SUR LE PROBLEME DE WARING ET LA METHODE DU CERCLE

Romdhane Younsi et Vincent Perrollaz

30 juin 2005

Sujet proposé par Régis de la Bretèche

Table des matières

1 METHODE DU CERCLE **2**
1.1 Notations . . . 2
1.2 La méthode de Hardy-Littlewood . . . 2
1.3 La variante de Vinogradov . . . 3

2 INEGALITE DE WEYL ET DE HUA **4**
2.1 Inégalité de Weyl . . . 4
2.2 Inégalité de Hua . . . 8

3 LA FORMULE ASYMPTOTIQUE **10**
3.1 Arcs majeurs et arcs mineurs . . . 10
3.2 Arcs mineurs . . . 10
3.3 Arcs majeurs . . . 11

4 LA SÉRIE SINGULIÈRE **15**

5 LES NOMBRES $G(k)$ **19**

L'objet de cet exposé est de traiter le problème de Waring qu'on peut voir comme étant une généralisation du résultat fort célèbre de Lagrange connu sous le nom du *Problème des Quatre Carrés*. En effet, en 1770, Edward Waring (1736-1798), s'est demandé si, pour tout entier naturel k, il existe un entier naturel s tel que tout entier soit la somme d'au plus s puissances k^{eme} d'entiers. La réponse, affirmative, fut apportée par David Hilbert en 1909, à l'aide d'une méthode essentiellement algébrique. Quelquefois, ce sujet est décrit comme le théorème de Hilbert-Waring. Pour chaque k, nous notons $g(k)$ le plus petit s vérifiant la condition de Waring. Plusieurs travaux au cours du vingtième siècle ont permis de calculer quelques valeurs de la fonction g. Ainsi, l'égalité g(3) = 9 fut établie en 1912 par Wieferich et A. J. Kempner, g(4) = 19 en 1986 par R. Balasubramanian, F. Dress, et J.-M. Deshouillers, g(5) = 37 en 1964 par Jing-Run Chen et g(6) = 73 en 1940 par Pillai. On suivra dans cet exposé la méthode du cercle d'Hardy-Littlewood permettant de transformer un problème d'équation diophantienne en un problème d'estimation de sommes d'exponentielles arithmétiques. Signalons, enfin, que Hardy et Littlewood, dans leurs travaux pionniers, ont "affaibli" la condition de Waring en introduisant, pour un entier naturel k donné, le nombre $G(k)$ représentant le plus petit entier s tel que tout entier suffisamment grand soit la somme d'au plus s puissances k^{ime} d'entiers.

1 METHODE DU CERCLE

On introduit les notations utilisées dans cette partie.

1.1 Notations

Définition. *On pose* $\forall (s,k) \in (\mathbb{N}^*)^2$

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

Définition. *On pose* $\forall k \in \mathbb{N}^*$

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

$$G(k) = \min\{s \in \mathbb{N}^* \mid \{N \in \mathbb{N}^* | r(N) = 0\} \textit{ est fini } \}$$

Remarque. *On peut intuitivement se dire que G représente une version lissée de g. En effet, cette définition permet d'éviter des cas isolés "plus difficiles" que la moyenne à représenter. On montrera à la fin du cours que $\frac{G(k)}{g(k)} \to 0$ pour $k \to \infty$.*

Définition.

$$\textit{on pose : } \forall t \in \mathbb{R},\ e(t) = e^{2i\pi t}$$

On va maintenant démontrer l'égalité fondamentale du sujet. Pour cela on va procéder en deux étapes, on va d'abord reprendre l'idée historique de Hardy-Littlewood puis raffiner la méthode telle que Vinogradov le préconise. On se placera maintenant à s et k fixés.

1.2 La méthode de Hardy-Littlewood

Définition. *On introduit la série génératrice. Soit f la fonction*

$$\forall z \in \mathbb{C},\ f(z) = \sum_{n=0}^{\infty} r(n) z^n$$

Remarque. *On peut déja noter que grâce à la majoration triviale*

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

le rayon de convergence de la série est supérieur ou égal à 1

On va maintenant utiliser la définition de r pour obtenir une identité intéressante sur f.

Proposition 1.1. *On pose d'abord*

$$D = \{z \in \mathbb{C} :\ |z| < 1\}$$

Et maintenant, on a

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

Démonstration. On écrit en fait :

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

et l'idée est maintenant de regrouper les termes pour $n_1^k + ... + n_s^k = N$ puis de sommer sur N et on obtient la définition exacte de f. On peut noter que l'on peut réarranger la série de cette façon, car la famille est sommable. □

Et maintenant on peut récupérer les coefficients de la série en intégrant la fonction sur un cercle (c'est ce qui donne son nom à cette méthode). Plus précisément on a la :

Proposition 1.2.

$$\forall N \in \mathbb{N}^* \text{ et } \forall \rho \in]0;1[\text{ on a : } r(N) = \frac{1}{2\pi\rho^N} \int_0^{2\pi} f\left(\rho e^{it}\right) e^{-iNt} dt$$

Démonstration. Il suffit d'intégrer terme à terme dans la définition de f et d'intervertir série et intégrale grace à la convergence uniforme de f sur le domaine. □

Cette égalité était le point de départ de Hardy et Littlewood, mais Vinogradov a introduit une idée légérement différente.

1.3 La variante de Vinogradov

Définition. *Lorsque $P \in \mathbb{N}^*$, on introduit T la fonction suivante*

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

On va maintenant considérer P fixé dans $\mathbb{N}^*$ et introduire des coefficients sous-jacents aux r(N) et dépendant (implicitement) de P.

Définition. *Pour $m \in \mathbb{N}$, soit*

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

Remarque. *Si P est suffisament grand par rapport à m, on a $r(m) = r'_P(m)$, et en fait la condition exacte est $m \leq P^k$.*

Et maintenant, on montre

Proposition 1.3. *On a*

$$\forall \alpha \in \mathbb{R}, (T(\alpha))^s = \sum_{m \geq 0} e(\alpha m)\, r'_P(m)$$

puis on en déduit

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

Démonstration. Les deux preuves sont similaires à celles qu'on a faites dans le cas de la série génératrice. Et on n'a plus aucun problème de convergence à régler. □

En prenant $P = E(m^{\frac{1}{k}})$ où E désigne la partie entière, on arrive à la formule qu'on utilisera dans toute la suite de l'exposé :

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

Dans cette section, on a obtenu une formule intégrale pour exprimer les $r(N)$. L'objectif de la suite est d'utiliser cette formule pour obtenir une formule asymptotique pour r.

Il parait judicieux d'expliquer ici la démarche adoptée.

Le problème va consister à évaluer l'intégrale obtenue dans la partie précédente. En fait, on peut faire une estimation large dans l'intégrale, en effet, on représente des nombres d'ordre P^k et on a un choix d'ordre P^s, en supposant une "équirépartition" des représentations, on arrive à une estimation de r en P^{s-k}. Pour estimer l'intégrale on néglige les α qui contribuent à l'intégrale à moins de P^{s-k}. Il est important de noter que même si l'estimation à priori est fausse le résultat obtenu restera juste car on a négligé des termes petits par rapport aux autres termes dans l'intégrale. Il reste donc à trouver les influences respectives des différents termes sur l'intégrale, pour cela on démontre deux inégalités dans la suite, celle de Weyl et celle de Hua.

2 INEGALITE DE WEYL ET DE HUA

On commence par montrer un lemme technique.

Lemme. *lemme préliminaire On a $\forall m \in \mathbb{N}^*$, si $d(m)$ est le nombre de diviseurs de m le résultat suivant :*

$$\forall \epsilon > 0 \qquad d(m) \ll m^\epsilon$$

Démonstration. Soit $m \in \mathbb{N}^*$ on écrit la décomposition en facteurs premiers de m $m = p_1^{\lambda_1}...p_n^{\lambda_n}$ alors si $\epsilon > 0$ on a

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

Or on voit facilement que si $x \geq e^{\frac{1}{\epsilon}}$, on a $\frac{\lambda_i+1}{x^{\epsilon\lambda_i}} \leq 1$.
Et finalement

$$\begin{aligned} \frac{d(m)}{m^\epsilon} &\leq \prod_{p_i \leq 2^{\frac{1}{\epsilon}}} \frac{\lambda_i + 1}{p_i^{\epsilon\lambda_i}} \\ &\leq \prod_{p_i \leq 2^{\frac{1}{\epsilon}}} \frac{\lambda_i + 1}{p_i^{\epsilon\lambda_i}} \end{aligned}$$

Or si $f(\lambda) = 2^{-\epsilon\lambda}(\lambda+1)$ on voit facilement que f est bornée donc on a $\frac{d(m)}{m^\epsilon} \leq C(\epsilon)$ et ce sans hypothèse sur les p_i ou les λ_i. On a donc bien

$$\forall \epsilon > 0 \qquad d(m) \ll m^\epsilon$$

□

2.1 Inégalité de Weyl

Proposition 2.1 (Inégalité de Weyl)**.** *Soit f le polynome de $\mathbb{R}[X]$ suivant :*

$$f(x) = \alpha x^k + \alpha_1 x^{k-1} + ... + \alpha_k$$

On suppose qu'il existe $(a, q) \in \mathbb{Z} \times \mathbb{N}^*$ tel que

$$a \wedge q = 1 \text{ et } |\frac{a}{q} - \alpha| \leq \frac{1}{q^2}$$

Alors si on note $K = 2^{k-1}$ on a

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

Remarque. *On rappelle que $\ll$ signifie qu'on a l'inégalité correspondante et qu'on a simplement omis une constante mutliplicative et de plus, la constante ne dépend pas de P.* ***En fait, on verra qu'on peut prendre une constante ne dépendant que de k.***

Démonstration. L'idée est de progressivement abaisser le degrès de f pour se ramener à un polynome de degrés 1 pour lequel on sait faire le calcul. En fait on va partir d'une somme plus générale.
On prend $P_1, P_2 \in \mathbb{Z}$ tels que $0 \leq P_2 - P_1 \leq P$ et alors on définit

$$S_k(f) = \sum_{x=P_1+1}^{P_2} e(f(x))$$

On va initier un raisonnement par récurence

$$\begin{aligned}
|S_k(f)|^2 &= \left(\sum_{x_2=P_1+1}^{P_2} e\left(f\left(x_2\right)\right)\right).\left(\sum_{x_1=P_1+1}^{P_2} e\left(-f\left(x_1\right)\right)\right) \\
&= \sum_{x_1,x_2=P_1+1}^{P_2} e\left(f\left(x_2\right)-f\left(x_1\right)\right) \\
&= P_2-P_1+\sum_{x_1\neq x_2}^{P_2} e\left(f\left(x_2\right)-f\left(x_1\right)\right) \\
&= P_2-P_1+2.\Re(\sum_{P_1+1\leq x_1<x_2\leq P_2} e\left(f\left(x_2\right)-f\left(x_1\right)\right)
\end{aligned}$$

On pose $y=x_2-x_1$ et on a

$$f(x_2)-f(x_1)=f(x_1+y)-f(x_1)=(\Delta_y f)(x_1)$$

Ceci nous donne doncla ligne suivante

$$|S_k(f)|^2=P_2-P_1+2.\Re\left(\sum_{y=1}^{P}\sum_{x}\left(\Delta_y f\right)(x)\right)$$

Remarque. *Il est essentiel ici de comprendre la sommation, la somme sur x se fait dans un ensemble d'entiers* ***qui est un intervalle dépendant de*** *y* ***mais qui est toujours compris dans*** *$[|P_1+1;P_2|]$, et on se permet de faire monter la somme jusqu'à P plutôt qu'à P_2-P_1 en jouant sur la sommation en x.*

Il convient maintenant de remarquer que $\Delta_y f$ est un polynôme de degrés $k-1$ donc on arrive à l'inégalité suivante

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

On élève alors cette inégalité au carré et on obtient :

$$|S_k(f)|^4\leq P^2+2P\sum_{y=1}^{P}|S_{k-1}(\Delta_y f)|+\left(\sum_{y=1}^{P}|S_{k-1}\left(\Delta_y f\right)|\right)^2$$

mais maintenant, en utilisant l'inégalité de Cauchy-Schwarz on a :

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

et comme on peut majorer le produit de deux nombres réels par la somme de leur carrés on obtient

$$|S_k(f)|^4\ll P^2+P.\sum_{y=1}^{P}|S_{k-1}(\Delta_y f)|^2$$

On s'intéresse maintenant à $\sum_{y=1}^{P}|S_{k-1}(\Delta_y f)|^2$ En reprenant la preuve pour S_n, on voit qu'on peut obtenir de la même façon :

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

On obtient donc

$$\begin{aligned}
|S_k(f)|^4 &\ll P^2 + P.\sum_{y=1}^{P}|S_{k-1}(\Delta_y f)|^2 \\
&\ll P^2 + P.\sum_{y=1}^{P} P + 2\sum_{z=1}^{P}|S_{k-2}(\Delta_{y,z}f)| \\
&\ll P^2 + P^3 + 2P\sum_{y=1}^{P}\sum_{z=1}^{P}|S_{k-2}(\Delta_{y,z}f)| \\
&\ll P^3 + 2P\sum_{y=1}^{P}\sum_{z=1}^{P}|S_{k-2}(\Delta_{y,z}f)|
\end{aligned}$$

On se ramène donc à montrer par récurence sur $\nu \leq k$ la formule suivante :

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

On a vu la formule pour le rang 1, on montre donc le passage du rang $\nu \leq k-1$ au rang $\nu+1$. Comme précédemment, on majore un produit par la somme des carrés et on obtient

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

On va maintenant travailler sur le deuxième terme, en utilisant ν fois l'inégalité de Cauchy-Schwarz comme auparavant on obtient :

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

Mais on a aussi

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

donc on obtient

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

On a bien démontré la formule voulue. Dans cette formule, on va prendre $\nu = k-1$.
On on a donc obtenu une somme sur un polynome de degrés 1.
En développant, on note

$$\begin{aligned}
(\Delta_y f)(x) &= \alpha\left[(x+y)^k - x^k\right] + \alpha_1\left[(x+y)^{k-1} - x^{k-1}\right] + ... + \alpha_{k-1}y \\
&= \alpha k y x^{k-1} + (...)x^{k-2} + ... + \alpha y^k + ... + \alpha_{k-1}y
\end{aligned}$$

Et en réitérant l'opération on obtient

$$(\Delta_{y_1,...,y_{k-1}}f)(x) = \alpha k! y_1..y_{k-1}x + \beta$$

Où β est un nombre dont on n'aura pas à s'occuper car :

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

Il est maintenant temps de se souvenir que la sommation sur x est fait sur un intervalle de $[|P_1+1;P_2|]$, la somme va donc être de la forme suivante $\sum_{x=x_1}^{x_2-1} e(\lambda x)$ avec $\lambda = k!\alpha y_1...y_{k-1}$ et on a

$$\begin{aligned}\sum_{x=x_1}^{x_2-1} e(\lambda x) &= e(\lambda x_1)\sum_{x=0}^{x_2-x_1-1}(e(\lambda))^x \\ &= \begin{cases} x_2-x_1 & \text{si } \lambda\in\mathbb{Z} \\ e(\lambda x_1)\frac{e(\lambda\frac{x_2-x_1}{2})}{e(\frac{\lambda}{2})}\frac{e(\lambda\frac{x_2-x_1}{2})-e(-\lambda\frac{x_2-x_1}{2})}{e(\frac{\lambda}{2})-e(-\frac{\lambda}{2})}) & \text{sinon}\end{cases}\end{aligned}$$

Et dans le dernier cas on obtient :

$$\begin{aligned}|S_1(\Delta_{y_1,...,y_{k-1}}f)| &= |\frac{\sin(\pi\lambda(x_2-x_1))}{\sin(\pi\lambda)}| \\ &\text{d'où} \\ |S_1(\Delta_{y_1,...,y_{k-1}}f)| &\ll \frac{1}{\sin(\pi\lambda)}\end{aligned}$$

On pose maintenant $||\lambda|| = d(\mathbb{Z},\lambda)$, et alors, toujours dans l'optique $\lambda\notin\mathbb{Z}$, on a un $k\in\mathbb{Z}$ tel que $||\lambda|| = |\lambda-k|$ puis :

$$\begin{aligned}|\sin(\pi\lambda)| &= |\sin(\pi(\lambda-k)+\pi k)| \\ &= |\sin(\pi(\lambda-k))| \\ &\text{puis comme } |\lambda-k|\leq\tfrac{1}{2} \\ |\sin(\pi(\lambda-k))| &\gg |\lambda-k| \\ &\gg ||\lambda||\end{aligned}$$

Et en regroupant tous les résultats on a alors

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

On va maintenant chercher à réorganiser les sommes en collectant par rapport à $y_1..y_{k-1}=m$. Le lemme assure que

$$\forall\epsilon>0, d(m)<m^\epsilon$$

Ceci permet d'obtenir

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

et delà

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

$$\forall \epsilon > 0 \text{ on a } |S_k(f)|^K \ll P^{K-1} + P^{K-k}.P^{\epsilon}.\sum_{m=1}^{k!P^{k-1}} \min(P, ||\alpha m||^{-1})$$

Il ne reste donc plus maintenant qu'à estimer la somme à droite, et c'est là qu'intervient l'hypothèse $|\frac{a}{q} - \alpha| \leq \frac{1}{q^2}$.
L'idée va être de diviser la somme en blocs de q-termes consécutifs (il y a donc un nombre $\ll \frac{P^{k-1}}{q} + 1$ de blocs) de la forme $\sum_{m=0}^{q-1} \min(P, ||\alpha(m_1 + m)||^{-1})$

$$\begin{aligned} \alpha(m_1 + m) &= \alpha m_1 + \frac{am}{q} + (\alpha - \frac{a}{q})m \\ &= \alpha m_1 + \frac{am}{q} + O(\frac{1}{q}) \end{aligned}$$

On constate alors que l'on peut sortir les entiers d'une $||\quad||$ mais aussi que

$$a \wedge q = 1 \Rightarrow am \text{ couvre } \mathbb{Z} \text{ pour } m : 0 \to q - 1$$

Un bloc ressemble donc en fait à

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

Puis en notant b l'entier le plus proche de $q\alpha m_1$ on a $|\frac{b}{q} - \alpha m_1| \leq \frac{1}{q}$ Alors au final

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

Puis si $s = |(r + b) \bmod q|$ on a $||\frac{r+b}{q} + O(\frac{1}{q})|| \gg \frac{s}{q}$ on en déduit

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

L'inégalité de Weyl est triviale si $q > P^k$ donc on peut supposer l'inégalité inverse et alors $\ln(q) \leq k.\ln(P) \ll P^{\epsilon}$, $\forall \epsilon > 0$. On finit alors par

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

et donc

$$\forall \epsilon > 0 \qquad |S_k(f)| \ll P^{1+\epsilon}(P^{-\frac{1}{K}} + q^{-\frac{1}{K}} + (\frac{P^k}{q})^{-\frac{1}{K}})$$

□

On a donc bien l'inégalité recherchée. On peut maintenant passer à la deuxième inégalité annoncée.

2.2 Inégalité de Hua

Proposition 2.2 (Inégalité de Hua). *Si T est la fonction de Vinogradov alors*

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

Démonstration. Si on note $I_\nu = \int_0^1 |T(\alpha)|^{2^\nu} d\alpha$ on va montrer par récurence sur $\nu \in [|0;k|]$ l'inégalité

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

Pour $\nu = 1$ on écrit

$$\begin{aligned} I_1 &= \int_0^1 \left(\sum_{x_1=1}^{P} e(\alpha x_1) \right) . \left(\sum_{x_2=1}^{P} e(-\alpha x_2) \right) d\alpha \\ &= P \\ \text{car} \quad & \int_0^1 e(\alpha(y_i^k - y_j^k)) d\alpha = \begin{cases} 1 & \text{si} \quad y_i = y_j \\ 0 & \text{sinon} \end{cases} \end{aligned}$$

On a donc bien la proposition au rang 1 si elle est vraie au rang $\nu < k$ en reprenant la démonstration de l'inégalité de Weyl on voit que si $f(x) = \alpha x^k$ on obtient $S_k(f) = T(\alpha)$ et alors

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

On obtient alors facilement

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

mais la dernière intégrale s'écrit aussi

$$\int_0^1 \left[\left(\sum_x e \left(\alpha \Delta_{y_1,\dots,y_\nu} (x^k) \right) \right) \left(. \sum_{u_1,\dots,u_{2^{\nu-1}}=1}^{P} \alpha \left(u_1^k + \dots + u_{2^{\nu-1}}^k \right) \right) \left(. \sum_{v_1,\dots,v_{2^{\nu-1}}=1}^{P} -\alpha \left(v_1^k + \dots + v_{2^{\nu-1}}^k \right) \right) \right] d\alpha$$

Et en développant, on a une somme d'intégrale du type

$$\int_0^1 e\Big(\alpha (\Delta_{y_1,\dots,y_\nu}(x^k) + u_1^k + \dots + u_{2^{\nu-1}}^k - v_1^k - \dots - v_{2^{\nu-1}}^k) \Big) d\alpha$$

Au final on obtient donc

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

où on définit N par

$$\begin{aligned} N = \#\{ & (y_1, \dots, y_\nu) \in [|1;P|]^\nu, (u_1, \dots, u_{2^{\nu-1}}) \in [|1;P|]^{2^{\nu-1}}, (v_1, \dots, v_{2^{\nu-1}}) \in [|1;P|]^{2^{\nu-1}}, x \in [|1;P|] \\ & \text{tels que } \Delta_{y_1,\dots,y_\nu}(x^k) + u_1^k + \dots + u_{2^{\nu-1}}^k - v_1^k - \dots - v_{2^{\nu-1}}^k = 0 \} \end{aligned}$$

Il ne reste plus alors qu'à estimer N, pour cela constatons d'abord que $y_1, \dots y_\nu$ divisent $\Delta_{y_1,\dots,y_\nu}(x^k)$ L'idée va être de fixer au coup par coup les (u_i) les (v_j) et x puis de majorer la quantité de (y_i) et par le nombres de diviseurs de $v_1^k + \dots + v_{2^{\nu-1}}^k - u_1^k - \dots - u_{2^{\nu-1}}^k$ grâce au lemme préliminaire, on peut obtenir

$$\begin{aligned} \forall \epsilon > 0 \text{ pour chaque } (y_i) \text{ un nombre de possibilités} \quad &\ll \quad 2^{\nu-1} . P^k \\ &\text{donc} \\ \forall \epsilon > 0 \text{ pour chaque } (y_i) \text{ un nombre de possibilités} \quad &\ll \quad P^\epsilon \end{aligned}$$

Enfin on peut noter que comme $\nu \leq k-1$ et que les y_i et x sont entiers on a $\Delta_{y_1,\dots,y_\nu}(x^k)$ est croissant en x donc au final on a

$$N \ll P^{2^\nu + \epsilon}$$

et donc

$$\begin{aligned} \forall \epsilon > 0 \qquad I_{\nu+1} &\ll P^{2^{\nu-1}} . P^{2^\nu - \nu + \epsilon} + P^{2^\nu - \nu - 1} . P^{2^\nu + \epsilon} \\ &\ll P^{2^{\nu+1} - (\nu+1) + \epsilon} \end{aligned}$$

On a donc bien achevé la récurrence et montré l'inégalité de Hua □

On peut maintenant passer au traitement de l'intégrale annoncé dans la première partie

3 LA FORMULE ASYMPTOTIQUE

On va maintenant poursuivre le programme présenté à la fin de la première partie.

3.1 Arcs majeurs et arcs mineurs

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

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

alors on trouve

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

Donc en particulier si on prend ϵ assez petit on obtient

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

Ce rapide calcul nous pousse donc à diviser $[0;1]$ en deux ensembles (dont on vérifiera facilement qu'ils sont mesurables). Celui des arcs majeurs contribuera au terme principal, celui des arcs mineurs sera négligeable.

3.2 Arcs mineurs

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

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

Démonstration. Si $\theta \in \mathbb{Q}$ le lemme est trivial donc on peut supposer qu'on n'est pas dans ce cas.
Tout d'abord si Q est entier on va considérer les nombres

$$0, 1, (q\theta - E(q\theta)) \text{ où } q : 1 \to Q$$

on a donc $Q+1$ nombres dans $[0;1]$ qu'on va répartir dans les Q intervalles de type $[\frac{u-1}{Q}; \frac{u}{Q}]$ où $u : 1 \to Q$ il est évident que deux de ces nombres sont dans le même intervalle. On en déduit

$$\exists (r_1, r_2, s_1, s_2) \in [|0; Q|]^2 \times \mathbb{Z}^2 \text{ tels que } 0 < |r_1 - r_2| = \rho < Q \text{ et } |r_1\theta - s_1 - (r_2\theta - s_2)| \leq \frac{1}{Q}$$

puis comme $|(r_1 - r_2)\theta - (s_1 - s_2)| \leq \frac{1}{Q}$ on prend $q = \rho$ et on a la proprieté. Enfin si Q n'est pas entier on applique ce qui précède à $E(Q) + 1$.

□

Définition. *On pose :*

$$\forall (a, q) \in \mathbb{Z} \times \mathbb{N}^* \text{ tel que } a \wedge q = 1$$

$$m_{a,q} = \{\alpha \in [0;1] \mid |\alpha - \frac{a}{q}| < P^{-k+\delta} \text{ lorsque } 1 \leq q \leq P^\delta \text{ et } 1 \leq a \leq q\}$$

Remarque. *Dans la définition on se place dans le cas où on a fixé δ une fois pour toute*

Remarque. *En fait, **les $m_{a,q}$ constituent les arcs majeurs et le complémentaire $\mathfrak{m}$ dans** $[0;1]$ **sera l'ensemble des arcs mineurs**.*

On a maintenant la

Proposition 3.1. *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 va d'abord supposer que

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

puis si $\alpha \in \mathfrak{m}$ comme $q^{-1}P^{\delta-k} < P^{\delta-k}$ alors on a forcément $q > P^{\delta}$ mais aussi

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

On se retrouve donc exactement dans le cas d'application de l'inégalité de Weyl et donc

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

puis comme $\frac{P^k}{q} \geq P^{\delta}$, que $\frac{1}{q} \leq P^{-\delta}$ et que δ est petit on en déduit

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

et avec ϵ assez petit on se retrouve dans le cas du calcul débutant la partie. On peut donc bien négliger l'intégrale sur $\mathfrak{m}$.

Il reste juste à montrer l'approximation dont on a supposé l'existence.

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

Et sous cette forme le problème est une application évidente du lemme de Dirichlet. □

On a alors fini le traitement des arcs mineurs.

3.3 Arcs majeurs

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

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

Où les max *sont pris sur* $[A;B]$

Démonstration. On va subdiviser l'intervalle par les entiers successifs qu'il contient, c'est à dire qu'on a $A < x_1 < ... < x_n \leq B$ Puis on va simplement écrire

$$\begin{aligned} |\int_A^B f(\nu)d\nu - \sum_{A<y\leq B} f(y)| &= \Big|\int_A^{x_1} f(\eta)d\eta + \int_{x_n}^B f(\eta)d\eta - f(x_n) + \sum_{x=x_1}^{x_{n-1}} \int_x^{x+1} [f(\eta) - f(x)]d\eta\Big| \\ &\leq 3.\big(\max|f(\nu)| + (B-A).\max|f'(\nu)|\big) \end{aligned}$$

□

Remarque. *Il est important ici de remarquer que la constante mutliplicative est indépendante de A, B .*

Lemme. *Soit Γ la fonction définie par*

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

Et si ϕ est définie par

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

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. Ceci est un résultat relativement classique d'analyse dont on trouvera la démonstration dans [4]. C'est en fait une généralisation d'une formule d'Euler

$$B(p,q) = \int_0^1 x^{p-1}(1-x)^{q-1}dx = \frac{\Gamma(p)\Gamma(q)}{\Gamma(p+q)}$$

□

On va maintenant supposer que $\alpha \in m_{a,q}$ on a donc

$$\alpha = \beta + \frac{a}{q} \qquad \text{où} \qquad |\beta| < P^{\delta-k}$$

Alors on a la

Proposition 3.2. *On peut écrire*

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

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

Démonstration. On a

$$\begin{aligned} T(\alpha) &= \sum_{x=1}^{P} e(\alpha.x^k) \\ &= \sum_{x=1}^{P} e((\beta+\frac{a}{q})x^k) \\ \text{puis on pose} \quad & x = q.y + z \\ T(\alpha) &= \sum_{z=1}^{q} \big[e(a\frac{z^k}{q}).\sum_y e(\beta(qy+z)^k)\big] \end{aligned}$$

On va maintenant chercher à relier $\sum_y e(\beta(qy+z)^k)$ à $I(\beta)$. On va utiliser le lemme sur la fonction $f(\eta) = e(\beta(q\eta+z)^k)$ et en remarquant

$$Max|f'| \leq q|\beta|P^{k-1} \qquad B-A << \frac{P}{q} \qquad Max|f| \leq 1$$

Ceci nous donne donc

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

Puis il suffit de remarquer que $S_{a,q} = \sum_{z=1}^{q} e(a\frac{z^k}{q}) = O(q) = O(P^\delta)$ car $\alpha \in m_{a,q}$ et donc on a bien

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

□

Puis maintenant, on obtient la

Proposition 3.3. *Si $\mathcal{M}$ représente l'ensemble des arcs majeurs, on a*

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

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

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

Démonstration. Tout d'abord, on peut vérifier facilement $|q^{-1}S_{a,q}I(\beta)| \leq P$, on obtient donc

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

puis en multipliant par $e(-N\alpha)$ et en intégrant sur $m_{a,q}$ i.e. $|\beta| < P^{\delta-k}$ on obtient

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

Et on peut sommer sur a,q sans changer la partie intégrale et on obtient alors

$$\int_{\mathcal{M}} (T(\alpha))^s e(-N\alpha)d\alpha = \mathfrak{S}(P^\delta, N) \int_{|\beta| < P^{\delta-k}} (I(\beta))^s e(-N\beta)d\beta + O(P^{s-k-1+5\delta})$$

On va maintenant remarquer que $N - P^k \ll P^{k-1}$ à cause de la définition de N et P. De là, on arrive à

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

Donc en substituant dans l'intégrale on a une erreur de l'ordre de $P^{s-k}.P^s.P^{\delta-1} = P^{s-k+2\delta-1}$ donc négligeable puis on fait les changements de variable suivant dans l'intégrale $\xi = P\xi' \, et \, \beta = P^{-k}\gamma$ et on obtient l'intégrale suivante

$$P^{s-k} \int_{|\gamma| < P^\delta} \Big(\int_0^1 e(\gamma\xi'^k)d\xi' \Big) d\gamma$$

ce qui correspond bien à $P^{s-k}J(P^\delta)$. Comme δ est petit, $\delta' = 1 - \delta > 0$ et on peut bien mettre le résultat sous la forme

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

□

On peut enfin conclure par le

Théorème 1. *On va appeler*

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

et

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

Alors si $s \geq 2^k + 1$

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

avec $\delta' > 0$

Démonstration. On sait que

$$\begin{aligned} r(N) &= \Big(\int_{\mathcal{M}} + \int_{\mathfrak{m}}\Big)\big(T(\alpha)\big)^s e(-N\alpha)d\alpha \\ &= P^{s-k}\mathfrak{S}(P^\delta, N)J(P^\delta) + O(P^{s-k-\delta'}) \end{aligned}$$

On a

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

puis si on prend $\zeta = \xi^k$ on obtient

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

et l'intégrale de droite est convergente pour $\gamma \to +\infty$ donc on en déduit

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

Puis grâce à cette majoration, si on pose

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

On vérifie trivialement que

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

On peut donc remplacer $J(P^\delta)$ par J et de la même façon P par $N^{\frac{1}{k}}$. Il ne reste alors plus qu'à remplacer $\mathfrak{S}(P^\delta, N)$ par $\mathfrak{S}(N)$ et à montrer que $J = C_{k,s}$.

Tout d'abord $S_{a,q} = \sum_{z=1}^q e(\frac{a}{q}z^k)$ donc en utilisant l'inégalité de Weyl avec $\alpha = \frac{a}{q}$ et $P = q$ on obtient

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

Et donc

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

Grâce à cette majoration on voit alors facilement que la série $\mathfrak{S}$ est normalement convergente. Et de ce fait on peut opérer la substitution.

Il ne reste donc plus qu'à montrer que $J = C_{k,s}$.

Tout d'abord remarquons que

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

D'où, on obtient

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

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

Mais le domaine d'intégration est tel que $u-1<\zeta_1+...+\zeta_{s-1}<u$. On va maintenant utiliser le theorème intégrale de Fourier (dont une démonstration pour une fonction régulière peut se faire à l'aide du lemme de Riemann-Lebesgue et l'intégrale de Drichlet (pour plus de précisions, voir [4])) qui assure

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

Sachant $A<C<B$ dans le cas qui nous intéresse on en déduit

$$\begin{aligned} k^sJ &= \phi(1) \\ &= \int_0^1...\int_0^1\Big(\zeta_1...\zeta_{s-1}(1-\zeta_1-...-\zeta_{s-1})\Big)^{-1+\frac{1}{k}}d\zeta_1...d\zeta_{s-1}\end{aligned}$$

Et à nouveau le domaine est rectifié pour que $0<\zeta_1+...+\zeta_{s-1}<1$

À partir de ceci, on a par le lemme $\phi(1)=\frac{\Gamma(\frac{1}{k})^s}{\Gamma(\frac{s}{k})}$, puis par intégration par partie on prouve facilement

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

Donc on obtient bien

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

ce qui conclut la démonstration.

□

4 LA SÉRIE SINGULIÈRE

Cette section permet de compléter et de valider la formule asymptotique en prouvant que si s$\geqslant 2^k+1$ alors $\mathfrak{S}$(N) est minoré par un réel C(k,s)>0 Rappelons tout d'abord l'expression de la série singulière introduite dans la formule asymptotique :

$$\mathfrak{S}(N)=\sum_{q=1}^{\infty}\left(\sum_{\substack{a=1\\(a,q)=1}}^{q}(q^{-1}S_{a,q})^s e\left(-\frac{aN}{q}\right)\right)$$

Pour simplifier les notations, posons :

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

de sorte que :

$$\mathfrak{S}(N)=\sum_{q=1}^{\infty}A(q)$$

La transformation $a\leftrightarrow q-a$ dans la somme définissant $A(q)$ nous donne directement la stabilité de $A(q)$ par conjugaison complexe. Ainsi, $\forall q\in\mathbb{N}$, $A(q)\in\mathbb{R}$. Nous allons prouver le théorème suivant :

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

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

Avant de le prouver, disons pourquoi il permet de répondre affirmativement au problème de Hilbert. En effet, s'il est vrai, le terme principal dans la formule asymptotique est $\gg N^{\frac{s}{k}-1}$ si s $\geqslant 2^k+1$. Par conséquent, et sous cette même condition sur s et k, $r(N) \to \infty$ quand $N \to \infty$. Ainsi, tout entier suffisamment grand est somme de 2^k+1 puissances k^{ime} (ceci démontre au passage que $G(k) \leq 2^k+1$). Quitte à régler un par un les petits rangs, on a immédiatement une réponse affirmative au problème de Hilbert.

Prouvons maintenant le théorème. L'une des difficultés pour traiter cette série singulière est que l'indice de la somme interne fait apparaître une condition de primalité entre deux entiers. Ce type de condition est a priori difficile à traiter sauf dans le cas où l'entier q est un nombre premier ou une puissance d'un nombre premier. Dans ce sens, nous avons besoin transformer cette somme à l'aide de termes plus contrôlables. Commençons tout d'abord par ce lemme :

Lemme. *Si $(q_1,q_2)=1$, alors : $A(q_1q_2)=A(q_1)A(q_2)$*

Démonstration. Notons : $f(a,q)=(q^{-1}S_{a,q})^s e\left(-\frac{aN}{q}\right)$

Le théorème de Bezout nous dit qu'il y a une correspondance bijective entre l'ensemble $\{a \in [1,q]$ tel que $(a,q)=1\}$ et l'ensemble des couples $\{(a_1,a_2) \in [1,q_1]\times[1,q_2]$ tel que $(a_1,q_1)=1$ et $(a_1,q_1)=1\}$ avec $q=q_1q_2$. Cette correspondance est donnée par :

$$\frac{a}{q} \equiv \frac{a_1}{q_1}+\frac{a_2}{q_2}[1]$$

Ce même théorème (i.e le théorème de Bezout) nous dit qu'il y a une correspondance bijective entre [1,q] et $[1,q_1]\times[1,q_2]$ donnée par :

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

avec $(z,z_1,z_2) \in [1,q]\times[1,q_1]\times[1,q_2]$

Ainsi

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

Or

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

D'où :

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

Puis sachant que $e\left(-\frac{aN}{q}\right) = e\left(-\frac{a_1 N}{q_1}\right) e\left(-\frac{a_2 N}{q_2}\right)$(car $\frac{a}{q} \equiv \frac{a_1}{q_1} + \frac{a_2}{q_2}[1]$)
Donc $f(a,q) = f(a_1,q_1)f(a_2,q_2)$ (toujours car $\frac{a}{q} \equiv \frac{a_1}{q_1} + \frac{a_2}{q_2}[1]$)
Ainsi par la correspondance rappelée ci-dessus, on a :

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

Ce qui achève la preuve du lemme. □

Ce lemme va nous permettre de transformer la série singulière en un produit et ceci est énoncé dans le lemme de transformation suivant :

Lemme. *Si* $s \geqslant 2^k + 1$, *alors :*

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

Démonstration. On a vu dans la section précédente que :

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

Il résulte du lemme démontré précedemment et par simple extension que si $q = \prod_i p_i^{\nu_i}$ alors

$$A(q) = \prod_i A\left(p_i^{\nu_i}\right)$$

D'où , par convergence de $\sum \mid A(q) \mid$:

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

Ceci est le résultat voulu. □

À ce stade, on a transformé la série singulière en un produit dont l'annulation est a priori plus visible que celle d'une somme brute. Maintenant, il faut travailler sur ce produit. Pour finir la preuve du théorème, nous allons prouver deux résultats :

Résultat 1. *Si* $s \geqslant 2^k + 1$, *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. On a vu dans la section précédente que :

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

(le δ dépend de k). Ceci implique :

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

Donc, par convergence de la série $\sum \ln(\chi(p))$(cette série est définie à partir d'un certain rang car $(\chi(p) - 1) \to 0$ et χ est un fonction réelle et il y a convergence car $\mid \ln(\chi(p)) \mid \ll \mid \chi(p) - 1 \mid \ll p^{-1-\delta}$), il existe $p_0(k)$ tel que :

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

Et le résultat découle en passant à l'exponentielle. □

Maintenant, énonçons le deuxième résultat utile pour la preuve :

Résultat 2. *Si* $s \geqslant 2^k + 1$, *alors il existe un réel* $C(p,k,s) > 0$ *(indépendant de* N*) tel que :*

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

Avant de prouver ce résultat, nous allons commencer par introduire quelques définitions et deux lemmes :

Définitions 1)On note $M(q)$ le nombre de solutions de la congruence :

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

2)Pour n'importe quel nombre premier p, on définit γ comme suit :

$$\gamma = \begin{cases} \mathcal{V}_p(k) + 1 & \text{si } p > 2 \\ \mathcal{V}_p(k) + 2 & \text{si } p = 2 \end{cases}$$

où $\mathcal{V}_p(k)$ désigne la valuation en p de k

Enonçons maintenant deux lemmes admis utiles pour la suite :

Lemme. *Si* $m \neq 0[p]$ *et s'il existe* y *tel que* $y^k \equiv m \pmod{p^\gamma}$ *alors la congruence* $x^k \equiv m \pmod{p^\nu}$ *est résoluble pour tout* $\nu \geq \gamma$

Démonstration. Ce lemme se démontre en utilisant le fait que le groupe $(\mathbf{Z}/_{p^\nu \mathbf{Z}})^*$ est cyclique si $p > 2$ et une affination pour le cas $p = 2$. Pour plus de détails, le lecteur peut consulter la référence principale [1]. □

Lemme. *Si* $s \geq 4k$, *la congruence*

$$x_1^k + \cdots + x_s^k \equiv N[p^\gamma]$$

a toujours une solution tel que $x_1, \ldots, x_s$ *non tous divisibles par* p

Une preuve détaillée du dernier lemme est donnée dans la référence principale.

Il est temps maintenant de prouver le résultat 2

Démonstration. On suppose que $s \geqslant 2^k + 1$. Nous allons utiliser la fonction M que nous avons introduite dans les définitions ci-dessus. En effet, nous allons faire un lien entre M et χ. Nous pouvons exprimer $M(q)$ sous la forme d'une somme d'une manière analogue avec ce que nous avons vu précedemment. On a alors :

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

car la somme sur t vaut q si la congruence est satisfaite et 0 sinon. Maintenant, dans cette somme, nous allons rassembler les t ayant le même p.g.c.d avec q. Ceci donne :

$$M(q) = q^{-1} \sum_{q_1/q} \sum_{\substack{u=1 \\ (u,q_1)=1}}^{q_1} \sum_{x_1=1}^{q} \cdots \sum_{x_s=1}^{q} e\left(\frac{u}{q_1}\left(x_1^k + \cdots + x_s^k - N\right)\right)$$

Or

$$\sum_{x=1}^{q} e\left(\frac{u}{q_1} x^k\right) = \sum_{z=0}^{\frac{q}{q_1}-1} \sum_{y=1}^{q_1} e\left(\frac{u}{q_1}(zq_1 + y)^k\right) = \frac{q}{q_1} \sum_{y=1}^{q_1} e\left(\frac{u}{q_1} y^k\right) = \frac{q}{q_1} S_{u,q_1}$$

D'où

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

Ainsi, en particulier quand $q = p^n$, cette dernière égalité donne :

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

et en faisant tendre n vers l'infini, on obtient :

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

Nous allons donc essayer de minorer le rapport pour atteindre notre but. Par le lemme admis, on sait qu'il existe $a_1, \ldots, a_s$ tel que : $a_1^k + \cdots + a_s^k \equiv N[p^\gamma]$ avec $a_1 \neq 0[p]$. Nous allons construire "beaucoup" de solutions de la congruence $x_1^k + \cdots + x_s^k \equiv N[p^\nu]$ avec $\nu \geq \gamma$. On choisit arbitrairement $x_2, \ldots, x_s$ tel que :

$$\forall j \in [2, s], x_j \equiv a_j[p^\gamma] \quad et \quad 0 < x_j \leq p^\nu$$

On a en fait $p^{(\nu-\gamma)(s-1)}$ choix possibles. Pour un de ces choix, on a toujours $a_1^k \equiv N - x_2^k - \cdots - x_s^k[p^\gamma]$. D'où, par le lemme admis, on peut trouver x_1 de sorte que :

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

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

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

Le résultat 2 est alors prouvé. □

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

Fin de la preuve 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 précédemment, on a :

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

5 LES NOMBRES $G(k)$

Dans cette section nous allons essayer de majorer la fonction G dont nous rappellons la définition. A tout entier naturel k, on associe le nombre $G(k)$ représentant le plus petit entier s tel que tout entier suffisamment grand soit la somme d'au plus s puissances k^{ime} d'entiers. Cette fonction a été introduite par Landau et largement étudiée par Hardy et Littlewood dans leurs travaux sur le problème de Waring. Elle a l'avantage d'éliminer les cas particuliers rendant pénible l'étude de la fonction g. En première approche, on peut espérer que cette fonction soit un peu plus régulière que la fonction g. Par le développement asymptotique prouvé dans les parties précédentes, on a directement : $G(k) \leq 2^k + 1$. Essayons maintenant de la minorer par un argument de densité. Soit k un entier naturel. Soit X un entier naturel. Le nombre $\rho(X)$ de $(k-1)$-uplets $(x_1, \ldots, x_{k-1})$ satisfaisant la condition $x_1^k + \cdots + x_{k-1}^k \leq X$ est majoré par $\left(X^{\frac{1}{k}}\right)^{k-1}$ (car chaque x_i est majoré par $X^{\frac{1}{k}}$), i.e $\forall X \in \mathbb{N}, \rho(X) \leqslant X^{1-\frac{1}{k}}$. Ainsi :

$$\lim_{X\to\infty} \frac{\rho(X)}{X} = 0$$

Or si $G(k) \leq k - 1$, ce rapport tendrait vers 1

Cet argument nous dit alors que $G(k) \geq k$
Maintenant, revenons à notre but initial. Nous allons prouver le théorème suivant :

Théorème 3. $\forall k \in \mathbb{N}, G(k) < 4k + 6k\ln(3k) + 3$

L'idée essentielle de la preuve est de considérer une représentation un peu différente de la représentation initiale de Waring. En effet, nous allons considérer les représentations d'un nombre N sous la forme spéciale :

$$N = x_1^k + \cdots + x_{4k}^k + u_1 + u_2 + y^k v$$

avec
$(i) \forall j \in [1, 4k], 1 \leq x_j \leq P$
$(ii) u_1$ et u_2 sont deux entiers inférieurs à $\frac{1}{4}P^k$ et représentables comme somme de l puissances k^{me} (l étant un entier arbitrairement fixé au départ)
$(iii) 1 \leq y \leq P^{\frac{1}{2k}}$
$(iv) v$ est un nombre inférieur à $\frac{1}{4}P^{k-\frac{1}{2}}$ représentable comme somme de l puissances k^{me}

Ainsi, tout nombre mis sous la forme spéciale est somme de $4k + 3l$ puissances k^{ime}. Pour prouver qu'une telle représentation existe, il faut choisir un l (en fonction de k) bien adapté. Après, nous choisirons $P = [N^{\frac{1}{k}}]+1$ de sorte que $\frac{1}{5}P^k < N - u_1 - u_2 - y^k v < P^k$. Dans la suite nous allons bien évidemment utiliser la méthode du cercle et notamment un découpage de celui-ci en arc mineur et arc majeur.

Commençons tout d'abord par définir les arcs majeurs.

Définition. *Soit a et q deux entiers naturels tel que : $(a, q) = 1$, $1 \leq a \leq q$ et $q \leq \sqrt{P}$.*
On définit l'arc majeur $\mathcal{M}_{a,q} = \{\alpha \in [0, 1]$ vérifiant $|q\alpha - a| < \frac{1}{2kP^{k-1}}\}$
L'arc majeur $\mathcal{M}$ est la totalité des arcs majeurs $\mathcal{M}_{a,q}$

Nous allons commencer par énoncer ce résultat sur l'arc majeur.

Résultat 3. *Supposons que $s \geq 4k$. Alors, si $\frac{1}{5}P^k \leq M \leq P^k$, on a :*

$$\int_{\mathcal{M}} T(\alpha)^s e(-M\alpha)\, d\alpha \gg P^{s-k}$$

La démonstration repose essentiellement sur les mêmes idées utilisées dans la partie démontrant la formule asymptotique (arc majeur) moyennant quelques lemmes techniques. Pour plus de précisions, le lecteur peut consulter la référence centrale.

Il reste à étudier l'arc mineur. Pour cela nous avons besoin de quelques lemmes.

Lemme. *(**Hardy et Littlewood**) Si $U_l(X)$ est le nombre d'entiers inférieurs à X représentables en somme de l puissances k^{ime}, alors :*

$$U_l(X) \gg X^{1-\lambda^l} \, avec \, \lambda = 1 - \frac{1}{k}$$

Démonstration. La preuve se fait par récurrence sur l.
En effet, si $l = 1$, $U_1(X) = \left[X^{\frac{1}{k}}\right]$ et le membre de droite vaut $X^{\frac{1}{k}}$. Faisons maintenant l'induction sur l.

Considérons les nombres de la forme $x^k + z$ avec :

$$\left(\frac{1}{4}X\right)^{\frac{1}{k}} < x < \left(\frac{1}{2}X\right)^{\frac{1}{k}} \, , \, 0 < z < \frac{1}{2}X^{1-\frac{1}{k}} \text{ et } z \text{ est somme de } l-1 \text{ puissances } k^{me}$$

Tous ces nombres sont deux à deux distincts. En effet, par l'absurde, si

$$x_1^k + z_1 = x_2^k + z_2 \text{ avec } x_1 > x_2$$

on a : $x_1^k - x_2^k > kx_2^{k-1} > k\left(\frac{1}{4}X\right)^{1-\frac{1}{k}} > \frac{1}{2}X^{1-\frac{1}{k}}$
(la deuxième inégalité vient des accroissements finis)
Alors que : $z_2 - z_1 < z_2 < \frac{1}{2}X^{1-\frac{1}{k}}$

Il y a donc une contradiction.

Le nombre de choix possibles pour x est $\gg X^{\frac{1}{k}}$ et celui pour z est $U_{l-1}(\frac{1}{2}X^{1-\frac{1}{k}})$. Ceci donne immédiatement $U_l(X) \gg X^{\frac{1}{k}}U_{l-1}(\frac{1}{2}X^{1-\frac{1}{k}})$

Donc, par l'hypothèse de récurrence :

$$U_l(X) \gg X^{\frac{1}{k}}X^{(1-\frac{1}{k})(1-\lambda^{l-1})} = X^{1-\lambda^l}$$

ce qui achève la récurrence et la preuve du lemme de Hardy-Littlewood. □

Corollaire 1. *(**Hardy et Littlewood**) Soit $R(\alpha) = \sum_{u<\frac{1}{4}P^k} e(\alpha u)$ où u est aussi une somme de l puissances k^{me}. Alors :*

$$\int_0^1 |R(\alpha)|^2 d\alpha = R(0) \ll P^{-k(1-\lambda^l)}R^2(0)$$

Démonstration. L'égalité entre l'intégrale et $R(0)$ est évidente. Le deuxième résultat découle du lemme précédent et plus précisemment du fait :

$$R(0) = U_l(\frac{1}{4}P^k) \gg P^{k(1-\lambda^l)}$$

□

Pour continuer, nous avons besoin d'un résultat dû à Vinogradov.

Lemme. *(**Vinogradov (admis)**) Soient X' un ensemble de X_0 entiers distincts inclus dans un intervalle de longueur X et Y' un ensemble de Y_0 entiers distincts inclus dans un intervalle de longueur Y. Supposons que $\alpha = \frac{a}{q} + O(q^{-2})$ où $(a,q) = 1, q > 1$. Alors :*

$$|\sum_{x\in X'}\sum_{y\in Y'} e(\alpha xy)|^2 \ll X_0Y_0\frac{\ln(q)}{q}(q+X)(q+Y)$$

Ce lemme est admis. Cependant, nous allons prouver un de ses corollaires.

Corollaire 2. *(**Vinogradov**) Soit $S(\alpha) = \sum_y \sum_v e(\alpha y^k v)$ où les conditions de sommation sont celles de (iii) et (iv) de la forme spéciale. Alors, si $\alpha = \frac{a}{q} + O(q^{-2})$ avec $\sqrt{P} < q \leq 2kP^{k-1}$, on a :*

$$|S(\alpha)| \ll S(0)P^{-\frac{1}{4k}+\frac{1}{2}(k-\frac{1}{2})\lambda^l+\epsilon}$$

avec ϵ un réel strictement positif quelconque.

Démonstration. Utilisons le lemme de Vinogradov avec :

$$X = [1, \frac{1}{4}P^{k-\frac{1}{2}}], \quad X_0 = U_l(\frac{1}{4}P^{k-\frac{1}{2}})$$

$$Y = \sqrt{P}, \quad Y_0 = P^{\frac{1}{2k}}$$

Ceci donne :

$$\begin{aligned} |S(\alpha)|^2 &\ll X_0P^{\frac{1}{2k}}\frac{\ln(q)}{q}(q+\frac{1}{4}P^{k-\frac{1}{2}})(q+\sqrt{P}) \\ &\ll X_0P^{\frac{1}{2k}}\ln(P)P^{k-\frac{1}{2}} \end{aligned}$$

Or $S(0) = P^{\frac{1}{2k}}X_0$

Donc $|\frac{S(\alpha)}{S(0)}|^2 \ll P^{-\frac{1}{2k}+(k-\frac{1}{2})+2\epsilon}X_0^{-1}$ ($\epsilon > 0$ quelconque)

Or le lemme de Hardy-Littlewood donne $X_0 \gg P^{(k-\frac{1}{2})(1-\lambda^l)}$

Donc, en prenant la racine carrée des inégalités, on a le corollaire de Vinogradov. □

Maintenant, le terrain est suffisamment préparé pour traiter l'arc mineur. Nous allons donc prouver ce résultat :

Résultat 4. *Notons m l'arc mineur qui est par définition le complémentaire de l'arc majeur $\mathcal{M}$.*
Si $l \geq 2k\ln(3k)$, on a :

$$\int_m |T(\alpha)|^{4k}|R(\alpha)|^2||S(\alpha)|d\alpha \ll P^{3k}R(0)^2S(0)P^{-\delta}$$

pour un certain $\delta > 0$

Démonstration. Le théorème d'approximation diophantienne de Dirichlet nous dit que pour tout α il existe a, q tel que :

$$(a,q) = 1,\ 1 \leq q \leq 2kP^{k-1},\ |\alpha - \frac{a}{q}| < \frac{1}{2kqP^{k-1}}$$

Donc si α n'est pas dans $\mathcal{M}_{a,q}$, nous devons forcément avoir $q > \sqrt{P}$. D'où par le corollaire de Vinogradov,

$$|S(\alpha)| \ll S(0)P^{-\frac{1}{4k}+\frac{1}{2}(k-\frac{1}{2})\lambda^l+\epsilon}$$

avec ϵ un réel strictement positif quelconque.
Par le corollaire de Hardy et Littlewood, on a :

$$\int_0^1 |R(\alpha)|^2 d\alpha \ll R(0)^2P^{-k(1-\lambda^l)}$$

Donc, en utilisant l'estimation triviale $|T(\alpha)| \leq P$, on trouve :

$$\begin{aligned}\int_{\mathrm{m}} |T(\alpha)|^{4k}|R(\alpha)|^2||S(\alpha)|d\alpha &\ll P^{3k}R(0)^2S(0)P^{-\frac{1}{4k}+\frac{3}{2}k\lambda^l+\epsilon-\frac{1}{4}\lambda^l} \\ &\ll P^{3k}R(0)^2S(0)P^{-\frac{1}{4k}+\frac{3}{2}k\lambda^l}\end{aligned}$$

Si $l \geq 2k\ln(3k)$, on a :

$$\ln(\lambda^l) = l\ln\left(1-\frac{1}{k}\right) < -\frac{l}{k} < -2\ln(3k)$$

Donc $\lambda^l < (3k)^{-2}$ et $\frac{3}{2}k\lambda^l < \frac{1}{6k}$
Finalement :

$$\int_{\mathrm{m}} |T(\alpha)|^{4k}|R(\alpha)|^2||S(\alpha)|d\alpha \ll P^{3k}R(0)^2S(0)P^{-\frac{1}{12k}}$$

□

À ce stade tout est prêt pour prouver le théorème énoncé au début de cette section.

Démonstration. Notons $r_1(N)$ le nombre de représentations de N sous forme spéciale. Donc

$$r_1(N) = \int_0^1 T(\alpha)^{4k}R(\alpha)^2S(\alpha)e(-N\alpha)d\alpha$$

Par le résultat 4 , la contribution de l'arc mineur dans cette intégrale a un ordre strictement inférieur à $P^{3k}R(0)^2S(0)$ si $l \geq 2k\ln(3k)$. Déterminons maintenant la contribution de l'arc majeur. Elle est égale à

$$\sum_{u_1}\sum_{u_2}\sum_{y}\sum_{v}\int_{\mathcal{M}} T^{4k}(\alpha)e(\alpha(-N+u_1+u_2+y^kv))d\alpha$$

Le nombre de termes est égal à $R(0)^2S(0)$, et comme remarqué précédemment (après la définition de la forme spéciale), on a toujours :

$$\frac{1}{5}P^k < N - u_1 - u_2 - y^kv < P^k$$

D'où, par le résultat 3 , l'intégrale sur $\mathcal{M}$ est $\gg P^{3k}$ ($s = 4k$). Ainsi :

$$r_1(N) \gg P^{3k}R(0)^2S(0)$$

Donc : $r_1(N) \to \infty$ quand $N \to \infty$ (car $P = [N^{\frac{1}{k}}] + 1$) Il suit, puisque ce qui précède est valable pour tout $l \geq 2k\ln(3k)$, $G(k) < 4k + 3(2k\ln(3k)+1)$
Ce qui achève la preuve du théorème central de cette section qui est le théorème de majoration de la fonction G. □

De ce théorème découle un autre théorème éclairant la notion de régularisation évoquée comme prétexte pour introduire la fonction G.

Théorème 4. *On a :*

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

Démonstration. On peut facilement minorer la fonction g. En effet, le nombre 2^k-1 ne peut être représenté comme somme de puissances k^{me} que par une somme à $2^k - 1$ de 1 . Donc, $\forall k \in \mathbb{N}, g(k) \geq 2^k$. Ainsi, en utilisant la majoration du théorème, on a :

$$\forall k \in \mathbb{N}, \frac{G(k)}{g(k)} \leq \frac{4k + 6k\ln(3k) + 3}{2^k}$$

Puis, il vient alors :

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

□

En conclusion, on peut remarquer qu'on a résolu un problème de nature arithmétique par des méthodes essentiellement analytiques, et de plus que ces méthodes sont facilement généralisables à des équations diophantiennes polynomiales. On peut également noter qu'il existe différents raffinements permettant d'obtenir de meilleurs conditions pour les inégalités.

Références

[1] H. Davenport. *Analytic methods for diophantine equations and diophantine inequalties.*

[2] D.R. Heath-Brown. *Weyl's inequality, Hua's inequality and Waring's problem* . J. London. Math. Soc. 38(1988) 216-230

[3] G. H. Hardy. *Trois problèmes célèbres de la théorie des nombres.* Les presses universitaires de France, 1931

[4] E.T. Whittaker et G.N.Watson. *Modern analysis.* Cambridge university.