ENS de Rennes
Université Rennes 1

Département de Mathématiques
Rapport de Stage

Problème de la discrépance d'Erdos

Élève :
Titouan Donnart

Encadrant :
Pierre-Yves Bienvenu

Introduction :

Une heuristique en théorie analytique des nombres stipule que les ensembles de nombres entiers positifs ne peuvent pas être simultanément structurés de manière additive et multiplicative. La vérification pratique de cette heuristique est à l'origine d'un grand nombre de problèmes difficiles. Les conjectures de ce type sont également au moins équivalentes sur le plan conceptuel à l'attente selon laquelle une fonction multiplicative quelconque se comporte de manière aléatoire sur des ensembles additifs.

Dans ce rapport, nous examinons l'un de ces problèmes qui est resté ouvert jusqu'en 2015 : *le problème de la discrépance d'Erdos*. Il s'agit de voir si oui ou non la borne supérieure prise (en module) par les sommes des éléments d'une suite $(f(n))_{n\in\mathbb{N}}$ à valeurs dans $\{-1,+1\}$ le long de progressions arithmétiques homogènes est infinie.

Après avoir rappelé divers résultats de base sur la théorie analytique des nombres, nous nous intéresserons au point de départ de la preuve du problème de la discrépance d'Erdos : les résultats obtenus par Matomaki et Radziwill en 2014 sur les moyennes de fonctions multiplicatives sur de petits intervalles. Ces résultats ont bouleversé la recherche en théorie analytique des nombres, et la direction de notre rapport emprunte seulement l'une des nombreuses conséquences importantes de ces résultats.

Cela nous amènera à discuter de la conjecture de Chowla et d'Elliott, ainsi que des versions dites "en moyenne" de ces conjectures, qui seront démontrées par les résultats obtenus par Matomaki et Radziwill. Enfin, nous nous intéresserons à la démonstration de Tao du problème de la discrépance d'Erdos.

Je tiens personnellement à remercier chaleureusement mon maître de stage, Pierre-Yves Bienvenu, de m'avoir fait découvrir ce domaine des mathématiques dont je n'avais presque aucune connaissance avant ce stage. Je tiens aussi à le remercier pour toute l'aide et toutes les connaissances qu'il m'a apportées pendant ces deux mois. Je tiens également à remercier l'ensemble du personnel du Trinity College de m'avoir permis de réaliser ce stage dans un bon cadre. Enfin, je remercie l'ENS de Rennes et le centre Henri Lebesgue de m'avoir octroyé une bourse pour que je puisse réaliser ce stage à Dublin malgré le coût très élevé du logement là-bas.

Je tiens enfin à signaler que ce présent n'est qu'un trés bref aperçu de mon travail réalisé pendant ces deux mois. Sur ma page web, on retrouvera mon rapport de stage complet comportant l'étude des résultats de Matomaki et Radziwill et de la démonstration de la conjecture d'Elliott en moyenne logarithmique ainsi que la plupart des démonstrations manquantes.

Table des matières

Notations :

— Si A est un ensemble fini on notera $|A|$ son cardinal.

— Si A est une partie de $\mathbb{R}$ mesurable (pour la mesure de Lebesgue), on notera mes(A) sa mesure.

— Si A est un ensemble, on notera $\mathbb{1}_A$ la fonction indicatrice de A ($\mathbb{1}_A(x) = 1$ si $x \in A$ et est égal à 0 sinon). De plus si S est un énoncé mathématique on notera $\mathbb{1}_S$ la fonction qui vaut 1 quand S est vraie et 0 quand S est fausse. Ainsi on notera par exemple $\mathbb{1}_{2|n}$ l'indicatrice des nombres pairs.

— On notera log le logarithme népérien.

— Si $x \in \mathbb{R}$, on notera $\lfloor x \rfloor$ sa partie entière.

— Si $x \in \mathbb{R}_+$, on notera une somme $\sum_{n \leqslant x}$ la somme $\sum_{n=0}^{\lfloor x \rfloor}$. Une somme indicée sur p sera toujours une somme sur les nombres premiers.

— Pour tous $m, n \in \mathbb{Z}$, on notera (m, n) leur PGCD.

— On rappelle qu'une fonction $f : \mathbb{N} \to \mathbb{C}$ est dite multiplicative si pour tous m, n premiers entre eux $f(mn) = f(m)f(n)$, on dit qu'elle est complètement multiplicative si celle égalité est valable pour tous $m, n \in \mathbb{N}$.

— Si $f : \mathbb{N} \to \mathbb{C}$, on notera $\mathcal{D}f$ sa série de Dirichlet qui vérifie pour tous $s \in \mathbb{C}$ (lorsque cette quantité est définie) :

$$\mathcal{D}f(s) = \sum_{n=0}^{+\infty} \frac{f(n)}{n^s}.$$

— On notera φ l'indicatrice d'Euler définie par $\varphi(n) = |\{1 \leq k \leq n;\ k \text{ est premier avec } n\}|$.

— On note μ la fonction de Mobiüs définie par $\mu(1) = 1$,$\mu(n) = 0$ si n possède un facteur carré et $\mu(n) = (-1)^k$ si n est le produit de k nombres premiers distincts. Elle est multiplicative.

— On note λ la fonction de Liouville définie par $\lambda(n) = (-1)^{\Omega(n)}$ où $\Omega(n)$ désigne le nombre de facteurs premiers comptés avec multiplicité de l'entier n. C'est une fonction complètement multiplicative.

— On note π la fonction qui à $x \in \mathbb{R}$ compte le nombre de nombres premiers inférieurs ou égaux à x.

— On adoptera les notations asymptotiques dans deux contextes, un où il n'y a pas de paramètre asymptotique présent et un où il y en a. Dans le contexte sans paramètre asymptotique, on utilisera $X = \mathcal{O}(Y)$, $X \ll Y$ ou $Y \gg X$ pour noter une estimation de la forme $|X| \leqslant CY$ où C est une constante fixe.

— Dans certains cas où la constante C dépend de paramètres additionnels comme k on le notera en indice comme ceci $X = \mathcal{O}_k(Y)$, $X \ll_k Y$ ou $Y \gg_k X$.

— Quand il existe un paramètre asymptotique (par exemple x) tous les objets mathématiques pourront dépendre de ce paramètre (à part contre-indications). On utilisera $X = \mathcal{O}(Y)$, $X \ll Y$ ou $Y \gg X$ pour noter une estimation de la forme $|X| \leqslant CY$ où C est une constante qui peut dépendre d'autre paramètres tant que ceux-ci sont fixés. On notera aussi $X = o(Y)$ pour noter une estimation de la forme $|X| \leqslant cY$ où c est une quantité qui tend vers 0 quand le paramètre asymptotique tend vers $+\infty$.

Les autres notations apparaissant dans ce rapport seront précisées au fur et à mesure du document.

I Rappels et quelques éléments de théorie analytique des nombres

I.1 Caractères, transformée de Fourier sur un groupe fini et sommes Gaussiennes

Dans cette partie on va s'intéresser aux caractères de Dirichlet et à la transformée de Fourier sur un groupe fini. Nous n'allons pas démontrer les résultats ici car ce sont plutôt des résultats classiques de cours de L3/M1 sur les représentations de groupes. Pour les preuves on fera référence à [1] (sauf contre-indication).

Définition I.1

— *Soit G un groupe fini abélien. On appelle* ***caractère*** *sur le groupe G, tout morphisme $\chi : G \to \mathbb{C}$. On notera $\hat{G}$ l'ensemble des caractères de G.*

— *Soit $q > 0$. On appelle* ***caractère de Dirichlet modulo*** *q toute fonction $\chi : \mathbb{N} \to \mathbb{C}$ telle qu'il existe un caractère $\tilde{\chi} : (\mathbb{Z}/q\mathbb{Z})^* \to \mathbb{C}$ tel que :*

$$\forall n \in \mathbb{N} : \chi(n) = \mathbb{1}_{(n,q)=1}\tilde{\chi}(n \mod q).$$

— *Le caractère de Dirichlet valant 1 sur les entiers premiers avec n et 0 ailleurs est appelé* ***caractère principal*** *modulo n.*

— *Le caractère de Dirichlet principal modulo 1 (valant 1 sur tous les entiers) est dit* ***caractère trivial****.*

Intéressons-nous maintenant à la transformée de Fourier sur un groupe fini abélien G que l'on fixe pour le reste de cette partie. Sur l'ensemble $\mathbb{C}[G]$ des applications de G dans $\mathbb{C}$, on définit le produit scalaire hermitien par :

$$\forall f, g \in \mathbb{C}[G] = \frac{1}{|G|}\sum_{x\in G} f(x)\overline{g(x)}.$$

Définition I.2

— *Soient $f \in \mathbb{C}[G]$ et $\chi \in \hat{G}$. On définit le* ***coefficient de Fourier*** *$c_f(\chi)$ par : $c_f(\chi) = \langle f \mid \chi\rangle$.*

— *On appelle transformée de Fourier sur G, l'application $\mathcal{F}$ qui à $f \in \mathbb{C}[G]$ associe $\hat{f}$ définie par :*

$$\forall \chi \in \hat{G} : \hat{f}(\chi) = |G|\, c_f(\overline{\chi}) = \sum_{x\in G} f(x)\chi(x).$$

Par les relations d'orthogonalité entre les caractères on obtient les deux résultats suivants :

Proposition I.3

Soit $f \in \mathbb{C}[G]$, on a la formule d'inversion :

$$f = \sum_{\chi\in\hat{G}} c_f(\chi)\chi = \frac{1}{|G|}\sum_{\chi\in\hat{G}} \hat{f}(\chi)\chi^{-1}.$$

Proposition I.4

Soient $f, g \in \mathbb{C}[G]$, on a la formule de Plancherel :

$$\sum_{s\in G} f(s)\overline{g(s)} = |G| \sum_{\chi\in\hat{G}} c_f(\chi)\overline{c_g(\chi)} = \frac{1}{|G|}\sum_{\chi\in\hat{G}} \hat{f}(\chi)\overline{\hat{g}(\chi)}.$$

On termine cette partie en énonçant un résultat sur les sommes gaussiennes (voir Théorème 8.7, [2]).

Proposition I.5

Soit χ un caractère de Dirichlet modulo q. On note pour tout $n \geqslant 1$:

$$G(n,\chi) := \sum_{m=1}^{q} \chi(m) e\left(\frac{mn}{q}\right).$$

Alors on a pour tout $n \geqslant 1$:

$$G(n,\chi) = \overline{\chi(n)} G(1,\chi).$$

I.2 Distance prétentieuse

On va introduire une notion de distance entre deux fonctions multiplicatives. Nous allons nous cantonner aux fonctions multiplicatives dite *1-bornées* c'est à dire des fonctions $f : \mathbb{N} \to \mathbb{C}$ vérifiant pour tout $n \in \mathbb{N} : |f(n)| \leqslant 1$.

Définition I.6

Soient f, g deux fonctions multiplicatives 1-bornées et fixons un seuil $X \in \mathbb{R}_+^* \cup \{+\infty\}$. ***La distance prétentieuse*** *$D(f,g;X)$ entre f et g à l'échelle X est :*

$$\mathbb{D}(f,g;X) = \sqrt{\sum_{p\leqslant X} \frac{1 - \mathcal{R}e\left(f(p)\overline{g(p)}\right)}{p}}.$$

La distance prétentieuse n'est pas une distance comme le fournit la proposition ci-dessous. Pourtant, elle possède quand même des propriétés appréciables que vérifie une distance comme l'inégalité triangulaire et la symétrie et c'est pour cela qu'elle est utile en pratique.

Proposition I.7

Soient f, g, h des fonctions multiplicatives 1-bornées et soit $X \geqslant 2$. On a les propriétés suivantes :

- $\mathbb{D}(f,g;X) \geqslant 0$ et il y a égalité si et seulement si $f(p) = g(p)$ et $|f(p)| = 1$ pour tout $p \leqslant X$,
- $\mathbb{D}(f,g;X) = \mathbb{D}(g,f;X)$,
- $\mathbb{D}(f,h;X) \leqslant \mathbb{D}(f,g;X) + \mathbb{D}(g,h;X)$.

On finit par introduire quelques définitions liées à la distance prétentieuse qui nous seront plutôt utiles dans les parties suivantes.

Définition I.8

Pour toute fonction multiplicative g 1-bornée, pour tout $Q \geqslant 1$ et pour tout $X \geqslant 2$, on introduit les quantités suivantes :

$$M(g;X) = \inf_{|t|\leqslant X} \mathbb{D}(g, n \mapsto n^{it}; X).$$

$$M(g;X,Q) = \inf_{\chi[q],q\leqslant Q} M(g\overline{\chi};X) \quad et \quad M(g;\infty,\infty) = \inf_{\chi,t} \mathbb{D}(g, n \mapsto \chi(n)n^{it}, \infty)^2.$$

Lorsque $M(g;X)$ est petit alors g "prétend" être $n \mapsto n^{it}$ et $M(g;X,Q)$ est petit lorsque g "prétend" être un caractère de Dirchlet modulo au plus Q tordu de facteur de torsion au plus X.

I.3 La conjecture de Chowla en moyenne logarithmique

I.3.1 Présentation de la conjecture de Chowla et de la conjecture d'Elliott

Connaître les corrélations à k points de fonctions multiplicatives est étroitement lié problèmes additifs dans les nombres premiers. On peut par exemple étudier le nombre de facteurs premiers d'un nombre n par rapport au nombre de facteurs premiers de $n+h$ pour $n, h \in \mathbb{N}$, s'intéresser aux corrélations à k points de la fonction de Liouville est donc une question naturelle.
En supposant la véracité de l'hypothèse de Riemann, la différence entre le nombre de valeurs de $n \leqslant x$ telles que $\lambda(n) = +1$ et le nombre de valeurs de $n \leqslant x$ telles que $\lambda(n) = -1$ est approximativement de l'ordre de $O\left(x^{1/2+\varepsilon}\right)$. Ceci est cohérent avec le comportement d'une suite de variables aléatoires indépendantes de Rademacher X_n (en supposant les valeurs de la fonction de Liouville comme indépendantes), prenant les valeurs +1 et -1 avec une probabilité égale par le théorème limite central.
Or, par indépendance des ces variables aléatoires, on sait que aussi que pour tout $k, n \in \mathbb{N}^*$, $h_1, \ldots, h_k$ des entiers naturels distincts et $\varepsilon_1, \ldots, \varepsilon_k \in \{-1, +1\}$: $\mathbf{P}(X_{n+h_1} = \varepsilon_1, \ldots, X_{n+h_k} = \varepsilon_k) = 2^{-k}$. Si les valeurs de λ sont effectivement essentiellement indépendantes, il est donc raisonnable de penser que les composantes des vecteurs $(\lambda(n+h_1), \ldots, \lambda(n+h_k))$ changent indépendamment lorsque n varie, c'est à dire :

$$\frac{1}{x}\left|\{n \leqslant x \quad \text{tel que} \quad \lambda(n+h_1) = \varepsilon_1, \ldots, \lambda(n+h_k) = \varepsilon_k\}\right| \xrightarrow[x\to+\infty]{} 2^{-k}.$$

Ceci est lié aux corrélations à k points de la fonction de Liouville par la proposition suivante :

Proposition I.9

Soient $k \in \mathbb{N}^*$, $\varepsilon_1, \ldots, \varepsilon_k \in \{-1, +1\}$, $h_1, \ldots, h_k \in \mathbb{N}^*$. Les deux propositions sont équivalentes :

(i) $\quad \frac{1}{x}\left|\{n \leqslant x \quad \text{tel que} \quad \lambda(n+h_1) = \varepsilon_1, \ldots, \lambda(n+h_k) = \varepsilon_k\}\right| \xrightarrow[x\to+\infty]{} 2^{-k}.$

(ii) $\quad \sum_{n=1}^{x} \lambda(n+h_1)\ldots\lambda(n+h_k) = o_{x\to+\infty}(x).$

Démonstration : Dans cette preuve on va adopter la notation suivante, pour $S \subset \{1, \ldots, k\}$, on posera $\varepsilon_S = \prod_{j\in S} \varepsilon_j$. On va procéder directement par équivalence : la proposition (i) est équivalente à

$$\lim_{x\to+\infty} \frac{1}{x} \sum_{n\leqslant x} \mathbb{1}_{\lambda(n+h_1)=\varepsilon_1} \ldots \mathbb{1}_{\lambda(n+h_k)=\varepsilon_k} = 2^{-k}.$$

Or comme on a pour tout $j \in \{1, \dots, k\}$: $\dfrac{1+\varepsilon_j \lambda(n+h_j)}{2} = \mathbb{1}_{\lambda(n+h_j)=\varepsilon_1}$, ceci est équivalent à :

$$\lim_{x\to+\infty} \frac{1}{x} \sum_{n\leqslant x} \prod_{j=1}^{k} (1+\varepsilon_j \lambda(n+h_j)) = 1.$$

C'est-à-dire :

$$\lim_{x\to+\infty} \frac{1}{x} \sum_{n\leqslant x} \sum_{S\subset\{1,\dots,k\}} \varepsilon_S \prod_{j\in S} \lambda(n+h_j) = 1,$$

ce que l'on peut encore réécrire :

$$\lim_{x\to+\infty} \sum_{S\subset\{1,\dots,k\}} \frac{1}{x} \sum_{n\leqslant x} \varepsilon_S \prod_{j\in S} \lambda(n+h_j) = 1.$$

Or, ici tous les termes de la somme sur $S \subset \{1, \dots, k\}$ sont positifs donc cette dernière proposition est équivalente à (ii) (en basculant de l'autre côté de l'égalité le terme associé à $S = \varnothing$). *De facto*, on vient de prouver l'équivalence entre (i) et (ii). □

C'est sous cette deuxième forme que Sarvadaman D. S. Chowla a émis cette conjecture dans [3].

Conjecture I.10: (Chowla)

Soient $k \in \mathbb{N}^*$, $\varepsilon_1, \dots, \varepsilon_k \in \{-1, +1\}$, $h_1, \dots, h_k \in \mathbb{N}^*$. On a :

$$\sum_{n=1}^{x} \lambda(n+h_1) \dots \lambda(n+h_k) = o_{x\to+\infty}(x).$$

C'est toujours à l'heure actuelle une conjecture mais les résultats de Matomaki et Radziwill permettent d'obtenir de nombreuses avancées. On va dans cette partie présenter une version "en moyenne" sur les paramètres $(h_1, \dots, h_k)$. Dans la partie suivante nous présenterons une autre version en moyenne.

Une généralisation de la conjecture de Chowla est la suivante, appelée conjecture d'Elliott :

Conjecture I.11: (Elliott)

Soient $g_1, \dots, g_k : \mathbb{N} \to \mathbb{R}$ des fonctions multiplicatives 1-bornées et soient $(a_1, \dots, a_k, b_1, \dots, b_k) \in \mathbb{N}^{2k}$ tels que les (a_i, b_i) soient $\mathbb{Q}$-libres deux à deux. On suppose de plus qu'il existe $j_0 \in \{1, \dots, k\}$ tel que $M(g_{j_0}; \infty, \infty) = +\infty$. Alors :

$$\sum_{1\leqslant n\leqslant X} \prod_{j=1}^{k} g_j(a_j n + b_j) = o(X).$$

Cette conjecture affirme que pour tous (a_i, b_i) $\mathbb{Q}$-libres deux à deux et pour toutes fonctions multiplicatives 1-bornées $g_1, \dots, g_k$, on a l'asymptotique ci-dessus à part si tous les g_j prétendent être un caractère de Dirichlet tordu. Comme la fonction λ de Liouville vérifie l'hypothèse de la conjecture d'Elliott, cette dernière implique la conjecture de Chowla. Si on veut généraliser ce résultat pour des fonctions multiplicatives à valeurs complexes il faut remplacer l'hypothèse sur les g_j par la suivante [1] :

$$\text{Il existe } j_0 \in \{1, \dots, k\} \text{ tel que pour tout } Q \geqslant 0 : \lim_{X\to+\infty} M(g_{j_0}; X, Q) = +\infty.$$

1. Elles sont d'ailleurs équivalentes dans le cas des fonctions g_i à valeurs réelles.

I.3.2 Moyenne logarithmique de fonctions multiplicatives

On va dans ce paragraphe introduire une nouvelle manière de considérer une moyenne d'une fonction multiplicative qui est moins contraignante et qui permettra d'établir des résultats "en moyenne". Pour cela on va introduire la grandeur suivante.

Définition I.12

Soit $f : \mathbb{N} \to \mathbb{C}$ une fonction arithmétique. On dit que f admet une ***moyenne logarithmique*** *si la limite suivante existe :*

$$\lim_{x\to+\infty} \frac{1}{\log(x)} \sum_{k\leqslant x} \frac{f(k)}{k}.$$

Le résultat principal de ce paragraphe est le suivant :

Proposition I.13

Soit f une fonction arithmétique. Si elle possède une moyenne alors elle possède une moyenne logarithmique et elles sont égales. La réciproque est fausse.

Démonstration : Le premier fait est une conséquence directe de la formule de sommation par parties. Pour le sens . Pour le sens réciproque, on remarque que la fonction multiplicative $n \mapsto n^{it}$ possède une moyenne logarithmique car pour tout $x \geqslant 1$ (on prend évidemment $t \neq 0$) :

$$\sum_{n\leqslant x} n^{it-1} = \int_1^x u^{it-1}\,\mathrm{d}u + \mathcal{O}\left(\int_1^x (it-1)u^{it-2}\,\mathrm{d}u\right).$$

Montrons que :

$$x \mapsto \frac{1}{x}\sum_{n\leqslant x} n^{it} \text{ n'a pas de limite quand } x \to +\infty.$$

En effet d'après la formule de sommation par parties :

$$\sum_{n=1}^{x} n^{it} = \lfloor x\rfloor\, x^{it} - it\int_1^x \lfloor u\rfloor\, u^{it-1}\,\mathrm{d}u = x^{it+1}\left(1+\frac{it}{it+1}\right) + \mathcal{O}(1).$$

Ainsi :

$$\frac{1}{x}\sum_{n\leqslant x} n^{it} \underset{x\to+\infty}{\sim} x^{it}\left(1+\frac{it}{it+1}\right).$$

On en déduit le fait que $n \mapsto n^{it}$. □

En fait, on remarque qu'en module l'équivalent calculé est constant mais qu'il varie en argument en fonction de x, c'est parce que la fonction $n \mapsto n^{it}$ oscille trop. Cette fonction joue un rôle important dans le cadre général, une fonction multiplicative qui se situera assez loin (au sens de la distance prétentieuse) de $n \mapsto n^{it}$ ou de cette fonction tordue par un caractère comme dans le théorème ci-dessous, alors on pourra "contrôler" la moyenne et certaines auto-corrélations de cette fonction multiplicative. La moyenne logarithmique ne prend pas en compte les oscillations de n^{it} lorsque n est grand ce qui donne une plus grande perméabilité quant à l'admission de moyenne logarithmique.

En utilisant une moyenne logarithmique à la place d'une moyenne uniforme dans la conjecture d'Elliott, on obtient une conjecture d'Elliott "en moyenne logarithmique" qui elle a été démontrée :

Théorème I.14

Soient $a_1, a_2 \in \mathbb{N}$, $b_1, b_2 \in \mathbb{Z}$ tels que $a_1 b_2 - a_2 b_1 \neq 0$. Soit $\varepsilon > 0$ et soit A suffisamment grand devant a_1, a_2, b_1, b_2 et $\frac{1}{\varepsilon}$. Soit $x \geqslant \omega \geqslant A$ et soient $g_1, g_2 : \mathbb{N} \to \mathbb{C}$ deux fonctions multiplicatives 1-bornées. Supposons que g_1 est non-prétentieuse, c'est-à-dire pour tout caractère de Dirichlet χ de module au plus A et pour tout $t \in [-Ax, +Ax]$:

$$\mathbb{D}(g_1; n \mapsto \chi(n) n^{it}, x) \geqslant A.$$

Alors :

$$\left| \sum_{\frac{x}{\omega} < n \leqslant x} \frac{1}{n} g_1(a_1 n + b_1) g_2(a_2 n + b_2) \right| \leqslant \varepsilon \log(\omega).$$

On en retrouvera une preuve (se basant sur les travaux de Matomaki, Radziwill et Tao) dans le rapport complet.

II Problème de la discrépance d'Erdös

II.1 Présentation du problème

Commençons par nous mettre en situation. Imaginons que nous devons guider par message quelqu'un qui se trouve sur la voie du milieu d'un pont à trois voies. Notre objectif est d'avancer sur ce pont sans jamais tomber, tout en respectant une règle essentielle : il est interdit d'avancer en ligne droite. Pour mieux visualiser la situation, nous pouvons subdiviser le pont comme suit :

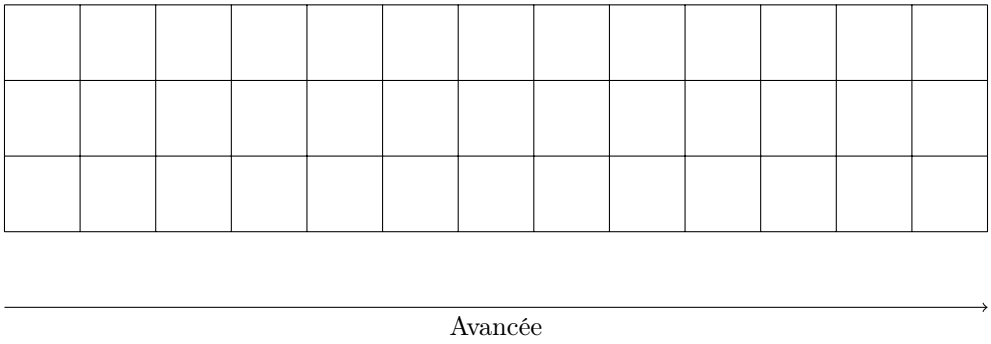

FIGURE 2 – Schématisation du pont

Une solution très simple pour progresser sur le pont sans tomber consiste à avancer en zigzag, comme illustré dans le schéma ci-dessous :

Nous représentons ce déplacement par la séquence suivante : $DGDGDGDG\ldots$, que l'on lit de gauche à droite. La lettre $'D'$ indique un déplacement en diagonale vers la droite, tandis que la lettre $'G'$ indique un déplacement en diagonale vers la gauche. C'est ainsi que nous communiquons ces instructions à la personne se trouvant sur le pont.
Maintenant, supposons qu'il soit difficile de communiquer directement avec cette personne, ce qui fait qu'elle pourrait ne comprendre qu'une lettre sur deux du message. Il est donc essentiel de s'assurer que si elle ne reçoit qu'une lettre sur deux, le message lui permettra tout de même de rester sur le pont sans jamais tomber.
Prenons l'exemple du message précédent et considérons uniquement une lettre sur deux. Nous obtenons alors le message suivant : $GGGGGG\ldots$. Évidemment, ce message fera tomber la personne du pont sur

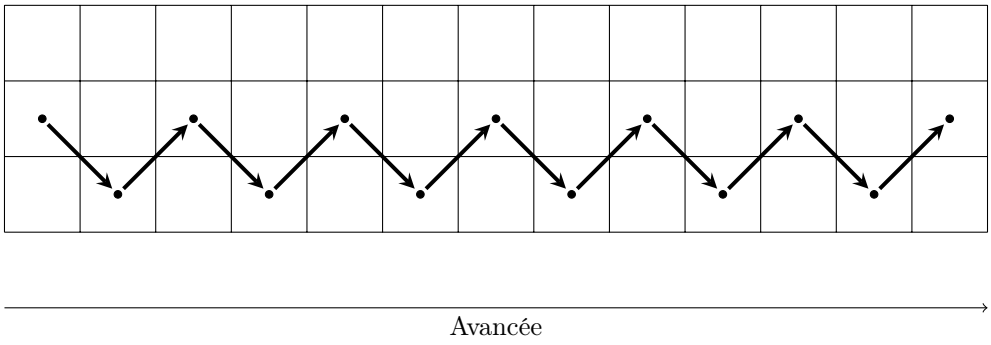

FIGURE 3 – Schématisation du déplacement en zigzag.

le schéma ci-contre cela revient à dire qu'en suivant uniquement les flèches rouges, la personne tombera du pont.

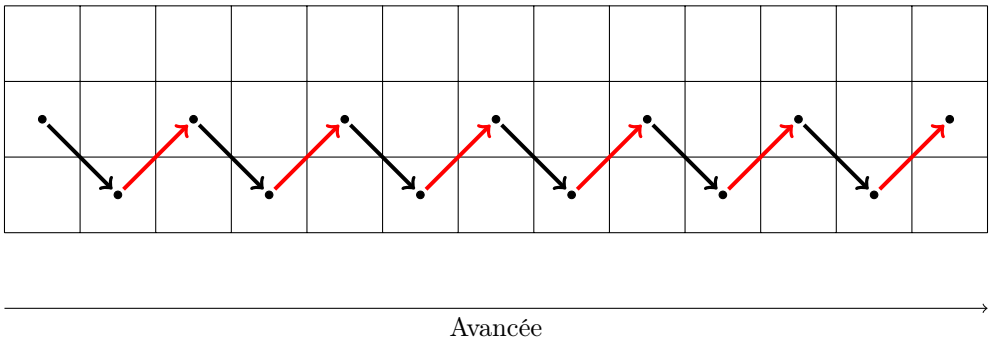

FIGURE 4 – Schéma illustrant que le déplacement "trivial" sur le pont n'est pas adapté si on ne considère qu'un déplacement sur deux.

Par conséquent, il est nécessaire de réfléchir plus en profondeur. Nous allons donc procéder étape par étape :

— Le premier déplacement est sans importance, nous choisissons donc D.

— Pour rester sur le pont, nous sommes obligés de choisir G pour le deuxième déplacement.

— Si nous choisissons D pour le troisième déplacement, en prenant un déplacement sur deux, le chemin devient DD, ce qui fera tomber la personne du pont. Nous sommes donc contraints de choisir G pour le troisième déplacement.

— Pour rester sur le pont, nous devons choisir D pour le quatrième déplacement.

— Nous continuons à prolonger ce chemin de manière périodique.

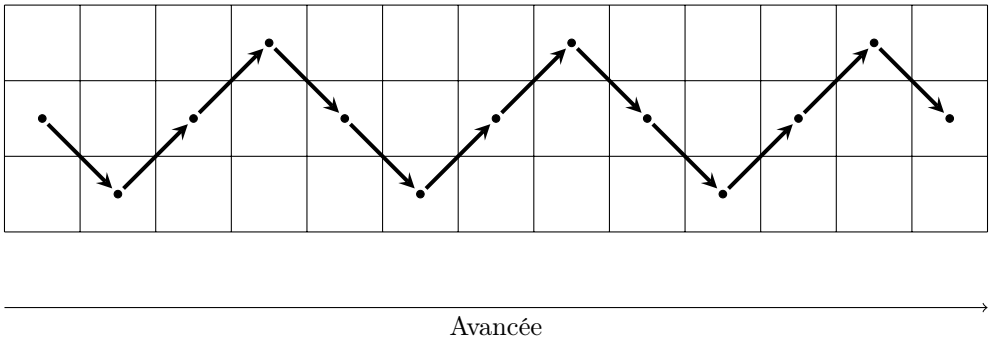

FIGURE 5 – Schématisation d'un chemin qui permet à la personne de rester sur le pont même un déplacement sur deux.

Ainsi, nous obtenons le chemin $DGGDDGGDDGGDDGG\ldots$, qui permettra à la personne de rester sur le pont s'il est transmis intact. Si le chemin est transmis en prenant une lettre sur deux, il devient $DGDGDGDG\ldots$, qui est évidemment un chemin permettant de rester sur le pont (voir figure 6).

Nous allons compliquer davantage le processus en supposant que la personne sur le pont ne peut comprendre aussi qu'un déplacement sur trois du message. Il est donc crucial de s'assurer que si nous considérons un déplacement sur trois, le chemin obtenu permettra à la personne de rester sur le pont. En examinant le message précédemment obtenu, le chemin résultant en prenant un déplacement sur trois commence par GG, ce qui fera tomber la personne du pont.

Nous devons donc trouver un nouveau chemin en poursuivant le même procédé.

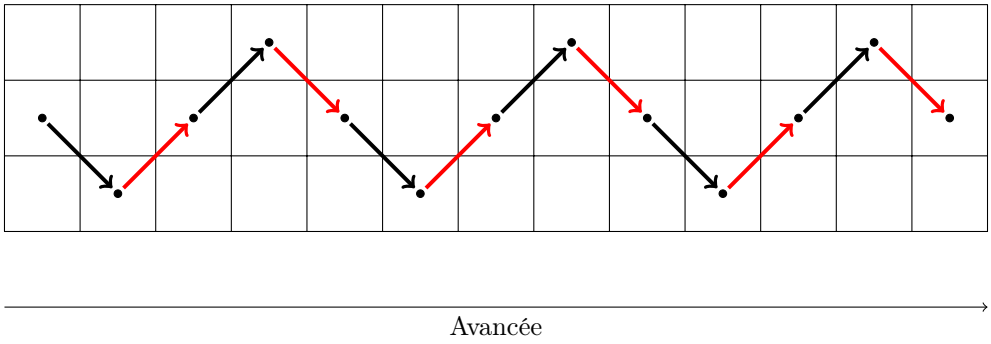

FIGURE 6 – Vérification qu'en considérant un déplacement sur deux, la personne sur deux restera sur le pont.

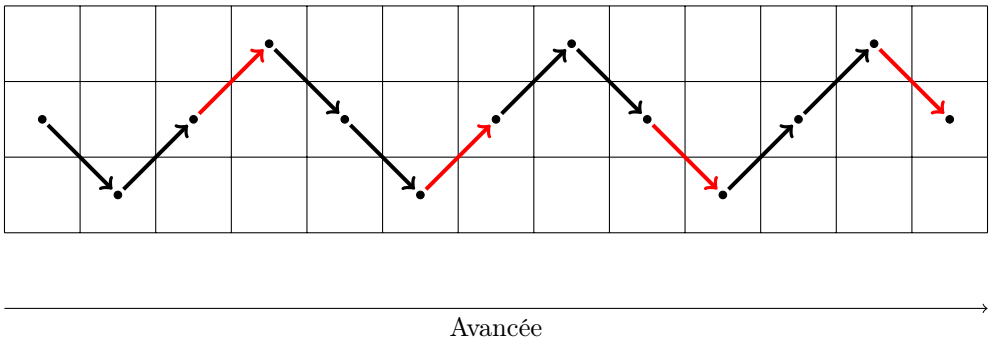

FIGURE 7 – En prenant le même chemin et en ne considérant qu'un déplacement sur trois alors la personne tombera du pont.

— Nous sommes contraints de reprendre les quatre premiers déplacements identiques.

— Si nous choisissons D pour le cinquième déplacement, nous serons contraints de choisir G pour le sixième, ce qui entraînera le problème décrit précédemment. Nous devons donc choisir G pour le cinquième déplacement et D pour le sixième.

— Le chemin doit donc commencer par $DGGDGD$. Ensuite, si nous choisissons G pour le septième déplacement, le huitième sera D et le chemin deviendra $DGGDGDGD$, ce qui ne respecte pas les conditions si l'on considère un déplacement sur deux. Nous devons donc prendre D comme septième déplacement et G comme huitième déplacement.

— Le chemin doit donc commencer par $DGGDGDDG$. Si nous choisissons D comme neuvième déplacement, le dixième sera forcément G, et comme indiqué précédemment, le onzième sera G et le douzième sera D (sinon le chemin ne fonctionnerait pas si nous ne considérons qu'un déplacement sur deux). Nous obtenons donc le chemin qui commence par $DGGDGDDGDGGD$. En considérant un déplacement sur trois, nous obtenons $GDDD$, ce qui fera tomber la personne du pont dans ce cas.

— Le chemin doit donc commencer par $DGGDGDDGGD$. Cependant, si nous continuons avec un déplacement sur trois en choisissant D comme neuvième déplacement, le dixième sera inévitablement G, et comme mentionné précédemment, le onzième sera également G et le douzième sera D (sinon le chemin ne fonctionnerait pas si nous ne considérons qu'un déplacement sur deux). Cela nous donnerait un chemin commençant par $DGGDGDDGDGGD$. En prenant un déplacement sur trois, nous obtenons $GDGG$, ce qui fera également tomber la personne du pont dans ce cas. Ainsi, nous pouvons conclure qu'il n'existe aucun chemin satisfaisant à nos conditions avec une longueur

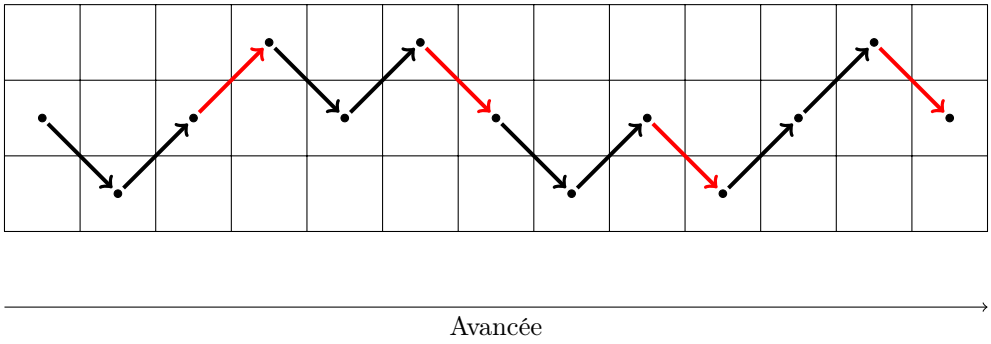

FIGURE 8 – Premier cas non concluant

minimale de 12 déplacements. En réalité, la situation est symétrique lorsque nous sommes à l'étape 8, et il y a autant de déplacements à droite qu'à gauche, que nous prenions tous les déplacements, un déplacement sur deux ou un déplacement sur trois. Par conséquent, nous aurions pu éviter de considérer ce cas. Ce qui pose problème ici, c'est que nous sommes contraints de raisonner par groupes de quatre afin d'éviter d'avoir deux fois le même déplacement en prenant un déplacement sur deux. Cependant, dans le quadruplet d'éléments supérieurs à huit, il y a deux multiples de trois qui se retrouveront nécessairement dans la même direction si nous raisonnons ainsi. Cela conduit à l'impossibilité de former un chemin d'une longueur supérieure ou égale à douze qui respecte les conditions énoncées.

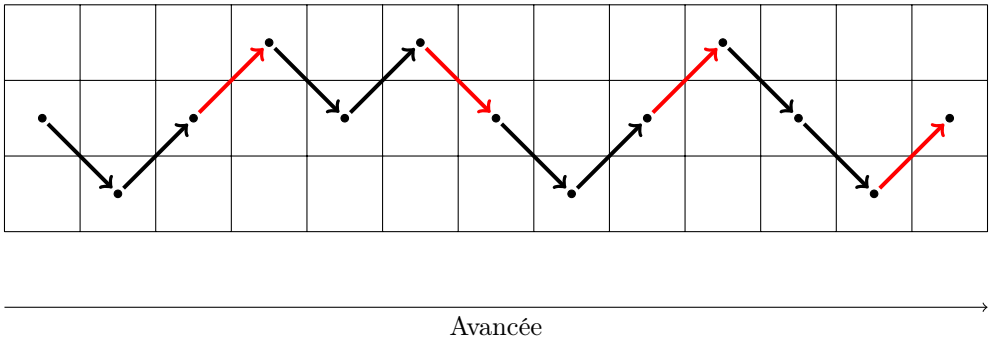

FIGURE 9 – Deuxième cas aussi non concluant : il est impossible de construire un chemin de longueur au moins 12 vérfiant les conditions demandées

On pourrait se demander comment résoudre le problème lorsque le pont est de taille plus grande et en considérant également toutes les progressions arithmétiques homogènes [2]. Cette question a été soulevée par Erdos au début des années 1930, et il a émis l'hypothèse que la réponse serait également négative dans le cas général, c'est-à-dire qu'il n'existerait pas de tels chemins. Pour formaliser davantage la situation, nous pouvons considérer le n-ème déplacement comme un élément $f(n) \in -1, +1$, qui représente les directions droite et gauche. Ainsi, la position de la personne sur le pont après le n-ème déplacement peut être exprimée par $\sum_{k=1}^{n} f(n)$. On peut dire que la personne tombera du pont si la valeur absolue de cette quantité devient trop grande le long de toute progression arithmétique homogène, on appelle cette quantité la discrépance de la $(f(n))$ [3] :

2. C'est-à-dire qu'il faudrait également tenir compte des suites de déplacements sur quatre, cinq, etc.

3. Le terme "discrépance" est peu fréquent en français ; en fait, il n'est même pas répertorié dans les dictionnaires traditionnels. Il dérive du latin "discrepantia" et peut être synonyme de "dissonance". Au sens figuré, il peut également signifier "divergence, dissemblance, discordance".

Définition II.1

Soit $(f(n))$ une suite de réels, on appelle ***discrépance*** *de la suite $(f(n))$ la quantité* $\sup_{d,n\in\mathbb{N}^*} \sum_{j=1}^{n} f(jd)$.

La conjecture d'Erdos peut finalement être formulée de la manière suivante :

Conjecture II.2: (Conjecture d'Erdos)

Pour toute suite d'éléments $(f(n))_{n\in\mathbb{N}^*}$ et pour tout $C \geqslant 0$, on a :

$$\sup_{n,d\in\mathbb{N}^*} \left|\sum_{k=1}^{n} f(dj)\right| \geqslant C.$$

On a montré précédemment que cette conjecture était vrai si $C = 2$. On peut même énoncer cette conjecture dans un cadre encore plus général.

Conjecture II.3: (Conjecture d'Erdos générale)

Soit $(H, \|\cdot\|_H)$ un espace vectoriel normé. Pour toute suite d'éléments $(f(n))_{n\in\mathbb{N}^*}$ de norme 1 et pour tout $C \geqslant 0$, on a :

$$\sup_{n,d\in\mathbb{N}^*} \left\|\sum_{k=1}^{n} f(dj)\right\|_H \geqslant C.$$

C'est cette version que l'on va démontrer dans la suite de cette partie.

II.2 Quelques remarques sur le problème

Avant de passer à des éléments de démonstration, il est intéressant de s'intéresser un peu à ce qu'il y a autour. Cette démonstration a été établie par Terence Tao en 2015 [4] alors que le problème a été posé plus de 80 ans auparavant. Roth a montré en 1964 dans [5] que le résultat est vrai si l'on considère la borne supérieure sur toutes les progressions arithmétiques (et non seulement les progressions arithmétiques homogènes comme dans la conjecture d'Erdos). En 2010, le projet PolyMath5 avait pour projet d'arriver à bout de cette conjecture, mais sans réel succès (malgré l'efficacité des différents projets PolyMath) même si on retrouve quelques éléments mis au point pendant ce projet dans la démonstration de Tao. Les seuls réels succès avant la preuve de Tao en toute généralité étaient des preuves par ordinateurs dans les cas où $C = 3$ et $C = 4$ [6] de 2014 seulement !

Essayons de se rendre compte de la difficulté du problème en cherchant des presque contre-exemples lorsque l'on modifie très peu les hypothèses.

Soit $\chi : \mathbb{N} \to \mathbb{C}$ un caractère de Dirichlet modulo q non principal. Par définition, χ est complètement multiplicatif et a pour moyenne 0 sur tout intervalle de longueur q, ainsi on a :

$$\forall j, n \in \mathbb{N}^* : \quad \left|\sum_{j=1}^{n} \chi(jd)\right| = |\chi(d)| \left|\sum_{j=1}^{n} \chi(j)\right| \leqslant q.$$

Ceci ne constitue évidemment pas un contre-exemple à la discrépance d'Erdos puisque que $\chi(n) = 0$ quand n et q ne sont pas premiers entre eux.

Maintenant ce que l'on peut faire c'est d'adapter un peu le contre-exemple précédent pour qu'il rentre dans les hypothèses du problème de la discrépance d'Erdos. On prend χ_3 le caractère de Dirichlet vérifiant $\chi_3(n) = +1$ ni $n \equiv 1[3]$, 0 si $n \equiv 0[3]$ et -1 si $n \equiv -1[3]$.

Soit H un espace de Hilbert de base orthonormale $e_0, e_1, \ldots$ et soit $f : n \to H$ définie par $f(3^a m) = \chi_3(m)e_a$ quand $a = 0, 1, 2, \ldots$ et $(m, 3) = 1$, f prend des valeurs dans $S_H(0, 1)$. Prenons $n = 1+3+\ldots+3^k$ pour k assez grand. On remarque que :

$$\sum_{j=1}^{n} f(j) = e_0 + \ldots + e_k.$$

Donc :

$$\left\| \sum_{j=1}^{n} f(j) \right\|_H = \sqrt{k+1} \gg \sqrt{\log(n)}.$$

De plus, on remarque par le théorème de Pythagore :

$$\left\| \sum_{j=1}^{n} f(jd) \right\|_H \ll \sqrt{\log(n)}.$$

Ainsi en modifiant un peu le contre-exemple précédant on obtient une discrépance d'ordre $\sqrt{\log(N)}$.

On n'a pas trouvé de fonctions arithmétiques qui admettent des discrépances beaucoup plus petites. D'ailleurs, cela peut nous donner une estimation (pas très fondée certes) du nombre de la taille d'une séquence $(f(n))$ de discrépance fixée. En effet les preuves par ordinateurs ont permis de montrer qu'il n'existe pas de chemin de longueur strictement plus grande que 1160 de discrépance d'au moins 3 et qu'il n'existe pas de chemin de longueur strictement plus grande que 127645 (!) de discrépance d'au moins 4. Et on remarque que $\sqrt{\log(1160)} \simeq 2.66 \in [2, 3]$ et $\sqrt{\log(127645)} \simeq 3.43 \in [3, 4]$. Ainsi on peut imaginer que la plus longue suite qui admettrait une discrépance C aurait environ $\exp\left(C^2\right)$ termes. Ainsi si on veut construire une très grande suite de discrépance 14, il faudrait sûrement s'aventurer à construire une suite possédant $\exp\left(14^2\right) \simeq 1.10^{85}$ ce qui environ autant de particules dans l'univers observable. Bref cela montre à quel point les chances pour obtenir une preuve exhaustive de la conjecture d'Erdos par ordinateur est vouée à l'échec avec les techniques les plus sophistiquées trouvées en 2014. C'est ici que la théorie analytique et probabiliste des nombres vient à la rescousse pour démontrer la conjecture d'Erdos, on utilisera dans la démonstration de cette conjecture la conjecture d'Elliott en moyenne logarithmique qui est une conséquence des travaux de Matomaki et Radziwill, les résultats qu'ils ont démontrés forment le point de départ de la démonstration.

II.3 Forme équivalente du problème

Le but de cette partie est de montrer que les théorèmes suivants sont des formes équivalentes de la conjecture d'Erdos (II.2).

Théorème II.4: (Forme probabiliste de la conjecture d'Erdos)

Soit $\mathbf{g} : \mathbb{N} \to \mathbf{S}^1$ une fonction stochastique complètement multiplicative. Alors :

$$\sup_{n\in\mathbb{N}} \mathbf{E}\left[\left(\sum_{j=1}^{n} \mathbf{g}(j)\right)^2\right] = +\infty.$$

Théorème II.5: (Formulation en théorie de la mesure de la conjecture d'Erdos)

Soient (Ω, μ) un espace probabilisé, $g : \Omega \to \left(\mathbf{S}^1\right)^{\mathbb{N}}$ une fonction mesurable telle que pour μ-presque tout $\omega \in \Omega$, $g(\omega)$ est complètement multiplicative, alors :

$$\sup_{n\in\mathbb{N}} \int_\Omega \left|\sum_{j=1}^{n} g(\omega)(j)\right|^2 \mathrm{d}\mu(\omega) = +\infty.$$

Ces deux formulations sont très clairement équivalentes.

Proposition II.6

Le théorème II.3 implique le théorème II.5

Démonstration : Soient (Ω, μ) et g comme dans le théorème II.5, on note H l'espace de Hilbert sont $L^2(\Omega, \mu)$. Pour tout $n \in \mathbb{N}$, on pose $f(n) \in H$ l'application $\omega \mapsto g(\omega)(n)$. Comme $g(\omega)(n) \in \S^1$ pour μ-presque tout $\omega \in \Omega$ et que μ est une mesure de probabilité on a pour tout $n \in \mathbb{N}$: $\|f\|_H = 1$. De plus, comme g est μ-presque partout complètement multiplicative, pour toute progression arithmétique homogène de raison d on a :

$$\left\|\sum_{j=1}^{n} f(jd)\right\|_H^2 = \int_\Omega \left|\sum_{j=1}^{n} g(\omega)(jd)\right|^2 \mathrm{d}\mu(\omega) = \int_\Omega \left|\sum_{j=1}^{n} g(\omega)(j)\right|^2 \mathrm{d}\mu(\omega).$$

Ainsi si on suppose le théorème II.3 vrai et en prenant la borne supérieure sur n dans la relation précédente, on obtient :

$$\sup_{n\in\mathbb{N}} \int_\Omega \left|\sum_{j=1}^{n} g(\omega)(j)\right|^2 \mathrm{d}\mu(\omega) = \sup_{n\in\mathbb{N}} \left\|\sum_{j=1}^{n} f(jd)\right\|_H^2 = +\infty.$$

On obtient alors dans ce cas que le théorème II.5 est vrai. □

L'implication réciproque est bien plus difficile, on aura besoin d'un résultat d'analyse fonctionnelle qui nécessite la définition suivante :

Définition II.7

Soit X un espace métrique et soient $(\mu_n)_{n\in\mathbb{N}}$ une suite de mesures de probabilités sur X. On dit que la suite $(\mu_n)_{n\in\mathbb{N}}$ ***converge étroitement*** *vers μ lorsque pour tout fonction f continue bornée sur X, on a :*

$$\int_X f(x)\,\mathrm{d}\mu_n(x) \underset{n\to+\infty}{\to} \int_X f(x)\,\mathrm{d}\mu(x).$$

Lemme II.8: (Théorème de Prokhorov - Cas compact)

Soit X un espace métrique compact et μ_n une suite de mesures de probas sur X. Alors il existe une sous-suite de μ_n qui converge étroitement vers un autre mesure de proba μ.

Démonstration : On sait que si X est un espace métrique compact alors $\mathcal{C}^0(X,\mathbb{C})$ est séparable. Donc par le théorème de Banach-Alaoglu la sphère unité de $\mathcal{M}(X)$, le dual de $\mathcal{C}^0(X,\mathbb{C})$ est séquentiellement compact pour la topologie faible-$*$.

Or pour tout $n\in\mathbb{N}$, on peut poser l'application continue suivante $T_{\mu_n} f \in \mathcal{C}^0(X,\mathbb{C}) \mapsto \displaystyle\int_X f\,\mathrm{d}\mu_n$.

Cette application est clairement continue de norme d'application égale à 1 (car les μ_n sont des mesures de probabilités sur X). Ainsi il existe une extractrice φ telle que $T_{\mu_{\varphi(n)}}$ converge faible-$*$ vers $T\in\mathcal{M}(X)$ de norme égale à 1. Or par le théorème de représentation de Riesz-Radon, il existe une mesure de probabilité μ telle que $T=T_\mu$. Cela revient à dire que $(\mu_{\varphi(n)})$ converge étroitement vers μ. □

Voici un second lemme qui consiste en l'application du théorème de Prokhorov.

Lemme II.9

Supposons que pour tout $X\geqslant 1$, il existe une fonction stochastique complètement multiplicative $\mathbf{g}_X$ [a] qui soit à valeurs dans $\mathbf{S}^1$ et telle que :

$$\forall n\leqslant X : \mathbf{E}\left[\left|\sum_{j=1}^{n}\mathbf{g}_X(j)\right|\right]^2 \ll_C 1.$$

Alors il existe une fonction $\mathbf{g}$ stochastique complètement multiplicative à valeurs dans $\mathbf{S}^1$ et telle que :

$$\forall n\in\mathbb{N} : \mathbf{E}\left[\left|\sum_{j=1}^{n}\mathbf{g}(j)\right|^2\right] \ll_C 1.$$

a. L'univers sur lequel est définie $\mathbf{g}_X$ peut dépendre de X

Démonstration : Dans cette preuve on notera $\mathcal{P}$ l'ensemble des nombres premiers. Soit $\mathcal{M}$ l'ensemble des fonctions complètement multiplicatives à valeurs dans $\mathbf{S}^1$. Comme les éléments de $\mathcal{M}$ sont déterminées uniquement par leurs valeurs sur les nombres premiers, on voit facilement que $\mathcal{M}$ est isomorphe à $\left(\mathbf{S}^1\right)^{\mathcal{P}}$. Comme produit dénombrable de compacts, $\mathcal{M}$ est compact pour la topologie produit. Or comme énoncé précédemment, on peut voir chaque $\mathbf{g}_X$ comme une application mesurable $f_X : \Omega_X \to \mathcal{M}$ telle que :

$$\forall n\leqslant X : \quad \int_{\Omega_X}\left|\sum_{j=1}^{n} f_X(\omega)(j)\right|^2 \mathrm{d}\mu_X(\omega) \ll_C 1.$$

On note ν_X la mesure image de μ_X par f_X, c'est une mesure sur $\mathcal{M}$ qui vérifie :

$$\forall F \in \mathcal{C}^0(\mathcal{M}, \mathbb{C}) : \int_{\mathcal{M}} F(g)\, \mathrm{d}\nu_X(g) = \mathbf{E}\left[F(g_X)\right] = \int_{\Omega_X} F(f_x(\omega))\, \mathrm{d}\mu_X(\omega).$$

On remarque que les fonctions $g \mapsto \left(\sum_{j=1}^{n} g(j)\right)^2$ sont continues sur $\mathcal{M}$, en effet on peut décomposer ces applications en polynômes en les $g \mapsto g(p)$ où p est premier, ces applications étant continues par définition de la topologie produit. Ainsi en appliquant la dernière estimation à ces fonctions, on obtient que :

$$\forall n \leqslant X : \int_{\mathcal{M}} \left|\sum_{j=1}^{n} g(j)\right|^2 \mathrm{d}\nu_X \ll_C 1.$$

Par le lemme de Prokhorov (II.8), on peut trouver une sous-suite ν_{X_j} de ν_X telle que $(\nu_{X_j})_{j\in\mathbb{N}}$ converge étroitement vers une mesure ν de probabilité sur $\mathcal{M}$. Donc on conclut que :

$$\forall n \in \mathbb{N} : \int_{\mathcal{M}} \left|\sum_{j=1}^{n} g(j)\right|^2 \mathrm{d}\nu(g) \ll_C 1.$$

On définit ensuite une fonction stochastique complètement multiplicative $\mathbf{g} : \mathbb{N} \to \mathbf{S}^1$ en choisissant $(\mathcal{M}, \nu)$ comme espace de probabilité ambiant et l'identité $g \mapsto g$ comme application mesurable. On obtient alors dans cet espace probabilisé :

$$\forall n \in \mathbb{N} : \mathbf{E}\left[\left|\sum_{j=1}^{n} \mathbf{g}(j)\right|^2\right] \ll_C 1.$$

□

On peut enfin démontrer la proposition suivante :

Proposition II.10

Le théorème II.4 implique le théorème *II.3*

Démonstration : Procédons par contraposée, on suppose qu'il existe $f : \mathbb{N} \to H$ à valeurs dans $S_H(0,1)$ et $C \geqslant 0$ tels que

$$\forall d \in \mathbb{N}^* : \quad \left\|\sum_{j=1}^{n} f(jd)\right\|_H \leqslant C. \tag{II.1}$$

Pour conclure notre preuve, il suffit de construire une fonction stochastique complètement multiplicative $\mathbf{g}$ à valeurs dans $\mathbf{S}^1$ telle que :

$$\forall n \in \mathbb{N} : \mathbf{E}\left[\left|\sum_{j=1}^{n} \mathbf{g}(j)\right|^2\right] \ll_C 1.$$

D'après le lemme II.9, il suffit de construire pour tout $X \geqslant 1$, une fonction stochastique complètement

multiplicative $\mathbf{g}_X$ qui soit à valeurs dans $\mathbf{S}^1$ et telle que :

$$\forall n \leqslant X : \mathbf{E}\left[\left|\sum_{j=1}^{n} \mathbf{g}_X(j)\right|\right]^2 \ll_C 1.$$

Soit $X \geqslant 1$, notons $p_1, \dots, p_r$ les nombres premiers inférieurs ou égaux à X rangés par ordre croissant. Soit $M \geqslant X$ un entier naturel que l'on suppose suffisamment grand devant C, X. On définit les fonctions suivantes : [4]

$$F : \begin{cases} (\mathbb{Z}/M\mathbb{Z})^r & \to H \\ (a_1[M], \dots, a_r[M]) & \mapsto f\left(p_1^{a_1} \dots p_r^{a_r}\right) \end{cases} \quad \text{et} \quad \pi : \begin{cases} [1, X] & \to (\mathbb{Z}/M\mathbb{Z})^r \\ p_1^{a_1} \dots p_r^{a_r} & \mapsto (a_1[M], \dots, a_r[M]) \end{cases}.$$

En appliquant l'équation II.1 pour tout $n \leqslant X$ et pour tout $d \in \mathbb{N}$ de la forme $d = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ avec pour tout $i \in \{1, \dots, r\} : 1 \leqslant \alpha_i \leqslant M - X$:

$$\left\|\sum_{j=1}^{n} f(jp_1^{\alpha_1} \dots p_r^{\alpha_r})\right\|_H \ll_C 1,$$

en notant $j = p_1^{\beta_{j_1}} \dots p_r^{\beta_{j_r}}$. Or pour tout $x = (x_1, \dots, x_r) \in (\mathbb{Z}/M\mathbb{Z})^r$:

$$\left\|\sum_{j=1}^{n} F(x + \pi(j)\right\|_H = \left\|\sum_{j=1}^{n} f(p_1^{x_1+\beta_{j_1}} \dots p_r^{x_r+\beta_{j_r}})\right\|_H.$$

Il y a donc $(M-X)^{r-1}$ choix de x (correspondants aux $(M-X)^{r-1}$ choix de d possibles) qui permettent d'avoir :

$$\left\|\sum_{j=1}^{n} F(x + \pi(j))\right\|_H \ll_C 1.$$

On obtient alors :

$$\frac{1}{M^r} \sum_{x \in (\mathbb{Z}/M\mathbb{Z})^r} \left\|\sum_{j=1}^{n} F(x + \pi(j))\right\|_H^2 \ll_C 1.$$

Or, on peux écrire pour tout $x \in (\mathbb{Z}/M\mathbb{Z})^r$:

$$F(x) = \sum_{\xi \in (\mathbb{Z}/M\mathbb{Z})^r} \hat{F}(\xi) e\left(\frac{x \cdot \xi}{M}\right) \quad \text{où} \quad \hat{F}(\xi) = \frac{1}{M^r} \sum_{\omega \in (\mathbb{Z}/M\mathbb{Z})^r} F(\omega) e\left(-\frac{\omega.\xi}{M}\right).$$

Ainsi par le théorème de Plancherel :

$$\frac{1}{M^r} \sum_{x \in (\mathbb{Z}/M\mathbb{Z})^r} \left\|\sum_{j=1}^{n} F(x + \pi(j))\right\|_H^2 = \sum_{\xi \in (\mathbb{Z}/M\mathbb{Z})^r} \left\|\hat{F}(\xi)\right\|_H^2 \left|\sum_{j=1}^{n} e\left(\frac{\pi(j).\xi}{M}\right)\right|^2.$$

4. Pour s'assurer que F est bien définie on considère que les a_i sont des éléments de $\{0, \dots, M-1\}$. Notons aussi que π est bien définie pour $M \geqslant X$

De plus, aussi d'après le théorème de Plancherel :

$$\sum_{\xi\in(\mathbb{Z}/M\mathbb{Z})^r} \left\|\hat{F}(\xi)\right\|_H^2 = 1.$$

Donc on peut interpréter $\left\|\hat{F}(\xi)\right\|_H^2$ comme une densité de probabilité d'une fréquence $\xi = (\xi_1, \dots, xi_r) \in (\mathbb{Z}/M\mathbb{Z})^r$. Ainsi avec cette interprétation :

$$\forall n \leqslant X : \mathbf{E}\left[\left|\sum_{j=1}^{n} e\left(\frac{\pi(j)\cdot\xi}{M}\right)\right|\right] \ll_C 1.$$

Si on définit la fonction stochastique complètement multiplicative $\mathbf{g}_X$ définie par : $\mathbf{g}_X(p_j) = e\left(\frac{\xi_j}{M}\right)$ pour $j \in \{1, \dots, r\}$ et $g_X(p)$ pour les autres nombres premiers (il n'interviennent pas ensuite), on obtient :

$$\forall n \leqslant X : \mathbf{E}\left[\left|\sum_{j=1}^{n} \mathbf{g}_X(j)\right|^2\right] \ll_C 1.$$

D'où le résultat. □

Remarque : Un point intéressant à remarquer est de voir notre preuve ne marche plus si on considère un caractère de Dirichlet χ. Il est bien de module souvent à valeurs dans le cercle unité mais pour $q \leqslant p_r$, la fonction qui à $(a_1, \dots, a_r)$ associe $\chi\left(p_1^{a_1} \dots p_r^{a_r}\right)$ est presque toujours nulle (comme l'argument est très souvent un multiple de q). Ainsi :

$$\sum_{\xi\in(\mathbb{Z}/M\mathbb{Z})^r} \left\|\hat{F}(\xi)\right\| \ll 1.$$

On ne peut donc pas définir une fonction $\mathbf{g}_X$ telle que dans le preuve ci-dessus.

II.4 Application de la conjecture d'Elliott logarithmique

Proposition II.11

Supposons que $\mathbf{g} : \mathbb{N} \to \mathbf{S}^1$ soit une fonction stochastique complètement multiplicative telle qu'il existe $C > 0$:

$$\forall n \in \mathbb{N} : \mathbf{E}\left[\left|\sum_{j=1}^{n} \mathbf{g}(j)\right|^2\right] \leqslant C^2.$$

Soit $\varepsilon > 0$ et supposons que X est suffisamment grand devant ε, C. Alors avec probabilité $1 - \mathcal{O}(\varepsilon)$, il existe un caractère de Dirichlet (stochastique) de période $\mathbf{q} = \mathcal{O}_{C,\varepsilon}(1)$ et un nombre réel (stochastique) $\mathbf{t} = \mathcal{O}_{C,\varepsilon}(X)$ tels que :

$$\sum_{p\leqslant X} \frac{1 - \mathcal{R}e\left(\mathbf{g}(p)\overline{\chi(p)}p^{-it}\right)}{p} \ll_{C,\varepsilon} 1.$$

Démonstration : Soient $\mathbf{g}, C, \varepsilon$ comme introduits ci-dessus. Soit $H \geqslant 1$ un nombre modérément large devant ε à choisir plus tard. On suppose que X est suffisamment grand devant X, ε. Par hypothèse et

par inégalité triangulaire, on a pour X suffisamment grand :

$$\mathbf{E}\left[\sum_{\sqrt{X}\leqslant n\leqslant X}\frac{1}{n}\left|\sum_{j=n+1}^{n+H}\mathbf{g}(j)\right|^2\right]\ll_C \log(X).$$

Ainsi par l'inégalité de Markov, avec probabilité $1-\mathcal{O}(\varepsilon)$:

$$\sum_{h_1,h_2\in[1,H]}\sum_{\sqrt{X}\leqslant n\leqslant X}\frac{\mathbf{g}(n+h_1)\mathbf{g}(n+h_2)}{n}=\sum_{\sqrt{X}\leqslant n\leqslant X}\frac{1}{n}\left|\sum_{h=1}^{H}\mathbf{g}(n+h)\right|^2\ll_{C,\varepsilon}\log(X).$$

Or dans la somme sur h_1,h_2 il est faicle de voir que le terme diagonal contribue pour $\gg H\log(X)$. Ainsi pour H suffisamment grand devant C,ε et d'après le principe des tiroirs, on peut trouver deux entiers (stochastiques) et distincts $h_1,h_2\in[1,X]$ tels que :

$$\left|\sum_{\sqrt{X}\leqslant n\leqslant X}\frac{\mathbf{g}(n+h_1)\mathbf{g}(n+h_2)}{n}\right|\gg_{C,\varepsilon,H}\log(X).$$

Donc par réciproque de la conjecture d'Elliott en moyenne logarithmique I.14, il existe un caractère de Dirichlet stochastique de période $\mathbf{q}=\mathcal{O}_{C,\varepsilon}(1)$ et un nombre réel stochastique $\mathbf{t}=\mathcal{O}_{C,\varepsilon}(X)$ tels que :

$$\sum_{p\leqslant X}\frac{1-\mathcal{R}e\Big(\mathbf{g}(p)\overline{\chi(p)}p^{-it}\Big)}{p}\ll_{C,\varepsilon}1.$$

Détaillons juste comment on peut s'arranger pour que $(\chi,\mathbf{t})$ soient pris mesurables (et ainsi stochastiques). Par le théorème I.14, on sait qu'il existe plusieurs couples (χ,t) tels que :

$$\sum_{p\leqslant x}\frac{1-g(p)\overline{\chi(p)}p^{-it}}{p}<a.$$

Et s'il existe $t_0\in\mathbb{R}$ tel que l'inégalité précédente est lieu pour $t=t_0$ alors par densité de $\mathbb{Q}$ dans $\mathbb{R}$, on peut trouver $t_0^{'}\in\mathbb{Q}$ tel que cette inégalité est aussi lieu pour $t=t_0^{'}$. Ainsi on peut s'arranger pour considérer un ensemble dénombrable de (χ,t) qui vérifie l'inégalité. Comme il est dénombrable, on peut lui construire un bon ordre sur cet ensemble. Or l'application $g\mapsto\left(\sum_{p\leqslant x}\frac{1-g(p)\overline{\chi}(p)p^{-it}}{p}\right)_{(\chi,t)}$ est continue donc mesurable et l'application qui à une suite (x_n) de réels associe l'unique $n\in\mathbb{N}$ tel que $x_n\leqslant a$ et pour tout $m\leqslant n: x_n>a$ est aussi mesurable[5]. Ainsi on peut trouver $(\chi,\mathbf{t})$ qui vérifie :

$$\sum_{p\leqslant X}\frac{1-\mathcal{R}e\Big(\mathbf{g}(p)\overline{\chi(p)}p^{-it}\Big)}{p}\ll_{C,\varepsilon}1.$$

□

5. On rappelle ici qu'on considère la tribu $\mathcal{P}(\mathbb{N})$ sur $\mathbb{N}$ et la tribu produit dans les espaces produits.

II.5 Preuve de la conjecture d'Erdos

Dans cette partie, on va prouver le théorème II.4 ce qui démontrera la conjecture d'Erdos. Pour cela, on va supposer par l'absurde qu'il est faux. Il existe donc une constante $C > 0$ et une fonction $\mathbf{g}$ stochastique complètement multiplicative à valeurs dans $\mathbf{S}^1$ telle que :

$$\forall n \in \mathbb{N} : \mathbf{E}\left[\left|\sum_{j=1}^{n} \mathbf{g}(j)\right|^2\right] \leqslant C^2.$$

On va maintenant considérer que toutes les constantes peuvent dépendre de C, ainsi on pourra écrire :

$$\forall n \in \mathbb{N} : \mathbf{E}\left[\left|\sum_{j=1}^{n} \mathbf{g}(j)\right|^2\right] \ll 1.$$

On introduit désormais les grandeurs suivantes $\varepsilon, H, \delta, k, X$ vérifiant :

$$C \ll \frac{1}{\varepsilon} \ll H \ll \frac{1}{\delta}, k \ll X.$$

D'après la proposition II.11, avec probabilité $1 - \mathcal{O}(\varepsilon)$, il existe un caractère de Dirichlet (stochastique) de période $\mathbf{q} = \mathcal{O}_{C,\varepsilon}(1)$ et un nombre réel (stochastique) $\mathbf{t} = \mathcal{O}_{C,\varepsilon}(X)$ tels que :

$$\sum_{p \leqslant X} \frac{1 - \mathcal{R}e\left(\mathbf{g}(p)\overline{\chi(p)}p^{-it}\right)}{p} \ll_{C,\varepsilon} 1.$$

Quitte à réduire χ, on peut supposer qu'il est primitif (car si χ' est un caractère primitif qui induit χ alors$\chi(p)$ et $\chi'(p)$ ne diffèrent qu'en les premiers p qui divisent le module de χ, dont il y en a un nombre fini).

Lemme II.12

Avec probabilité $1 - \mathcal{O}(\varepsilon)$, $\mathbf{t} = \mathcal{O}_{\varepsilon}\left(X^{\delta}\right)$.

Démonstration : Preuve admise, elle se base sur des résultats d'analyse complexe qu'on a pas eu le temps d'aborder pendant le stage. On pourra en trouver une démonstration dans (Lemme 4.1, [7]). □

On se conditionne maintenant sur ces deux évènements de probabilité $1 - \mathcal{O}(\varepsilon)$.

On écrit pour tout $n \in \mathbb{N}$: $\mathbf{g}(n) = \tilde{\chi(n)}n^{it}\mathbf{h}(n)$ où on définit :

— pour tout p premier ne divisant pas $\mathbf{q}$: $\tilde{\chi}(p) = \chi(p)$ et $\mathbf{h}(p) = \mathbf{g}(p)\overline{\chi(p)}p^{it}$,

— pour tout p premier divisant $\mathbf{q}$: $\tilde{\chi}(p) = \mathbf{g}(p)p^{-it}$ et $\mathbf{h}(p) = 1$.

Avec ces notations on peut écrire :

$$\left|\sum_{p \leqslant X} \frac{1 - \mathcal{R}e\left(\mathbf{h}(p)\right)}{p}\right| \ll_{\varepsilon} 1. \tag{II.2}$$

Lemme II.13

Conditionné à l'évènement de probabilité $1-\mathcal{O}(\varepsilon)$, on a :

$$\frac{1}{H}\sum_{H<H'\leqslant 2H}\sum_{n\in\mathbb{N}}\frac{1}{n^{1+\frac{1}{\log(X)}}}\left|\sum_{m=1}^{H'}\tilde{\chi}(n+m)\mathbf{h}(n+m)\right|^2 \ll_\varepsilon \log(X).$$

Démonstration : Par hypothèse sur $\mathbf{g}$ et par inégalité triangulaire :

$$\forall n\in\mathbb{N}:\mathbf{E}\left[\frac{1}{H}\sum_{H<H'\leqslant 2H}\left|\sum_{m=1}^{H'}\mathbf{g}(n+m)\right|^2\right]\ll 1.$$

Soit $n\geqslant X^{2\delta}$, d'après le lemme II.12 on sait que $\mathbf{t}=\mathcal{O}_\varepsilon\left(X^\delta\right)$ donc par un simple développement limité :

$$\forall m\leqslant H^{'}:(n+m)^{i\mathbf{t}}=n^{i\mathbf{t}}+\mathcal{O}_{\varepsilon,H,\delta}\left(X^{-\delta}\right).$$

Ainsi on a :

$$\forall n\geqslant X^{2\delta}:\mathbf{E}\left[\frac{1}{H}\sum_{H<H'\leqslant 2H}\left|\sum_{m=1}^{H'}\tilde{\chi}(n+m)n^{i\mathbf{t}}\mathbf{h}(n+m)\right|^2\right]\ll 1.$$

Si $n<X^{2\delta}$ alors on majore cette même quantité par H^2 trivialement. Ainsi pour δ suffisamment petit on obtient en moyennisant par la densité $\frac{1}{n^{1+\frac{1}{\log(X)}}}$:

$$\mathbf{E}\left[\frac{1}{H}\sum_{H<H'\leqslant 2H}\sum_{n\in\mathbb{N}}\frac{1}{n^{1+\frac{1}{\log(X)}}}\left|\sum_{m=1}^{H'}\tilde{\chi}(n+m)\mathbf{h}(n+m)\right|^2\right]\ll\log(X).$$

On obtient le résultat demandé par l'inégalité de Markov. □

Définition II.14

Dans cette partie et uniquement dans cette partie, on dira qu'une classe a modulo $\mathbf{q}^k$ est ***mauvaise*** *si pour tout $m\in\{1,\dots,2H\}$, il existe un facteur premier p de $\mathbf{q}$ tel que $a+m$ soit divisible par p^k. Sinon, on dira que cette classe est* ***bonne****.*

Lemme II.15

Avec les définitions précédentes, on a :

$$\frac{1}{\mathbf{q}^k}\sum_{a\text{ bonne}}\frac{1}{H}\sum_{H<H'\leqslant 2H}\left|\sum_{m=1}^{H'}\tilde{\chi}(a+m)\right|^2\ll_\varepsilon 1.$$

Démonstration : On reprend le résultat du lemme précédent en se restreignant à l'évènement de

probabilité $1-\mathcal{O}(\varepsilon)$ et en ne sommant que sur les bonnes classes :

$$\frac{1}{H}\sum_{H<H'\leqslant 2H}\sum_{\substack{a \text{ bonne}\\ n\equiv a[\mathbf{q}^k]}}\frac{1}{n^{1+\frac{1}{\log(X)}}}\left|\sum_{m=1}^{H'}\tilde{\chi}(n+m)\mathbf{h}(n+m)\right|^2 \ll_\varepsilon \log(X).$$

Donc d'après l'inégalité de Cauchy-Scwharz :

$$\frac{1}{H}\sum_{H<H'\leqslant 2H}\sum_{a \text{ bonne}}\left|\sum_{n\equiv a[\mathbf{q}^k]}\frac{1}{n^{1+\frac{1}{\log(X)}}}\sum_{m=1}^{H'}\tilde{\chi}(n+m)\mathbf{h}(n+m)\right|^2 \ll_\varepsilon \frac{\log(X)^2}{\mathbf{q}^k}.$$

Or on remarque que si n appartient à une bonne classe a alors $\tilde{\chi}(n+m)=\tilde{\chi}(a+m)$ (c'est en fait pour cela qu'on les a introduites). Ainsi on obtient facilement :

$$\frac{1}{H}\sum_{H<H'\leqslant 2H}\sum_{a \text{ bonne}}\left|\sum_{m=1}^{H'}\tilde{\chi}(a+m)\sum_{n\equiv a+m[\mathbf{q}^k]}\frac{1}{n^{1+\frac{1}{\log(X)}}}\mathbf{h}(n)\right|^2 \ll_\varepsilon \frac{\log(X)^2}{\mathbf{q}^k}.$$

On va maintenant estimer $\displaystyle\sum_{n\equiv a+m[\mathbf{q}^k]}\frac{1}{n^{1+\frac{1}{\log(X)}}}\mathbf{h}(n)$. On remarque tout d'abord par le second théorème de Mertens et par hypothèse sur $\mathbf{h}$ II.2 que :

$$\log(X)\ll_\varepsilon \mathcal{D}\mathbf{h}\left(1+\frac{1}{\log(X)}\right)\ll_\varepsilon \log(X). \tag{II.3}$$

Maintenant on va regarder cette quantité quand χ est un caractère de Dirichlet : $\displaystyle\sum_{n\in\mathbb{N}}\frac{\chi(n)\mathbf{h}(n)}{n^{1+\frac{1}{\log(X)}}}$.

— Supposons que χ_1 est un caractère de Dirichlet non-principal de période divisant $\mathbf{q}^k$ alors par analycité en 1 de la série de Dirichlet associée à χ_1 :

$$\mathcal{D}\chi_1\left(1+\frac{1}{\log(X)}\right)\ll_{\mathbf{q},k} 1.$$

De plus en développant en produit eulérien on a l'égalité suivante :

$$\sum_{n\in\mathbb{N}}\frac{\chi_1(n)\mathbf{h}(n)}{n^{1+\frac{1}{\log(X)}}}=\mathcal{D}\chi_1\left(1+\frac{1}{\log(X)}\right)\prod_p\left(\left(1-\frac{\mathbf{h}(\mathbf{p})\chi_{\mathbf{1}}(\mathbf{p})}{p^{1+\frac{1}{\log(X)}}}\right)^{-1}\left(1-\frac{\chi_1(p)}{p^{1+\frac{1}{\log(X)}}}\right)\right).$$

On en déduit l'estimation suivante (en ne gardant que les termes dans le produit sur p en $\dfrac{1}{p^{1+\frac{1}{\log(X)}}}$) :

$$\sum_{n\in\mathbb{N}}\frac{\chi_1(n)\mathbf{h}(n)}{n^{1+\frac{1}{\log(X)}}}\ll_{\mathbf{q},k}\exp\left(\sum_p\frac{|1-\mathbf{h}(p)|}{p^{1+\frac{1}{\log(X)}}}\right).$$

Ainsi comme la série de terme général $\frac{|1-\mathbf{h}(p)|}{p^{1+\frac{1}{\log(X)}}}$ est convergente, on a :

$$\exp\left(\sum_{p}\frac{|1-\mathbf{h}(p)|}{p^{1+\frac{1}{\log(X)}}}\right)=\exp\left(\sum_{p\leqslant X}\frac{|1-\mathbf{h}(p)|}{p^{1+\frac{1}{\log(X)}}}\right)+\mathcal{O}(1)\ll\exp\left(\sum_{p\leqslant X}\frac{|1-\mathbf{h}(p)|}{p}\right).$$

On en déduit par l'inégalité de Cauchy-Scwharz puis le deuxième théorème de Mertens (**??**) et enfin l'hypothèse II.2 sur $\mathbf{h}$:

$$\begin{aligned}\sum_{n\in\mathbb{N}}\frac{\chi_1(n)\mathbf{h}(n)}{n^{1+\frac{1}{\log(X)}}}&\ll_{\mathbf{q},k}\exp\left(\sum_{p\leqslant X}\frac{\mathcal{O}\left(1-\mathcal{R}e\left(\mathbf{h}(p)\right)\right)^{\frac{1}{2}}}{p}\right),\\&\ll_{\mathbf{q},k}\exp\left(\mathcal{O}\left(\log\log(X)\sum_{p\leqslant X}\frac{(1-\mathcal{R}e(\mathbf{h}(p))}{p}\right)^{\frac{1}{2}}\right),\\&\ll_{\mathbf{q},k}\exp\left(\mathcal{O}_{\varepsilon}\left(\sqrt{\log\log(X)}\right)\right).\end{aligned}$$

— Maintenant supposons que χ_0 soit un caractère principal de période $r|\mathbf{q}^k$. On peut alors écrire en développant en produit eulérien et en se rappelant que $\mathbf{h}(p)=1$ pour tout p divisant r (donc $\mathbf{q}^k$) :

$$\begin{aligned}\sum_{n\in\mathbb{N}}\frac{\chi_0(n)\mathbf{h}(n)}{n^{1+\frac{1}{\log(X)}}}&=\mathcal{D}\mathbf{h}\left(1+\frac{1}{\log(X)}\right)\prod_{p|r}\left(1-\frac{1}{p^{1+\frac{1}{\log(X)}}}\right)\\&=\mathcal{D}\mathbf{h}\left(1+\frac{1}{\log(X)}\right)\left(1+\mathcal{O}_{\varepsilon}\left(\frac{1}{\log(X)}\right)\right)\prod_{p|r}\left(1-\frac{1}{p}\right)\\&=\frac{\varphi(r)}{r}\mathcal{D}\mathbf{h}\left(1+\frac{1}{\log(X)}\right)+\mathcal{O}_{\varepsilon}\left(\frac{\varphi(r)}{r}\mathcal{D}\mathbf{h}\left(1+\frac{1}{\log(X)}\right)\frac{1}{\log(X)}\right)\\&=\frac{\varphi(r)}{r}\mathcal{D}\mathbf{h}\left(1+\frac{1}{\log(X)}\right)+\mathcal{O}_{\varepsilon}(1)\end{aligned}$$

où la dernière estimation à été obtenue grâce à l'estimation II.3.

De ces deux points par orthogonalité des caractères, on en déduit pour toute classe de résidus primitives $b[r]$ ($i.e$ $(b,r)=1$), on a :

$$\sum_{n\equiv b[r]}\frac{\mathbf{h}(n)}{n^{1+\frac{1}{\log(X)}}}=\frac{1}{r}\mathcal{D}\mathbf{h}\left(1+\frac{1}{\log(X)}\right)+\mathcal{O}_{\mathbf{q},k}\left(\exp\left(\mathcal{O}_{\varepsilon}(\sqrt{\log\log(X)})\right)\right).$$

Si $b[r]$ est une classe de résidus non-primitive alors en notant $r'=\frac{r}{(b,r)}$ et $b'=\frac{b}{(b,r)}$:

$$\sum_{n\equiv b'[r']}\frac{\mathbf{h}(n)}{n^{1+\frac{1}{\log(X)}}}=\frac{1}{r}\mathcal{D}\mathbf{h}\left(1+\frac{1}{\log(X)}\right)+\mathcal{O}_{\mathbf{q},k}\left(\exp\left(\mathcal{O}_{\varepsilon}(\sqrt{\log\log(X)})\right)\right).$$

Donc en utilisant l'estimation II.3, on obtient quelque soit la classe de résidus $b[r]$:

$$\sum_{n\equiv b[r]}\frac{\mathbf{h}(n)}{n^{1+\frac{1}{\log(X)}}}=\frac{1}{r}\mathcal{D}\mathbf{h}\left(1+\frac{1}{\log(X)}\right)+\mathcal{O}_{\mathbf{q},k}\left(\exp\left(\mathcal{O}_{\varepsilon}(\sqrt{\log\log(X)})\right)\right).$$

Ainsi en réinsérant cette expression dans celle de départ :

$$\frac{1}{H}\sum_{H<H'\leqslant 2H}\sum_{a\text{ bonne}}\left|\sum_{m=1}^{H'}\frac{\tilde{\chi}(a+m)}{\mathbf{q}^k}\mathcal{D}\mathbf{h}\left(1+\frac{1}{\log(X)}\right)+\mathcal{O}_{\mathbf{q},k}\left(\exp\left(\mathcal{O}_\varepsilon(\sqrt{\log\log(X)})\right)\right)\right|^2\ll_\varepsilon\frac{\log(X)^2}{\mathbf{q}^k}.$$

Or la contribution de $\mathcal{O}_{\mathbf{q},k}\left(\exp\left(\mathcal{O}_\varepsilon(\sqrt{\log\log(X)})\right)\right)$ est $\ll_\varepsilon \frac{\log(X)^2}{\mathbf{q}^k}$ pour X suffisamment grand. On en déduit le fait annoncé en utilisant II.3. □

Lemme II.16

Pour tous $d_1\neq d_2$ diviseurs de $\mathbf{q}^{k-1}$ et $m_1,m_2\in\{1,\dots,H'\}$, on a :

$$\sum_{\substack{a=1\\ d_1\mid a+m_1\\ d_2\mid a+m_2}}^{\mathbf{q}^k}\chi\left(\frac{a+m_1}{d_1}\right)\overline{\chi\left(\frac{a+m_2}{d_2}\right)}=0.$$

Démonstration : Nous n'allons pas faire en détails cette preuve. D'après les résultats du paragraphe I.1, on peut dire que le terme que l'on cherche à rendre nul est une combinaison linéaire de termes de la forme : $e\left(\frac{\xi a}{d_1\mathbf{q}}\right)$ pour $(\xi,d_1\mathbf{q})=1$ et $e\left(\frac{\xi a}{d_2\mathbf{q}}\right)$ pour $(\xi,d_2\mathbf{q})=1$. Comme $d_1\neq d_2$ toutes les fréquences qui vont apparaître seront non nulles et ainsi leur somme sera elle nulle. □

Fin de la démonstration du théorème II.4 On va maintenant utiliser les deux lemmes précédents pour démontrer la démonstration du théorème II.4. On se rappelle que l'on procède par l'absurde.

Si on est dans l'évènement $\mathbf{q}=1$ alors χ est constant égal à 1 et donc d'après le lemme II.15 on a le fait suivant :

$$H\ll\frac{1}{H}\sum_{H<H'\leqslant 2H}\left(H'\right)^2\ll_\varepsilon 1,$$

ce qui est absurde pour H suffisamment grand devant ε. On se restreint maintenant à l'évènement $\mathbf{q}>1$, ainsi χ sera non-principal. Encore d'après le lemme II.15 :

$$\frac{1}{H}\sum_{H<H'\leqslant 2H}\sum_{m_1,m_2=1,\dots,H'}\sum_{a\text{ bonne}}\tilde{\chi}(a+m_1)\overline{\tilde{\chi}(a+m_2)}\ll_\varepsilon\mathbf{q}^k.$$

On écrit $d_1=(a+m_1,\mathbf{q}^k)$ et $d_2=(a+m_2,\mathbf{q}^k)$ ainsi d_1,d_2 divisent $\mathbf{q}^{k-1}$. Ainsi :

$$\sum_{d_1,d_2\mid\mathbf{q}^{k-1}}\sum_{H<H'\leqslant 2H}\frac{\tilde{\chi}(d_1)\overline{\tilde{\chi}(d_2)}}{H}\sum_{m_1,m_2=1,\dots,H'}\sum_{\substack{a\text{ bonne}\\ d_1=(a+m_1,\mathbf{q}^k)\\ d_2=(a+m_2,\mathbf{q}^k)}}\chi\left(\frac{a+m_1}{d_1}\right)\overline{\chi\left(\frac{a+m_2}{d_2}\right)}\ll_\varepsilon\mathbf{q}^k.$$

Or on remarque que le nombre de mauvaises classes a est au plus $H\sum p|\mathbf{q}\left(\frac{\mathbf{q}}{p}\right)^k\ll H2^{-k}\mathbf{q}^k$. Ainsi on peut écrire :

$$\sum_{d_1,d_2\mid\mathbf{q}^{k-1}}\sum_{H<H'\leqslant 2H}\frac{\tilde{\chi}(d_1)\overline{\tilde{\chi}(d_2)}}{H}\sum_{m_1,m_2=1,\dots,H'}\sum_{\substack{a\\ d_1\mid a+m_1\\ d_2\mid a+m_2}}\chi\left(\frac{a+m_1}{d_1}\right)\overline{\chi\left(\frac{a+m_2}{d_2}\right)}\ll_\varepsilon\mathbf{q}^k.$$

D'après le lemme II.16 on obtient :

$$\frac{1}{H}\sum_{d|\mathbf{q}^{k-1}}\sum_{H<H'\leqslant 2H}\sum_{m_1,m_2=1,\dots,H'}\sum_{\substack{a\\ d|a+m_1\\ d|a+m_2}}\chi\left(\frac{a+m_1}{d}\right)\overline{\chi\left(\frac{a+m_2}{d}\right)}\ll_\varepsilon \mathbf{q}^k.$$

On peut réécrire ceci sous cette forme :

$$\frac{1}{H}\sum_{d|\mathbf{q}^{k-1}}\sum_{H<H'\leqslant 2H}\sum_{a}\left|\sum_{\substack{m\in[1,H']\\ d|a+m}}\chi\left(\frac{a+m}{d}\right)\right|^2\ll_\varepsilon \mathbf{q}^k.$$

On voit ici que tous les termes de la somme sur d sont positifs ainsi on peut se restreindre à ceux qui s'écrivent $\mathbf{q}^i$ avec $\mathbf{q}^i<\sqrt{H}$:

$$\frac{1}{H}\sum_{i:\mathbf{q}^i<\sqrt{H}}\sum_{H<H'\leqslant 2H}\sum_{a}\left|\sum_{\substack{m\in[1,H']\\ \mathbf{q}^i|a+m}}\chi\left(\frac{a+m}{\mathbf{q}^i}\right)\right|^2\ll_\varepsilon \mathbf{q}^k.$$

Observons que par inégalité triangulaire on a :

$$\sum_{i:\mathbf{q}^i<\sqrt{H}}\frac{1}{H}\sum_{H'\in\left[H,\frac{3}{2}H\right]}\sum_{a}\left|\sum_{\substack{H'<m\leqslant H'+\mathbf{q}^i\\ \mathbf{q}^i|a+m}}\chi\left(\frac{a+m}{\mathbf{q}^i}\right)\right|^2\ll_\varepsilon \mathbf{q}^k.$$

Donc il existe $H'\in\left[H,\dfrac{3H}{2}\right]$ tel que :

$$\sum_{i:\mathbf{q}^i<\sqrt{H}}\sum_{a}\left|\sum_{\substack{H'<m\leqslant H'+\mathbf{q}^i\\ \mathbf{q}^i|a+m}}\chi\left(\frac{a+m}{\mathbf{q}^i}\right)\right|^2\ll_\varepsilon \mathbf{q}^k.$$

Et on peut le réécrire sous la forme :

$$\sum_{i:\mathbf{q}^i<\sqrt{H}}\sum_{a\leqslant\frac{\mathbf{q}^k}{2}}\left|\sum_{\substack{H'<m\leqslant H'+\mathbf{q}^i\\ \mathbf{q}^i|a+m}}\chi\left(\frac{a+m}{\mathbf{q}^i}\right)\right|^2\ll_\varepsilon \mathbf{q}^k.$$

Or on observe que la condition $0<m\leqslant\mathbf{q}^i$
$\mathbf{q}^i|a+m$ n'est vérifiée que par un seul entier m et il vérifie : $\dfrac{a+m}{\mathbf{q}^i}=\left\lfloor\dfrac{a}{\mathbf{q}^i}\right\rfloor+1$. Donc par changement de variable (et en retirant quelques termes parasites positifs) :

$$\sum_{i:\mathbf{q}^i<\sqrt{H}}\sum_{b\in[1,\mathbf{q}^{\frac{k-i}{4}}]}|\chi(b)|^2\ll_\varepsilon \mathbf{q}^k.$$

Or $b \mapsto |\chi(b)|^2 \gg_\varepsilon \mathbf{q}^{k-i}$ est périodique de période $\mathbf{q}$ et de moyenne $\gg_\varepsilon 1$. On en déduit :

$$\sum_{i:\mathbf{q}^i<\sqrt{H}} \sum_{b\in[1,\mathbf{q}^{\frac{k-i}{4}}]} |\chi(b)|^2 \ll_\varepsilon \sum_{i:\mathbf{q}^i<\sqrt{H}} 1.$$

Des deux dernières estimations on en déduit que :

$$\sum_{i:\mathbf{q}^i<\sqrt{H}} 1 \ll_\varepsilon 1.$$

Et ceci est absurde quand H est suffisamment grand. On en déduit le théorème II.3 et donc la conjecture d'Erdos est démontrée.

Références

[1] G. Peyré. *L'algèbre discrète de la transformée de Fourier : niveau M1*. Mathématiques à l'université : cours et exercices corrigés. Ellipses, 2004. ISBN : 9782729818678. URL : https://books.google.fr/books?id=WFp8AAAACAAJ.

[2] Gérald Tenenbaum. *Introduction à la théorie analytique et probabiliste des nombres : Cours et exercices*. Dunod, 2022.

[3] S. Chowla. *The Riemann Hypothesis and Hilbert's Tenth Problem*. Mathematics and its applications. Gordon et Breach, 1966. ISBN : 9780677001401.

[4] Terence Tao. *The Erdos discrepancy problem*. 2017. arXiv : 1509.05363 [math.CO].

[5] K. Roth. "Remark concerning integer sequences". eng. In : *Acta Arithmetica* 9.3 (1964), p. 257-260. URL : http://eudml.org/doc/207480.

[6] Boris Konev et Alexei Lisitsa. "Computer-aided proof of Erd**H**os discrepancy properties". In : *Artificial Intelligence* 224 (2015), p. 103-118.

[7] Terence Tao. "The Logarithmically averaged Chowla and Elliott conjectures for two-point correlations". In : *Forum of Mathematics, Pi* 4 (2016), e8. DOI : 10.1017/fmp.2016.6.

[8] Terence Tao. *Elementary multiplicative number theory*. https://terrytao.wordpress.com/2014/11/23/254a-notes-1-elementary-multiplicative-number-theory/. 2022.

[9] Terence Tao. *Mean values of nonpretentious multiplicative functions*. https://terrytao.wordpress.com/2019/12/17/254a-notes-10-mean-values-of-nonpretentious-multiplicative-functions/. 2019.

[10] Terence Tao. *Second moment and entropy methods*. https://terrytao.wordpress.com/2019/11/12/254a-notes-9-second-moment-and-entropy-methods/. 2019.

[11] Terence Tao. *A cheap version of Halasz's inequality*. https://terrytao.wordpress.com/2015/11/23/a-cheap-version-of-halaszs-inequality/. 2015.

[12] Olivier Bordellès. *Arithmetic tales*. Springer, 2012.

[13] Jérémy Bettinger. *Le théorème des nombres premiers*.

[14] Kaisa Matomäki et Maksym Radziwiłł. "Multiplicative functions in short intervals". In : *Annals of Mathematics* (2016), p. 1015-1056.

[15] Adrian Dudek. "An Elementary Proof of an Asymptotic Formula of Ramanujan". In : *arXiv preprint arXiv :1401.1514* (2014).

[16] Kaisa Matomäki, Maksym Radziwiłł, Terence Tao et al. "An averaged form of Chowla's conjecture". In : *Algebra Number Theory* 9.9 (2015), p. 2167-2196.

[17] Hugh L Montgomery et Robert C Vaughan. *Multiplicative number theory I : Classical theory*. 97. Cambridge university press, 2007.

[18] Henryk Iwaniec et Emmanuel Kowalski. *Analytic number theory*. T. 53. American Mathematical Soc., 2004.

[19] Kannan Soundararajan. "The Liouville function in short intervals [after Matomaki and Radziwill]". In : *arXiv preprint arXiv :1606.08021* (2016).