Institut de Mathématique d'Orsay

Problème de Waring et méthode du cercle

Marouane Izmar, Hakim Ahamada, Manuel Boisseau

Encadrant : Kevin Destagnol

Projet TER 2021-2022

Table des matières

Chapitre 1

Introduction

1.1 Le problème de Waring

On considère le problème suivant : sachant un entier k fixé, on veut déterminer l'existence d'un entier s tel que tout entier n est la somme d'au plus s nombres entiers à la puissance k :

$$\exists s,\ \forall n,\ n = {x_1}^k + {x_2}^k + ... + {x_s}^k \tag{1.1}$$

Conjecturée par 1770 par le mathématicien Edward Waring, cette proposition a été démontrée pour la première fois par David Hilbert en 1909 par des arguments de combinatoire algébrique. Les travaux de G. H. Hardy et J. E. Littlewood introduisent alors une méthode de démonstration - celle dont nous allons traiter ici - utilisant des outils analytiques, inspirée d'un article écrit par Hardy et Ramanujan en 1918. Plus tard, en 1937 Ivan Vinogradov perfectionne la méthode de Hardy-Littlewood pour obtenir d'autres résultats de théorie des nombres.
On note $g(k)$ le plus petit entier s satisfaisant cette propriété. Les valeurs de $g(k)$ sont connues pour les entiers les plus petits, certaines depuis les années 1800 :

Valeur de k	Valeur de $g(k)$
1	1
2	4
3	9
4	19
5	37
6	73

Par exemple, $g(2)$ se calcule grâce aux théorèmes des trois carrés et des quatre carrés de Lagrange.
Un autre entier qui apparaît rapidement est $G(k)$, défini tel qu'à partir d'un entier N assez grand, tout entier $n \geq N$ est somme d'au plus $G(k)$ puissances k-ièmes d'entiers.

En pratique, pour démontrer (1.1), nous allons montrer que $G(k)$ est fini pour $n \geq N$ puis observer que tout entier $n < N$ est somme de n puissances k-ièmes de 1 : ainsi on aura $g(k) \leq \max(G(k), N)$, ce qui permettra de conclure que $g(k)$ est fini.

1.2 La méthode du cercle

Pour démontrer (1.1), on va utiliser une méthode courante en théorie analytique des nombres appelée *méthode du cercle*. Cette méthode consiste à évaluer la valeur de $G(k)$ asymptotiquement à l'aide de résultats d'analyse complexe. On part d'un ensemble d'entiers strictement positifs $A = (a_m)_{m\geq 1}$, on fixe un entier P et on définit le polynôme

$$f(z) := \sum_{m=1}^{P} z^{a_m}$$

On remarque qu'en évaluant f à la puissance s, on obtient

$$f^s(z) = \sum_{n=1}^{s\cdot a_P} r_{A,s}(n) z^n$$

où $r_{A,s}(n)$ est le nombre de représentations de n comme somme de s éléments de A. Le polynôme f étant une fonction entière,on peut accéder à la valeur de $r_{A,s}(n)$ par la formule de Cauchy en intégrant sur le cercle unité $C(0,1)$:

$$r_{A,s}(n) = \frac{1}{2i\pi} \int_{C(0,1)} \frac{f^s(z)}{z^{n+1}} dz$$

Pour simplifier les notations, on définit $e(\alpha) := e^{2i\pi\alpha}$ et $F(\alpha) := f(e(\alpha))$. Pour revenir à notre problème, on choisit $A = \{m^k; m \in \mathbb{N}_{\geq 1}\}$ et $P = \lfloor n^{\frac{1}{k}} \rfloor$ .On note $r_{k,s}(n)$ le nombre de représentations de n comme somme de s puissances k-ièmes d'entiers. On obtient la formule d'intégration suivante :

$$\forall k \leq n,\ r_{k,s}(n) = \int_0^1 F^s(\alpha) e(-n\alpha) d\alpha$$

On montrera alors la formule asymptotique suivante, démontrée par Hardy-Littlewood en 1919, pour $s \geq 2^k + 1$ et $n \geq 2^k$:

$$r_{k,s}(n) = \sigma(n) \frac{\Gamma(1+1/k)^s}{\Gamma(s/k)} n^{s/k-1} + O_{n\to+\infty}(n^{(s/k)-1-\delta}) \tag{1.2}$$

où δ est un réel positif dépendant uniquement de s et k. Cette formule garantit $\lim_{n\to+\infty} r_{k,s}(n) = +\infty$, on a donc $r_{k,s}(n) > 0$ à partir d'un certain rang, soit $G(k) < +\infty$.

Pour obtenir (1.2), on va procéder en découpant le cercle unité en plusieurs ensembles : des arcs dits "mineurs" où l'on pourra minorer f et son intégrale par une quantité négligeable, et des arcs dits "majeurs" où l'on pourra évaluer la valeur asymptotique de l'intégrale. Les arcs majeurs correspondent aux réels de $[0, 1]$ pouvant bien "être approchés" par des rationnels. On décomposera l'intégrale de f sur ces ensembles comme le produit de deux termes $J(n)$ (intégrale singulière), qui fera apparaître les termes faisant intervenir Γ, et $\sigma(n)$ (série singulière). L'intégrale sur les arcs mineurs correspond au terme en $O()$ dans la formule (1.2), minorée en utilisant l'inégalité de Weyl et le lemme de Hua. Nous démontrons ces résultats dans les sections suivantes, puis terminons dans une troisième partie la preuve.

Chapitre 2

Résultats préliminaires

2.1 Théorème de Dirichlet

Théorème 2.1.1 (Dirichlet)**.** *Soit $\alpha, Q \in \mathbb{R}$ avec $Q \geq 1$. Alors*

$$\exists (a,q) \in \mathbb{Z}^2,\ 1 \leq q \leq Q,\ a \wedge q = 1 \text{ et } \left|\alpha - \frac{a}{q}\right| < \frac{1}{qQ}$$

Démonstration. Posons $n = \lfloor Q \rfloor$ et $\{x\} := x - \lfloor x \rfloor \in [0,1[$. On fait 3 cas :

1. $\{q\alpha\} \in [0, \frac{0}{n+1}[$ pour un certain $q \leq n$: on pose $a := \lfloor q\alpha \rfloor$, alors

$$0 \leq \{q\alpha\} = q\alpha - \lfloor q\alpha \rfloor = q\alpha - a < \frac{1}{n+1}$$

   Donc

$$\left|\alpha - \frac{a}{\alpha}\right| \leq \frac{1}{q(n+1)} \leq \frac{1}{qQ}$$

2. $\{q\alpha\} \in [\frac{n}{n+1}, 1[$ pour un certain $q \leq n$: on pose $a := \lfloor q\alpha \rfloor + 1$, alors

$$\frac{n}{n+1} \leq q\alpha - a + 1 < 1$$

   Donc

$$\left|\alpha - \frac{a}{\alpha}\right| \leq \frac{1}{q(n+1)} \leq \frac{1}{qQ}$$

3. pour tout $q \in [\![1; n]\!]$, chacun des n réels $\{q\alpha\}$ sont dans un des n-1 intervalles $[\frac{i}{n+1}, \frac{i+1}{n+1}[$. Alors, par le principe des tiroirs de Dirichlet

$$\exists i \in [\![1; n-1]\!], \exists (q_1, q_2) \in [\![1; n]\!]^2,\ q_1 < q_2 \text{ et } \{q_1\alpha\}, \{q_2\alpha\} \in \left[\frac{i}{n+1}, \frac{i+1}{n+1}\right]$$

Posons $q := q_2 - q_1 \in [\![1; n-1]\!]$ et $a := \lfloor q_2\alpha \rfloor - \lfloor q_1\alpha \rfloor$, alors

$$|q\alpha - a| = |\{q_2\alpha\} - \{q_1\alpha\}| < \frac{1}{n+1} < \frac{1}{Q}$$

□

2.2 Inégalité de Weyl

Théorème 2.2.1 (Inégalité de Weyl)**.** *Soit f une fonction polynomiale de degré $k \geq 2$ et de coefficient dominant α qui vérifie $|\alpha - \frac{a}{q}| \leq \frac{1}{q^2}$, avec $q \geq 1$ et $a \wedge q = 1$. On pose*

$$S(f) := \sum_{m=1}^{n} e(f(m))$$

On pose $K := 2^{k-1}$. Alors pour tout $\varepsilon > 0$

$$S(f) \ll n^{1+\varepsilon} \left(n^{-1} + q^{-1} + n^{-k}q\right)^{\frac{1}{K}}$$

La notation $a_n \ll b_n$ signifie que $\exists C > 0 / \ |a_n| \leq Cb_n$ à partir d'un certain rang. Pour prouver ce théorème, on va passer par plusieurs lemmes.

Lemme 2.2.2. *On se place dans le cadre du théorème précédent. Alors*

$$|S(f)|^k \ll n^{K-1} + n^{K-k+\varepsilon} \sum_{m=1}^{k!n^{k-1}} \min(n, \|m\alpha\|^{-1})$$

Lemme 2.2.3. *Soit $l \in \mathbb{N}$, $n_1 < n_2$ tels que $0 \leq n_2 - n_1 \leq n$. Soit $(g(n))_{n\leq 1} \in \mathbb{C}^{\mathbb{N}}$ et $S(g) := \sum_{m=n_1+1}^{n_2} e(g(m))$, alors*

$$|S(g)|^{2^l} \leq (2n)^{2^l - l - 1} \sum_{|d_1|<n} \dots \sum_{|d_l|<n} S_{d_l,\dots,d_1}(g)$$

où

$$S_{d_l,\dots,d_1}(g) = \sum_{m \in I(d_l,\dots,d_1)} e(\Delta_{d_l,\dots,d_1}(g)(m))$$

avec $\Delta_d(g)(m) := g(m+d) - g(m)$ et $I(d_l, \dots, d_1)$ un intervalle d'entiers consécutifs contenus dans $[\![n_1 + 1, n_2]\!]$ et $\Delta_{d_2,d_1}(g)(m) := \Delta_{d_2}(\Delta_{d_1}(g))(m)$.

Démonstration. Lemme 2.2.3. On va procéder par récurrence sur l.
Pour $l = 1$ et d entier, $I(d) = [\![n_1 + 1 - d, n_2 - d]\!] \cap [\![n_1 + 1, n_2]\!]$. Alors

$$\begin{aligned}
|S(g)|^2 &= S(g)\overline{S(g)} \\
&= \sum_{m=n_1+1}^{n_2} \sum_{p=n_1+1}^{n_2} e(g(m) - g(p)) \\
&= \sum_{m=n_1+1}^{n_2} \sum_{d=n_1+1-m}^{n_2-m} e(g(m+d) - g(m)) \\
&= \sum_{d=-(n_2-n_1-1)}^{n_2-n_1-1} \sum_{m \in I(d)} e(\Delta_d(g)(m)) \\
&\leq \sum_{|d|<n} \sum_{m \in I(d)} e(\Delta_d(g)(m)) \\
&= \sum_{|d|<n} S_d(g)
\end{aligned}$$

Désormais, on suppose le résultat vrai au rang $l \geq 1$, alors par hypothèse

$$\begin{aligned}
|S(g)|^{2^{l+1}} &= \left(|S(g)|^{2^l}\right)^2 \\
&\leq \left((2n)^{2^l - l - 1} \sum_{|d_1|<n} \dots \sum_{|d_l|<n} |S_{d_l,\dots,d_1}(g)| \right)^2 \\
&\leq (2n)^{2^{l+1} - 2l - 2} (2n)^l \sum_{|d_1|<n} \dots \sum_{|d_l|<n} |S_{d_l,\dots,d_1}(g)|^2
\end{aligned}$$

Pour chaque $d_1, \dots, d_l$, il existe un intervalle $I(d_{l+1}, d_l, \dots, d_1) \subset I(d_l, \dots, d_1) \subset [\![n_1+1, n_2]\!]$ tel que

$$\begin{aligned}
|S_{d_l,\dots,d_1}(g)|^2 &= \left| \sum_{m \in I(d_l,\dots,d_1)} e(\Delta_{d_l,\dots,d_1}(g)(m)) \right|^2 \\
&= \sum_{|d_{l+1}|<n} \sum_{m \in I(d_{l+1},\dots,d_1)} e(\Delta_{d_{l+1},\dots,d_1}(g)(m)) \\
&= \sum_{|d_{l+1}|<n} S_{d_{l+1},\dots,d_1}(g)
\end{aligned}$$

Finalement

$$|S(g)|^{2^{l+1}} \leq (2n)^{2^{l+1}-(l+1)-1} \sum_{|d_{l+1}|<n} ... \sum_{|d_1|<n} |S_{d_{l+1},...,d_1}(g)|$$

□

Démonstration. Lemme 2.2.2. Appliquons le résultat précédent à $l = k-1 \geq 1$, alors

$$|S(f)|^K \leq (2n)^{K-k} \sum_{|d_1|<n} ... \sum_{|d_{k-1}|<n} |S_{d_{k-1},...,d_1}(f)|$$

Or

$$|S_{d_{k-1},...,d_1}(f)| \leq \sum_{m \in I(d_{k-1},...,d_1)} |e(\Delta_{d_{k-1},...,d_1}(f)(m))| \leq \sum_{m \in I(d_{k-1},...,d_1)} 1$$

De plus, $I(d_{k-1},...,d_1) \subset [\![1,n]\!]$, donc $|S_{d_{k-1},...,d_1}(f)| \leq n$.

Or, en écrivant $f(m) = \sum_{j=0}^{k} \alpha_j m^j$, on a

$$\begin{aligned}
\Delta_{d_{k-1},...,d_1}(f)(m) &= \sum_{j=0}^{k} \alpha_j \Delta_{d_{k-1},...,d_1}(m^j) \\
&= d_{k-1}...d_1 \left(\frac{k!}{(k-(k-1))!} \alpha m^{k-(k-1)} + ... \right) \\
&= \lambda m + \beta
\end{aligned}$$

avec $\lambda := d_{k-1}...d_1\alpha$ et $\beta \in \mathbb{R}$, donc

$$|S_{d_{k-1},...,d_1}(f)| \leq \left| \sum_{m=1}^{n} e(\lambda m + \beta) \right| \leq \left| \sum_{m=1}^{n} e(\lambda n) \right| \leq \left| \sum_{m=1}^{n} e(\lambda)^m \right|$$

Or $\lambda \notin \mathbb{Z}$ donc $e(\lambda) \neq 1$ et

$$|S_{d_{k-1},...,d_1}(f)| \leq \left| \frac{e(\lambda(n+1))-1}{e(\lambda)-1} \right| \leq \frac{2}{|e(\lambda)-1|}$$

puis

$$|S_{d_{k-1},...,d_1}(f)| \leq \frac{2}{|e(\lambda/2)-e(-\lambda/2)|} = \frac{2}{|2i\sin(\pi\lambda)|} = \frac{1}{|\sin(\pi\lambda)|}$$

Or, pour $x \in [0, \frac{1}{2}]$, $\sin(\pi x) \geq 2x$, donc

$$|S_{d_{k-1},...,d_1}(f)| \leq \frac{1}{\sin(\pi\|\lambda\|)} \leq \frac{1}{2\|\lambda\|}$$

où $\|\lambda\| = \min(\{\lambda\}, 1-\{\lambda\}) \in]0, \frac{1}{2}]$, car $\lambda \notin \mathbb{Z}$.
Finalement

$$|S_{d_{k-1},\dots,d_1}(f)| \leq \min(n, \|\lambda\|^{-1})$$

Donc

$$|S(f)|^K \leq (2n)^{K-k} \sum_{|d_1|<n} \dots \sum_{|d_{k-1}|<n} \min(n, \|\lambda\|^{-1})$$

Or, il y a moins de $(k-1)(2n)^{k-2}$ choix de $d_1, \dots d_{k-1}$ tels que $\Pi_i d_i = 0$, et chaque choix garantit $\min(n, \|\lambda\|^{-1}) = n$, donc

$$\begin{aligned}
|S(f)|^K &\leq (2n)^{K-k}(k-1)(2n)^{k-2}n + (2n)^{K-k} \sum_{1\leq|d_1|<n} \dots \sum_{1\leq|d_{k-1}|<n} \min(n, \|\lambda\|^{-1}) \\
&\leq k(2n)^{K-1} + (2n)^{K-k}2^{k-1} \sum_{1\leq|d_1|<n} \dots \sum_{1\leq|d_{k-1}|<n} \min(n, \|\lambda\|^{-1}) \\
&\ll_n n^{K-1} + n^{K-k} \sum_{1\leq|d_1|<n} \dots \sum_{1\leq|d_{k-1}|<n} \min(n, \|\lambda\|^{-1})
\end{aligned}$$

Or $1 \leq \Pi_i d_i k! \leq k! n^{k-1}$ et $\forall \varepsilon > 0$, $d(m) \ll_\varepsilon m^\varepsilon$, où $d(m)$ est le nombre de diviseurs de m. Alors le nombre de représentations de m sous la forme $\Pi_i d_i k!$ est $\ll m^\varepsilon \ll n^\varepsilon$. Donc

$$|S(f)|^K \ll n^{K-k} n^\varepsilon \sum_{m=1}^{k!n^{k-1}} \min(n, \|m\alpha\|^{-1})$$

□

Les deux premiers lemmes démontrés, on considère finalement un troisième lemme pour prouver l'inégalité de Weyl :

Lemme 2.2.4.

$$\forall u \in \mathbb{R}\ , \sum_{1\leq m\leq u} \min(n, \|m\alpha\|^{-1}) \ll \left(q + u + n + \frac{u\cdot n}{q}\right) \max(1, \log q)$$

Démonstration. On a

$$\sum_{1\leq m\leq u} \min(n, \|m\alpha\|^{-1}) \leq \sum_{0\leq n<u/q} \sum_{1\leq r\leq q} min(n, \|(nq+r)\alpha\|^{-1})$$

1. Si $h = 0$ et $1 \leq r \leq \frac{q}{2}$ alors montrons que

$$\sum_{1\leq r\leq q/2} \min(n, \|r\alpha\|^{-1}) \leq \sum_{1\leq r\leq q/2} \|r\alpha\|^{-1} \ll q \log q$$

Le résultat est immédiat pour $q = 1$. Supposons $q \geq 2$. Pour tout $r \geq 1$ il existe $s(r) \in [0, \frac{q}{2}]$ et $m(r) \in \mathbb{N}$ tels que

$$\frac{s(r)}{q} = \left\| \frac{ar}{q} \right\| = \pm \left(\frac{ar}{q} - m(r) \right)$$

où a est un entier premier avec q. Alors $s(r) = 0 \Leftrightarrow q|r$, donc $s(r) \in [1, \frac{1}{2}]$, si $r \in [1, \frac{q}{2}]$. Posons $\alpha - \frac{a}{q} = \frac{\theta}{q^2}$, avec $\theta \in [-1, 1]$, alors

$$\alpha r = \frac{ar}{q} + \frac{\theta}{q^2} = \frac{ar}{q} + \frac{\theta'}{2q}$$

où $|\theta'| = \left| \frac{2\theta r}{q} \right| \leq |\theta| \leq 1$, donc

$$\|\alpha r\| = \left\| \frac{ar}{q} + \frac{\theta'}{2q} \right\| = \left\| m(r) \pm \frac{S(r)}{q} + \frac{\theta'}{2q} \right\| = \left\| \frac{S(r)}{q} \pm \frac{\theta'}{2q} \right\|$$

Puis

$$\|\alpha r\| \geq \left\| \frac{S(r)}{q} \right\| - \left\| \frac{\theta'}{2q} \right\| \geq \frac{S(r)}{q} - \frac{1}{2q} \geq \frac{1}{2q}$$

Soit $1 \leq r_1 \leq r_2 \leq \frac{q}{2}$. Si $\left\| \frac{ar_1}{q} \right\| = \left\| \frac{ar_2}{q} \right\|$, alors

$$\pm \left(\frac{ar_1}{q} - m(r_1) \right) = \pm \left(\frac{ar_2}{q} - m(r_2) \right)$$

Donc $ar_1 \equiv ar_2[q]$, or $a \wedge q = 1$ et $1 \leq r_1 \leq r_2 \leq \frac{q}{2}$, donc $r_1 = r_2$, puis $s(r_1) = s(r_2) \Longleftrightarrow r_1 = r_2$. Ainsi

$$\left\{ \left\| \frac{ar}{q} \right\| \mid 1 \leq r \leq \frac{q}{2} \right\} = \left\{ \frac{S(r)}{q} \mid 1 \leq r \leq \frac{q}{2} \right\} = \left\{ \frac{s}{q} \mid 1 \leq s \leq \frac{q}{2} \right\}$$

Donc

$$\sum_{1 \leq r \leq q/2} \|\alpha r\|^{-1} \leq \sum_{1 \leq r \leq q/2} \left(\frac{S(r)}{q} - \frac{1}{2q} \right)^{-1} = \sum_{1 \leq s \leq q/2} \left(\frac{s}{q} - \frac{1}{2q} \right)^{-1} = 2q \sum_{1 \leq s \leq q/2} \frac{1}{2s-1}$$

Puis, par comparaison série-intégrale, avec $f(x) = \frac{1}{x}$:

$$2q \sum_{1 \leq s \leq q/2} \frac{1}{2s-1} \leq 2q \sum_{1 \leq s \leq q/2} \frac{1}{s} \ll q \log q$$

2. Montrons que

$$\sum_{r=1}^{q} \min(n, \|(hq+r)\alpha\|^{-1}) \ll n + q\log q$$

Posons $\alpha - \frac{a}{q} = \frac{\theta}{q^2}$ avec $\theta \in [-1,1]$, alors

$$\alpha(hq+r) = ah + \frac{ar}{q} + \frac{\theta h}{q} + \frac{\theta r}{q^2} = ah + \frac{ar}{q} + \frac{\lfloor \theta h \rfloor + \{\theta h\}}{q} + \frac{\theta r}{q^2}$$

Donc

$$\alpha(hq+r) = ah + \frac{ar + \lfloor \theta h \rfloor + \delta(r)}{q}$$

Avec $\delta(r) = \{\theta h\} + \frac{\theta r}{q} \in [-1, 2[$. De plus, pour tout $r \in [\![1, q]\!]$, il existe un unique $r \in \mathbb{N}$ tel que

$$\{\alpha(hq+r)\} = \frac{ar + \lfloor \theta h \rfloor + \delta(r)}{q} - r'$$

Soit $t \in [0, 1 - \frac{1}{q}]$. Si $r \leq \{\alpha(hq+r)\} \leq t + \frac{1}{q}$ alors

$$qt \leq ar - qr' + \lfloor \theta h \rfloor + \delta(r) \leq qt + 1$$

Donc

$$qt - \lfloor \theta h \rfloor - 2 < qt - \lfloor \theta h \rfloor - \delta(r) \leq ar - qr' \leq qt - \lfloor \theta h \rfloor + 1 - \delta(r) \leq qr - \lfloor \theta h \rfloor + 2$$

Ainsi, $ar - qr' \in]qt - \lfloor \theta h \rfloor - 2\ ,\ qt - \lfloor \theta h \rfloor + 2[=: J$ un intervalle de longueur égale à 4, contenant exactement 4 entiers distincts.

Soit $1 \leq r_1 \leq r_2 \leq q$ tels que $ar_1 - qr_1{}' = ar_2 - qr_2{}'$, alors $ar_1 \equiv ar_2[q]$ et $a \wedge q = 1$, donc $r_1 = r_2$. Donc, pour tout $t \in [0, 1 - \frac{1}{q}]$, il y au plus 4 nombres $r \in [\![1, q]\!]$ tels que $\{\alpha(hq+r)\} \in [t, t + \frac{1}{q}]$.

De plus, $\|\{\alpha(hq+r)\}\| \in [r, r + \frac{1}{q}] \iff \{\alpha(hq+r)\} \in [r, r + \frac{1}{q}]$ ou $1 - \{\alpha(hq+r)\} \in [r, r + \frac{1}{q}]$. Donc

$$\|\{\alpha(hq+r)\}\| \in [r, r + \frac{1}{q}] \iff \{\alpha(hq+r)\} \in [r', r' + \frac{1}{q}]$$

où $r = 1 - \frac{1}{q} - t \in [0, 1 - \frac{1}{q}]$. Donc, pour tout $t \in [0, 1 - \frac{1}{q}]$, il y a au plus huit $r \in [\![1, q]\!]$ tels que $\|\alpha(hq+r)\| \in [t, t + \frac{1}{q}]$.

En particulier, si on pose pour $s \geq 0$, $J(s) := [\frac{s}{q}, \frac{s+1}{q}]$, alors $\|\alpha(hq+r)\| \in J(s)$ pour au plus huit $r \in [\![1, q]\!]$.

Si $\|\alpha(hq+r)\| \in J(0)$, on a $\min(n, \|\alpha(hq+r)\|^{-1}) \leq n)$

Sinon $\|\alpha(hq+r)| \in J(s)$, pour $s \geq 1$ et $\min(n, \|\alpha(hq+r)\|^{-1}) \leq \|\alpha(hq+r)\|^{-1} \leq \frac{q}{s}$

Or $s < \frac{\alpha}{2}$, car $\|\alpha(hq+r)\| \in [0, \frac{1}{2}]$, donc

$$\sum_{1 \leq r \leq q} \min(n, \|(h\alpha + r)\alpha\|^{-1} \leq 8n + 8 \sum_{1 \leq s < q/2} \frac{q}{s} \ll n + q \log q$$

encore par comparaison série-intégrale.

Donc

$$\begin{aligned}
\sum_{1 \leq m \leq u} \min(n, \|m\alpha\|^{-1}) &\ll q \log q + \sum_{0 \leq h < \frac{u}{q}} (n + q \log q) \\
&\ll q \log q + \left(\frac{u}{q} + 1\right)(n + q \log q) \\
&= q \log q + u \log q + n + \frac{un}{q} \\
&\ll (q + u + n + \frac{un}{q}) \max(1, \log q)
\end{aligned}$$

□

On peut désormais démontrer l'inégalité de Weyl :

Démonstration. Inégalité de Weyl. Comme $|S(f)| \leq n$, on a le résultat pour $q \geq n^k$, alors supposons $1 \leq q < n^k$, donc $\log q \ll \log n \ll n^\varepsilon$. Le lemme 2.2.4. nous donne que

$$\begin{aligned}
\sum_{m=1}^{k! n^{k-1}} \min(n, \|m\alpha\|^{-1}) &\ll \left(q + k! n^{k-1} + n + \frac{k! n^k}{q}\right) \max(1, \log q) \\
&\ll \left(q + n^{k-1} + \frac{n^k}{q}\right) \log n \\
&\ll n^k (q n^{-K} + n^{-1} + q^{-1}) n^\varepsilon
\end{aligned}$$

D'après le lemme 2.2.2., on a alors

$$|S(f)|^K \ll n^{K-1} + n^{K+\varepsilon}(q n^{-k} + n^{-1} + q^{-1}) \ll n^{K+\varepsilon}(q n^{-k} + n^{-1} + q^{-1})$$

□

2.3 Lemme de Hua

Théorème 2.3.1 (Lemme de Hua). *Soit $k \geq 2$ et $T : \alpha \mapsto \sum_{m=1}^{n} e(\alpha m^k)$, alors*

$$\int_0^1 |T(\alpha)|^{2^k} d\alpha \ll n^{2^k - k + \varepsilon}.$$

Démonstration.

$$\int_0^1 |T(\alpha)|^2 d\alpha = \sum_{m=1}^{n} \sum_{p=1}^{n} \int_0^1 e(\alpha(m^k - p^k)) d\alpha = n \ll n^{\varepsilon}$$

Supposons le lemme vrai pour $j \in [\![1, k-1]\!]$ et posons $f : x \mapsto \alpha x^k$. Alors

$$\Delta_{d_j,\dots,d_1}(f)(x) = \alpha_j d_j \dots d_1 p_{k-j}(x)$$

avec p_{k-j} une fonction polynomiale de degré $k-j$ à coefficients entiers. Par le lemme 2.2.3., on a

$$\begin{aligned} |T(\alpha)|^{2^j} &\leq (2n)^{2^j - j - 1} \sum_{|d_1|<n} \dots \sum_{|d_j|<n} \sum_{m \in I(d_j,\dots,d_1)} e(\alpha d_j \dots d_1 p_{k-j}(m)) \\ &\leq (2n)^{2^j - j - 1} \sum_{d} r(d) e(\alpha d) \end{aligned}$$

où $r(d)$ est le nombre de factorisations de d sous la forme $d_1 \dots d_j p_{k-j}(m)$. Or $d \ll n^k$, donc $r(d) \ll \|d\|^{\varepsilon} \ll n^{\varepsilon}$, pour $d \neq 0$, mais p_{k-j} a au plus $k-j$ racines, donc $r(0) \ll n^j$. De plus

$$\begin{aligned} |T(\alpha)|^{2^j} &= T(\alpha)^{2^{j-1}} T(-\alpha)^{2^{j-1}} \\ &= \left(\sum_{x=1}^{n} e(\alpha x^k) \right)^{2^{j-1}} \left(\sum_{y=1}^{n} e(-\alpha y^k) \right)^{2^{j-1}} \\ &= \sum_{x_1=1}^{n} \dots \sum_{x_{2^{j-1}}=1}^{n} \sum_{y_1=1}^{n} \dots \sum_{y_{2^{j-1}}=1}^{n} e\left(\alpha \left(\sum_{i=1}^{2^{j-1}} x_i^k - \sum_{i=1}^{2^{j-1}} y_i^k \right) \right) \\ &= \sum_{d} s(d) e(-\alpha d) \end{aligned}$$

où $s(d)$ est le nombre de représentations de d sous la forme $\left(\sum_{i=1}^{2^{j-1}} y_i^k - \sum_{i=1}^{2^{j-1}} x_i^k\right)$. Alors

$$\sum_d s(d) = |T(0)|^{2^j} = n^{2^j}$$

Or par hypothèse de récurrence

$$s(0) = \int_0^1 |T(\alpha)|^{2^j} d\alpha \ll n^{2^j - j + \varepsilon}$$

Donc

$$\begin{aligned}
\int_0^1 |T(\alpha)|^{2^{j+1}} d\alpha &= \int_0^1 |T(\alpha)|^{2^j} |T(\alpha)|^{2^j} d\alpha \\
&\leq (2n)^{2^j - j - 1} \int_0^1 \sum_{d'} r(d') e(\alpha d') \sum_d s(d) e(-\alpha d) d\alpha \\
&= (2n)^{2^j - j - 1} \sum_d r(d) s(d) \\
&\leq (2n)^{2^j - j - 1} r(0) s(0) + (2n)^{2^j - j - 1} \sum_{d \neq 0} r(d) s(d) \\
&\ll n^{2^j - j - 1} n^j n^{2^j - j + \varepsilon} + n^{2^j - j - 1} n^\varepsilon \sum_d s(d) \\
&\ll n^{2^{j+1} - (j+1) + \varepsilon} + n^{2^j - j - 1} n^\varepsilon n^{2^j} \\
&\ll n^{2^{j+1} - (j+1) + \varepsilon}
\end{aligned}$$

□

Chapitre 3

Démonstration de la conjecture

3.1 Arcs mineurs et majeurs

Soit $n \geq 2^k$, alors $P = \lfloor n^{1/k} \rfloor \geq 2$. Soit $\nu \in]0, \frac{1}{5}[$, $1 \leq q \leq P^\nu$, $0 \leq a \leq q$ tels que $a \wedge q = 1$. On définit un arc majeur comme

$$\mathfrak{M}(q,a) := \left\{ \alpha \in [0,1] \mid \left| \alpha - \frac{a}{q} \right| \leq \frac{1}{P^{k-\nu}} \right\}$$

et l'ensemble de tous les arcs majeurs comme

$$\mathfrak{M} := \bigcup_{1 \leq q \leq P^\nu} \bigcup_{\substack{a=0 \\ a \wedge q = 1}}^{q} \mathfrak{M}(q,a)$$

Remarque 1.

$$\mathfrak{M}(1,0) = \left[0, \frac{1}{P^{k-\nu}}\right], \ \mathfrak{M}(1,1) = \left[1 - \frac{1}{P^{k-\nu}}, 1\right]$$

et pour $q \geq 2$, on a

$$\mathfrak{M}(q,a) = \left[\frac{a}{q} - \frac{1}{P^{k-\nu}}, \frac{a}{q} + \frac{1}{P^{k-\nu}}\right]$$

Les arcs majeurs sont constitués des réels proches de rationnels, dans le sens où ils sont à distance au plus $P^{\nu-k}$ d'un rationnel dont le dénominateur est $\leq P^\nu$.

Lemme 3.1.1. *Les $\mathfrak{M}(q,a)$ sont deux à deux disjoints.*

Démonstration. Si $\alpha \in \mathfrak{M}(q,a) \cap \mathfrak{M}(q',a')$, avec $\frac{a}{q} \neq \frac{a'}{q'}$, alors $|aq' - a'q| \geq 1$ et

$$\frac{1}{P^{2\nu}} \leq \frac{1}{qq'} \leq \left|\frac{a}{q} - \frac{a'}{q'}\right| \leq \left|\alpha - \frac{a}{q}\right| + \left|\alpha - \frac{a'}{q'}\right| \leq \frac{2}{P^{k-\nu}}$$

ie. $P^{k-3\nu} \leq 2$, ce qui est impossible, car $P, k \geq 2$. □

Par la Remarque 1, $\mathfrak{M}(1,0) \cup \mathfrak{M}(1,1)$ et $\mathfrak{M}(q,a)$ $(q \geq 2)$ sont de mesure $2P^{\nu-k}$. Or $\#\{a \in [\![1,q]\!] \mid a \wedge q = 1\} = \phi(q)$, donc, par le Lemme 3.1.1.,

$$\begin{aligned}
\mu(\mathfrak{M}) &= \frac{2}{P^{k-\nu}} \sum_{1 \leq q \leq P^\nu} \phi(q) \\
&\leq \frac{2}{P^{k-\nu}} \sum_{1 \leq q \leq P^\nu} q \\
&\leq \frac{2}{P^{k-\nu}} \frac{P^\nu(P^\nu+1)}{2} \\
&\leq \frac{2}{P^{k-3\nu}} \underset{P \to +\infty}{\longrightarrow} 0
\end{aligned}$$

On définit maintenant les arcs mineurs comme le "reste" du segment $[0,1]$

$$\mathfrak{m} := [0,1] \backslash \mathfrak{M}$$

On a alors

$$\mu(\mathfrak{m}) = 1 - \mu(\mathfrak{M}) > 1 - \frac{2}{P^{k-3\nu}}$$

mais même si $\mu(\mathfrak{m})$ est "grand", dans le sens où $\mu(\mathfrak{m}) \underset{P \to +\infty}{\longrightarrow} 1$, on va montrer que l'intégrale sur $\mathfrak{m}$ ne contribue que de manière négligeable à $r_{k,s}(n)$.

3.2 Cas $k = 1$

Théorème 3.2.1. *Pour $s \geq 1$ et $n \geq 1$, on a :*

$$r_{k,s}(n) = \binom{n-1}{s-1} = \frac{n^{s-1}}{(s-1)!} + O(n^{s-2}).$$

Démonstration. Soit $n \geq s$, alors

$$n = a_1 + ... + a_s \text{ est une décomposition en } s \text{ parties} > 0$$

$$\iff n - s = (a_1 - 1) + ... + (a_s - 1) \text{ en est une en } s \text{ parties} \geq 0$$

De plus, $r_{1,s}(n) = R_{1,s}(n-s)$, avec

$$R_{1,s}(m) = \#\left\{(x_1, ..., x_s) \in \mathbb{N}^s \mid m = \sum_{i=1}^{s} x_i\right\}$$

Soit la fonction f définie sur $\mathbb{D} = \{z \in \mathbb{C} \mid |z| < 1\}$ par

$$f : z \longmapsto \frac{1}{1-z} = \sum_{n=0}^{+\infty} z^n$$

alors

$$f(z)^s = \sum_{n=0}^{+\infty} R_{1,s}(n) z^n$$

or

$$\begin{aligned}
f(z)^s &= \frac{1}{(1-z)^s} \\
&= \frac{1}{(s-1)!}\left(\frac{d}{dz}\right)^{s-1}\left(\frac{1}{1-z}\right) \\
&= \frac{1}{(s-1)!}\left(\frac{d}{dz}\right)^{s-1}\left(\sum_{n=0}^{+\infty} z^n\right) \\
&= \sum_{n=s-1}^{+\infty} \frac{n(n-1)...(n-s+2)}{(s-1)!} z^{n-s+1} \\
&= \sum_{n=s-1}^{+\infty} \binom{n}{s-1} z^{n-s+1} \\
&= \sum_{n=0}^{+\infty} \binom{n+s-1}{s-1} z^n
\end{aligned}$$

donc

$$R_{1,s}(n) = \binom{n+s-1}{s-1}$$

donc

$$r_{1,s}(n) = \binom{n-1}{s-1}$$

□

3.3 Intégrale sur les arcs mineurs

Théorème 3.3.1. *Soit $k \geq 2$ et $s \geq 2^k + 1$,*

$$\exists \delta_1 > 0 / \int_{\mathfrak{m}} F(\alpha)^s e(-n\alpha) d\alpha = O(P^{s-k-\delta_1}).$$

Démonstration. Posons $Q = P^{k-\nu}$. Par le théorème de Dirichlet, pour chaque $\alpha \in \mathbb{R}$, on associe une fraction $\frac{a}{q}$ telle que $1 \leq q \leq Q$, $a \wedge q = 1$ et

$$\left| \alpha - \frac{a}{q} \right| \leq \frac{1}{qQ} \leq \min\left(\frac{1}{Q}, \frac{1}{q^2} \right).$$

Si $\alpha \in \mathfrak{m}$ alors $\alpha \notin \mathfrak{M}(1,0) \cup \mathfrak{M}(1,1)$, donc

$$\frac{1}{Q} < \alpha < 1 - \frac{1}{Q} \text{ et } 1 \leq a \leq q-1.$$

Si $q \leq P^\nu$, alors

$$\left| \alpha - \frac{a}{q} \right| \leq \frac{1}{P^{k-\nu}} \implies \alpha \in \mathfrak{M}(q,a)$$

or $\mathfrak{M}(q,a) \subset \mathfrak{M} = [0,1] \backslash \mathfrak{m}$, ce qui est absurde, donc $P^\nu < q \leq P^{k-\nu}$.
Posons $K = 2^{k-1}$ et $f : x \mapsto \alpha x^k$, alors par l'inégalité de Weyl, on a :

$$\begin{aligned} F(\alpha) &\ll P^{1+\varepsilon} \left(P^{-1} + q^{-1} + P^{-k} q \right)^{1/K} \\ &\ll P^{1+\varepsilon} \left(P^{-1} + P^{-\nu} + P^{-k} P^{k-\nu} \right)^{1/K} \\ &\ll P^{1+\varepsilon-(\nu/K)} \end{aligned}$$

et par le lemme de Hua, on a finalement :

$$\begin{aligned} \left| \int_{\mathfrak{m}} F(\alpha)^s e(-n\alpha) d\alpha \right| &= \left| \int_{\mathfrak{m}} F(\alpha)^{s-2^k} F(\alpha)^{2^k} e(-n\alpha) d\alpha \right| \\ &\leq \max_{\alpha \in \mathfrak{m}} F(\alpha)^{s-2^k} \int_{\mathfrak{m}} |F(\alpha)|^{2^k} d\alpha \\ &\ll (P^{1+\varepsilon-(\nu/K)})^{s-2^k} P^{2^k-k+\varepsilon} \\ &= P^{s-k-\left(\frac{\nu(s-2^k)}{K} - (s-2^k+1)\varepsilon \right)} \end{aligned}$$

donc

$$\int_{\mathfrak{m}} F(\alpha)^s e(-n\alpha) d\alpha = O(P^{s-k-\delta_1})$$

avec $\delta_1 := \frac{\nu(s-2^k)}{K} - (s-2^k+1)\varepsilon$, où $\varepsilon > 0$ est suffisamment petit pour que $\delta_1 > 0$. $\square$

3.4 Intégrale sur les arcs majeurs

3.4.1 Première écriture de l'intégrale

Introduisons

$$v : \beta \mapsto \sum_{m=1}^{n} \frac{1}{k} m^{(1/k)-1} e(\beta m) \text{ et } S(q,a) := \sum_{r=1}^{q} e\left(\frac{ar^k}{q}\right).$$

On va montrer que si $\alpha \in \mathfrak{M}(q,a)$, alors

$$F(\alpha) = \frac{S(q,a)}{q} v\left(\alpha - \frac{a}{q}\right) + \text{"}terme\ erreur\text{"}.$$

On va commencer par estimer ces fonctions. On a clairement $|S(q,a)| \leq q$. Par l'inégalité de Weyl, $S(q,a) \ll q^{1-(1/K)+\varepsilon}$, donc

$$\frac{S(q,a)}{q} \ll q^{-(1/K)+\epsilon}.$$

Lemme 3.4.1. *Si $|\beta| \leq \frac{1}{2}$, alors $v(\beta) \ll \min(P, |\beta|^{-1/k})$.*

Démonstration. $f : x \mapsto \frac{1}{k} x^{(1/k)-1}$ définie pour $x \geq 1$ est continue, positive et décroissante, donc par comparaison série-intégrale, on a :

$$|v(\beta)| \leq \sum_{m=1}^{n} \frac{1}{k} m^{(1/k)-1} \leq f(1) + \int_1^n \frac{1}{k} x^{(1/k)-1} dx < n^{1/k} \ll P.$$

— Si $|\beta| \leq \frac{1}{n}$, alors $P \leq n^{1/k} \leq |\beta|^{-1/k}$, donc $v(\beta) \ll \min(P, |\beta|^{-1/k})$.

— Supposons $\frac{1}{n} < |\beta| \leq \frac{1}{2}$, alors $|\beta|^{-1/k} \ll P$. Posons $M := \lfloor |\beta|^{-1} \rfloor$, alors $M \leq \frac{1}{\beta} < M+1 \leq n$. Posons $U : t \mapsto \sum_{m \leq t} e(\beta m)$, on a démontré au cours du lemme 2.2.2. que

$$\forall \alpha \in \mathbb{R},\ \forall N_1, N_2 \in \mathbb{N}, N_1 < N_2 \Rightarrow \sum_{m=N_1+1}^{N_2} e(\alpha m) \ll \min(N_2 - N_1, \|\alpha\|^{-1})$$

ici, on a alors $U(t) \ll \|\beta\|^{-1} = |\beta|^{-1}$, car $|\beta| \leq \frac{1}{2}$. Par le critère d'Abel, en

utilisant que

$$f(m+1)-f(m)=\int_m^{m+1} f'(t)dt \text{ et } \forall t\in[m,m+1[,\ U(t)=U(m)$$

on a alors que

$$\begin{aligned}\sum_{m=M+1}^{n} f(m)e(\beta m) &= f(n)U(n)-f(M)U(M)-\int_M^n U(t)f'(t)dt\\ &\ll \frac{M^{(1/k)-1}}{|\beta|}\leq |\beta|^{-1/k}\ll \min(P,|\beta|^{-1/k})\end{aligned}$$

donc

$$v(\beta)=\sum_{m=1}^{M} f(m)e(\beta m)+\sum_{m=M+1}^{n} f(m)e(\beta m)\ll \min(P,|\beta|^{-1/k}).$$

□

Lemme 3.4.2. *Soit $(q,a)\in\mathbb{Z}^2$ tel que $1\leq q\leq P^\nu$, $0\leq a\leq q$ et $a\wedge q=1$. Si $\alpha\in\mathfrak{M}(q,a)$, alors*

$$F(\alpha)=\frac{S(q,a)}{q}v\left(\alpha-\frac{a}{q}\right)+O(P^{2\nu}).$$

Démonstration. Posons $\beta=\alpha-\frac{a}{q}$, alors $|\beta|\leq P^{\nu-k}$, par définition de $\mathfrak{M}(q,a)$, et

$$\begin{aligned}F(\alpha)-\frac{S(q,a)}{q}v(\beta) &= \sum_{m=1}^{P} e(\alpha m^k)-\frac{S(q,a)}{q}\sum_{m=1}^{n}\frac{1}{k}m^{(1/k)-1}e(\beta m)\\ &= \sum_{m=1}^{P} e\left(\frac{am^k}{q}\right)e(\beta m^k)-\frac{S(q,a)}{q}\sum_{m=1}^{n}\frac{1}{k}m^{(1/k)-1}e(\beta m)\\ &= \sum_{m=1}^{n} u(m)e(\beta m),\ \text{car } P=\lfloor n^{1/k}\rfloor\end{aligned}$$

$$\text{avec } u(m):=\begin{cases} e(\frac{am}{q})-\frac{S(q,a)}{q}\frac{1}{k}m^{(1/k)-1} & \text{si m est une puissance de k}\\ -\frac{S(q,a)}{q}\frac{1}{k}m^{(1/k)-1} & \text{sinon}\end{cases}$$

— Soit $y \geq 1$, comme $|S(q,a)| \leq q$, alors :

$$\begin{aligned}\sum_{1\leq m\leq y} e\left(\frac{am^k}{q}\right) &= \sum_{r=1}^{q} e\left(\frac{ar^k}{q}\right) \#\{1 \leq m \leq y \mid m \equiv r[q]\}, \text{ par périodicité de } e \\ &= \sum_{r=1}^{q} e\left(\frac{ar^k}{q}\right)\left(\frac{y}{q} + O(1)\right) \\ &= y\frac{S(q,a)}{q} + O(q)\end{aligned}$$

— Soit $t \geq 1$, comme $v(\beta) \ll P$, alors en posant $U(t) := \sum_{1\leq m\leq t} u(m)$, on a :

$$\begin{aligned}U(t) &= \sum_{1\leq m\leq t^{1/k}} e\left(\frac{am^k}{q}\right) - \frac{S(q,a)}{q}\sum_{1\leq m\leq t}\frac{1}{k}m^{(1/k)-1} \\ &= t^{1/k}\frac{S(q,a)}{q} + O(q) - \frac{S(q,a)}{q}\left(t^{1/k} + O(1)\right) \\ &= O(q)\end{aligned}$$

— Par le critère d'Abel, on a :

$$\begin{aligned}\sum_{m=1}^{n} u(m)e(\beta m) &= e(\beta n)U(n) - \int_1^n (2i\beta\pi e(\beta t))U(t)dt \\ &= O(q) - 2i\pi\beta\int_1^n e(\beta t)O(q)dt \\ &\ll (1+|\beta|n)q \\ &\ll (1+P^{\nu-k}P^k)P^\nu \\ &\ll P^{2\nu}\end{aligned}$$

□

Théorème 3.4.3. *Soit*

$$\sigma(n,Q) := \sum_{1\leq q\leq Q}\sum_{\substack{a=0\\ a\wedge q=1}}^{q}\left(\frac{S(q,a)}{q}\right)^s e\left(-\frac{na}{q}\right) \text{ et } J^*(n) := \int_{-P^{\nu-k}}^{P^{\nu-k}} v(\beta)^s e(-n\beta)d\beta$$

alors, en posant $\delta_2 := 1 - 5\nu > 0$, *on a :*

$$\int_{\mathfrak{M}} F(\alpha)^s e(-n\alpha)d\alpha = \sigma(n,P^\nu)J^*(n) + O(P^{s-k-\delta_2}).$$

Démonstration. Soit $\alpha \in \mathfrak{M}(q,a)$ et $\beta = \alpha - \frac{a}{q}$. Posons $V = V(\alpha,q,a) = \frac{S(q,a)}{q} v(\beta)$. Comme $|S(q,a)| \leq q$, alors le lemme 3.4.1. donne que $|V| \ll P$. Posons $F = F(\alpha)$, alors $|F| \leq P$. Or le lemme 3.4.2. donne que $F - V = O(P^{2\nu})$, donc

$$F^s - V^s = (F-V)\sum_{i=0}^{s-1} F^i V^{s-1-i} \ll P^{2\nu} P^{s-1} = P^{s-1+2\nu}.$$

Comme $\mu(\mathfrak{M}) \ll P^{3\nu-k}$, alors

$$\int_{\mathfrak{M}} |F^s - V^s| d\alpha \ll P^{3\nu-k} P^{s-1+2\nu} = P^{s-k-\delta_2}, \text{ avec } \delta_2 = 1 - 5\nu > 0$$

donc

$$\begin{aligned}\int_{\mathfrak{M}} F(\alpha)^s e(-n\alpha) d\alpha &= \int_{\mathfrak{M}} V^s e(-n\alpha) d\alpha + O(P^{s-k-\delta_2}) \\ &= \sum_{1 \leq q \leq P^\nu} \sum_{\substack{a=0 \\ a \wedge q = 1}}^{q} \int_{\mathfrak{M}(q,a)} V^s e(-n\alpha) d\alpha + O(P^{s-k-\delta_2})\end{aligned}$$

— pour $q \geq 2$,

$$\begin{aligned}\int_{\mathfrak{M}(q,a)} V^s e(-n\alpha) d\alpha &= \int_{\frac{a}{q} - P^{\nu-k}}^{\frac{a}{q} + P^{\nu-k}} V^s e(-n\alpha) d\alpha \\ &= \int_{-P^{\nu-k}}^{P^{\nu-k}} V\left(\beta + \frac{a}{q}, q, a\right)^s e\left(-n\left(\beta + \frac{a}{q}\right)\right) d\beta \\ &= \left(\frac{S(q,a)}{q}\right)^s e\left(-\frac{na}{q}\right) \int_{-P^{\nu-k}}^{P^{\nu-k}} v(\beta)^s e(-n\beta) d\beta \\ &= \left(\frac{S(q,a)}{q}\right)^s e\left(-\frac{na}{q}\right) J^*(n)\end{aligned}$$

— pour $q = 1$, $V(\alpha,1,0) = v(\alpha)$ et $V(\alpha,1,1) = v(\alpha-1)$, alors :

$$\begin{aligned}\int_{\mathfrak{M}(1,0) \cup \mathfrak{M}(1,1)} V^s e(-n\alpha) d\alpha &= \int_0^{P^{\nu-k}} v(\alpha)^s e(-n\alpha) d\alpha + \int_{1-P^{\nu-k}}^{1} v(\alpha-1)^s e(-n\alpha) d\alpha \\ &= \int_0^{P^{\nu-k}} v(\beta)^s e(-n\beta) d\beta + \int_{-P^{\nu-k}}^{0} v(\beta)^s e(-n\beta) d\beta \\ &= J^*(n)\end{aligned}$$

donc

$$\int_{\mathfrak{M}} F(\alpha)^s e(-n\alpha)d\alpha = \sum_{1\le q\le P^\nu} \sum_{\substack{a=0\\ a\wedge q=1}}^{q} \left(\frac{S(q,a)}{q}\right)^s e\left(-\frac{na}{q}\right) J^*(n) + O(P^{s-k-\delta_2})$$
$$= \sigma(n, P^\nu)J^*(n) + O(P^{s-k-\delta_2}).$$

□

3.4.2 Intégrale singulière

Définition 3.4.1.

$$J(n) := \int_{-1/2}^{1/2} v(\beta)^s e(-n\beta)d\beta$$

est appelée intégrale singulière pour le problème de Waring.

Théorème 3.4.4. *Il existe $\delta_3 > 0$ telle que $J(n) \ll P^{s-k}$ et*

$$J^*(n) = J(n) + O(P^{s-k-\delta_3}).$$

Démonstration. Par le lemme 3.4.1.,

$$\begin{aligned} J(n) &\ll \int_0^{1/2} \min(p, |\beta|^{-1/k})^s d\beta \\ &= \int_0^{1/n} P^s d\beta + \int_{1/n}^{1/2} \beta^{-s/k} d\beta \\ &\ll n^{\frac{s-k}{k}} \\ &\ll P^{s-k} \end{aligned}$$

donc

$$\begin{aligned} J(n) - J^*(n) &= \int_{P^{\nu-k}\le|\beta|\le 1/2} v(\beta)^s e(-n\beta)d\beta \\ &\ll \int_{P^{\nu-k}}^{1/2} |v(\beta)|^s d\beta \\ &\ll \int_{P^{\nu-k}}^{1/2} \beta^{-s/k} d\beta \\ &\ll P^{(k-\nu)((s/k)-1)} = P^{s-k-\delta_3} \end{aligned}$$

avec $\delta_3 = \nu(\frac{s}{k} - 1) > 0$, car $s \geq 2^k + 1$. □

Lemme 3.4.5. *Soit $\alpha, \beta \in \mathbb{R}$ tels que $0 < \beta < 1$ et $\alpha \geq \beta$, alors*

$$\sum_{m=1}^{n-1} m^{\beta-1}(n-m)^{\alpha-1} = n^{\alpha+\beta-1}\frac{\Gamma(\alpha)\Gamma(\beta)}{\Gamma(\alpha+\beta)} + O(n^{\alpha-1}).$$

Démonstration. Soit $g : x \mapsto x^{\beta-1}(n-x)^{\alpha-1}$ positive, continue et intégrable sur $]0, n[$.

$$\int_0^n g(x)dx = n^{\alpha+\beta-1}\int_0^1 t^{\beta-1}(1-t)^{\alpha-1}dt = n^{\alpha+\beta-1}B(\alpha,\beta) = n^{\alpha+\beta-1}\frac{\Gamma(\alpha)\Gamma(\beta)}{\Gamma(\alpha+\beta)}$$

$$\begin{aligned}
\Gamma(\alpha)\Gamma(\beta) &= \int_0^{+\infty} e^{-t_1}t_1^{\alpha-1}dt_1 \int_0^{+\infty} e^{-t_2}t_2^{\beta-1}dt_2 \\
&= 4\int_0^{+\infty}\int_0^{+\infty} e^{-u^2}e^{-v^2}u^{2\alpha-2}v^{2\beta-2}uv\ dudv \\
&= 4\int_0^{+\infty}\int_0^{+\infty} e^{-(u^2+v^2)}u^{2\alpha-1}v^{2\beta-1}dudv \\
&= 4\int_0^{+\infty}\int_0^{\pi/2} e^{-r^2}r^{2(\alpha+\beta-1)}\cos^{2\alpha-1}\theta\sin^{2\beta-1}\theta\ rdrd\theta \\
&= \int_0^{+\infty} e^{-(r^2)}(r^2)^{\alpha+\beta-1}2rdr\int_0^{\pi/2} 2(\cos^2\theta)^{\alpha-1}(\sin^2\theta)^{\beta-1}\cos\theta\sin\theta\ d\theta \\
&= \int_0^{+\infty} e^{-t}t^{\alpha+\beta-1}dt\int_1^0 -t^{\alpha-1}(1-t)^{\beta-1}dt \\
&= \Gamma(\alpha+\beta)B(\alpha,\beta)
\end{aligned}$$

— si $\alpha \geq 1$, alors

$$g'(x) = g(x)\left(\frac{\beta-1}{x} - \frac{\alpha-1}{n-x}\right) < 0$$

donc g décroît strictement sur $]0, n[$, donc par comparaison série-intégrale

$$0 < \int_0^n g(x)dx - \sum_{m=1}^{n-1} g(m) < \int_0^1 g(x)dx \leq n^{\alpha-1}\int_0^1 x^{\beta-1}dx = \frac{n^{\alpha-1}}{\beta}$$

— si $\beta \leq \alpha < 1$, alors $0 < \alpha + \beta < 2$ et g a un minimul local en

$$c = \frac{(1-\beta)n}{2-\alpha-\beta} \in \left[\frac{n}{2}, n\right[$$

— Comme g est strictement décroissante sur $]0, c[$, alors

$$\begin{aligned}\int_c^n g(x)dx &> \sum_{m=1}^{\lfloor c\rfloor} g(m)\\ &\geq \int_1^{\lfloor c\rfloor} g(x)dx + g(\lfloor c\rfloor)\\ &> \int_1^c g(x)dx\\ &\geq \int_0^c g(x)dx - \frac{n^{\alpha-1}}{\beta}\end{aligned}$$

— Comme g est strictement croissante sur $]c, n[$, alors

$$\begin{aligned}\int_c^n g(x)dx &> \sum_{m=\lfloor c\rfloor+1}^{n-1} g(m)\\ &\geq \int_{\lfloor c\rfloor+1}^{n-1} g(x)dx + g(\lfloor c\rfloor+1)\\ &> \int_c^{n-1} g(x)dx\\ &\geq \int_c^n g(x)dx - \frac{n^{\beta-1}}{\alpha}\end{aligned}$$

donc

$$0 < \int_0^n g(x)dx - \sum_{m=1}^{n-1} g(m) < \frac{n^{\alpha-1}}{\beta} + \frac{n^{\beta-1}}{\alpha} \leq \frac{2n^{\alpha-1}}{\beta}$$

donc

$$\sum_{m=1}^{n-1} g(m) = \int_0^n g(x)dx + O(n^{\alpha-1}).$$

□

Théorème 3.4.6. *Si $s \geq 2$, alors*

$$J(n) = \Gamma\left(1+\frac{1}{k}\right)^s \Gamma\left(\frac{s}{k}\right)^{-1} n^{(s/k)-1} + O(n^{((s-1)/k)-1}).$$

Démonstration. Posons

$$J_s(n) = \int_{-1/2}^{1/2} v(\beta)^s e(-n\beta)d\beta.$$

Nous allons la calculer par récurrence sur s.

— Comme $v(\beta) = \sum_{m=1}^{n} \frac{1}{k} m^{(1/k)-1} e(\beta m)$, alors

$$\begin{aligned} v(\beta)^s &= \frac{1}{k^s} \sum_{m_1=1}^{n} ... \sum_{m_s=1}^{n} \prod_{i=1}^{s} m_i^{(1/k)-1} e(\beta m_i) \\ &= \frac{1}{k^s} \sum_{m_1=1}^{n} ... \sum_{m_s=1}^{n} (m_1...m_s)^{(1/k)-1} e(\beta(m_1 + ... + m_s)) \end{aligned}$$

donc

$$\begin{aligned} J_s(n) &= \frac{1}{k^s} \sum_{m_1=1}^{n} ... \sum_{m_s=1}^{n} (m_1...m_s)^{(1/k)-1} \int_{-1/2}^{1/2} e(\beta(m_1 + ... + m_s - n)) d\beta \\ &= \frac{1}{k^s} \sum_{\substack{m_1+...+m_s=n \\ 1 \leq m_i \leq n}} (m_1...m_s)^{(1/k)-1} \end{aligned}$$

— Pour $s = 2$, par le lemme 3.4.5., avec $\alpha = \beta = 1/k \in]0, 1[$, on a :

$$\begin{aligned} J_2(n) &= \frac{1}{k^2} \sum_{m=1}^{n} m^{(1/k)-1} (n-m)^{(1/k)-1} \\ &= \frac{1}{k^2} \frac{\Gamma(1/k)^2}{\Gamma(2/k)} n^{(2/k)-1} + O(n^{(1/k)-1}) \\ &= \frac{\Gamma(1 + (1/k))^2}{\Gamma(2/k)} n^{(2/k)-1} + O(n^{(1/k)-1}) \end{aligned}$$

— Soit $s \geq 2$, supposons le théorème vrai au rang s, alors :

$$\begin{aligned} J_{s+1}(n) &= \int_{-1/2}^{1/2} v(\beta)^{s+1} e(-n\beta) d\beta \\ &= \int_{-1/2}^{1/2} \sum_{m=1}^{n} \frac{1}{k} m^{(1/k)-1} e(\beta m) v(\beta)^s e(-n\beta) d\beta \\ &= \sum_{m=1}^{n} \frac{1}{k} m^{(1/k)-1} J_s(n-m) \\ &\overset{H.R.}{=} \frac{\Gamma(1 + (1/k))^s}{\Gamma(s/k)} \sum_{m=1}^{n} \frac{1}{k} m^{(1/k)-1} (n-m)^{(s/k)-1} \\ &\quad + O\left(\sum_{m=1}^{n} \frac{1}{k} m^{(1/k)-1} (n-m)^{((s-1)/k)-1} \right) \end{aligned}$$

or, par le lemme 3.4.5., avec $\alpha = s/k$ et $\beta = 1/k$, on a :

$$\sum_{m=1}^{n-1} \frac{1}{k} m^{(1/k)-1}(n-m)^{(s/k)-1} = \frac{(1/k)\Gamma(1/k)\Gamma(s/k)}{\Gamma((s+1)/k)} n^{((s+1)/k)-1} + O(n^{(s/k)-1})$$

et de même, avec $\alpha = (s-1)/k$ et $\beta = 1/k$, on a :

$$\sum_{m=1}^{n} \frac{1}{k} m^{(1/k)-1}(n-m)^{((s-1)/k)-1} = O(n^{(s/k)-1})$$

donc

$$\begin{aligned} J_{s+1}(n) &= \frac{(1/k)\Gamma(1/k)\Gamma(s/k)}{\Gamma((s+1)/k)} \frac{\Gamma(1+(1/k))^s}{\Gamma(s/k)} n^{((s+1)/k)-1} + O(n^{(s/k)-1}) \\ &= \frac{\Gamma(1+(1/k))^{s+1}}{\Gamma((s+1)/k)} n^{((s+1)/k)-1} + O(n^{(s/k)-1}) \end{aligned}$$

□

3.4.3 Série singulière

Dans le théorème 3.4.3., on a introduit la fonction

$$\sigma(n, Q) = \sum_{1 \leq q \leq Q} A_n(q), \text{ avec } A_n(q) = \sum_{\substack{a=0 \\ a \wedge q = 1}}^{q} \left(\frac{S(q,a)}{q}\right)^s e\left(-\frac{na}{q}\right).$$

Définition 3.4.2. *On définit la série singulière du problème de Waring comme la fonction arithmétique*

$$\sigma(n) := \sum_{q=1}^{+\infty} A_n(q).$$

Soit $\varepsilon \in \left]0, \frac{1}{sK}\right[$. Comme $s \geq 2^k + 1 = 2K + 1$, alors $\frac{s}{K} - 1 - s\varepsilon \geq 1 + \frac{1}{K} - s\varepsilon = 1 + \delta_4$, où $\delta_4 := \frac{1}{K} - s\varepsilon$. On a vu au début du paragraphe "Première écriture de l'intégrale" que $\frac{S(q,a)}{q} \ll q^{-(1/K)+\varepsilon}$, alors

$$A_n(q) \ll \frac{q}{q^{(s/K)-s\varepsilon}} \leq \frac{1}{q^{1+\delta_4}}$$

donc $\sum A_n(q)$ converge absolument et uniformément (Riemann). En particulier, il

existe $c_2 = c_2(k,s)$ telle que pour tout $n \in \mathbb{N}^*$, $|\sigma(n)| < c_2$. De plus,

$$\sigma(n) - \sigma(n, P^\nu) = \sum_{q > P^\nu} A_n(q) \ll \sum_{q > P^\nu} \frac{1}{q^{1+\delta_4}} \ll P^{-\nu\delta_4}.$$

On va montrer que :

$$\forall n \in \mathbb{N}^*,\ \sigma(n) \in \mathbb{R}_+^* \text{ et } \exists c_1 = c_1(k,s) > 0 / \ \forall n \in \mathbb{N}^*,\ 0 < c_1 < \sigma(n) < c_2.$$

On commence par voir que A_n est une fonction multiplicative (en q).

Lemme 3.4.7. *Si $q \wedge r = 1$, alors $S(qr, ar + bq) = S(q,a)S(r,b)$.*

Démonstration. Comme $q \wedge r = 1$, les ensembles $\{xr \mid 1 \leq x \leq q\}$ et $\{yq \mid 1 \leq y \leq r\}$ sont des systèmes complets de résidus modulo q et r respectivement, ie. les ensembles contiennent q et r éléments qui ne sont pas deux à deux congrus modulo q et r, on peut alors les mettre en bijection avec $[\![0, q-1]\!]$ et $[\![0, r-1]\!]$, ou $[\![1, q]\!]$ et $[\![1, r]\!]$ en conservant les propriétés de non congruence deux à deux. Comme chaque classe de congruence modulo qr peut être écrite de façon unique de la forme $xr + yq$, avec $1 \leq x \leq q$, $1 \leq y \leq r$, on a que :

$$\begin{aligned}
S(qr, ar+bq) &= \sum_{m=1}^{qr} e\left(\frac{(ar+bq)m^k}{qr}\right) \\
&= \sum_{x=1}^{q}\sum_{y=1}^{r} e\left(\frac{(ar+bq)(xr+yq)^k}{qr}\right) \\
&= \sum_{x=1}^{q}\sum_{y=1}^{r} e\left(\left(\frac{ar+bq}{qr}\right)\sum_{i=0}^{k}\binom{k}{i}(xr)^i(yq)^{k-i}\right) \\
&= \sum_{x=1}^{q}\sum_{y=1}^{r} e\left(\left(\frac{ar+bq}{qr}\right)\left((xr)^k + (yq)^k\right)\right) \\
&= \sum_{x=1}^{q}\sum_{y=1}^{r} e\left(\frac{a(xr)^k}{q}\right) e\left(\frac{b(yq)^k}{r}\right) \\
&= \sum_{x=1}^{q} e\left(\frac{ax^k}{q}\right)\sum_{y=1}^{r} e\left(\frac{by^k}{r}\right) \\
&= S(q,a)S(r,b)
\end{aligned}$$

□

Lemme 3.4.8. *Si $q \wedge r = 1$, alors $A_n(qr) = A_n(q)A_n(r)$, ie. A_n est multiplicative.*

Démonstration. Soit $c \in [\![0, qr]\!]$, si $c \wedge qr = 1$, alors $\exists!(a, b) \in [\![0, q]\!] \times [\![0, r]\!]$ / $a \wedge q = b \wedge r = 1$ et $c \equiv ar + bq\ [qr]$, alors :

$$\begin{aligned}
A_n(qr) &= \sum_{\substack{c=0 \\ c\wedge qr=1}}^{qr} \left(\frac{S(qr,c)}{qr}\right)^s e\left(-\frac{nc}{qr}\right) \\
&= \sum_{\substack{a=0 \\ a\wedge q=1}}^{q} \sum_{\substack{b=0 \\ b\wedge r=1}}^{r} \left(\frac{S(qr,ar+bq)}{qr}\right)^s e\left(-\frac{n(ar+bq)}{qr}\right) \\
&= \sum_{\substack{a=0 \\ a\wedge q=1}}^{q} \sum_{\substack{b=0 \\ b\wedge r=1}}^{r} \left(\frac{S(q,a)}{q}\right)^s \left(\frac{S(r,b)}{r}\right)^s e\left(-\frac{na}{q}\right) e\left(-\frac{nb}{r}\right) \\
&= \sum_{\substack{a=0 \\ a\wedge q=1}}^{q} \left(\frac{S(q,a)}{q}\right)^s e\left(-\frac{na}{q}\right) \sum_{\substack{b=0 \\ b\wedge r=1}}^{r} \left(\frac{S(r,b)}{r}\right)^s e\left(-\frac{nb}{r}\right) \\
&= A_n(q)A_n(r)
\end{aligned}$$

□

Pour $q \in \mathbb{N}^*$, notons

$$M_n(q) := \#\left\{(x_1, ..., x_s) \in [\![1, q]\!]^s \mid \sum_{i=1}^{s} x_i^k \equiv n[q]\right\}.$$

Lemme 3.4.9. *Soit $s \geq 2^k + 1$. Pour chaque $p \in \mathcal{P}$, $\chi_n(p) := 1 + \sum_{h=1}^{+\infty} A_n(p^h)$ converge et*

$$\chi_n(p) = \lim_{h\to+\infty} \frac{M_n(p^h)}{p^{h(s-1)}}.$$

Démonstration. Comme, pour $h \geq 1$, $A_n(p^h) \ll p^{-h(1+\delta_4)}$, on a convergence de $\chi_n(p)$.

— Si $a \wedge q = d$, alors

$$\begin{aligned}
S(q,a) &= \sum_{x=1}^{q} e\left(\frac{ax^k}{q}\right) = \sum_{x=1}^{q} e\left(\frac{(a/d)x^k}{q/d}\right) \\
&= d\sum_{x=1}^{q/d} e\left(\frac{(a/d)x^k}{q/d}\right) = dS\left(\frac{q}{d}, \frac{a}{d}\right)
\end{aligned}$$

— Comme

$$\frac{1}{q}\sum_{a=1}^{q} e\left(\frac{am}{q}\right) = \begin{cases} 1 & \text{si } m \equiv 0\ [q] \\ 0 & \text{sinon} \end{cases}$$

alors, pour $x_1, ..., x_s$ entiers :

$$\frac{1}{q}\sum_{a=1}^{q} e\left(\frac{a(x_1^k + ... + x_s^k - n)}{q}\right) = \begin{cases} 1 & \text{si } x_1^k + ... + x_s^k \equiv n\ [q] \\ 0 & \text{sinon} \end{cases}$$

et

$$\begin{aligned} M_n(q) &= \sum_{x_1=1}^{q} ... \sum_{x_s=1}^{q} \frac{1}{q}\sum_{a=1}^{q} e\left(\frac{a(x_1^k + ... + x_s^k - n)}{q}\right) \\ &= \frac{1}{q}\sum_{a=1}^{q}\sum_{x_1=1}^{q} e\left(\frac{ax_1^k}{q}\right) ... \sum_{x_s=1}^{q} e\left(\frac{ax_s^k}{q}\right) e\left(-\frac{na}{q}\right) \\ &= \frac{1}{q}\sum_{a=1}^{q} S(q,a)^s e\left(-\frac{na}{q}\right) \\ &= \frac{1}{q}\sum_{d|q}\sum_{\substack{a=1 \\ a\wedge q=d}}^{q} S(q,a)^s e\left(-\frac{na}{q}\right) \\ &= \frac{1}{q}\sum_{d|q}\sum_{\substack{a=1 \\ a\wedge q=d}}^{q} d^s S\left(\frac{q}{d}, \frac{a}{d}\right)^s e\left(-\frac{n(a/d)}{q/d}\right) \\ &= \frac{1}{q}\sum_{d|q}\sum_{\substack{a=1 \\ a\wedge q=d}}^{q} q^s \left(\frac{S\left(\frac{q}{d}, \frac{a}{d}\right)}{q/d}\right)^s e\left(-\frac{n(a/d)}{q/d}\right) \\ &= q^{s-1}\sum_{d|q} A_n\left(\frac{q}{d}\right) \end{aligned}$$

donc, pour chaque $q \geq 1$,

$$\sum_{d|q} A_n\left(\frac{q}{d}\right) = q^{1-s} M_n(q).$$

— En particulier, pour $q = p^h$,

$$1 + \sum_{j=1}^{h} A_n(p^j) = \sum_{d|p^h} A_n\left(\frac{p^h}{d}\right) = p^{h(1-s)} M_n(p^h)$$

donc

$$\chi_n(p) = \lim_{h\to+\infty} \left(1 + \sum_{j=1}^{h} A_n(p^j)\right) = \lim_{h\to+\infty} p^{h(1-s)} M_n(p^h).$$

□

Lemme 3.4.10. *Si $s \geq 2^k + 1$, alors $\sigma(n) = \prod_{p\in\mathcal{P}} \chi_n(p)$.*
De plus, il existe $c_2 = c_2(k,s) > 0$ telle que pour tout n, $0 < \sigma(n) < c_2$, et il existe $p_0 = p_0(k,s) \in \mathcal{P}$ tel que pour tout $n \geq 1$,

$$\frac{1}{2} \leq \prod_{p>p_0} \chi_n(p) \leq \frac{3}{2}.$$

Lemme 3.4.11. *Soit f une fonction multiplicative non identiquement nulle. Si $\sum_{n\geq 1} f(n)$ converge absolument, alors*

$$\sum_{n=1}^{+\infty} f(n) = \prod_{p\in\mathcal{P}} \left(1 + \sum_{k=1}^{+\infty} f(p^k)\right).$$

Démonstration. Lemme 3.4.11. Si $\sum_{n\geq 1} |f(n)| < +\infty$, alors :

$$\forall p \in \mathcal{P},\ a_p = \sum_{k=1}^{+\infty} f(p^k) < +\infty$$

donc

$$\sum_{p\in\mathcal{P}} |a_p| \leq \sum_{p\in\mathcal{P}} \sum_{k=1}^{+\infty} |f(p^k)| < \sum_{n=1}^{+\infty} |f(n)| < +\infty$$

donc $\prod_{p\in\mathcal{P}} (1 + a_p)$ converge.
Soit $\varepsilon > 0$ et $n_0 \in \mathbb{N}$ tels que $\sum_{n>n_0} |f(n)| < \varepsilon$.
Pour $n \geq 1$, notons $P(n) = \max\{p \in \mathcal{P} \mid p \mid n\}$. Soit $N \geq n_0$, par unicité de la factorisation en produits de facteurs premiers, on a

$$\prod_{p\leq N} \left(1 + \sum_{k=1}^{+\infty} f(p^k)\right) = \sum_{P(n)\leq N} f(n)$$

donc

$$\begin{aligned}\left|\sum_{n=1}^{+\infty} f(n) - \prod_{p\leq N}\left(1+\sum_{k=1}^{+\infty} f(p^k)\right)\right| &= \left|\sum_{n=1}^{+\infty} f(n) - \sum_{P(n)\leq N} f(n)\right| \\ &\leq \sum_{P(n)>N} |f(n)| \\ &\leq \sum_{n>N} |f(n)| \\ &\leq \sum_{n>n_0} |f(n)| \\ &< \varepsilon\end{aligned}$$

donc

$$\sum_{n=1}^{+\infty} f(n) = \lim_{N\to+\infty} \prod_{p\leq N}\left(1+\sum_{k=1}^{+\infty} f(p^k)\right) = \prod_{p\in\mathcal{P}}\left(1+\sum_{k=1}^{+\infty} f(p^k)\right).$$

□

Démonstration. Lemme 3.4.10. Si $s \geq 2^k+1$, comme $A_n(q) \ll q^{-(1+\delta_4)}$, alors $\sum_q |A_n(q)| < +\infty$, avec A_n multiplicative, donc $\prod_{p\in\mathcal{P}} \chi_n(p)$ converge.
En particulier, $\forall n,\ \forall p,\ \chi_n(p) \neq 0$. Or, $\forall h,\ M_n(p^h)p^{-h(s-1)} \geq 0$, donc $\chi_n(p) \geq 0$, donc $\chi_n(p) > 0$, donc $\sigma(n) > 0$, et

$$0 < \sigma(n) \ll \sum_{q=1}^{+\infty} \frac{1}{q^{1+\delta_4}} =: c_2 < +\infty$$

De plus,

$$|\chi_n(p) - 1| \leq \sum_{h=1}^{+\infty} |A_n(p^h)| \ll \sum_{h=1}^{+\infty} \frac{1}{p^{h(1+\delta_4)}} \ll \frac{1}{p^{1+\delta_4}}$$

donc il existe $c = c(k,s) > 0$ telle que

$$\forall n,\ \forall p,\ 1 - \frac{c}{p^{1+\delta_4}} \leq \chi_n(p) \leq 1 + \frac{c}{p^{1+\delta_4}}$$

or $\sum c/(p^{1+\delta_4}) < +\infty$, donc

$$\prod_{p\in\mathcal{P}}\left(1 \pm \frac{c}{p^{1+\delta_4}}\right) \text{ convergent,}$$

donc il existe $p_0 = p_0(k,s) \in \mathcal{P}$ tel que

$$\prod_{p>p_0}\left(1-\frac{c}{p^{1+\delta_4}}\right) \geq \frac{1}{2} \text{ et } \prod_{p>p_0}\left(1+\frac{c}{p^{1+\delta_4}}\right) \leq \frac{3}{2}$$

donc

$$\frac{1}{2} \leq \prod_{p>p_0} \chi_n(p) \leq \frac{3}{2}.$$

□

On veut montrer que $\sigma(n)$ est borné "loin de 0" uniformément pour tout n. Par le lemme 3.4.10, il suffit de montrer que pour tout $p \in \mathcal{P}$, $\chi_n(p)$ est uniformément borné "loin de 0". Soit $p \in \mathcal{P}$, $k = p^\tau k_0$, avec $\tau \geq 0$ et $p \wedge k_0 = 1$. On définit

$$\gamma = \begin{cases} \tau+1 & \text{si } p > 2 \\ \tau+2 & \text{si } p = 2 \end{cases}$$

Lemme 3.4.12. *Soit m un entier non multiple de p. Si $x^k \equiv m[p^\gamma]$ admet une solution, alors pour tout $h \geq \gamma$, $y^k \equiv m[p^h]$ admet une solution.*

Démonstration. Soit m un entier non multiple de p.

— Si $p > 2$, pour $h \geq \tau + 1$, on a

$$k \wedge \phi(p^h) = k_0 p^\tau \wedge (p-1)p^{h-1} = (k_0 \wedge (p-1))p^\tau = k \wedge \phi(p^\gamma).$$

L'ensemble des classes d'équivalence pour la congruence modulo p^h, qui sont premiers avec p, ie. $(\mathbb{Z}/p^h\mathbb{Z})^\times$, est un groupe cyclique d'ordre $\phi(p^h) = (p-1)p^{h-1}$. Soit g un générateur de ce groupe cyclique, appelé racine primitive modulo p^h, alors g est aussi une racine primitive modulo p^γ.
Soit x une solution de $x^k \equiv m[p^\gamma]$, $x \wedge p = 1$. Choisissons r et u entiers tels que $x \equiv g^u[p^h]$ et $m \equiv g^r[p^h]$, or $ku \equiv r[\phi(p^\gamma)]$, donc $r \equiv 0[k \wedge \phi(p^\gamma)]$, donc $r \equiv 0[k \wedge \phi(p^h)]$, donc il existe un entier v tel que $kv \equiv r[\phi(p^h)]$. Posons $y = g^v$, alors $y^k \equiv m[p^h]$.

— Si $p = 2$, alors m est impair, donc x solution est aussi impair.

  — Si $\tau = 0$, alors $k = k_0$ est impair. Or, $y \in \{\bar{z} \in \mathbb{Z}/p^h\mathbb{Z} \mid z \text{ impair}\}$ ssi y^k aussi, donc $\forall h \geq 1,\ y^k \equiv m[p^h]$ admet une solution.

  — Si $\tau \geq 1$, alors k est pair et $m \equiv x^k \equiv 1[4]$, car x est impair. De plus, $x^k = (-x)^k$, donc on peut supposer que $x \equiv 1[4]$.
  $\{z \in \mathbb{Z}/2^h\mathbb{Z} \mid z \equiv 1[4]\}$ est un sous groupe cyclique d'ordre 2^{h-2}, engendré par 5, car $\mathbb{Z}/2^h\mathbb{Z}$ peut être partitionné en 4 parties, de même cardinal (ceux congrus à i modulo 4, $0 \leq i \leq 3$) et que celui indroduit contient $\langle 5 \rangle$, qui est

d'ordre 2^{h-2}, donc égal à $\langle 5 \rangle$.
Soit r et u entiers tels que $m \equiv 5^r[2^h]$ et $x \equiv 5^u[2^h]$. Comme $x^k \equiv m[2^\gamma]$, alors $ku \equiv r[2^{\gamma-2}]$, donc r est multiple de $k \wedge 2^\tau = 2^\tau = k \wedge 2^{h-2}$, donc il existe un entier v tel que $kv \equiv r[2^{h-2}]$. Posons $y = 5^v$, alors $y^k \equiv m[2^h]$.

□

Lemme 3.4.13. *Soit $p \in \mathcal{P}$. S'il existe des entiers $a_1, ..., a_s$ non tous divisibles par p tels que*

$$a_1^k + ... + a_s^k \equiv n \ [p^\gamma],$$

alors

$$\chi_n(p) \geq p^{\gamma(1-s)} > 0.$$

Démonstration. Supposons que $a_1 \not\equiv 0[p]$. Soit $h > \gamma$, pour tout $i \in [\![2, s]\!]$, il existe $p^{h-\gamma}$ entiers x_i deux à deux incongrus tels que $x_i \equiv a_i[p^h]$. Comme

$$x_1^k \equiv n - \sum_{i=2}^{s} x_i^k \ [p^\gamma]$$

est résoluble avec $x_1 = a_1 \not\equiv 0[p]$, par le lemme 3.4.12., il existe y_1 tel que

$$y_1^k \equiv n - \sum_{i=2}^{s} x_i^k \ [p^h]$$

donc $M_n(p^h) \geq p^{(h-\gamma)(s-1)}$, donc

$$\chi_n(p) = \lim_{h \to +\infty} \frac{M_n(p^h)}{p^{h(s-1)}} \geq \frac{1}{p^{\gamma(s-1)}} > 0.$$

□

Lemme 3.4.14. *Si $s \geq 2k$, pour k impair, ou $s \geq 4k$, pour k pair, alors*

$$\chi_n(p) \geq p^{\gamma(1-s)} > 0.$$

Démonstration. Par le lemme 3.4.13., il suffit de montrer que

$$\sum_{i=1}^{s} a_i^k \equiv n[p^\gamma] \tag{3.1}$$

admette une solution $(a_1, ..., a_s)$ où les a_i ne sont pas tous divisibles par p.

— Si $n \not\equiv 0[p]$, alors au moins un des a_i est premier avec p.

— Si $n \equiv 0[p]$, alors il suffit de montrer que

$$\sum_{i=1}^{s-1} a_i^k + 1^k \equiv n[p^\gamma]$$

admet une solution, ie.

$$\sum_{i=1}^{s-1} a_i^k \equiv n - 1[p^\gamma]$$

et dans ce cas $(n-1) \wedge p = 1$.

donc il suffit de montrer que, pour $n \wedge p = 1$, (3.1) admette une solution pour $s \geq 2k-1$, pour k impair, ou $s \geq 4k-1$, pour k pair.

— Si $p > 2$, soit g une racine primitive modulo p^γ, alors $ord(g) = \phi(p^\gamma) = (p-1)p^\tau$. Soit m tel que $m \wedge p = 1$, alors

$$\text{m est un résidu d'une puissance } k^e \text{ modulo } p^\gamma \iff \exists x/\ x^k \equiv m[p^\gamma].$$

Soit r tel que $m \equiv g^r[p^\gamma]$, alors

$$\exists x/\ x^k \equiv m[p^\gamma] \iff \exists v/\ x \equiv g^v[p^\gamma] \text{ et } kv \equiv r[(p-1)p^\tau].$$

Comme $k = k_0 p^\tau$, avec $k_0 \wedge p = 1$, alors

$$\exists v/\ kv \equiv r[(p-1)p^\tau] \iff r \equiv 0[(k_0 \wedge (p-1))p^\tau]$$

il y a donc

$$\frac{\phi(p^\gamma)}{(k_0 \wedge (p-1))p^\gamma} = \frac{p-1}{k_0 \wedge (p-1)}$$

résidus distincts d'une puissance k^e modulo p^γ.
Notons $s(n) = \min\{s \mid (3.1) \text{ admette une solution}\}$ et $C(j) = \{\bar{n} \in \mathbb{Z}/p^\gamma\mathbb{Z} \mid n \wedge p = 1,\ s(n) = j\}$. En particulier, $C(1)$ est l'ensemble des résidus d'une puissance k^e modulo p^γ. Si $m \wedge p = 1$ et $n' = m^k n$, alors $s(n') = s(n)$, donc les $C(j)$ sont stables par la multiplication par un résidu d'une puissance k^e modulo p^γ, donc

$$C(j) \neq \emptyset \Longrightarrow \#C(j) \geq \frac{p-1}{k_0 \wedge (p-1)}$$

Posons $N = \max\{w \mid C(w) \neq \emptyset\}$. Soit $j < N$ et $n = \min\{w \mid w \wedge p = 1,\ s(w) > j\}$. Comme $p \in \mathcal{P}\backslash\{2\}$, alors pour $i \in \{1, 2\}$, $(n-i) \wedge p = 1$ et $s(n-i) \leq j$. Comme $n = (n-1)+1^k$ et $n = (n-2)+1^k+1^k$, alors $j+1 \leq s(n) \leq s(n-i)+2 \leq j+2$, donc $s(n-i) = j$ ou $j-1$.
Alors, pour $j \in [\![1, N]\!]$, on ne peut pas avoir deux $C(j)$ consécutifs vides, donc le nombre de $C(j)$ non vides est d'au moins $\frac{N+1}{2}$.

Or les $C(j)$ sont deux à deux disjoints, donc

$$(p-1)p^\gamma = \phi(p^\gamma) = \sum_{\substack{j=1 \\ C(j)\neq\emptyset}}^{N} \#C(j) \geq \frac{N+1}{2}\frac{p-1}{k_0 \wedge (p-1)}$$

donc $N \leq 2p^\tau(k_0 \wedge (p-1)) - 1 \leq 2k-1$, donc $s(n) \leq 2k-1$ si $p \in \mathcal{P}\backslash\{2\}$ et $n \wedge p = 1$.

— Si $p = 2$,

  — si k est impair, alors tout nombre impair est un résidu d'une puissance k^e modulo 2^γ, alors pour tout n impair, $s(n) = 1$

  — si k est pair, alors $k = 2^\tau k_0$, avec $\tau \geq 1$ et $\gamma = \tau + 2$. On peut supposer que $1 \leq n \leq 2^\gamma - 1$. Si $s = 2^\gamma - 1 = 4.2^\tau - 1 \leq 4k-1$, alors (3.1) admet toujours une solution en choisissant $a_i = 1$ pour $1 \leq i \leq n$ et $a_i = 0$ pour $n+1 \leq i \leq s$, donc pour tout n impair, $s(n) \leq 4k-1$.

□

Théorème 3.4.15. *Il existe $c_1 = c_1(k,s) > 0$ et $c_2 = c_2(k,s) > 0$ telles que*

$$c_1 < \sigma(n) < c_2.$$

De plus, pour tout n suffisamment grand,

$$\sigma(n, P^\nu) = \sigma(n) + O(P^{-\nu\delta_4}).$$

Démonstration. Il existe $p_0 = p_0(k,s) \in \mathcal{P}$ tel que pour tout $n \geq 1$,

$$\frac{1}{2} \leq \prod_{p>p_0} \chi_n(p) \leq \frac{3}{2}.$$

Comme pour tout n et tout $p \in \mathcal{P}$, on a $\chi_n(p) \geq p^{\gamma(1-s)} > 0$, alors

$$\sigma(n) = \prod_{p\in\mathcal{P}} \chi_n(p) \geq \frac{1}{2}\prod_{p\leq p_0} \chi_n(p) \geq \frac{1}{2}\prod_{p\leq p_0} p^{\gamma(1-s)} =: c_1 > 0.$$

Le reste a été vu après la définition de $\sigma(n)$. □

3.5 Conclusion

Théorème 3.5.1 (Hardy-Littlewood)**.** *Soit $k \geq 2$ et $s \geq 2^k + 1$. Notons*

$$r_{k,s}(n) = \# \left\{ (x_1, ..., x_s) \in \mathbb{N}_*^s \mid n = \sum_{i=1}^{s} x_i^k \right\}.$$

Il existe $\delta = \delta(k,s) > 0$ tel que

$$r_{k,s}(n) = \sigma(n)\Gamma\left(1 + \frac{1}{k}\right)^s \Gamma\left(\frac{s}{k}\right)^{-1} n^{(s/k)-1} + O\left(n^{(s/k)-1-\delta}\right)$$

où σ est une fonction arithmétique telle qu'il existe $c_1, c_2 > 0$ telles que pour tout n, $c_1 < \sigma(n) < c_2$.

Démonstration. Posons $\delta_0 = \min(1, \delta_1, \delta_2, \delta_3, \nu\delta_4)$, alors :

$$\begin{aligned}
r_{k,s}(n) &= \int_0^1 F(\alpha)^s e(-n\alpha)d\alpha = \int_{\mathfrak{m}} F(\alpha)^s e(-n\alpha)d\alpha + \int_{\mathfrak{M}} F(\alpha)^s e(-n\alpha)d\alpha \\
&= \sigma(n, P^\nu)J^*(n) + O(P^{s-k-\delta_2}) + O(P^{s-k-\delta_1}) \\
&= (\sigma(n) + O(P^{-\nu\delta_4}))(J(n) + O(P^{s-k-\delta_3})) + O(P^{s-k-\delta_2}) + O(P^{s-k-\delta_1}) \\
&= \sigma(n)J(n) + O(P^{s-k-\delta_0}) \\
&= \sigma(n)\Gamma\left(1 + \frac{1}{k}\right)^s \Gamma\left(\frac{s}{k}\right)^{-1} n^{(s/k)-1} + O(n^{((s-1)/k)-1}) + O(n^{(s/k)-1-(\delta_0/k)}) \\
&= \sigma(n)\Gamma\left(1 + \frac{1}{k}\right)^s \Gamma\left(\frac{s}{k}\right)^{-1} n^{(s/k)-1} + O(n^{(s/k)-1-\delta})
\end{aligned}$$

avec $\delta := \frac{\delta_0}{k}$ □

Chapitre 4

Bibliographie

1. Harold Davenport, *Analytic methods for diophantine equations and diophantine inequalities*, Cambridge University Press, 2005
2. R.C. Vaughan, *The Hardy-Littlewood method, Second Edition*, Cambridge University Press, 1997
3. Melvyn B. Nathanson, *Additive Number Theory, The Classical Bases*, Springer Science+Business Media, LLC, 1996