtient :

$$\exists \mu > 0, \int_I |T(\alpha)|^s d\alpha \ll P^{s-k-\mu} = o(P^{s-k})$$

On utilisera cette majoration afin de montrer que la contribution des arcs mineurs dans la formule asymptotique est négligeable.

4.1 Les arcs mineurs

Lemme. *(Théorème d'approximation diophantienne de Dirichlet). Soient θ et $Q \in \mathbb{R}_+^*$. On a la propriété suivante :*

$$\exists q \in \mathbb{N}^* \text{ tel que } 0<q<Q \text{ et } d(q\theta, \mathbb{Z}) \leq \frac{1}{Q}$$

Démonstration. Supposons Q entier naturel non nul et soit n tel que $0 \leq n < Q$.

Dans un premier temps, signalons que si θ est rationnel de la forme $\theta = \frac{a}{b}$ avec $0 < b \leq Q$, alors le résultat est immédiat, car dans ce cas on pose $q = b$ et on a $d(q\theta, \mathbb{Z}) = 0$. Supposons donc que θ n'est pas de cette forme.

On considère alors l'ensemble $E = \{n\theta \mod 1\} \subset \mathbb{R}/\mathbb{Z}$.
$\#(E) = Q$ et, d'après le principe des tiroirs, il est clair que :

$$\exists m, n \text{ tel que } 0 \leq m < n < Q \text{ et } n\theta - m\theta \in [-\frac{1}{Q}; \frac{1}{Q}] \mod 1$$

Ainsi,

$$\exists p \in \mathbb{Z} \text{ tel que } |(n-m)\theta - p| \leq \frac{1}{Q}$$

On pose $q = n - m$, ce qui achève la démonstration pour Q entier. Si Q n'est pas entier, il suffit d'appliquer ce qui précède à $E(Q) + 1$ □

On va maintenant fixer q tel que $1 \leq q \leq P^\delta$ et a tel que $1 \leq a \leq q$ avec $a \wedge q = 1$. On note

$$m_{a,q} = \left\{ \alpha \in [0,1] \text{ tel que } |\alpha - \frac{a}{q}| < P^{-k+\delta} \right\}$$

Définition. *On définit l'ensemble des arcs majeurs noté $\mathfrak{M}$ par :*

$$\mathfrak{M} = \bigcup_{\substack{q \leq P^\delta \\ 0 \leq a \leq q}} m_{a,q}$$

Définition. *On définit l'ensemble des arcs mineurs, noté $\mathfrak{m}$, comme le complémentaire des arcs majeurs sur $[0,1]$:*

$$\mathfrak{m} = \complement_{[0,1]}(\mathfrak{M})$$

Lemme. *On a*

$$\forall \alpha \in [0;1] \quad \exists (a,q) \in \mathbb{Z} \times \mathbb{N}^* \text{tel que } a \wedge q = 1, 1 \leq q \leq P^{k-\delta} \text{ et } |\alpha - \frac{a}{q}| < \frac{1}{q.P^{k-\delta}}$$

Démonstration. On applique le théorème de Dirichlet pour $0 < q < P^{k-\delta} + 1$. Alors on a :

$$\exists q \in [|1; P^{k-\delta}|] \text{ tel que } d(q\alpha, \mathbb{Z}) < \frac{1}{P^{k-\delta}} \iff |q\alpha - a| < \frac{1}{P^{k-\delta}}$$
$$\iff |\alpha - \frac{a}{q}| < \frac{1}{q}.\frac{1}{P^{k-\delta}}$$

□

Proposition. *Si $s \geq 2^k + 1$, alors*

$$\int_{\mathfrak{m}} |T(\alpha)|^s d\alpha \ll P^{s-k-\delta'}$$

pour un certain $\delta' > 0$.

Démonstration. On a par le lemme précédent :

$$\forall \alpha \in [0;1] \;\; \exists (a,q) \in \mathbb{Z} \times \mathbb{N}^* \text{tel que } a \wedge q = 1,\; 1 \leq q \leq P^{k-\delta} \text{ et } |\alpha - \frac{a}{q}| < \frac{1}{q.P^{k-\delta}}$$

Si $\alpha \in \mathfrak{m}$, on a forcément $q > P^\delta$ et donc :

$$|\alpha - \frac{a}{q}| < \frac{1}{q.P^{k-\delta}} \leq \frac{1}{q^2}$$

On peut donc appliquer l'inégalité de Weyl ce qui nous donne :

$$\forall \epsilon > 0 \; |T(\alpha)| \ll P^{1+\epsilon} \left(P^{-\frac{1}{K}} + q^{-\frac{1}{K}} + \left(\frac{P^k}{q}\right)^{-\frac{1}{K}} \right).$$

Comme on a $\frac{P^k}{q} \geq P^\delta$ et $\frac{1}{q} \leq P^{-\delta}$ avec δ petit, on néglige alors $q^{-\frac{1}{K}}$, et on en déduit que :

$$\forall \epsilon > 0 \; |T(\alpha)| \ll P^{1+\epsilon-\frac{\delta}{K}}$$

et avec ϵ assez petit, on peut appliquer le calcul vu en début de partie. L'intégrale de $T(\alpha)^s$ sur les arcs mineurs sera donc négligeable. □

4.2 Les arcs majeurs

Lemme. *Si f est une fonction dérivable sur un ouvert de $\mathbb{R}$ contenant l'intervalle $[A;B]$, on a :*

$$\left| \int_A^B f(\nu)d\nu - \sum_{A<y\leq B} f(y) \right| \ll \max|f(\nu)| + (B-A) \cdot \max|f'(\nu)|$$

où les max *sont pris sur $[A;B]$ et la somme se fait sur les entiers compris dans $]A;B]$*

Démonstration. Notons y_1,y_2,...,y_n les entiers compris dans $]A;B]$ (que l'on peut supposer rangés par ordre croissant). Alors on a :

$$\begin{aligned}
\left|\int_A^B f(\nu)d\nu - \sum_{A<y\leq B} f(y)\right| &= \left|\int_A^{y_1} f(\nu)d\nu + \sum_{i=1}^{n-1}\int_{y_i}^{y_{i+1}} (f(\nu)-f(y_i))d\nu + \int_{y_n}^{B} f(\nu)d\nu - f(y_n)\right| \\
&\leq \left|\int_A^{y_1} f(\nu)d\nu\right| + \left|\int_{y_n}^{B} f(\nu)d\nu\right| + |f(y_n)| + \sum_{i=1}^{n-1}\int_{y_i}^{y_{i+1}} ||f'||_\infty(\nu-y_i)d\nu \\
&\leq 3||f||_\infty + \sum_{i=1}^{n-1}\int_{y_i}^{y_{i+1}} ||f'||_\infty(\nu-y_i)d\nu \\
&\leq 3||f||_\infty + \sum_{i=1}^{n-1} ||f'||_\infty \times \frac{1}{2} \\
&\leq 3||f||_\infty + \frac{1}{2}(B-A)||f'||_\infty \\
&\leq 3(||f||_\infty + (B-A)||f'||_\infty)
\end{aligned}$$

Ceci achève la démonstration.

□

Proposition. *Soit $\alpha \in m_{a,q}$. Alors on a : $\alpha = \beta + \frac{a}{q}$ où $|\beta| < P^{\delta-k}$*

$$T(\alpha) = \frac{1}{q}\cdot S_{a,q}.I(\beta) + O(P^{2\delta})$$

où

$$S_{a,q} = \sum_{z=1}^{q} e\left(a\frac{z^k}{q}\right) \quad et \quad I(\beta) = \int_0^P e(\beta\xi^k)d\xi$$

et T est la fonction définie dans la section variante de Vinogradov.

Démonstration. Par définition :

$$T(\alpha) = \sum_{x=1}^{P} e(\alpha\cdot x^k) = \sum_{x=1}^{P} e\left(\left(\beta+\frac{a}{q}\right)x^k\right)$$

Posons $x = qy + z$ où y et z sont entiers.

$$\begin{aligned}
T(\alpha) &= \sum_{\substack{y,z \\ 1\leq z\leq q}} e((\beta+\frac{a}{q})(qy+z)^k) \\
&= \sum_{\substack{y,z \\ 1\leq z\leq q}} e(\beta(qy+z)^k)e(\frac{a}{q}(qy+z)^k)
\end{aligned}$$

Remarquons que :

$$e(\frac{a}{q}(qy+z)^k) = e(\frac{a}{q}(z^k+R))$$

où les termes de R ont un q en facteur. Donc :

$$e(\frac{a}{q}(qy+z)^k) = e(a\frac{z^k}{q})$$

On obtient ainsi :

$$T(\alpha) = \sum_{z=1}^{q}\left[e\left(a\frac{z^k}{q}\right)\cdot\sum_y e(\beta(qy+z)^k)\right]$$

On va maintenant chercher à exprimer $\sum_y e(\beta(qy+z)^k)$ en fonction de $I(\beta)$. On va utiliser le lemme démontré en début de section sur la fonction $f(\eta) = e(\beta(q\eta+z)^k)$ en considérant l'intégrale entre 0 et P. On a également les inégalités suivantes :

$$\max|f'| \leq q|\beta|P^{k-1} \quad ; \quad B-A \ll \frac{P}{q} \quad ; \quad \max|f| \leq 1$$

Par le lemme, on obtient :

$$\begin{aligned}\left|\sum_y e(\beta(q\eta+z)^k) - \frac{1}{q}\cdot\int_0^P e(\beta\xi^k)d\xi\right| &\ll \frac{P}{q}\cdot q|\beta|P^{k-1}+1\\ &\ll |\beta|P^k\\ &\ll P^\delta\end{aligned}$$

Puis, en observant que $S_{a,q} = O(q) = O(P^\delta)$ car α est un arc majeur, on a bien :

$$T(\alpha) = \frac{1}{q}\cdot S_{a,q}\cdot I(\beta) + O(P^{2\delta})$$

□

On rappelle que $P = \lfloor N^{\frac{1}{k}}\rfloor + 1$.

Proposition. *Si $\mathfrak{M}$ représente l'ensemble des arcs majeurs, on a*

$$\int_{\mathfrak{M}}(T(\alpha))^s.e(-N\alpha)d\alpha = P^{s-k}.\mathfrak{S}(P^\delta,N).J(P^\delta) + O(P^{s-k-\delta'})$$

et ce pour un certain $\delta' > 0$ et avec

$$\mathfrak{S}(P^\delta,N) = \sum_{\substack{q\leq P^\delta\\(a,q)=1}}\sum_{a=1}^{q}\left(\frac{S_{a,q}}{q}\right)^s e\left(-N\frac{a}{q}\right) \quad et \quad J(P^\delta) = \int_{|\gamma|<P^\delta}\left(\int_0^1 e(\gamma\xi^k)d\xi\right)^s e(-\gamma)d\gamma$$

Démonstration. On a facilement

$$|q^{-1}S_{a,q}I(\beta)| \leq P$$

donc

$$(T(\alpha))^s = (q^{-1}S_{a,q}I(\beta))^s + O(P^{s-1+2\delta})$$

On multiplie chaque membre par $e(-N\alpha)$ et on intègre sur les arcs majeurs c'est à dire sur les $|\beta| < P^{\delta-k}$ pour le membre de droite. On obtient :

$$\int\limits_{m_{a,q}} (T(\alpha))^s e(-N\alpha)d\alpha = (q^{-1}S_{a,q})^s e\left(-N\frac{a}{q}\right) \int\limits_{|\beta|<P^{\delta-k}} (I(\beta))^s e(-N\beta)d\beta + O(P^{s-k-1+3\delta})$$

Les intégrandes ne dépendant pas de a et q, on peut sommer facilement ; on obtient donc :

$$\int\limits_{\mathfrak{M}} (T(\alpha))^s e(-N\alpha)d\alpha = \mathfrak{S}(P^\delta, N) \int\limits_{|\beta|<P^{\delta-k}} (I(\beta))^s e(-N\beta)d\beta + O(P^{s-k-1+3\delta})$$

Par définition de N et P, on observe que $P = \lfloor N^{\frac{1}{k}} \rfloor + 1$ donc $N - P^k \ll P^{k-1}$.

$$|e(-\beta N) - e(-\beta P^k)| \ll |\beta| P^{k-1} \ll P^{\delta-k}P^{k-1} \ll P^{\delta-1}$$

Comme $|q^{-1}S_{a,q}| \leq 1$, alors $\mathfrak{S}(P^\delta, N) \leq P^{2\delta}$ (le nombre de termes dans la double somme est majoré par $P^{2\delta}$)

On a également : $|I(\beta)|^s \leq P^s$

En remplaçant dans l'intégrale du membre de droite N par P^k, on commet donc une erreur négligeable. En fait, avec les estimations de $|I(\beta)|^s \leq P^s$ et de $\mathfrak{S}(P^\delta, N)$, l'erreur générale commise dans l'intégrale est de l'ordre de $P^{2\delta} \cdot P^s \cdot P^{-k+\delta} \cdot P^{-1+\delta}$ i.e de l'ordre de $P^{s-k-1+4\delta}$. Cela donne donc une erreur négligeable.

On a donc le droit d'écrire :

$$\int\limits_{|\beta|<P^{\delta-k}} (I(\beta))^s e(-N\beta)d\beta + O(P^{s-k-1+3\delta}) = \int\limits_{|\beta|<P^{-k+\delta}} \left(\int\limits_0^P e(\beta\xi^k)d\xi\right)^s e(-P^k\beta)d\beta + O(P^{s-k-1+4\delta})$$

Il reste à poser $\xi = P\xi'$ et $\beta = P^{-k}\gamma$, et l'on obtient

$$\int\limits_{|\beta|<P^{-k+\delta}} \left(\int\limits_0^P e(\beta\xi^k)d\xi\right)^s e(-P^k\beta)d\beta = P^{s-k}J(P^\delta).$$

Comme δ est petit et $\delta' = 1 - \delta > 0$, on peut bien mettre le résultat sous la forme

$$\int\limits_{\mathfrak{M}} (T(\alpha))^s e(-N\alpha)d\alpha = P^{s-k} \cdot \mathfrak{S}(P^\delta, N) \cdot J(P^\delta) + O(P^{s-k-\delta'})$$

□

Lemme. *Soit Γ la fonction définie par*

$$\Gamma(u) = \int_0^\infty x^{u-1}e^{-x}dx$$

Si ϕ est définie par

$$\phi(u) = \int_0^1 ... \int_0^1 (\zeta_1...\zeta_{s-1}(u - \zeta_1 - ... - \zeta_{s-1}))^{-1+\frac{1}{k}} \, d\zeta_1...d\zeta_{s-1}$$

avec le domaine d'intégration rectifié de manière à ce que $u - 1 < \zeta_1 + ... + \zeta_{s-1} < u$, alors on a la formule suivante :

$$\phi(1) = \frac{\Gamma(\frac{1}{k})^s}{\Gamma(\frac{s}{k})}$$

Démonstration. Ce lemme sera admis mais une démonstration peut être trouvée dans [2] (p 258)

□

Théorème. *On pose*

$$\mathfrak{S}(N) = \sum_{q=1}^{+\infty} \sum_{\substack{a\in[|1;q|] \\ a\wedge q=1}} (q^{-1}S_{a,q})^s e(-N\frac{a}{q})$$

et

$$C_{k,s} = \frac{\Gamma(1+\frac{1}{k})^s}{\Gamma(\frac{s}{k})}$$

Alors, si $s \geq 2^k + 1$, on a :

$$r(N) = C_{k,s}N^{\frac{s}{k}-1}\mathfrak{S}(N) + O(N^{\frac{s}{k}-1-\delta'}) \qquad \text{avec } \delta' > 0$$

Démonstration. On a (par le lemme précédent et la dernière proposition de la section 4.1) :

$$r(N) = \int_{\mathfrak{M}} (T(\alpha))^s e(-N\alpha)d\alpha + \int_{\mathfrak{m}} (T(\alpha))^s e(-N\alpha)d\alpha$$

$$r(N) = P^{s-k}\mathfrak{S}(P^\delta, N)J(P^\delta) + O(P^{s-k-\delta'})$$

On a :

$$J(P^\delta) = \int_{|\gamma|<P^\delta} \left(\int_0^1 e(\gamma\xi^k)d\xi \right)^s e(-\gamma)d\gamma$$

puis en posant le changement de variable $\zeta = \xi^k$, on obtient :

$$\int_0^1 e(\gamma\xi^k)d\xi = \frac{1}{k}\int_0^1 e(\gamma\zeta)\zeta^{-1+\frac{1}{k}}d\zeta = k^{-1}\gamma^{-\frac{1}{k}}\int_0^\gamma \zeta^{-1+\frac{1}{k}}e(\zeta)d\zeta$$

La fonction $\zeta \longmapsto e(\zeta)$ est bornée (son module est majoré par 1) et $\zeta \longmapsto \zeta^{-1+\frac{1}{k}}$ est une fonction qui décroît vers 0. Donc par le théorème d'Abel-Dirichlet, l'intégrale du membre de droite est convergente si $\gamma \to +\infty$. Il vient :

$$\left|\int_0^1 e(\gamma\xi^k)d\xi\right| \ll |\gamma|^{-\frac{1}{k}}$$

Notons

$$J = k^{-s}\int_{-\infty}^{+\infty}\left(\int_0^1 \zeta^{-1+\frac{1}{k}}e(\gamma\zeta)d\zeta\right)^s e(-\gamma)d\gamma$$

L'intégrale intérieure de J est en $O(\gamma^{-\frac{s}{k}})$, on peut également remarquer que

$$\left|\int_{\gamma\geq P^\delta}\gamma^{-\frac{s}{k}}d\gamma\right| \leq (P^\delta)^{-\frac{s}{k}+1}$$

On a donc :

$$J(P^\delta) = J + O(P^{-(\frac{s}{k}-1)})$$

Sans commettre d'erreur trop grande, on peut donc remplacer $J(P^\delta)$ par J et P par $N^{\frac{1}{k}}$.

Il ne reste donc plus qu'à remplacer $\mathfrak{S}(P^\delta, N)$ par $(N) = \mathfrak{S}(P^\delta, N)$ pour $\delta \to \infty$ (sous réserve de montrer la convergence de cette série, ce que l'on fera en fin de section).

On va maintenant montrer que $J = C_{k,s}$:

Il est facile de voir que :

$$\int_{-\lambda}^{\lambda} e(\mu\gamma)d\gamma = \frac{sin(2\pi\lambda\mu)}{\pi\mu}$$

On obtient alors :

$$\begin{aligned}
k^s J &= \int_{-\infty}^{+\infty}\left(\int_0^1 \zeta^{-1+\frac{1}{k}}e(\zeta)d\zeta\right)^s e(-\gamma)d\gamma \\
&= \lim_{\lambda\to\infty}\int_0^1 ...\int_0^1\int_{-\lambda}^{\lambda}(\zeta_1...\zeta_s)^{-1+\frac{1}{k}}e(\gamma(\zeta_1+...+\zeta_s-1))d\gamma d\zeta_1...d\zeta_s \\
&= \lim_{\lambda\to\infty}\int_0^1 ...\int_0^1 (\zeta_1...\zeta_s)^{-1+\frac{1}{k}}\frac{sin(2\pi\lambda(\zeta_1+...+\zeta_s-1))}{\pi(\zeta_1+...+\zeta_s-1)}d\zeta_1...d\zeta_s \\
&= \lim_{\lambda\to\infty}\int_0^s \phi(u)\frac{sin(2\pi\lambda(u-1))}{\pi(u-1)}du
\end{aligned}$$

où l'on a posé : u est la somme des ζ_i, et :

$$\phi(u) = \int_0^1 ... \int_0^1 (\zeta_1 ... \zeta_{s-1}(u - \zeta_1 - ... - \zeta_{s-1}))^{-1+\frac{1}{k}} \, d\zeta_1 ... d\zeta_{s-1}$$

Ici, le domaine d'intégration est tel que $u - 1 < \zeta_1 + \cdots + \zeta_{s-1} < u$.

Nous allons maintenant utiliser le théorème intégral de Fourier sur un intervalle fini qui nous assure (sous certaines hypothèses) que

$$\lim_{\lambda \to \infty} \int_A^B \phi(u) \frac{sin 2\pi\lambda(u - C)}{\pi(u - C)} du = \phi(C)$$

sous condition que $A < C < B$. Si on admet que ce théorème est applicable (l'énoncé précis et la démonstration de ce théorème est dans [2] 9.43), on en déduit que :

$$k^s J = \phi(1) = \int_0^1 ... \int_0^1 (\zeta_1 ... \zeta_{s-1}(1 - \zeta_1 - ... - \zeta_{s-1}))^{-1+\frac{1}{k}} \, d\zeta_1 ... d\zeta_{s-1}.$$

où le domaine d'intégration est tel que : $0 < \zeta_1 + \cdots + \zeta_{s-1} < 1$

Par le lemme précédent, on obtient :

$$\phi(1) = \frac{\Gamma(\frac{1}{k})^s}{\Gamma(\frac{s}{k})}$$

Par intégration par parties, il est facile de voir que :

$$\frac{1}{k}\Gamma(\frac{1}{k}) = \Gamma(1 + \frac{1}{k})$$

Ainsi, on obtient

$$J = \frac{\left(\Gamma(1 + \frac{1}{k})\right)^s}{\Gamma(\frac{s}{k})} = C_{k,s}$$

□

Remarque. *Dans la démonstration, nous avons laissé en suspens la preuve de la convergence de $\mathfrak{S}$: on applique l'inégalité de Weyl à $S_{a,q} = \sum_{z=1}^{q} e(\frac{a}{q} z^k)$ avec $\alpha = \frac{a}{q}$ et $P = q$. On obtient :*

$$\forall \epsilon > 0, \quad |S_{a,q}| \ll q^{1 - \frac{1}{2^{k-1}} + \epsilon}$$

Donc

$$|(q^{-1} S_{a,q})^s e\left(-N\frac{a}{q}\right)| \ll q^{-\frac{s}{2^{k-1}} + \epsilon} \ll q^{-2 - \frac{1}{2^{k-1}} + \epsilon}$$

Par cette majoration, on voit que la série est absolument convergente. Ce résultat sera utilisé dans le chapitre suivant.

Chapitre 5

La série singulière

Rappelons d'abord le résultat de la section précédente : si $s \geq 2^k + 1$,

$$r(N) = C_{k,s}\mathfrak{S}(N)N^{\frac{s}{k}-1} + O(N^{\frac{s}{k}-1-\delta'})$$

avec $\mathfrak{S}(N) = \sum_{q=1}^{\infty} A(q)$ la série singulière, où on a simplifié la notation en introduisant la fonction :

$$A(q) = \sum_{\substack{a=1 \\ a\wedge q=1}}^{q} (q^{-1}S_{a,q})^s e\left(-\frac{aN}{q}\right)$$

De cette définition, il est clair que $A(q) = \overline{A(q)}$ via la transformation $a \leftrightarrow q-a$, et par conséquent $\forall q \in \mathbb{N}, A(q) \in \mathbb{R}$.

Dans cette section nous allons minorer la série singulière par un réel strictement positif qui ne dépend pas de N (toujours avec $s \geq 2^k+1$), ce qui valide la formule asymptotique $r(N) \gg N^{\frac{s}{k}-1}$. Ainsi, on démontre enfin que tout entier suffisamment grand est somme de $s \geq 2^k + 1$ puissances k-ièmes, et répond affirmativement au problème de Hilbert-Waring (et, au passage, on montre que $G(k) \leq 2^k + 1$). Le dernier pas vers la réponse positive du problème de Waring est donc le théorème suivant, dont la démonstration sera reportée à la fin de la section :

Théorème (de la Série Singulière)**.** *Si $s \geq 2^k + 1$, alors il existe un réel $C(k,s) > 0$ tel que :*

$$\forall N \in \mathbb{N}, \mathfrak{S}(N) \geq C(k,s)$$

5.1 La série singulière comme produit

La présence d'une condition de primalité entre deux entiers rendra la série singulière a priori difficile à traiter. Nous allons profiter du fait que $A(q)$ est une fonction arithmétique multiplicative pour réécrire la série singulière comme un produit sur les nombres premiers, où la condition de primalité devient plus simple.

Lemme. *$A(q)$ est une fonction multiplicative, i.e. si $q_1 \wedge q_2 = 1, \quad A(q_1, q_2) = A(q_1)A(q_2)$*

Démonstration. Soient $q_1, q_2 \in \mathbb{N}$ tel que $q_1 \wedge q_2 = 1$ et soit $q = q_1 q_2$. Notons :

$$f(a,q) = (q^{-1}S_{a,q})^s e(-\frac{aN}{q})$$

Par le théorème de Bézout, il existe une bijection entre l'ensemble $\{a \in [|1,q|] | a \wedge q = 1\}$ et l'ensemble des couples $\{(a_1, a_2) \in [|1,q_1|] \times [|1,q_2|] \mid a_1 \wedge q_1 = 1 \text{ et } a_2 \wedge q_2 = 1\}$, donnée par l'équation :

$$\frac{a}{q} \equiv \frac{a_1}{q_1} + \frac{a_2}{q_2} \mod 1 \quad (2)$$

Et il y a aussi une bijection entre $[|1,q|]$ et $[|1,q_1|] \times [|1,q_2|]$ donnée par :

$$\frac{z}{q} \equiv \frac{z_1}{q_1} + \frac{z_2}{q_2} \mod 1$$

De cette dernière équation :

$$S_{a,q} = \sum_{z=1}^{q} e(\frac{az^k}{q}) = \sum_{z_1=1}^{q_1}\sum_{z_2=1}^{q_2} e\left(\frac{a}{q}q^k\left(\frac{z_1}{q_1}+\frac{z_2}{q_2}\right)^k\right)$$

Or

$$\begin{aligned}\frac{a}{q}q^k\left(\frac{z_1}{q_1}+\frac{z_2}{q_2}\right)^k &= \frac{a}{q}(z_1q_2 + z_2q_1)^k \\ &\equiv \frac{a}{q}\left((z_1q_2)^k(z_2q_1)^k\right) \mod 1 \\ &\equiv \frac{a_1}{q_1}(z_1q_2)^k + \frac{a_2}{q_1}(z_2q_1)^k \mod 1\end{aligned}$$

Ainsi :

$$\begin{aligned}S_{a,q} &= \sum_{z_1=1}^{q_1}\sum_{z_2=1}^{q_2} e\left(\frac{a_1}{q_2}(z_1q_2)^k + \frac{a_2}{q_2}(z_2q_2)^k\right) \\ &= \sum_{z_1=1}^{q_1}\sum_{z_2=1}^{q_2} e\left(\frac{a_1}{q_2}(z_1q_2)^k\right) e\left(\frac{a_2}{q_2}(z_2q_2)^k\right) \\ &= \sum_{z_1=1}^{q_1} e\left(\frac{a_1}{q_2}(z_1q_2)^k\right) \sum_{z_2=1}^{q_2} e\left(\frac{a_2}{q_2}(z_2q_2)^k\right) \\ &= S_{a_1q_1}S_{a_2q_2}\end{aligned}$$

Puis à partir de (2) on obtient aisément : $e\left(-\frac{aN}{q}\right) = e\left(-\frac{a_1 N}{q_1}\right) e\left(-\frac{a_2 N}{q_2}\right)$, et ensuite : $f(a,q) = f(a_1,q_1)f(a_2,q_2)$

Finalement, toujours par (2), on arrive à :

$$A(q) = \sum_{\substack{a=1 \\ (a,q)=1}}^{q} f(a,q) = \left(\sum_{\substack{a_1=1 \\ (a_1,q_1)=1}}^{q_1} f(a_1,q_1) \right) \left(\sum_{\substack{a_2=1 \\ (a_2,q_2)=1}}^{q_2} f(a_2,q_2) \right) = A(q_1)A(q_2)$$

□

La multiplicativité de $A(q)$ nous permet de transformer la série singulière en un produit :

Proposition. *Si $s \geq 2^k + 1$, alors :*

$$\mathfrak{S}(N) = \prod_p \chi(p) \quad avec \quad \chi(p) = \sum_{\nu=0}^{\infty} A(p^\nu)$$

Démonstration. Dans la remarque finale du chapitre précédent, on a montré que :

$$\exists \delta > 0 \quad \text{tel que} \quad |A(q)| \ll q^{-1-\delta}$$

C'est-à-dire que $\mathfrak{S}(N)$ converge absolument, ce qui nous amène directement à

$$\mathfrak{S}(N) = \sum_{q=1}^{\infty} A(q) = \prod_p \left(\sum_{\nu=0}^{\infty} A(p^\nu) \right) = \prod_p \chi(p)$$

□

5.2 Minorations

Pour finir la démonstration du théorème, on va prouver deux résultats qui minorent le produit obtenu ci-dessus. Mais tout d'abord, présentons quelques définitions et lemmes nécessaires :

Définitions. *1. Pour un entier naturel q, on note $M(q)$ le nombre de solutions de la congruence :*

$$x_1^k + \cdots + x_s^k \equiv N \mod q \quad avec \quad 0 < x_1, \cdots, x_s \leq q$$

2. Soit p un nombre premier. On définit $\gamma_p = \gamma(p,k)$ comme suit :

$$\gamma_p = \begin{cases} \nu_p(k) + 1 & si \quad p > 2 \\ \nu_p(k) + 2 & si \quad p = 2 \end{cases}$$

où $\nu_p(k)$ désigne la valuation en p de k.

Lemme 1. *Soit $s \geq 2^k + 1$. Pour tout nombre premier p,*

$$\chi(p) = \lim_{n\to\infty} \left(\frac{M(p^n)}{p^{n(s-1)}} \right)$$

Démonstration. Remarquons que

$$\sum_{t=1}^{q} e\left(\frac{t}{q}(x_1^k + \cdots + x_s^k - N)\right) = \begin{cases} q, & \text{si} \quad x_1^k + \cdots + x_s^k - N \equiv 0 \bmod p \\ 0, & \text{sinon} \end{cases}$$

On utilise cette sorte de fonction caractéristique pour réécrire la fonction $M(q)$:

$$M(q) = q^{-1} \sum_{t=1}^{q} \sum_{x_1=1}^{q} \cdots \sum_{x_s=1}^{q} e\left(\frac{t}{q}(x_1^k + \cdots + x_s^k - N)\right)$$

Nous rassemblons maintenant les t qui ont le même pgcd avec q :

$$\begin{aligned} M(q) &= q^{-1} \sum_{q_1 | q} \sum_{\substack{u=1 \\ u \wedge q_1 = 1}}^{q_1} \sum_{x_1=1}^{q} \cdots \sum_{x_s=1}^{q} e\left(\frac{u}{q_1}(x_1^k + \cdots + x_s^k - N)\right) \\ &= q^{-1} \sum_{q_1 | q} \sum_{\substack{u=1 \\ u \wedge q_1 = 1}}^{q_1} \left(\sum_{x=1}^{q} e\left(\frac{u}{q_1}(x^k)\right) \right)^s e\left(-\frac{uN}{q_1}\right) \end{aligned}$$

Or,

$$\sum_{x=1}^{q} e\left(\frac{u}{q_1} x_1^k\right) = \sum_{z=1}^{\frac{q}{q_1}} \sum_{y=1}^{q_1} e\left(\frac{u}{q_1}(zq_1 + y)^k\right) = \frac{q}{q^1} \sum_{y=1}^{q_1} e\left(\frac{u}{q_1} y^k\right) = \frac{q}{q_1} S_{u,q_1}$$

Alors nous arrivons à :

$$\begin{aligned} M(q) &= q^{-1} \sum_{q_1 | q} \sum_{\substack{u=1 \\ u \wedge q_1 = 1}}^{q_1} \left(\frac{q_1}{q} S_{u,q_1} \right)^s e\left(-\frac{uN}{q_1}\right) \\ &= q^{s-1} \sum_{q_1 | q} \left(\sum_{\substack{u=1 \\ u \wedge q_1 = 1}}^{q_1} (q_1 S_{u,q_1})^s e\left(-\frac{uN}{q_1}\right) \right) \\ &= q^{s-1} \sum_{q_1 | q} A(q_1) \end{aligned}$$

Maintenant, dans le cas particulier $q = p^n$, on obtient :

$$\sum_{\nu=0}^{n} A(p^\nu) = \frac{M(p^n)}{p^{n(s-1)}}$$

Et finalement, le résultat découle en faisant tendre n vers l'infini :

$$\chi(p) = \lim_{n\to\infty} \left(\frac{M(p^n)}{p^{n(s-1)}} \right)$$

□

Les lemmes suivants ne seront pas démontrés dans cette étude. Des preuves détaillés se trouvent sur la référence principale [1] (PP36-40).

Lemme 2. *Soit p un nombre entier. Si $m \neq 0 \mod p$ et s'il existe y tel que $y^k \equiv m \mod p^{\gamma_p}$, la congruence $x^k \equiv m \mod p^\nu$ est résoluble pour tout $\nu \geq \gamma_p$.*

Lemme 3. *Soit p un nombre entier. Si $s \geq 2^k + 1$, la congruence*

$$x_1^k + \cdots + x_s^k \equiv N \mod p^{\gamma_p}$$

a toujours une solution tel que $x_1, \cdots, x_s$ ne sont pas tous divisibles par p.

Maintenant, énonçons les deux résultats principals de la section :

Résultat 1. *Soit $s \geq 2^k + 1$. Pour tout nombre premier p, il existe un réel $C(p,k,s) > 0$ (indépendant de N) tel que :*

$$\chi(p) \geq C(p,k,s)$$

Démonstration. Par le lemme 3, on sait qu'il existe $a_1, \cdots, a_s$ tel que : $a_1^k + \cdots + a_s^k \equiv N \mod p^{\gamma_p}$ avec $a_1 \neq 0 \mod p$. Nous allons construire beaucoup de solutions de la congruence $x_1^k + \cdots + x_s^k \equiv N \pmod{p^\nu}$ avec $\nu \geq \gamma_p$. On choisit arbitrairement $x_2, \cdots, x_s$ tel que :

$$\forall j \in [2,s], x_j \equiv a_j \mod p^{\gamma_p} \quad \text{et} \quad 0 < x_j \leq p^\nu$$

On a en fait $p^{(\nu-\gamma_p)(s-1)}$ choix possibles. Pour chacun de ces choix, on a toujours

$$a_1^k \equiv N - x_2^k - \cdots - x_s^k \mod p^{\gamma_p}$$

D'où, par le lemme 2, on peut trouver x_1 de sorte que :

$$x_1^k \equiv N - x_2^k - \cdots - x_s^k \mod p^\nu$$

Ainsi $\forall \nu \geq \gamma_p, M(p^\nu) \geq p^{(\nu-\gamma_p)(s-1)} = C(p,k,s)p^{\nu(s-1)}$, avec $C(p,k,s) = p^{-\gamma_p(s-1)}$

Donc par le lemme 1, $\chi(p) = \lim_{\nu\to\infty} \left(\frac{M(p^\nu)}{p^{\nu(s-1)}}\right) \geq C(p,k,s)$.

Le résultat est alors prouvé. □

Finalement, on arrive au deuxième résultat :

Résultat 2. *Si $s \geq 2^k + 1$, alors il existe un entier naturel $p_0(k)$ tel que :*

$$\frac{1}{2} \leq \prod_{p > p_0(k)} \chi(p) \leq \frac{3}{2}$$

Démonstration. Dans la remarque finale du chapitre précédent, on a montré que :

$$\exists \delta > 0 \quad \text{tel que} \quad |A(q)| \ll q^{-1-\delta}$$

où le δ dépend seulement de k. Ainsi :

$$|\chi(p) - 1| \ll \sum_{\nu=1}^{\infty} p^{-\nu(1+\delta)} = \frac{p^{-1-\delta}}{1 - p^{-1-\delta}} \ll p^{-1-\delta}$$

Or, remarquons que $\chi(p)$ est une fonction réelle et $(\chi(p) - 1) \to 0$, donc

$$|\log(\chi(p))| \ll |\chi(p) - 1| \ll p^{-1-\delta}$$

Ainsi, la série $\sum_p log(\chi(p))$ (définie à partir d'un certain rang) converge absolument, et par conséquent il existe $p_0 = p_0(\delta) = p_0(k)$ tel que :

$$\log\left(\frac{1}{2}\right) \leq \sum_{p > p_0(k)} \log(\chi(p)) \leq \log\left(\frac{3}{2}\right)$$

Et le résultat désiré suit immédiatement. □

Il reste maintenant à finir la preuve du théorème central de cette partie :

Démonstration du Théorème de la Série Singulière. On a prouvé dans un lemme précédent que :

$$\mathfrak{S}(N) = \prod_p \chi(p)$$

D'où, par les deux résultats démontrés précédement, on a :

$$\mathfrak{S}(N) = \prod_{p > p_0(k)} \chi(p) \prod_{p \leq p_0(k)} \chi(p) \geq \frac{1}{2} \prod_{p \leq p_0(k)} C(p, k, s) = C(k, s) > 0$$

□

Chapitre 6

Conclusion

Au cours de cette étude, nous avons démontré, pour k fixé :

$$\forall s \geq 2^k + 1, r(n) \overset{n \to \infty}{\to} \infty$$

Ce qui signifie en fait, d'après la définition de la limite :

$$\forall s \geq 2^k + 1, \forall C \in \mathbb{N}, \exists N_0 \textit{ tel que } \forall n > N_0, r(n) \geq C$$

On a donc montré l'existence d'un nombre s tel que tout entier peut s'écrire comme somme d'au plus s puissances k-ièmes, pour k fixé, ce qui prouve la conjecture de Waring.

A fortiori, ce résultat est vrai pour $C = 1$. Donc :

$$\min\{s \in \mathbb{N}^* | \exists N_0 \in \mathbb{N}^*, \forall n \geq N_0, r(n) > 0\} \leq 2^k + 1$$

Ce minimum est la définition de $G(k)$, donc on a montré que :

$$G(k) \leq 2^k + 1$$

Par exemple, pour $k = 3$, $G(3) \leq 9$. (En fait, $G(k) = 7$.)

Chapitre 7

Complément : Travail sur Maple

Nous allons nous intéresser ici à la fonction suivante :

$$R_3(n) = \min\{s \in \mathbb{N}^* | r_3(n) \neq 0\}$$

Il s'agit en fait du nombre minimal de cubes nécessaires pour sommer et obtenir n. On remarque au passage que :

$$g(3) = \max_{n \in \mathbb{N}^*} R_3(n)$$

C'est pour cela qu'en admettant $g(3) = 9$ (démontré en 1912 par Arthur Wieferich et Aubrey J. Kempner), on peut prendre 9 comme borne supérieure pour s. (On notera au passage que l'égalité $g(4) = 19$ a été démontrée en 1986 par deux chercheurs de l'Université Bordeaux 1, à savoir François Dress et Jean-Marc Deshouillers, en collaboration avec Ramachandran Balasubramanian). Afin d'obtenir quelques valeurs numériques de R_3, et de tracer un graphe représentant C_{R_3} pour n allant de 1 à 80, nous avons créé plusieurs algorithmes à l'aide de Maple 13.

Le premier est un algorithme qui prend en entrée un entier naturel non nul n et qui renvoie la liste des s-uplets (où $s \leq 9$) vérifiant l'égalité de Waring à la puissance $k = 3$ pour n. Cet algorithme est naïf ; en effet, il s'agit de 9 boucles emboîtées sur les x_i où ceux-ci parcourent $[|0, n^{\frac{1}{3}}|]$, et où l'on vérifie à chaque exécution l'égalité de la somme des cubes avec n :

```
> Cub := proc (n) local x1, x2, x3, x4, x5, x6, x7, x8, x9,
                        y1, y2, y3, y4, y5, y6, y7, y8, y9, L, N;
L := NULL; N := floor(n^(1/3));
for x9 from 1 to N do y9 := x9^3;
 for x8 from 1 to N do y8 := x8^3;
```

```
 for x7 from 1 to N do y7 := x7^3;
  for x6 from 1 to N do y6 := x6^3;
   for x5 from 1 to N do y5 := x5^3;
    for x4 from 1 to N do y4 := x4^3;
     for x3 from 1 to N do y3 := x3^3;
      for x2 from 1 to N do y2 := x2^3;
       for x1 from 1 to N do y1 := x1^3;
        if y1 = n then
         L := L, [x1] end if;
        if y1+y2 = n then
         L := L, [x1, x2] end if;
        if y1+y2+y3 = n then
         L := L, [x1, x2, x3] end if;
        if y1+y2+y3+y4 = n then
         L := L, [x1, x2, x3, x4] end if;
        if y1+y2+y3+y4+y5 = n then
         L := L, [x1, x2, x3, x4, x5] end if;
        if y1+y2+y3+y4+y5+y6 = n then
         L := L, [x1, x2, x3, x4, x5, x6] end if;
        if y1+y2+y3+y4+y5+y6+y7 = n then
         L := L, [x1, x2, x3, x4, x5, x6, x7] end if;
        if y1+y2+y3+y4+y5+y6+y7+y8 = n then
         L := L, [x1, x2, x3, x4, x5, x6, x7, x8] end if;
        if y1+y2+y3+y4+y5+y6+y7+y8+y9 = n then
         L := L, [x1, x2, x3, x4, x5, x6, x7, x8, x9] end if
       end do
      end do
     end do
    end do
   end do
  end do
 end do
end do
```

```
end do;
return [L] ; end;
```

Appliquons-le à 23 :

```
> Cub(23);

      [[2, 2, 1, 1, 1, 1, 1, 1, 1], [2, 1, 2, 1, 1, 1, 1, 1, 1],
        [1, 2, 2, 1, 1, 1, 1, 1, 1], [2, 1, 1, 2, 1, 1, 1, 1, 1],
        [1, 2, 1, 2, 1, 1, 1, 1, 1], [1, 1, 2, 2, 1, 1, 1, 1, 1],
        [2, 1, 1, 1, 2, 1, 1, 1, 1], [1, 2, 1, 1, 2, 1, 1, 1, 1],
        [1, 1, 2, 1, 2, 1, 1, 1, 1], [1, 1, 1, 2, 2, 1, 1, 1, 1],
        [2, 1, 1, 1, 1, 2, 1, 1, 1], [1, 2, 1, 1, 1, 2, 1, 1, 1],
        [1, 1, 2, 1, 1, 2, 1, 1, 1], [1, 1, 1, 2, 1, 2, 1, 1, 1],
        [1, 1, 1, 1, 2, 2, 1, 1, 1], [2, 1, 1, 1, 1, 1, 2, 1, 1],
        [1, 2, 1, 1, 1, 1, 2, 1, 1], [1, 1, 2, 1, 1, 1, 2, 1, 1],
        [1, 1, 1, 2, 1, 1, 2, 1, 1], [1, 1, 1, 1, 2, 1, 2, 1, 1],
        [1, 1, 1, 1, 1, 2, 2, 1, 1], [2, 1, 1, 1, 1, 1, 1, 2, 1],
        [1, 2, 1, 1, 1, 1, 1, 2, 1], [1, 1, 2, 1, 1, 1, 1, 2, 1],
        [1, 1, 1, 2, 1, 1, 1, 2, 1], [1, 1, 1, 1, 2, 1, 1, 2, 1],
        [1, 1, 1, 1, 1, 2, 1, 2, 1], [1, 1, 1, 1, 1, 1, 2, 2, 1],
        [2, 1, 1, 1, 1, 1, 1, 1, 2], [1, 2, 1, 1, 1, 1, 1, 1, 2],
        [1, 1, 2, 1, 1, 1, 1, 1, 2], [1, 1, 1, 2, 1, 1, 1, 1, 2],
        [1, 1, 1, 1, 2, 1, 1, 1, 2], [1, 1, 1, 1, 1, 2, 1, 1, 2],
        [1, 1, 1, 1, 1, 1, 2, 1, 2], [1, 1, 1, 1, 1, 1, 1, 2, 2]]
```

Ensuite, voici un algorithme qui exploite les résultats de l'algorithme précédent, et qui pour un n donné en entrée, renvoie la longueur minimale des s-uplets pour lesquels l'égalité de Waring est vérifiée. Cet algorithme renvoie donc $R_3(n)$:

```
> R_3 := proc (n) local L, l, i, i0, k;
L := Cub(n); l := nops(L); i0 := nops(L[1]);
for k from 1 to l do
 i := nops(L[k]);
 if i < i0 then i0 := i end if
end do;
return i0 end;
```

Calculons donc $R_3(100)$ et $R_3(23)$:

```
> R_3(100);
                                    4
> R_3(23);
                                    9
```

Enfin, un algorithme « technique »nécessaire au tracé de la courbe C_{R_3}, qui associe à tout n la liste des coordonnées des points $(i, R_3(i))$, pour tous les $i \in [|1, n|]$:

```
> L_R3 := proc (n) local L, i;
L := NULL;
for i to n do
 L := L, [i, R_3(i)]
end do;
return [L];
end;
```

On calcule cette liste pour $n = 50$:

```
> L_R3(50);

 [[1, 1], [2, 2], [3, 3], [4, 4], [5, 5], [6, 6], [7, 7],
  [8, 1], [9, 2], [10, 3], [11, 4], [12, 5], [13, 6], [14, 7],
  [15, 8], [16, 2], [17, 3], [18, 4], [19, 5], [20, 6], [21, 7],
  [22, 8], [23, 9], [24, 3], [25, 4], [26, 5], [27, 1], [28, 2],
  [29, 3], [30, 4], [31, 5], [32, 4], [33, 5], [34, 6], [35, 2],
  [36, 3], [37, 4], [38, 5], [39, 6], [40, 5], [41, 6], [42, 7],
  [43, 3], [44, 4], [45, 5], [46, 6], [47, 7], [48, 6], [49, 7],
  [50, 8]]
```

Et on rédige enfin un algorithme qui trace la courbe recherchée :

```
> DrawN := proc (N) local L; L := L_R3(N);
plot(L, x = 0 .. N)
end;
```

Sur la page suivante se trouve le tracé de la courbe pour $n = 80$.

Même si 80 valeurs de test ne suffisent pas pour prouver un résultat, nous pouvons quand même observer que cette courbe ne dépasse pas 9 ; on peut donc conjecturer que $g(3) = 9$, et de plus à partir d'un certain rang elle ne dépassera pas 7, donc on peut supposer que $G(3) = 7$. En fait, seuls 23 et 239 nécessitent 9 cubes, et seuls 15, 22, 50, 114, 167, 175, 186, 212, 213, 238, 303, 364, 420, 428, et 454 nécessitent 8 cubes.

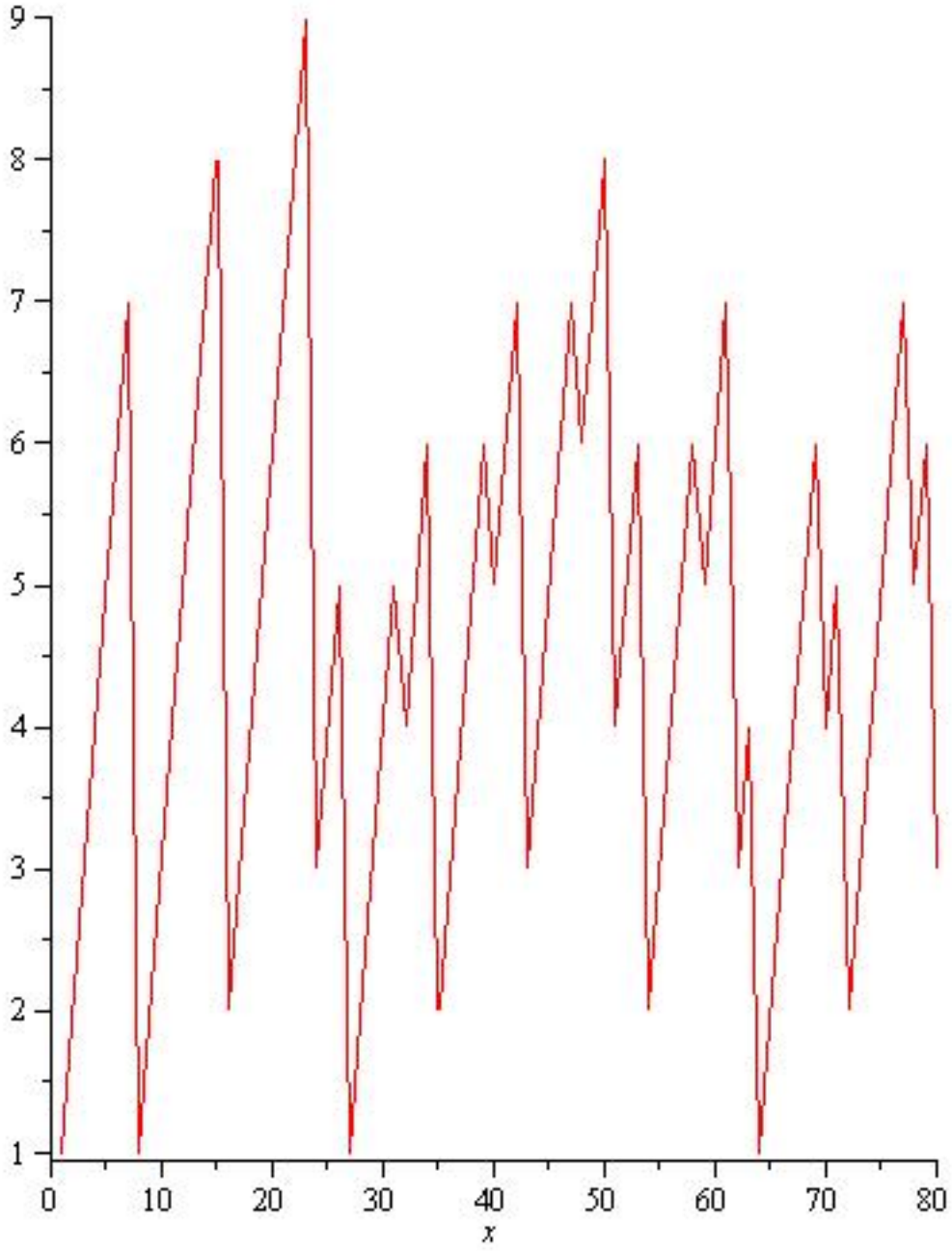

FIGURE 7.1 – Tracé de la courbe C_{R_3}

Chapitre 8

Références

Nous nous sommes appuyés sur les travaux suivants :

[1] Harold Davenport, *Analytics methods for diophantine equations and diophantine inequalities*, University of Michigan, 1962

[2] Edmund Taylor Whittaker et George Neville Watson, *Modern Analysis*, Cambridge University, 1915

[3] Jean-Marc Deshouillers, *L'étude des formes cubiques rationnelles via la méthode du cercle*, 1990